EXECUTIVE SUMMARY

A STRATEGY FOR IMPROVED COALITION NETWORKING

INTRODUCTION

1. The ability of nations to participate successfully in multinational (MN) operations is critically dependent on being able to seamlessly exchange and share information. Increasingly this is done by means of operational coalition wide area networks that provide a rich set of collaboration and planning applications and information sharing capabilities. Over the past several years, nations either independently or in collaboration have developed information exchange networks to support the planning and conduct of coalition operations at both the operational-tactical and strategic–operational levels of command. These are, however, exclusively non-interoperable and there is an urgent operational and financial need to foster rationalization and interoperability

AIM

2. This paper will propose a strategy and supporting models for coalition networking that will provide improved information exchange between coalition partners all levels by providing guidance for the development and where practical, convergence of MN networks.

END STATE

3. The desired End State is a single coalition domain supporting information exchange requirements at different security classification and releasability levels between different coalition partners and communities at all levels of command. But the desired End State cannot be achieved until Multi-Level Security (MLS) solutions are developed for the full range of services to be provided. The likely achievable End State will involve a Two Tier model. At Tier 1 allied nations will exchange information between permanently inter-connected national classified C2 systems over multiple security domains. At Tier 2, information sharing at all command levels within a coalition or with nations without national C2 systems will be by means of standalone networks and systems. In order to meet this desired End State, the single coalition domain should exhibit the following characteristics:

- Provide seamless integration through the exchange of information between national C2 systems of coalition nations.
- Provide selected coalition services inherent on national C2 systems.
- Utilize the necessary guards to reduce the threat to national C2 systems.
- As the technology becomes available, utilize multi-level security to permit information flow to various security domains.
- Provide the necessary reliability to ensure mission accomplishment.
- In the event of systems failures, provide technical implementation that supports graceful degradation of service

MULTINATIONAL INFORMATION SHARING ISSUES

4. Domains. Domains consisting different communities of interest are identified as:

- National Domains. National Domains enable the internal sharing of information using nationally provided and managed network infrastructure, applications and services.

- Allied Domains. Allied bilateral or MN domains are formed from the permanent interconnection of national domains. They do not need a specific coalition operation to be formed, and they enable the permanent and protected environment for the sharing of classified or sensitive information. The Griffin capability is an example of an allied domain.

- Coalition Domains. Coalition Domains are formed using (often stand-alone) networks and applications between coalition partners. A separate domain may be created for each operation or for a specific purpose. CENTRIXS is an example of a Coalition domain.

5. Functional Requirements. The MIC has identified functional requirements and priorities for information sharing at the strategic-operational levels of command. User requirements for coalition information sharing are usually identified and provided by the Lead Nation[1]

6. Architecture. Effective and coherent design, development and management of MN networks is vital to improving information exchange. An architectural approach, based on the US DoD Architecture Framework (DoDAF), will guide the implementation of complementary, integrated and interoperable MN networks. This approach will guide further development, improve the effectiveness and efficiency of current capabilities, and increase commonality and enable reuse of design.

7. Tactical Networking Initiatives. Tactical networks enable direct information exchange between mobile elements without 'reaching back' through their national strategic networks. Ongoing work on tactical networking by Single Service Fora and other MN complement this strategy.

8. Information Management and Data Modeling. There are currently no MN-agreed information management or data standardisation/modelling standards. Resilient and responsive information repositories, capable of being accessed through both fixed and deployed CIS to support the assembly, processing and transformation of information is required. Multilateral Interoperability Program (MIP) is leading MN efforts on developing data models and data exchange mechanisms.

TIERED CONCEPT

9. The Two-Tier model provides the framework to rationalize and evolve current capabilities and guide future network development.

10. **Tier 1** capabilities are those with Boundary Protection Service (BPS) that allow connection to national C2 systems. **Tier 2** capabilities are those that do not have BPS solutions and therefore need a

[1] MIC Coalition Building Guide

stand-alone infrastructure. The availability of BPS solutions and associated security accreditation will govern the direction and timescales for achieving the End State

MIGRATION STRATEGY

11. As new BPS solutions allow more services and capability to be transferred to Tier-1 and where the required utility and reach is available, the need for Tier-2 capabilities will be reduced. There will be network convergence and elimination of duplicated network capabilities can be achieved.

FUNDING MODELS

12. A range of funding options for the provision and support of MN networks have been identified. Funding may be the responsibility of a Lead Nation, or may be shared between participating nations using a pre-agreed model. The selection of an appropriate option will be determined by the circumstances.

WAY AHEAD

13. The adoption of this Strategy and the Two-Tier model will provide a framework for the development, evolution, management, support and resourcing of existing and future Multinational Information Sharing capabilities in a coordinated, focused and planned manner.

14. Future coalition networking solutions must address design, technology, support and management aspects to ensure the deployment of an effective capability. Nations will need to scope the level of effort required and resource these requirements through appropriate national programs and agreed cost sharing models. The CCEB, as the recognized body for coordinating C4 issues, will coordinate the development, consolidation and evolution of coalition networking solutions.

CONCLUSION

15. The desired solution for allied and coalition information exchange and collaborative planning is between national C2 systems, with the integrity of national information being maintained by BPS. Until the necessary MLS solutions are developed, this End State is not achievable and the Two-Tier model provides a model to develop capabilities and evolve current and future networks.

16. Tier 1 capabilities are those with BPS solutions that can be connected to national C2 systems. Tier 2 capabilities are those that do not have BPS solutions and require standalone coalition infrastructure. The Two-Tier model allows for the rationalization, convergence or migration of current information exchange capabilities. The availability of BPS solutions and associated security accreditation will govern the direction and timescales for achieving the End State.

17. Requirements for new capabilities to support operational planning and conduct of operations have been agreed and prioritized through the MIC. The implementation of coalition networks based on this Strategy, combined with allocation of appropriate resources from each nation, will assure the success of information sharing in any type of operation.

A STRATEGY

FOR

IMPROVED COALITION NETWORKING

INTRODUCTION

1. Modern military operations increasingly involve two or more nations acting in a Coalition to achieve a political objective. The ability of nations to participate successfully in multinational (MN) operations is critically dependent on being able to seamlessly exchange and share information electronically with other participating nations. This capability is dependent on mutually agreed standards, procedures, interoperable equipment/systems, harmonized doctrine, training and development mechanisms.

