Re-framing "The AMN": A case study eliciting and modelling a System of Systems using the Afghan Mission Network

Duncan Ki-Aries, Shamal Faily, Huseyin Dogan
Bournemouth University
Fern Barrow, Poole, UK
{dkiaries,sfaily,hdogan}@bournemouth.ac.uk

Christopher Williams
Defence Science and Technology Laboratory
Porton Down, UK
cwilliams@mail.dstl.gov.uk

***Abstract*—The term *System of Systems* (SoS) is often used to classify an arrangement of independent and interdependent systems delivering unique capabilities. There appear to be many examples of SoSs, but the term has become a source of confusion. While many approaches have been proposed for engineering SoSs, there are few illustrative examples demonstrating their initial classification and resulting SoS structure. This paper presents an approach for framing a candidate SoS using the Afghan Mission Network defined as an Acknowledged SoS, and presents issues associated with SoSs stakeholders, human factors and interoperability considerations resulting from such an approach.**

***Index Terms*—System of Systems, Systems Engineering, Afghan Mission Network.**

I. Introduction

The term *System of Systems* (SoS) is used to refer to a collection of inter-connected systems that at times may come together for a common purpose or goal at a SoS level, where individual systems may also operate with a degree of autonomy in their own right. However, the term can also be used inconsistently across audiences, creating ambiguity towards how a SoS may be represented, emphasising the need for clarity when defining and characterising a SoS. For example, SoSs may be considered complex, adaptive, large-scale and may also be constrained by geographical considerations, yet it is not always clear in which context a system or systems become complex, or indeed whether the notion of large-scale is a direct result of geographical boundaries, or the number of systems and inter-connections used within the SoS. Consequently, it is easy to become confused by the use of the term *SoS*, and how SoSs should be categorised and defined for a given context, e.g. SoSs from an engineering or security viewpoint.

In addition to specific SoS design, engineering and ongoing operational needs, individual systems in the SoS usually retain their own identities along with their own authorities, responsibilities, and resources to support current and evolving user needs [1]. However, with evolving systems and collaborations, a more diverse approach is required when designing, developing and maintaining larger scaled systems or SoS. A single system approach may overlook certain aspects, such as all stakeholder needs, security, interoperability, or vital situational awareness supporting resilience; this may lead to increased levels of un-assessed risk.

While there is some diversity in the approaches proposed for engineering SoSs, a gap is evident towards a formal process for defining and characterising a SoS, with few examples illustrating their SoS outputs. It would, therefore, be useful to identify a candidate SoS, and illustrate how this candidate might be framed as a SoS given its characteristics, enabling a platform for applying suitable design techniques to SoS components appropriate to SoS type and complexity, considering where issues may exist if the management and participation spans multiple SoSs. Such an example could be modelled, to not only illustrate the coming together of systems forming a SoS, but to start reaping the benefits that its framing as a SoS should allow.

To address this gap, we present a process for eliciting, modelling and characterising the Afghan Mission Network (AMN) as a SoS. We consider the existing work and elicitation processes for SoSs in Section II before presenting an approach for framing a candidate SoS in Section III, using the AMN and its SoS characteristics in Section III-A to walk through a process where this is framed as an Acknowledged SoS in Section III-B. We conclude by discussing some of the implications of our approach in Section IV, and presenting some directions for future work in Section V.

II. Related Work

A. SoS Examples

Before considering how SoSs may be defined, it is useful to consider examples of SoSs. A pervasive example is the smartphone, which is made up of a number of various functional components while externally providing data connections traversing global networks. These networks could themselves be viewed as a SoSs. Software applications on the smartphone may be operated by users to connect to and control other smart systems such as home security, communications systems, or assistive technology [2]. The smartphone therefore goes beyond providing basic capabilities of voice and text-based data transmissions, and as with other smart devices, may at times

978-1-5090-5476-3/17/$31.00

become a business or personal central Command & Control device. This demonstrates how an inter-connected reliance and coming together of systems to achieve collaborative objectives may be considered within examples of a SoS. Other SoSs include general business information systems, sensor networks [1], and emergency response units [3] that bring together independently owned and managed systems and services such as fire, police, ambulance, and other facilities collaborating to deliver a service on which reliance is placed to achieve the SoS level objective or mission [4].

