24th ICCRTS Paper Abstracts

24th ICCRTS Paper 1 Abstract

Multi Domain Command and Control (MDC2) an Execution Concept

Dr. Marvin L. “Lenard” Simpson, Jr.

There has been outstanding effort describing the expected conceptual outcomes of Multi Domain Command and Control (MDC2). The challenge has been transposing the conceptual language into executable output products, as efforts have shied away from overall global improvement in Command and Control (C2). Improving data flow/storage and improving C2 are conjoined sets, but not overlapping conceptual sets. Information flow is made up of both noise and signal. It is not the volume of data that matters, but rather the signal that matters. Having everyone share a gigantic common “data lake” or even a commonly replicated “data ponds” does not by default, make better fisherman of information seekers. Just as pushing more data into one end of any comm pipe, database or someone’s cloud with the hope the operator will somehow extract just more signal on the other end is not a valid assertion. The goal of this paper is to use the lens of C2 theory, Air Force history and cutting-edge technology to see what can be accomplished to improve global C2 in an MDC2 world. This paper attempts to lay out an execution vision regardless which of the four classical program advancement techniques any solution providers decide to use. Therefore, a sub goal of this paper is to simplify the operational vision of the future MDC2 to help the acquisition community to provide the first physical version of the MDC2 quicker, cheaper and with all needed military capability.
Key Words: MDC2, Multi Domain Command and Control, C2, Command and Control

24th ICCRTS Paper 2 Abstract

Balancing Cyber Risk and Investment with Mission Execution and Success
– Are Improvements Available?
– Balance Factors' Discussion and Suggestions

Russell E. Bryant

With the impetus and emphasis, attention garnered for information, data security; and, all aspects of information, electronic, cyber security – Is the attention well placed and balanced? There are ongoing discussions of whether information technology, cyber operations are primary or secondary level skills and capabilities, capacities. This is akin to the classic supporting or supported command, execution, and operations tasks and duties.
To address this and the balance point a review of the underlying terms' origins and their definitions is appropriate to establish a reasonable frame of reference for further discussion. It is supposed that some originate from the fourth estate, intelligence, exploitation community. Some arise from the electronics, information technology community. Some may be point to their origination within the mathematics, or even the ethics historical communities.
The terrain of responsibility along with organization changes seems to have a bearing on perspective and authorities. Both of which are due for discussion and possible clarification or changes.
The author will attempt through these sub areas and terms of reference presentation to offer a perspective related to balance and well placed attention for a potential path forward. All to contribute and instigate discussions, while potentially removing some aspects of approach biases.

24th ICCRTS Paper 3 Abstract

Aligning Command and Control (C2) and Cyber Risk to Mission

Mr. Ken D. Teske

Mission Partner and Coalition Command and Control (C2) and Cyber forces must develop options and capabilities that enhance inter-dependence and further their alignment "harmonization" to increase everyone's effectiveness and understanding, while reducing the Cyber risk to the mission. The following four principles are a necessity in order to achieve alignment and integration: Common view with goals and objectives, Common understanding of capabilities, Alignment of efforts to ensure coherency, and Assessment to change course or direction as needed.

Both alignment and integration will help address the challenges associated with any Cyber Risk to Mission in today's ever-changing environment. Applying and evolving a framework approach that was discussed in the 19th ICCRTS, paper (003), 21st ICCRTS, paper (001), and 22nd ICCRTS, paper (004) demonstrates the importance of comprehending that each and every partner; Special Operations, Conventional Forces, Ministries, Departments, Bureaus, or Agencies are important to better understand and confront C2 and Cyber risk, problems, and issues.

We must use our collective lessons learned, best practices, approaches, and strategies identifying common goals, areas of interest, capabilities, and common categories of effort to be applied by each of the organizations as the focus area to maximize our Cyber-enabled capabilities

24th ICCRTS Paper 4 Abstract

Is a Bespoke Design for Multi-Domain C2 Necessary?

David S Alberts

The growing interest in Multi-Domain C2 (MDC2) is directly related to the need to orchestrate a heterogeneous set of entities and the operations they undertake in multiple domains, domains as different as the physical, virtual, and cognitive/social domains, in order to create 'synchronized' kinetic and non-kinetic effects.

This paper focuses on a fundamental issue for those involved in Multi-Domain Operations, that is, whether or not they need to design a bespoke MDC2 Arrangement for a given Multi-Domain Operation (MDO). The : 1) provides a conceptual framework for thinking about MDC2; 2) presents the results of an initial set of ELICIT experiments designed to explore the appropriateness of various MDC2 Arrangements under a set of scenarios from different regions of an MDO Endeavor Space; and, 3) presents some initial findings with regard to the need to customize entity C2 in order for a MDO to be effectively managed.