2. Over the past several years, nations either independently or in collaboration have developed information exchange networks to support the planning and conduct of coalition operations. Some capabilities have been developed by a single (Lead) nation to meet immediate warfighter requirements in emerging crisis situations, or to meet regional/theatre information exchange needs. These networks have been primarily focused at the operational and tactical levels of warfighting; the US-sponsored CENTRIXS suite of networks is one such capability. Other capabilities have been more deliberately planned and rigorously accredited, with MN collaboration to meet needs of warfighters at the strategic and operational levels of command; an example of this type of capability is the multinationally-developed and supported "Griffin " which enables information exchange between national classified C2 systems.

3. The Multinational Interoperability Council (MIC)[2] determined that a coalition wide area network (CWAN) capability was to be established as a permanent information-sharing environment for collaborative planning activities and the conduct of operations between participating nations' strategic, operational and tactical level headquarters. A key driver for the CWAN was that users would primarily exchange information across the CWAN by using their existing national C2 workstations. The original information sharing vision for the CWAN was:

"The CWAN, when fully implemented, will provide an apparently seamless and robust network capable of exchanging, and sharing information that is operationally relevant to all coalition partners involved in multinational operations"[3].

4. The Combined Communications Electronics Board (CCEB)[4] directed that a strategy should be developed to guide the future development and, where practical, convergence of coalition capabilities

---

[2] MIC Meeting in October 1999. The MIC is composed of senior operations, doctrine, and C4I officials from AS, CA, FR, GE, UK and US. It's purpose is to provide a multinational forum for identifying interoperability issues and articulating actions, which if nationally implemented, would contribute to more effective coalition operations

[3] MIC CWAN CONOPS – CWAN Vision

[4] CCEB Meeting in June 2003. The CCEB is composed of senior J6 officers from AS, CA, NZ, UK and US. Its purpose is to optimize information sharing by delivering capabilities, policies and procedures in order to maximize the effectiveness of the warfighter in coalition operations.

and rationalization of infrastructure. A more coherent approach to coalition networking will assist in the efficient management of current and the development of future Communications and Information Systems (CIS) capabilities.

5. This strategy provides a model for both permanent, accredited and robust information exchange capabilities between national classified C2 capabilities at the strategic and operational levels. It also guides the timely establishment of networks with richer applications to meet immediate needs at the operational and tactical levels between non-traditional coalition partners, or where necessary security protection is not available. It will build upon existing and future initiatives and will provide a framework to guide the design, management, support and operation of coalition networking capabilities. Adoption of this strategy should enhance warfighters' information sharing abilities across all levels of command, and result in the more effective use and efficient support of coalition networking.

6. In this strategy, coalition networking refers to the spectrum of MN information sharing capabilities. It includes not only to the physical infrastructure that provides the transport and protection of information, but also the applications and services that enable a user to share information with coalition partners.

AIM

7. The aim of this paper is to propose a strategy and supporting models for coalition networking to deliver effective, efficient and interoperable capabilities in order to improve information exchange.

END STATE

8. The desired End State is a net-centric environment supporting the requirements for exchange of information at different security classification and releasability levels between different nations and communities of interest at all levels of command available to users at their national C2 workstation. In order to meet this desired End State, the single coalition domain should exhibit the following characteristics:

- Provide seamless integration through the exchange of information between national C2 systems of coalition nations. Operators working on their national C2 system should be provided a high level of assurance that they can effectively communicate with Coalition Partners working on their own national C2 system.

- Provide selected coalition services inherent on national C2 systems. The services provided on any coalition network such as CHAT and WEB must mimic whenever possible those found on national systems in order to reduce operator-training time and provide a similar look and feel.

- Utilize the necessary guards to reduce the threat to national C2 systems. Nations must be confident that when their national C2 system is connected to the coalition network, they remain safe from either malicious or unintentional network attack.

- As the technology becomes available, utilize multi-level security to permit information flow to various security domains. There is an increasing need to move authorized information between security domains.

- Provide the necessary reliability to ensure mission accomplishment. It is essential that the operational community has the full trust and confidence in their coalition network or else they will cease to use it.

- In the event of systems failures, provide technical implementation that supports graceful degradation of service. When operating a coalition network in a hostile environment, contingency plans must be developed in the event of systems failure. Single points of failure, even in the rear echelon operating area, must be eliminated. A coalition network must be able to sustain system failures and continue to operate in some diminished capacity.

SCOPE

9 The paper will propose a strategy for improved coalition networking. It will:

a. Confirm the high level requirement statement for CWAN as specified by the MIC;

b. Propose architecture and technology capabilities that support the requirements;

c. Identify priorities and sequencing for information exchange services;

d. Propose prioritization and capability costs to meet the requirements;

e. Outline opportunities for network convergence and eliminate duplication of services as MN networking capabilities develop; and

f. Propose a model for resource sharing.

10. Regrettably, the desired End State cannot yet be achieved. Until Multi-Level Security (MLS) solutions are developed, the realistic and achievable End State is the exchange of information between national classified systems using multiple, cryptographically-separated domains to connect different nations and communities of interest. However, some coalitions will consist of technologically disparate nations and may include some who do not have national C2 systems, or there may be reluctance by a nation to connect a potential coalition partner to their national classified C2 system. Because of this, there will always be a requirement for additional coalition networks. These will be complementary to the more permanent information exchange capabilities and they form an integral part of this coalition networking strategy.

DOMAINS

11. Coalition operations involve different domains within which there are communities of interest. The domains are:

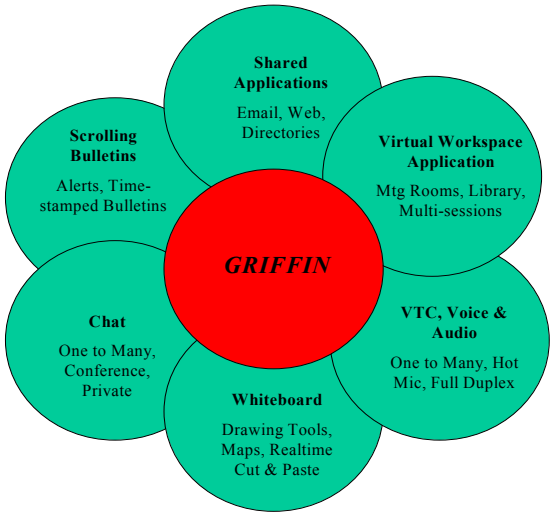
- National Domain. The internal sharing of information is assumed to be seamless where proven technology allows full information exchange. The national domain uses the nationally provided and managed network infrastructure, applications and services. National classified C2 systems reside in the national domain. The reach of the national domain into the tactical/mobile/deployed environment is determined by each nation, and will affect the reach of MN information exchange that uses national systems and infrastructure.