These examples illustrate where confusion may exist when defining and classifying inter-connected systems as being a SoS. On one end of the scale a hand-held device may be considered a SoS, however, military and defence systems may also be perceived as being a SoS, but on a much larger scale with quite different characteristics. When considering these characteristics across different examples, a distinction can be made as to the likely level of complexity and governance involved in the management and operations of the systems inter-connecting into the SoS to achieve its goal and purpose, which can better assist in categorising and defining SoSs.

B. Systems and SoS

A distinction should be drawn when understanding what constitutes a System in comparison to a SoS and its related boundaries. For example, a system could be defined as being a functionally, physically, and/or behaviourally related group of regularly interacting or interdependent elements; that group of elements forming a unified whole [5]. INCOSE [6] suggest a system is a combination of interacting elements organized to achieve one or more stated purposes, whereas a SoS applies to a System-of-Interest (SOI) whose system elements are themselves systems. Typically these are large scale inter-disciplinary problems with multiple heterogeneous distributed systems [6]. Boardman and Sauser [7] believe the difference between a system and SoS lies in its composition, and is based on how the parts and relationships are gathered together and therefore in the nature of the emergent whole.

Maier [8] argues the inter-connected systems are formed of substantially independently and operated elements. These elements do not solely contribute to an overall purpose or set of functions, but rather individually fulfil useful purposes. Therefore, in order to be classified as being a SoS, the system should correspond with the following parameters [8]:

- The elements of the system are themselves sufficiently complex to be considered systems;
- Operating together, the elements produce functions and fulfil purposes not produced or fulfilled by the elements alone;
- Each element possess operational independence and fulfils useful purposes whether or not connected to the assemblage. If disconnected, the element continues to fulfil useful purposes;
- Each element possess managerial independence, and managed, at least in part, for its own purposes rather than the purposes of the collective;
- A SoS is typically geographically distributed such that its elements exchange only information rather than mass or energy;
- A SoS typically evolves over time and space. It does not have a unique configuration, but rather evolves and changes.

Maier further defines SoSs by certain combinations related to managerial and operational independence. These are defined as being *Directed*, *Collaborative* and *Virtual* [9]. However, Sommerville [10] claims these classifications fail to reflect the distinctions between different types of SoSs. For example, when considering systems as Virtual this is confusing given the term is also used to describe something that is usually implemented by software, e.g. virtual machines [10]. Additionally, Dahmann and Baldwin [11] introduce a fourth definition of an *Acknowledged* SoS, which can be specifically identified within certain Department of Defense (DoD) activities. These have capability objectives, management, and resources to support the SoS, are comprised of existing systems along with new developments, and posses qualities of Collaborative and to a degree Directed SoSs.

To help distinguish Acknowledged SoSs, we highlight four main categories of SoSs. While SoSs generally fall into one of these categories, the distinction is not always clean. In some scenarios, a system may also be considered to be a different type of SoS within its own operational environment. In other scenarios, a Collaborative SoS may need to formulate into an Acknowledged SoS due to the importance of the missions supported by the SoS, or the complexities of the cross-cutting SoS capabilities [12].

Directed SoSs: Are built and managed to fulfil specific purposes; they are centrally managed during long-term operation to continue to fulfil and evolve those purposes. Component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose [9].

Acknowledged SoSs: Have recognised objectives, a designated manager, and resources for the SoS, but constituent systems retain their independent ownership, objectives, funding, as well as development and sustainment approaches. Changes to systems are based on collaboration between the SoS and systems [11].

Collaborative SoSs: Are distinct from Directed SoSs in that the central management organisation does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfil the agreed upon central purposes [9].

Virtual SoSs: Lack both a central management authority and centrally agreed upon purposes, may exist deliberately or accidentally, and large-scale behaviour emerges, which may be desirable [9]. Participants informally collaborate and manage their own systems to maintain the system as a whole [10].

C. SoSs Stakeholders

Given the distinct differences and challenges between interconnections of the SoS, when eliciting and modelling a SoS

it is imperative to consider all stakeholders as well as its inter-connections towards identifying the boundaries of the SoS. For example, the ownership and operation of constituent systems within a SoS by independent stakeholders may lead to limitations on the exchange of information [4]. Stakeholders may not always be recognised across the SoS, or stakeholders of individual systems may have little interest, or resist the SoS demands on their system giving lower priority to the SoS [5].