The paper begins with a brief description of a generic MDO, an explanation of what is meant by MDC2, and an extension of the Entity C2 Approach Space to MDO that encompasses the full set of MDC2 Arrangement options that could be considered. Six MDC2 baseline options are selected from the MDO C2 Arrangement Space for the analysis. The MDO Endeavor Space is then introduced with eight regions and a corresponding set of scenarios that reflect the challenges associated with each of these regions. Results from a baseline set of 48 experimental runs (one for each of the six baseline MDC2 options paired with each of the eight scenarios) are presented. An alternate set of scenarios and a bespoke MDC2 Arrangement are introduced. A second set of experimental runs provides the basis for a comparative analysis to see if there is anything to be gained by moving beyond the baseline set of MDC2 Arrangement options to a bespoke MDC2 Arrangement.

This paper draws heavily upon the ongoing work of the North Atlantic Treaty Organization (NATO) Scientific Technology Office (STO) Research Group SAS-143 and its interim products. Thus, the experiments and the analysis of their results reported upon here are continuing. The final report of SAS-143 is expected to be completed in the Spring of 2021.

24th ICCRTS Paper 5 Abstract

Risk-based cyber mission assurance model, process and metrics

Francois Rheaume

The objective behind cyber mission assurance is to ensure that missions can be performed successfully despite operating in a cyber contested environment. This requires the ability to not only assess potential cybersecurity events, but also to assess their impacts in the first place, and to develop resilience to both the events and their impacts. Resilience is the ability to avoid, withstand or recover from potential adverse events and their impacts.

Building from existing guidelines and frameworks, this paper presents a cohesive set of tools that project managers can use to develop a cyber mission assurance program, define requirements or build a cyber mission assurance capacity. The goal is not to reinvent the CMA concepts but rather to provide a structured way to decompose the necessary CMA activities, to execute them and to measure their results. Three complementary elements are described: a layered model that structures types of risks and their relations, a process that assesses the risks and that develops the resilience, and a set of metrics to measure the effectiveness and performance of cyber mission assurance in projects. Attempts at measuring the state of cyber resilience alone are not enough; stakeholders must first measure their state of awareness about the risks of operating in the cyber space. Only on the basis of this awareness can the state of resilience be measured. The presented process and metrics, along with the underlying model, explicitly manage this correlation, therefore supporting informed decision-making during all phases of the life cycle of systems.

24th ICCRTS Paper 8 Abstract

Quantum Probability Models for Decision Making

Timothy Darr[1], Richard Mayer, R. David Jones, Timothy Ramey, Ryder Smith, Chris Zimmerman

Knowledge Based Systems Incorporated College Station, TX

Research has demonstrated that human judgment and decision making is sometimes enigmatic; that is, there are situations in which human decision making deviates from classical probability and utility models. Examples include: sunk cost fallacies, anchoring, availability heuristics, Halo effects, group think, bandwagon effects, etc. Not only do our own decisions suffer from this condition, but more importantly, the actions of other actors are often hard to predict or interpret. In an atmosphere of uncertainty and lack of consensus, decisions by the various actors in a situation may seem irrational and ambiguous.

In recent years, the mathematics of quantum probability theory has proven well suited to effectively modeling some of the enigmatic human decision making behavior. Similar to its application in physics, quantum probability theory allows the analyst to model multidimensional features in the decision space. Decisions-to-act are represented as wave functions over these features. Interference among these wave functions model observed enigmatic behaviors.

We posit that an application of quantum probability theory to decision modeling and simulation will lead to clearer and more substantial understanding of the environment and better situation awareness. In this paper, we present an overview of practical methods and tools for applying the mathematics of quantum probability to understand, explain and predict human decision-making behavior. These methods and tools will be discussed in the context of several operational use cases including enemy course of action analysis.

24th ICCRTS Paper 9 Abstract

Time-pressure improves decisions in generalized Colonel Blotto games

Daniel Houser * Jianxin Wang † Timothy Darr ‡ Richard Mayer §.

We report data from generalized Colonel Blotto game experiments using human participants. When played with complete information, our game has a unique pure strategy Nash Equilibrium which we use as a baseline against which to measure actual play. We show that humans are better able to achieve Nash Equilibrium, and make empirically better decisions, when playing the game under time pressure and with imperfect information. These results caution against 'overthinking' strategic decisions and highlight the importance of 'gut' reasoning during combat.

Keywords: Time Pressure, Nash Equilibrium, Generalized Colonel Blotto Game, Decision making under imperfect information

24th ICCRTS Paper 10 Abstract

Determination of asset criticality for decision support in operational networks

Maxwell Dondo
Defence Research and Development Canada 3701 Carling Avenue, Ottawa ON K2G 6R7 Canada

Abstract—Understanding the criticality of information tech- nology infrastructure (ITI) assets is crucial for effective decision making in an organisation's computer network defence (CND). Criticality is a measure of an asset's relative importance to the organisation's cyber capability delivery. This measure applies to all ITI assets that could adversely impact an organisation's ability to operate in cyber space if lost or degraded. Existing approaches to determine asset criticality focus on ranking assets without consideration of where and how they are deployed, and the methods used do not provide scores that could be used in further computations such as risk analysis.