- Allied Domains. These do not need a specific coalition operation to be formed, rather they require a permanent and protected environment for the sharing of classified or sensitive information. Bilateral domains offer the richest exchange of information between nations based on firm trust and mutual understanding, facilitated by common standards and proven technology shared between two nations. Griffin provides the means for information exchange between National Domains.

- Coalition Domains. Wider coalitions require robust but flexible C2. The MIC Coalition Building Guide calls for a Lead-Nation to provide a mechanism for the exchange of information between the coalition partners[5]. A separate domain may be created for each operation so that a coalition can work together, ideally, at all levels of command and at the necessary security level. Coalition domains are established for a specific operation or purpose and will include non-traditional partners. CENTRIXS provides the means for information exchange within a Coalition Domain.

MIC FUNCTIONAL REQUIREMENTS

12. Figure 1 provides an overview of the original MIC functional requirements.[6]



[5] MIC Coalition Building Guide Executive Summary – "The Lead Nation will coordinate for, create, or provide communications and information management structures. The coalition partners must be brought into the planning process early and interact continuously to anticipate and solve problems likely to arise from a lack of compatibility among partners' organic command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) equipment".
[6] Multinational Combined Wide Area Network (CWAN), Concept of Operations (CONOPS), December 11, 2001

Figure 1. MIC Functional Requirements

13. Griffin capabilities have been developed to deliver MIC-defined functional requirements. The initial capability delivered on Griffin [7] is SECRET e-mail plus approved attachments between the CCEB nations. Additional applications including Enhanced Directory Services and a basic Web Browsing capability will be progressively introduced. While this will permit CCEB nations to conduct limited campaign planning between strategic and fixed operational headquarters, it will not immediately provide a full suite of collaborative planning tools and applications due to current security and accreditation constraints.

14. Coalition domains will always be required because of these constraints in exchanging information across national boundaries. These networks, which are not connected to National domains, are usually provided by the Lead Nation[8] in an operation and they provide the user with richer applications and reach into the operational and tactical environment.

DRIVERS FOR COALITION NETWORKING INTEROPERABILITY

Political

15. When committing forces MIC and CCEB nations need to operate within an agreed political coalition framework with a high degree of interoperability, trust and confidence. Governments will determine the composition of Coalition Joint Task Forces (CJTF), and other non-traditional partners may be included in the coalition. Therefore, flexible and adaptive CIS solutions must be provided to enable information exchange within a variety of traditional and ad hoc coalitions.

Operational

16. Network Centric Warfare (NCW) supports highly reactive CJTFs through smaller and more agile mission groups. The emerging lessons identified from Operation IRAQI FREEDOM highlighted the need for resilient and interoperable CIS to support campaign planning, mission rehearsal and the conduct of coalition operations. Commanders will have differing information requirements across the various levels of command and will require near-real time and real time information. Regardless of the specific operation, Coalition partners need to share information in a seamless, coherent and timely manner.

Financial

17. Responsibility for the establishment, management and support for permanent and ad hoc capabilities will be a significant driver in implementing coalition networks. Agreed funding models will offer options for determining responsibility for funding and resourcing arrangements. The shared

[7] To take Griffin forward as a Richer, Deeper and Wider capability. **Richer** – increasing suite of applications such as Web Browsing, Directory Services, Messaging, File Transfer and Coalition Planning Tools; **Deeper** – increasing Reach to tactical level and includes legacy system and 'Reachback'; **Wider** – connection to more nations, and establishment of permanent and ad hoc domains.

[8] MIC Coalition Building Guide

resourcing[9] approach by the CCEB and MIC nations provides an efficient means to meet operational requirements for a permanent network.

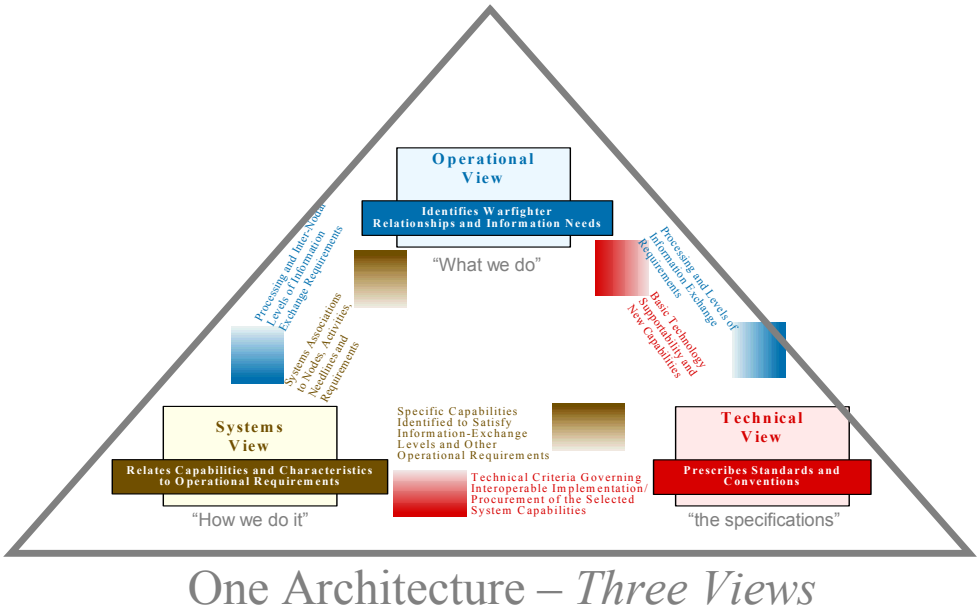
ARCHITECTURE APPROACH

18. Effective and coherent design, development and management of coalition networks across all levels of command are vital to improving information exchange. The network architecture will guide the implementation of complementary, integrated and interoperable networks across MN organizational boundaries.

19. This Strategy proposes that an information sharing architecture should be developed to guide the design, implementation and support of future coalition networking initiatives. The architecture should be based on the DoD Architecture Framework (DoDAF), which includes All, Operational, Systems, and Technical Views.