Examples of stakeholders would be considered throughout the System life-cycle stages of engineering, development, transfer for production or use, logistics and maintenance, operation, and disposal [13]. SoS projects may engage a diverse group of stakeholders, however all stakeholders should be valued and recognised as being unique individuals assisting in the discovery of socio-technical and psychological factors relevant to project requirements [14].

III. Approach and Case Study

Despite various engineering guides [5] [6], or systems engineering approaches [15], [16], [17], there appears to be no commonly used formal framework for classifying and modelling a candidate SoS; only commonly used descriptions have been posited. To address this challenge, we propose aligning the SoS definition and characteristics noted in Section II, and consider the differences between a system and a SoS [7], along with Maier's parameters [8] to determine if it is a SoS. If it is, it can then be defined by the characteristics from one of the four SoS types.

Based on our approach, which is grounded in a review of its related literature, and interviews with its stakeholders, we propose the Afghan Mission Network (AMN) as a working example of an Acknowledged SoS. This is supported by findings demonstrating the combined systems interaction of the AMN, using the sub-categories described by Dahmann and Baldwin [16] to frame the AMN as an Acknowledged SoS. The AMN was formed out of necessity from a previous SoS supporting Afghan operations, which could be viewed as a Collaborative SoS, incorporating Directed SoSs representing each of the partners and Troop Contributing Nations (TCNs).

A. Considering the AMN as a SoS

The AMN was a meshing of the communication links and data feeds used by the North Atlantic Treaty Organisation (NATO) International Security Assistance Force (ISAF) during the Afghanistan campaign missions [18]. Prior to the creation of the AMN, each TCN communicated across on its own non-federated network, operating without a common core making information sharing a challenge [19]. To improve this, a shift in cultural mind-set was required from a 'Need to Know' to a 'Share to Win' approach, specifically as ISAF recognised data restriction created greater risks [20], although this approach was complicated by national concerns and restrictions on data sharing [21]. It was also found the technical problems of net-centric warfare were relatively minor compared to cultural issues and human factors, particularly as personnel interacting with intelligence information could no longer be considered as secondary actors [18]. Robust information management was therefore required to meet the needs of people, process and technology, and timely decision making within the AMN [20].

By placing all information exchange on the common ISAF Secret network, during 2010, the AMN become the primary communications network for ISAF forces [20], extending across Afghanistan to 48 TCNs servicing a total force of over 130,000 combined military and civilian personnel with human-to-human exchanges of basic services for text-based chat, audio-based Voice-over-Internet-Protocol (VoIP) telephone connectivity, video-based Secure Video Teleconferencing (SVTC), email, web access, and office productivity tools [22]. The AMN provided Command & Control (C2) to support growing mission and coalition partners needs, and evolved into the primary Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C5ISR) [22]. This supported rapid decision making within the AMN by using coalition data and Common Operational Pictures (COPs) [22] to improve Situational Awareness (SA) of the security environments [23].

B. Framing the AMN as an Acknowledged SoS

A review of the AMN identified dominant systems and stakeholders with designated management and oversight interconnecting in a collaborative nature, reliant upon the core of the AMN collaboration between NATO/ISAF and TCNs. Representative systems responsible for the acquisition, implementation and operations, testing & validation, in-theatre users, and other external entities can be identified, although all systems have overlapping boundaries with differing priorities and dependencies, presenting a strong indication the AMN would be classed as an Acknowledged SoS.

AMN Management and Oversight

Stakeholder Involvement: In Acknowledged SoS, stakeholders are at both System level and SoS levels, and includes the system owners, with competing interests and priorities. In some cases, the system stakeholder has no vested interest in the SoS and all stakeholders may not be recognized [11].

For the success of the AMN, considering stakeholder needs was an important challenge to ensure a continuous operation of local, military and civilian interaction priorities were met. Primary stakeholders included NATO/ISAF, TCNs and partners. The list of direct and in-direct stakeholders was extensive across all SoS and System levels, although stakeholders at system level would have a vested interest in the SoS given the nature of their participation. Other important in-direct stakeholders reliant upon the information flow of the AMN included NATO's civilian representation, the Afghanistan government, the UN Assistance Mission in Afghanistan, Non-Governmental Organisations (NGO's), other international organisations supporting humanitarian or aid efforts [24], and the Afghan population working to implement mutual goals for their nation.

Governance: In Acknowledged SoS, there are added levels of complexity due to management and funding for both the SoS and individual systems, meaning the SoS does not have authority over all the systems [11].