20. The **"All Views"** summarizes the architecture, and uses a consolidated dictionary as an architecture development guide to enable a "common language" throughout the architectural effort. The **"Operational View"** will describe the tasks and activities, operational elements, and information flows required to accomplish or support the aim of coalition information exchange. The nature of the information exchanges will be specified in sufficient detail to determine required interoperability requirements. The **"System View"** will identify which required capabilities support the operational view requirements. The required degree of interoperability will be translated into a set of needed system capabilities. Current/postulated implementations will be compared with needed capabilities. It is a description, including graphics, of systems and interconnections providing for, or supporting, operational functions. The **"Technical View"** will reference the technical standards that apply to the architecture and how they need to be, or have been, implemented. It also defines emerging / future standards related to the architecture.

[9] Including common management, operator and technical training, logistics support, shared use of infrastructure and use of common equipment types.



One Architecture – *Three Views*

Figure 2.

21. The Architecture needs to be flexible enough to accommodate the introduction of new coalition partners and maintain congruence with accelerating technological advances. It should also continue to use MN initiatives and demonstrations - Joint Warrior Interoperability Demonstration (JWID) and the Combined Federated Battle Labs Network (CFBLNet) - to examine potential 'quick-wins' through the continued cycle of experimentation, demonstration, and implementation. The security standards for coalition networks need to be developed and be continually reviewed in light of updates to the associated Threat Assessment.

22. One of the main benefits from adopting an architectural approach to coalition networking is to achieve increased commonality and reuse of design and development efforts. An additional important benefit is to guide further development and making more effective and efficient use of current MN information exchange capabilities.

23. To achieve these benefits, this Strategy proposes that participating nations and organizations should adopt a commonly-agreed architectural approach to MN information sharing with the primary mission of designing and implementing interoperable or complementary networks across all levels of command, and between different coalition groupings.

A TIERED COALITION NETWORKING CONCEPT

24. For users to be able to exchange information and collaboratively plan from their national C2 systems, the integrity of national information must be maintained by Boundary Protection Services (BPS). Currently, BPS are not available for all applications and services, and until such time as they are, two types of information exchange capabilities exist; ones with BPS and ones without. Until now, no model was available that described this current two state coalition networking environment.

25. The focus of effort for nations and organizations such as the CCEB should be to promote and encourage the development and accreditation of BPS for all relevant applications and services. Until a novel approach (that is one that does not require the use of duplicated guard infrastructure to separate domains) for the protection of national information appears, new capabilities will continue to be introduced which need their own specific BPS solution.

26. This Two-Tier model describes the initial coalition-networking environment and provides a framework to evolve current capabilities, and guide future information sharing capability development. The model assumes that the ability to extend reach from the strategic to tactical/deployed environment is determined by the reach of national domains.

27. This model does not account for tactical networking between deployed elements (for example ships at sea operating as part of a MN Task Group) or between deployed Land Elements engaged in coalition operations. The work of the single Service Fora in developing multination tactical networks is complementary to other efforts that are the focus of this Strategy.

28. Tier 1 capabilities are those with BPS solutions and can be connected to national domains. Tier 2 capabilities are those that do not have BPS solutions and require additional separate infrastructure.

29. Both Tiers require the development of multinationally agreed domain policy, procedures and standards that include security and Computer Network Defence. Figures 3, 4 and 5 below show the conceptual Two-Tier model and the transition of capabilities from Tier 2 to Tier 1 towards an achievable end state.

30. The initial state (Figure 3) depicts the current situation where some applications (for example email with attachments) can be exchanged between nationally classified C2 systems with protection provided by nationally accredited BPS. However, no accredited BPS exist for other capabilities (for example collaborative planning tools and Web Services), so Tier 2 terminals are required.

31. In coalitions where the connection of national domains is not possible or desired, the provision of Tier 2 capabilities must be provided and maintained. Nations C and D depict a coalition partner who has no national C2 system or does not have the ability/willingness to connect their C2 system to that of another nation. They could also be coalition partners with whom Nation A and/or B need to exchange and share information, but who are unwilling to allow Nations C and D to interconnect (even via BPS) to their national classified C2 system.

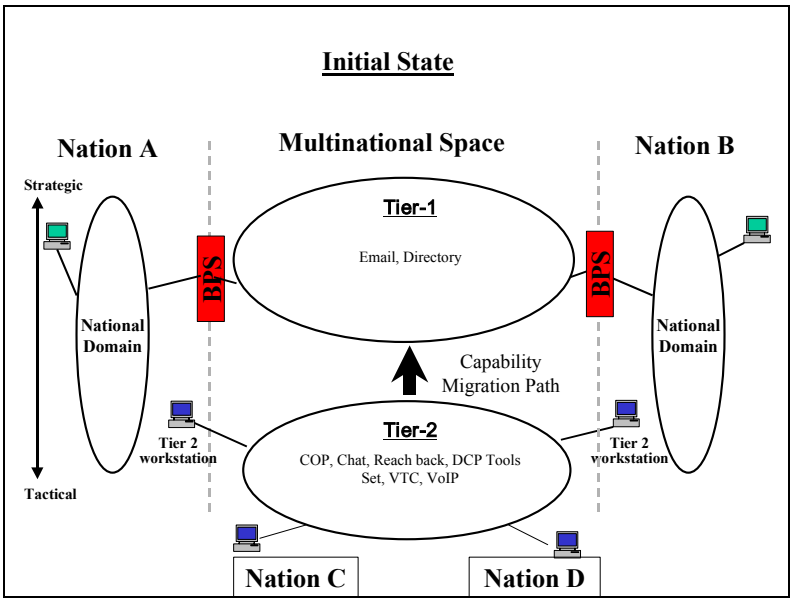


Figure 3.

32. The Transition State (Figure 4) depicts the situation where an increasing number and range of capabilities can be provided in a Tier 1 environment because of the increasing availability of accredited BPS. When specific capabilities (e.g. email, Web, COP, Chat, Reach Back) are available in both Tier 1 and Tier 2, meaning their full utility and reach are available to all required users at their national C2 workstation, there is unnecessary duplication. In this situation, those specific capabilities may be discontinued in Tier 2, unless information-sharing capabilities need to be maintained with Nations C and D in a Tier 2 environment.

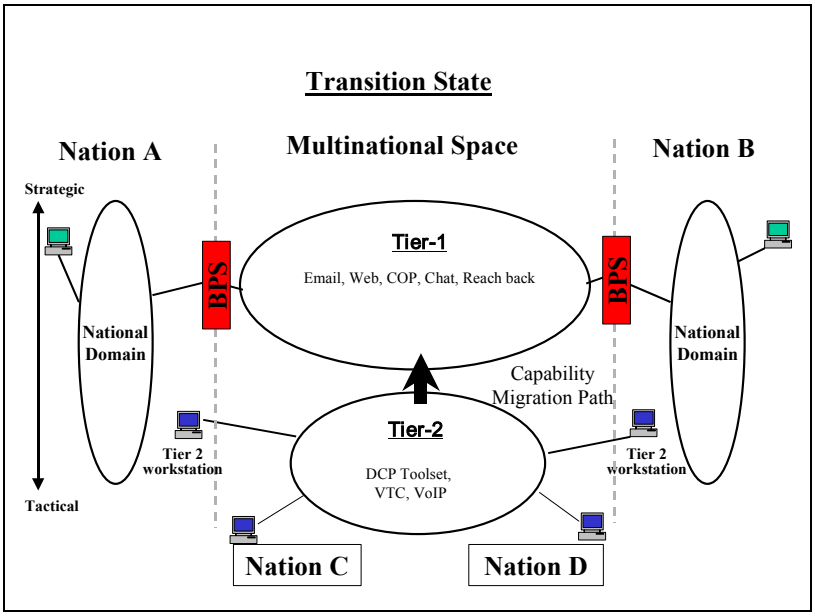


Figure 4.

33. The achievable End State (Figure 5) depicts the situation when all Tier 2 capabilities with their full utility and required reach are available on Tier 1 to users at their national C2 workstation. In this

situation, information sharing capabilities may be required to be maintained with Nations C and D in a Tier 2 environment.

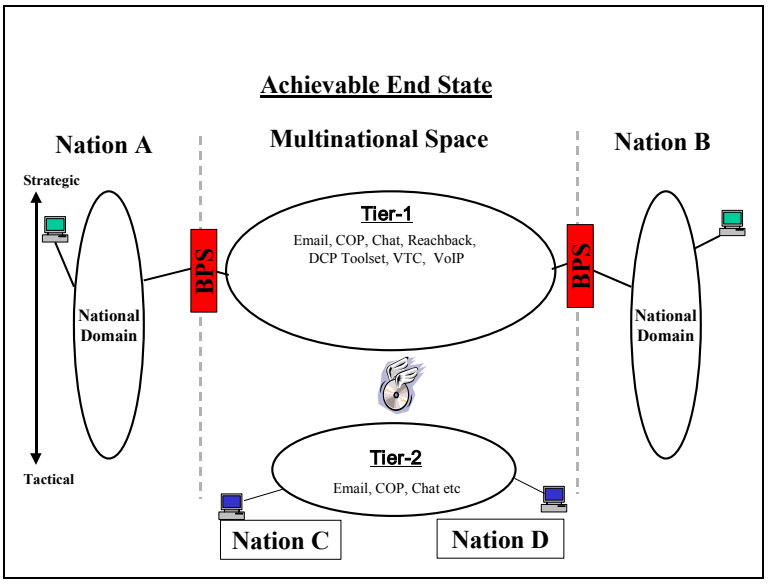


Figure 5.

TACTICAL NETWORKING AND INFORMATION EXCHANGE INITIATIVES

34. The ongoing activities within the Single Service Fora and other MN organizations to enhance tactical networking to support MN information exchange complement this strategy. Deployed coalition forces need the ability to directly exchange information without 'reaching back' through their national strategic networks. Therefore, tactical networks and interfaces that support the direct exchange of information between deployed Force Elements constitute an integral part of MN information sharing. Examples of initiatives in the tactical maritime and land environments should be considered in this Strategy.

35. The AUSCANNZUKUS Naval C4 Organization is developing the Maritime Tactical Wide Area Network (MTWAN), which will extend Internet Protocol (IP) networking into the low bandwidth high latency tactical environment utilising existing commercial and military communications bearers. The MTWAN CONOPS and operating instructions are promulgated in ACP 200, Maritime Tactical Wide Area Networks.

36. The Multinational Interoperability Program (MIP) is enhancing international interoperability of Command and Control Information Systems (C2IS) at all levels from corps and below to support MN, combined and joint operations. MIP has developed a C2 Information Exchange Data Model and exchange mechanisms (the Message Exchange Mechanism and the Data Exchange Mechanism) to exchange information between co-operating C2 systems.

MIGRATION STRATEGY

37. The 2-Tier model will guide the rationalization of current information sharing capabilities, but in the interim, emerging BPS solutions and associated security accreditation will govern the direction and timescales for achieving the End State.