Governance within the AMN was achieved at a number of levels, e.g. NATO/ISAF AMN Operations, testing and validation collectives, and other national level input. Therefore, added levels of complexity arise across all levels of the SoS Governance. Funding was focused at the SoS level, whereas individual systems connecting to and forming the AMN were funded, managed and operated by relevant participating nations, thus retaining a level of autonomy.

AMN Operational Environment

Operational Focus: In Acknowledged SoS, they are called upon to meet a set of operational objectives using systems whose objectives may or may not align with the SoS objectives [11].

The NATO Communication and Information Systems Services Agency (NCSA) and its Mission Detachment to ISAF (NMD-I) were responsible for the operation of in-theatre Communication and Information Systems (CIS) services. Meeting the needs of operational objectives and mission threads were, therefore, aligned with the SoS objectives. However, TCNs and other agencies were likely to have national objectives separate or in addition to SoS objectives. Within the AMN, the Joint Mission Threads (JMTs) such as Battlespace Awareness, Medical Evacuation, and Freedom of Movement, together with applicable services critical to their functioning were the primary means of aligning the goals and activities of the SoS to achieve its mission [22], thus being integral systems within the SoS.

AMN Implementation

Acquisition: In Acknowledged SoS, added complexity exists due to multiple system life-cycles across acquisition programs, involving legacy systems, developmental systems, new developments, and technology insertion, which typically have stated capability objectives up front that may need to be translated into formal requirements [11].

The NATO Consultation, Command and Control Agency (NC3A) primary role was to develop, acquire and implement capabilities using their expertise of C2 through to C5ISR, providing vital communications and data services supporting NATO forces across Afghanistan [25]. To meet the operational needs of the NMD-I, Thales were tasked by the AMN Architecture Working Group (AMN AWG) with the provision, operation and maintenance of a complete network, end-to-end logistics and integration of systems, including transfer of all equipment throughout the theatre of operations in Afghanistan [26]. However, participants at a system level were responsible for ensuring their legacy systems could interface with the AMN. Complexity existed across the multiple system life-cycles, but were reduced using tried and tested solutions, supported by testing and validation programmes providing feedback for improvements to core technology, systems and configurations within the SoS.

Test & Evaluation: In Acknowledged SoS, testing is more challenging due to the difficulty of synchronizing across multiple systems life-cycles, given the complexity of all the moving parts and potential for unintended consequences [11].

The Coalition Interoperability Assurance and Validation (CIAV) programme provided in-theatre mission-based assurance testing & validation, and verified the status of interoperability among current, future, and experimental systems that would be deployed within the AMN [22]. The CIAV Working Group (CIAV WG) were responsible for interoperability improvements within AMN governance structure, and integrated with accreditation groups providing security of coalition information and networks established under the Combined Federated Battle Laboratories Network (CFBLNet) [27]. The CFBLNet facilitated development of coalition interoperability, doctrine, procedures, and protocols that could be transitioned to operational networks in future coalition operations, carried out through 17 dedicated integrated labs based in ten nations [28], and bi-annual testing with the Coalition Test and Evaluation Environment (CTE2) and Coalition Warrior Interoperability Exercise (CWIX) [29] for new systems and architecture of specified CIAV assessments [30].

AMN Engineering and Design Considerations

Boundaries and Interfaces: In Acknowledged SoS, the focus is on identifying the systems that contribute to the SoS objectives and enabling the flow of data, control, and functionality across the SoS while balancing needs of the systems [11].

The AMN AWG developed the architecture and modelling of the AMN mission threads to support multi-national C5ISR planning at the enterprise level [31]. SoS boundaries and interfacing requirements were identified through the NC3A, Thales, AMN AWG, and implemented by the NMD-I over a single core network at the classification level of ISAF Secret. The AMN boundary generally ends with the connections to each of the TCNs, although some data distributed through the AMN may be disseminated through national level command structures, under national policy and control. Boundaries are also considered in different contexts, covering networks, people, process, and technology, across land, sea, air, space and cyber domains, where different parameters, characteristics and interfacing requirements exist.

Performance & Behaviour: In Acknowledged SoS, performance is across the SoS that satisfies SoS user capability needs while balancing needs of the systems [11].

NMD-I and Thales managed and monitored on-going performance of objectives to meet the SoS objectives of secure C5ISR data flow, with further performance and interoperability feedback provided by TCNs and the CIAV programme. Direction, oversight and monitoring of security behaviour for Cyber Defence was conducted by the NATO Cyber Defence Management Authority (NCDMA), whilst the NATO Computer Incident Response Capability (NCIRC) provided capabilities for maintaining the end-to-end network security.

Security risks faced by the AMN often emanated from targeted network attacks using malicious software and Denial-of-Service (DoS) attacks, spam, malware, web defacements, or poor maintenance related vulnerabilities, system privilege abuse, authorised user indiscretions, and classified information leakage [32].

IV. Discussion

In the context of a mission-driven Acknowledged SoS, each direct stakeholder had a vested interest towards the AMN achieving its SoS mission objective, with differing input either at a SoS, System or Component level, although some stakeholders also become users reliant upon the SoS or in-direct benefactors of its output. Stakeholders should, therefore, be viewed as multi-dimensional and their interaction at differing levels should be understood, with a focus towards understanding a system's stakeholder objectives towards the SoS and the role it plays at each stage of achieving the SoS mission, including bi-directional dependencies on people, processes and technology for implementation and operation of systems participating with the AMN or similar Acknowledged SoS.

To support set-up of operations in future SoSs environments, with applicable stakeholders providing differing inputs and outputs at varying stages of the systems and development life-cycles, joining options should be more straight-forward with proven solutions for integration. Common service management and cost-effective cross provisioning of services incorporating data labelling for easier information sharing should be considered [33], which can have a positive effect towards interoperability.

The AMN as a SoS supports the agile 'Come as you are' approach where future mission networks must interoperate with differing mission types and partners, with the need to communicate information at specified security classification levels [34]. There is, however, a duty of the system entities within the SoS to identify a unified approach that answers the question 'How should we come?' This reinforces the need for global standardisation of data types, system and network configurations to improve interoperability. This need will become more prevalent in Acknowledged, Collaborative and Virtual SoS as central management or control is reduced.

Commonly defined and understood mission threads should be used to guide the development of future coalition data-sharing enterprises, and be supported with assurance & validation through programmes such as CIAV and the CFBLnet [22], who could both be viewed as individual SoSs. Testing was an iterative process that should focus on the end-state and mission thread success requirements, considering that components are put into systems, systems are put into platforms, platforms must interoperate with other families of platforms, and these family of platforms must interoperate via networks [31]. This demonstrates the consideration towards a need for components and systems to scale-up to interoperate with higher groupings of systems to achieve its purpose as a SoS.

To achieve a standardised, consistent and interoperable approach in a single, common mission-centric federated network such as the AMN, requirements may include the use of Commercial Off-The-Shelf (COTS) hardware and software, as opposed to developing expensive in-house alternatives, while maximising the use of other current applications, interfaces, web services [32], reducing costs and resources. Further consideration should also be given towards dependencies from the use of COTS products and risks created within the supply chain relating to product availability, or ensuring security and reliability of products before use and implementation in SoS.

Human Factor interoperability considerations were another challenge faced by the AMN, particularly when considering end-users in-theatre were dependent upon systems that were easy to administer and operate, and possessed the ability to provide reliable and timely CIS and SA in emergency scenarios [35]. Related work in emergency services found that a key characteristic of an SoS is its inherent socio-technical nature, where social factors can become even more complex than technical interoperability [3].

V. Conclusion

In this paper, we present an approach for framing a candidate SoS as an Acknowledged SoS using the AMN. Applying this process assisted in defining and characterising a SoS, enabling a platform for applying suitable design techniques to SoS components appropriate to SoS type and complexity. By considering the structure, management, and participation of systems and stakeholders within the SoS, this helped identify where dependencies and constraints may exist towards the SoS achieving its SoS mission objectives.

Findings suggest considerations for SoSs and future mission networks should include a specific focus towards identifying all relevant SoS stakeholders and individual mission-driven needs, including relevant human factor implementation and operational considerations. Cultural, environmental and geographical considerations were of key importance in the AMN, with a high dependence on the cyber domain, creating a greater dependency on interoperability for availability of systems and networks. Information and data sharing needs should be agreed and utilise common data labelling and classification formats using appropriate information management, security, and risk approaches. Moreover, to support timely integration when forming a robust SoS, this may incorporate COTS hardware and software over in-house development, using tried, tested and supported solutions that operate in a standardised manner and consider human factors and interoperability as a standard requirement.