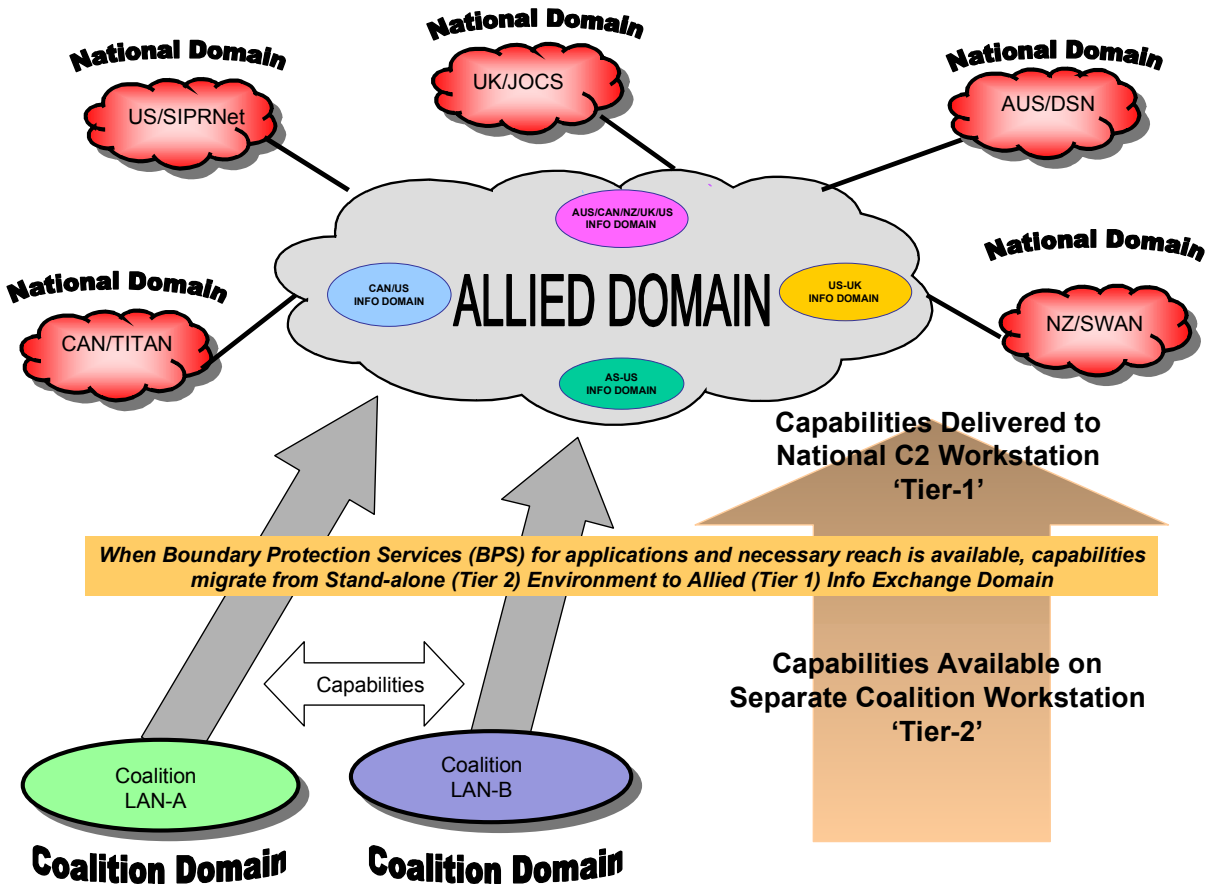


Figure 6. Coalition Networking Migration Model

38. To migrate Tier 2 capabilities to Tier 1 or develop new capabilities in Tier 1, rigorous acceptance criterion needs to be agreed and adhered to. An application, which is perceived to be suitable for collaborative planning, should first be demonstrated using the CFBLNet and JWID. Once the application has been fully tested, verified and accredited for use, it can then be implemented on operational systems. Ultimately, as Tier-1 capabilities become richer, the need for Tier-2 capabilities should reduce, and hence greater network convergence or elimination of duplicated capabilities can be achieved. CFBLNet should reflect accepted Tier 1 and Tier 2 capabilities.

39. Coalition environments that do not connect to national domains or do not have BPS solutions for specific capabilities will continue to be needed for information sharing. However, as BPS solutions for specific capabilities are developed and accredited, and where the full utility and reach is available to all required users, these capabilities will be able to migrate to a Tier 1 environment. Over time, the same

capabilities will be available in both Tier 1 and Tier 2 environments, thus allowing reduction of Tier 2 infrastructure. Figure 7 illustrates a possible migration/convergence path for existing MN information sharing capabilities. Further details are at Annex G.

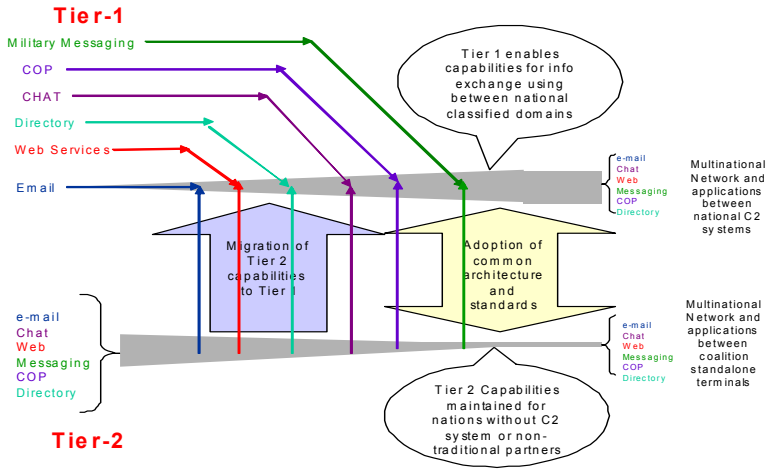


Figure 7. Illustrative Migration Path

PROPOSED NEXT & FUTURE TIER 1 SERVICES

40. Next and future services have been agreed and prioritized through the MIC as the users' requirements to support operational planning and conduct of operations[10]. The services outlined below are in the priority order identified by the MIC.

Next Services

41. Next Services are those applications where BPS solutions are being developed or accredited, and it is anticipated that they will be able to be used in the near to mid term (next 24 months). A brief overview of each capability is at Annex A, and indicative timeframes for implementation are at Annex B.

a. Initial Web Capability. This is the ability to share simple web page based information between Nations.

b. Directory Services. As the Tier 1 user community expands, the Directory Service will be enhanced.

c. Chat. Chat provides operators with an ability to hold real time or near real time informal discussions with other operational planners.

d. Basic Common Operating Picture (COP). A common and accurate view of the battlespace is essential to the conduct of coalition operation.

e. Military Messaging. Military Messaging is essential for the transfer of accurate, timely and non-repudiated information.

[10] Multinational Combined Wide Area Network (CWAN), Concept of Operations (CONOPS), December 11, 2001

f. Reachback. Reachback will provide a capability for a nation to extend its national domain to remote, deployed or liaison national elements embedded within another nation.

Future Services.

42. Future Services are those recognized as MIC requirements but where BPS solutions are not anticipated to be available for use in the near to mid term (after 24 months). Future services include but are not restricted to:

a. VTC (Video).

b. IP Telephony (Voice/Audio).

c. Whiteboarding.

d. Advanced Web services

e. Shared applications

f. Virtual Workspace Applications

g. Scrolling Bulletins

INFORMATION MANAGEMENT AND STANDARDISATION

43. The exponential growth of information availability and sources will require robust information management processes and procedures to ensure that the right information is available at the right time and in the desired format. To achieve full coalition information availability, coalition networking will need to address the challenges posed by the use of diverse data models and data exchange mechanisms that are currently being developed, are in use today, or are used in legacy systems. The data modeling initiatives and data exchange mechanisms being developed by the MIP should be considered by CCEB to improve data standardization for MN information exchange.

44. Future coalition networking will also need to provide a resilient and responsive information repository, capable of being accessed through both fixed and deployed CIS to support the assembly, processing and transformation of a coherent set of information for improved Situational Awareness.

45. To ensure future alignment of new capabilities, ease migration to Tier-1 and to allow increased efficiencies, it is essential that agreed standards required for coalition interoperability and common architecture are adopted. The CCEB as Lead C4 Coordinator and the only MN Joint C4-focussed organization is best placed to lead this work.

COALITION NETWORKING RESOURCE MODELLING

46. Adequate funding for the operation and support of coalition networking are essential pre-requisites to the successful implementation of such capabilities. In the MN environment, funding these capabilities may be primarily the responsibility of a Lead Nation, or may be shared between

participating nations using a pre-agreed model. Regardless of what funding arrangements are implemented, it is imperative that nations allocate appropriate financial and manpower resources and align their budget timelines to deliver coherent Tier-1 and Tier-2 capabilities.

47. So far Griffin capabilities between the CCEB nations have been delivered using 'quick-wins' expenditure by some nations, but as a result of this 'fast tracking' approach, ongoing funding for the operation, future development and support of the Griffin capability is not necessarily included in each nation's long-term programme.

48. Current Tier-1 Griffin capabilities are being operated and supported using an equitable resource-sharing model between participating nations. This model could form the basis for resourcing other Tier-1 capabilities. Once the long-term budgets for Griffin are programmed, each nation will be responsible for the provision of necessary resources to establish and operate their portion of Griffin and to gain access to common components such as DISN.

49. Under the Lead Nation concept, a nation accepts responsibility for providing, managing and supporting the majority of equipment, applications and services required for information exchange among coalition partners. The CENTRIXS construct is an example where the US, as the CENTRIXS sponsor, is shouldering the burden for developing, fielding, managing and maintaining this capability.

50. Annex C details the rough order of costs spent on current Tier-1 and Tier-2 capabilities by each nation, coupled with an outline estimate of future costs to meet the Next and Futures Services detailed in this paper.

51. The following three funding models were investigated:

- Option A, resources (funding) from each participating nation pooled in a central area, and then used to acquire coalition information sharing capabilities.
- Option B, provision of resources (capability) divided or shared amongst participating nations on a *quid-pro-quo* basis.
- Option C, the Lead Nation provides and funds the coalition network infrastructure, applications, services and management, with participating nations providing some national infrastructure and paying access charges.

Recommendations

52. Option A could potentially be a future solution if an appropriate funding mechanism can be developed. Option B has been implemented successfully by CCEB nations but requires continued equitable sharing, and is recommended for allied domains. Option C has been implemented for some ad hoc networks.

WAY AHEAD

53. The establishment of coalition networking will be aided by the adoption of the proposed 2 Tier model to provide a framework for the development and evolution of existing and future capabilities in a coordinated, focused and planned manner. The adoption of a coalition networking architecture will ensure a structured approach and common design when both Tier 1 and Tier 2 capabilities are established. The adoption of standard Tier 1 and Tier 2 solutions will lead to cost efficiencies by minimizing development, training, maintenance, and support overheads. The standardization of Tier 1 and Tier 2 solutions requires the development of complimentary information management and security policies and procedures.

54. The CCEB, as the recognized body for coordinating C4 interoperability between the nations, will lead the development, consolidation and evolution of both Tier 1 and Tier 2 solutions. The CCEB will assist in the coordination, rationalization or convergence (as appropriate) of existing Griffin, CENTRIXS, AUSCANNZUKUS MTWAN, MIP and other relevant initiatives. It will lead or co-ordinate efforts to ensure that the standards used for fielded systems are incorporated into the development of Tier 1 and Tier 2 capabilities. The development and evolution of solutions must address design, technology, support and management aspects to ensure the deployment of an effective capability. Nations will need to scope the level of effort required and resource these requirements through appropriate national programs and agreed cost sharing model.

CONCLUSIONS

55. A number of diverse coalition networking environments have been developed either by individual nations or collaboratively, to meet different needs. There are two key current coalition networking capabilities. CENTRIXS provides a rich set of information sharing capabilities within a domain at the operational and tactical levels of warfighting. Griffin is a permanent multinationally-developed, accredited and supported capability that permits information sharing capabilities between national domains. CENTRIXS and Griffin are complementary (not competing) capabilities that allow coalition warfighters to share information across all levels of command.

56. This strategy lays the foundation to meet all the MIC functional requirements. It provides a means to harmonize and rationalize the approaches to MN information exchange and provides a supportable way forward. The coalition networking architecture approach facilitates integration and interoperability across Joint and multi-national organizational boundaries. Consequently, the nations participating in coalition networking initiatives need to adopt an architectural approach, based on the US DoDAF, to ensure that future capabilities are designed and developed in a coherent and common fashion, resulting in the more effective and efficient information sharing.

57. The desired solution for allied and coalition information sharing and collaborative planning is between national domains, with the integrity of national information being maintained by Boundary Protection Services. The 2-Tier model describes the coalition networking environment and provides a model to develop and evolve current and future capabilities. Tier 1 capabilities are those with BPS solutions that can be connected to national domains. Tier 2 capabilities are those that do not have BPS solutions and therefore require additional separate infrastructure. The 2-Tier model will guide the rationalization, convergence or migration of current information sharing capabilities, but in the interim,

emerging BPS solutions and associated security accreditation will govern the direction and timescales for achieving the End State.

58. New capabilities have been agreed and prioritized through the MIC to support operational planning and conduct of operations. The implementation of coalition information sharing capabilities based on the Coalition Networking Strategy, combined with allocation of appropriate resources from each nation, will assure the success of information sharing in any type of operation.

Annexes:

A. Overview – Applications and Services
B. Timelines for Improved Coalition Networking
C. CIS Resources

ANNEX A TO
COALITION NETWORKING STRATEGY

OVERVIEW – APPLICATIONS AND SERVICES

1. WEB CAPABILITY

After email with attachments, web service is the most sought after capability desired for Griffin. However, web service may also be the most difficult to implement. The http protocol is one of the most powerful protocols in the TCP/IP suite and also presents some of the most critical and persistent vulnerabilities. As such, any automated web service must pass intense national accreditation criteria. Initial user defined capabilities that a Griffin web implementation must provide have been agreed and categorized as essential and highly desirable. A multinational virtual web design has been agreed in principle and nations are designing their interface specifications that meet those criteria.