We believe our work makes a contribution towards current research challenges relating to SoSs and supports future work considering other examples of SoS types to clearly differentiate between characteristics and their challenges. Future work will continue build upon a case-study approach to apply the characteristics of a given SoS leading to analysis from an operational, security or engineering view of security and risk assessment in SoSs.

ACKNOWLEDGEMENT

The research described in this paper was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RASOS. We are also grateful to DSTL for their sponsorship of this work.

REFERENCES

[1] K. Baldwin, J. Dahmann, and J. Goodnight, "Systems of Systems and Security: A Defense Perspective," *Insight*, vol. 14, no. 2, pp. 11–14, 2011.

[2] P. Whittington and H. Dogan, "Smartpowerchair: Characterization and usability of a pervasive system of systems," *IEEE Transactions on Human-Machine Systems*, 2016.

[3] H. Dogan, S. A. Pilfold, and M. Henshaw, "The role of Human Factors in addressing Systems of Systems complexity," in *Systems, Man, and Cybernetics (SMC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1244–1249.

[4] C. B. Nielsen, P. G. Larsen, J. Fitzgerald, J. Woodcock, and J. Peleska, "Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions," *ACM Comput. Surv.*, vol. 48, no. 2, pp. 18:1–18:41, Sep. 2015.

[5] Office of the Deputy Under Secretary of Defense for Acquisition and Technology. Systems and Software Engineering, *Systems and Software Engineering. Systems Engineering Guide for Systems of Systems*, 1st ed., Washington, DC: ODUSD(A&T)SSE, 2008, 2008.

[6] International Council of Systems Engineering (INCOSE), *Systems Engineering Handbook*, version 3.1 ed., INCOSE, Aug. 2007.

[7] J. Boardman and B. Sauser, "System of systems-the meaning of of," in *2006 IEEE/SMC International Conference on System of Systems Engineering*. IEEE, 2006, p. 6.

[8] M. W. Maier, "Research challenges for Systems-of-Systems," in *2005 IEEE International Conference on Systems, Man and Cybernetics*, vol. 4. IEEE, 2005, pp. 3149–3154.

[9] M. W. Maier, "Architecting principles for systems-of-systems," in *INCOSE International Symposium*, vol. 6, no. 1. Wiley Online Library, 1996, pp. 565–573.

[10] I. Sommerville, *Software Engineering*, 10th ed. Pearson, 2015.

[11] J. S. Dahmann and K. J. Baldwin, "Understanding the current state of US defense systems of systems and the implications for systems engineering," in *Systems Conference, 2008 2nd Annual IEEE*. IEEE, 2008, pp. 1–7.

[12] J. A. Lane and D. Epstein, "What is a System of Systems and why should I care?" *University of Southern California*, 2013. [Online]. Available: http://csse.usc.edu/TECHRPTS/2013/reports/usc-csse-2013-500.pdf

[13] SEBoK Authors, *The Guide to the Systems Engineering Body of Knowledge (SEBoK)*, 1st ed. Hoboken, NJ: The Trustees of the Stevens Institute of Technology.: BKCASE, 2016, ch. Stakeholder Needs and Requirements.

[14] J. Cleland-Huang, "Stakeholders on the prowl," *IEEE Software*, vol. 33, no. 2, pp. 29–31, 2016.

[15] J. O. Clark, "System of Systems Engineering from a Standards V-Model and from a Standards, V-Model, and Dual V-Model Perspective," in *Systems and Software Technology Conference*, Apr. 2009.

[16] J. S. Dahmann, G. Rebovich Jr, and J. A. Lane, "Systems Engineering for Capabilities," DTIC Document, Tech. Rep., 2008.

[17] J. Dahmann, G. Rebovich, M. McEvilley, and G. Turner, "Security Engineering in a System of Systems environment," in *Systems Conference (SysCon), 2013 IEEE International*. IEEE, 2013, pp. 364–369.

[18] W. Finn, "Afghan Mission Network: The Human Factor," http://amrel.com/2011/02/02/afghan-mission-network-the-human-factor/, Feb 2011.

[19] P. Buxbaum, "Network for a Mission," *Military Information Technology*, vol. 14, no. 9, Oct. 2010.

[20] J. Nankervis, "Afghan Mission Network," in *Command and Control In Network Enabled Capabilities Environment: Seminar Review Document*. NATO / National Defence University, 2011, pp. 24–25.