Time lines. Web services have been tested on CFBLNet and are being trialed bilaterally. IOC is 2004.

2. DIRECTORY SERVICES

Directory Services is defined as a set of distributed information bases that support the exchange of agreed identity management information (such as contact details, PKI certificates, gateway/device information etc), and is based upon internationally agreed standards that enable information sharing between Nations. Directory Services adopt architecture, protocols, schema, policies, and procedures that support combined and joint operations in the strategic and tactical environments.

The Directory Service is being developed in three migratory phases. An Initial phase was implemented to provide limited access to contact information during the informal messaging development. The Interim phase is intended to provide a fully supported and managed Directory Service for informal messaging. The Enhanced phase is planned to support military messaging on Griffin.

Initial Directory Services

- The Initial Directory Service is being facilitated by the ad-hoc exchange of text files between the Griffin Nations.

Interim Directory Services

- The Interim DS protocols are based on the use of LDIF attachments, transferred over the informal messaging service, with additional control information.

Enhanced Directory Services

- The Enhanced Directory Service provide support for the Griffin Military Messaging service. It will be based on the Interim DS use of LDIF Attachments, with an extended and use ACP 145 protocols to assure authentication and integrity.

Time lines

- Initial Directory Services - In Service
- Interim Directory Services - IOC 2004)
- Enhanced Directory Services - IOC after national implementation of Military Messaging.

3. CHAT

An initial CHAT capability will support near-realtime one to one chat sessions. Although the initial service will not facilitate multi-chat sessions (chat-room facility) it will add a near real time dimension to augment the current email plus attachment capability.

Timeline CHAT services have been tested on CFBLNet and are being trialed bilaterally during 2004. Planned IOC is by EOY 2004.

4. COMMON OPERATIONAL PICTURE

The ability of warfighters to collaboratively plan and conduct successful operations is largely dependent on them having a common situational awareness of the environment in which they are operating – this can be at the strategic, operational or tactical levels of command. Operational planners and joint and coalition warfighting commanders now have the ability to review and share information and intelligence on their adversary.

A Common Operational Picture (COP) may provide real-time, near real-time and non real-time situational awareness of the adversary, along with an awareness of location and status of own forces. Depending on the purpose of the COP and its access to other information, a wide range of supporting information may be displayed on the COP to improve the situational awareness of the user.

Timeline IOC in 2006.

5. MILITARY MESSAGING

The CCEB has developed a solution that enables interoperability between each CCEB nation's ACP123 (X.400) high-grade military messaging systems. The solution[11] is based on messaging Gateways between those national ACP123 systems being rolled out between now and Dec 05. It has been agreed that Griffin will be used to provide transport services for exchanging military messaging between CCEB nations.

For non-Tier 1 nations with ACP123/145 capabilities, exchange of messages could be achieved across a separate domain on Griffin with appropriate BPS to allow transfer between domains or via Tier 2 environment. Nations outside of the Allied or coalition domains can still achieve formal military messaging requirements using ACP123 or legacy ACP127/128 systems.

[11] The CCEB issued a draft Allied Comms Publication (ACP) 145 on 1 May 03 that defines the standards to be used for interoperable military messaging between nations. The standard is based on gateways using X.400 P.772, with S/MIME & ESS labels for security. PKI is used to provide authentication and integrity security services between the gateways. France, Germany, and NATO are involved in ACP 145 development through the Multinational Interoperability Council (MIC) and are likely to incorporate this standard in their future military messaging programmes.

Timeline. IOC – 2005 (defined as 2 nations exchanging military messages on Griffin).

6. REACHBACK

Reachback is a cost-effective solution to provide connectivity for a deployed/remote user to access information on his national network. Reachback utilizes existing wide area network (WAN) infrastructure within and between nations to extend national connectivity to remote, deployed or liaison elements embedded/located within another nation. Depending on how the capability is implemented, Reachback enables a remote user to access either national Eyes-Only information or coalition releasable information residing on his national/home classified network.

The primary benefits Reachback offer are the ability for deployed/remote users to access information on their national classified system using existing multinational WAN connectivity between nations. This means that separate rear-link circuits do not need to be established with resultant improved efficiencies and potentially greater data transfer rates.

National Eyes-Only Reachback enables a remote/deployed user to access "eyes-only" information and services on their national classified network. Establishment of a "National Eyes-Only" Domain within another nation's space may be constrained by security and national policies of the Host Nation and of the visiting nation.

Coalition Releasable Reachback enables a deployed/remote user, operating within another nation's facility, to use "coalition releasable" equipment to exchange information with other coalition nations; this includes the Host and Parent Nation, as well as other partners participating in the coalition and connected to the coalition domain.

Timeline. From a technical perspective, Reachback can be implemented relatively easily and in the near future. However, national security policies and user requirements will dictate implementation schedules.

ANNEX B TO
COALITION NETWORKING
STRATEGY

TIMELINES FOR IMPROVED COALITION NETWORKING

1. The current Griffin Tier-1 Program as envisaged under the original MIC requirement remains a legitimate plan. A CCEB Griffin domain with e-mail + attachments has been created, enhanced directory services are to be implemented by 1Q04, and initial web services will be in-service in 2Q04. The establishment of a MIC Griffin domain is being progressed and the necessary multinational info exchange agreements are being negotiated. As we progress from Mar 04, it will be essential that JWID and CFBLNet are fully engaged and utilized to ensure the necessary guard technology that are now available in the commercial market are accredited and available for military applications. Figure 1 shows an outline of the forecast timelines for enriching the CCEB Griffin Tier-1 capability, while Table 1 provides similar information on current and future capabilities in matrix format.

Application	Current		Next		Future	
	Tier-1	Tier-2	Tier-1	Tier-2	Tier-1	Tier-2
Email with Attachments	Yes	Yes	Yes	Yes	Yes	Yes
Initial Web Capability	No	Yes	Yes	Yes	Yes	Yes
Enhanced Directory Services	No	No	Yes	Yes	Yes	Yes
Chat	No	Yes	Yes	Yes	Yes	Yes
CROP	No	Yes	No	Yes	Yes	Yes
Military Messaging	No	No	Yes	No	Yes	No
Reachback	No	No	Yes	No	Yes	No
VTC	No	No	No	No	Yes	No
Voice over IP	No	No	No	No	Yes	No
Whiteboarding	No	Yes	No	Yes	Yes	Yes

Table 1. Matrix of Current, Next & Future Capabilities