[21] G. I. Seffers, "Combat communicators bust paradigms," *SIGNAL Magazine, AFCEA International*, Jan. 2011. [Online]. Available: http://www.afcea.org/content/?q=combat-communicators-bust-paradigms

[22] C. C. Serena, I. R. Porche III, J. B. Predd, J. Osburg, and B. Lossing, "Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network," DTIC Document, Tech. Rep., 2014.

[23] R. D. Thiele, "Enabling Cooperation via Common Situational Awareness Pragmatic Considerations on NATO-China Cooperation," Institut fr Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW, Tech. Rep. 220, Mar. 2013.

[24] L. Brooke-Holland and C. Mills, "Afghanistan: The Timetable for Security Transition," House of Commons Library, International Affairs and Defence Section, techreport Commons Briefing papers SN05851, Jul. 2012. [Online]. Available: http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN05851

[25] H. S. Kenyon, "NATO Focuses on the Bottom Line to Support Warfighters," *SIGNAL Magazine, AFCEA International*, Sep. 2010. [Online]. Available: http://www.afcea.org/content/?q=nato-focuses-bottom-line-support-warfighters

[26] Thales, "Thales and NATO strengthen partnership," Jun. 2008. [Online]. Available: {https://www.thalesgroup.com/en/content/thales-and-nato-strengthen-partnership}

[27] CFBLNet, "CFBLNet Publication 1 Annex A, CFBLNet Terms of Reference," Combined Federated Battle Laboratories Network (CFBLNet), Tech. Rep. v8, Jul. 2015. [Online]. Available: http://www.disa.mil/CFBLNet/Docs

[28] NATO Communications and Information Agency, "CFBLNet," NCI Agency Website, Nov. 2013. [Online]. Available: https://www.ncia.nato.int/Documents/Agency%20publications/CFBLNet.pdf

[29] Anonymous, "Coalition Warrior Interoperability Exercise (CWIX)," NATO Command and Control Centre of Excellence (C2COE) C2pedia Website, Apr. 2010. [Online]. Available: http://www.c2coe.org/c2pedia/index.php?title=Coalition_Warrior_Interoperability_Exercise_(CWIX)

[30] J. Rose, "Coalition Inoperability Assurance and Validation Charter," Coalition Interoperability Assurance & Validation (CIAV), Document Version 1.02, Dec. 2011. [Online]. Available: https://wss.apan.org/2525/CIAV/CIAV%20Charter%20v1.02.pdf

[31] T. Rissinger, "13058 - Coalition Interoperability Assurance & Validation (CIAV) and Coalition Test & Evaluation Environment (CTE2)-A Model for Coalition Interoperability in a Distributed Construct," in *Track 6 - Mission 3, Effective Test and Evaluation*, NDIA 14th Annual Systems Engineering Conference. San Diego, CA, USA: NDIA, Oct. 2011. [Online]. Available: www.dtic.mil/ndia/2011system/13058_RissingerWednesday.pptx

[32] K. Herrmann, "Assured and Secure End-to-End CIS Services Provision in Network-Enabled Environment," in *TechNet International 2010: Session II*. AFCEA, Oct. 2010. [Online]. Available: http://www.afcea.org/europe/events/tni/10/documents/LtGenHerrmann.pdf

[33] G. Friedrich, "From Afghanistan Mission Network to Federated Mission Networking," in *NATO C4ISR Industry Conference & TechNet International 2014: Session 2 New Generation C2 Services*. AFCEA Europe, NCI Agency, Mar. 2014. [Online]. Available: https://www.eiseverywhere.com/file_uploads/2f6043f27e1576122f1b3e0319d5b1d8_FromAMNtoFMN-Friedrich.pdf

[34] S. Whitehead, "Achieving Joint Force 2020 Through Coalition Information Sharing," Association for Enterprise Information (Website), 2014. [Online]. Available: http://www.afei.org/PE/4A05/Documents/Whitehead_4A05%20%20AFEI%20Draft%205%20Mar%2014%20(Smooth)1630.pdf

[35] K. F. Veit, "The Afghanistan Mission Network (AMN) A model for network enabled capabilities," in *Berlin Security Conference: Panel VIII - C4ISR in NATO and EU - Command and Control in Operations*, Nov. 2011. [Online]. Available: http://www.european-defence.com/Review/2011/binarywriterservlet?imgUid=a3740d83-f8c1-b331-76b8-d77407b988f2&uBasVariant=11111111-1111-1111-1111-111111111111