This paper provides a criticality measure that addresses these gaps by characterising the relative importance of ITI assets to the organisation's cyber capability. Our approach determines the asset criticality scores based on criteria representing assets' relative importance to meeting the organisation's missions and functional objectives. Individual scores are determined using an adapted multi-attribute decision making (MADM) technique and then rolled up into aggregate criticality scores at the organisational, site, and service levels.

The approach is demonstrated using a hypothetical network and a simulation of a real military operational network. Our results, which are shown to be self-consistent, are validated using criticality scores determined from human operator input. The resulting criticality scores can be used to inform cyber risk management and prioritisation of cyber activities such as course of action (COA) selection or capability acquisitions.

24th ICCRTS Paper 11 Abstract

Framework for Implementing a Data Science Capability in a Military Intelligence System

S.V. Ball (Council for Scientific and Industrial Research)

M.C. van't Wout (Council for Scientific and Industrial Research)

Dr R. Oosthuizen (Council for Scientific and Industrial Research)

Modern day conflicts give rise to complex problems that traditional military intelligence approaches and tools struggle to resolve. There is a need for prediction and/or forecasting in the military domain based on effective intelligence processing capabilities for pro-active measures as well as reactive responses. Intelligence processes and tools are becoming increasingly inadequate to support the decisions of commanders and other decision makers. The tsunami of data of the current age requires a system of new processing and analysis tools, with the supporting skills, to provide the intelligence required for making decisions about complex situations. The Internet of Battlefield Things (IoBT) and resulting Big Data is a reality for current and future military operations. The field of Data Science provides a foundation for processing and analytic tools, processes and skills. This paper assesses current literature on intelligence analysis and Big Data to define a framework that will guide the implementation of a Data Science Capability for modern military operations. The intelligence system is viewed from a sociotechnical system perspective to identify high-level requirements for implementation of a proposed Data Science framework for intelligence systems. The framework is derived from mapping the requirements of the traditional intelligence cycle to the various Data Science methods, tools and skills.

24th ICCRTS Paper 13 Abstract

Evaluation of Cyber Effects in a Perception-Based Campaign Model

Charles D. "Chuck' Burdick, CAP

Dr. Deepinder P. Sidhu

The Joint Analysis System (JAS), is a GOTS, multi-domain campaign simulation whose agents base their decisions on sensor-driven perceptions, not ground truth. Information transfer in the model occurs over simulated networks whose disruption causes delay or loss of specific information, which cause measurable operational effects. JAS can be paused or slowed to wall clock time to allow replacing C2 agents with human decisions- makers. The humans can read the same status reports as the computer agents, observe the same map-based perceived Common Operational Picture and then use their own perceptions to make decisions which can show the impact of information disruption within the model for a given time. To determine the length of that time, the authors propose employing cyber data from documented cyberattacks, penetration tests, cyber exercises, and both hardware-based and virtualized cyber ranges, and an emerging network technology which provides low-cost network emulation using virtual hardware. Used by government Information Assurance agencies the system emulates specific networks by mapping them in full detail and reverse engineers them to create full-fidelity clones of the target networks.

Cyber training conducted in these cloned virtual environments can provide credible estimates of the time needed to detect specific vulnerabilities in actual networks and mimic the effects of cyber-attacks on those networks passing information in the large campaign model. Collecting data from these full fidelity cyber training environments can potentially provide estimates of how often cyber-attacks are thwarted, and, when successful, how long it takes to remediate the damage. With that data, the campaign model can represent the data losses occurring during those outage times and also portray alternative communications paths, back-up databases, etc. and evaluate their ability to assist in recovery from the attacks. The struggle in the network exercises and cyber ranges/emulators should provide an estimate of where cyber-attacks are likely to occur, what types of attacks are most effective, and how long outages will occur, while the campaign model reflects the operational impact of the disruption of its information flows.

24th ICCRTS Paper 14 Abstract

Towards friendly force tracking with MQTT over LoRa

Frank T. Johnsen[a], Trude H. Bloebaum[a], and Philip Ø. Puente[b] [a]Norwegian Defence Research Establishment (FFI), Kjeller, Norway

[b]Norwegian University of Science and Technology (NTNU), Trondheim, Norway

With the steady growth of the Internet of Things (IoT) in the civilian commercial sector, the question arises as to whether such IoT concepts can also be used for defense purposes. Military needs, especially those that depend on tactical communications, can be regarded as more challenging to solve than the needs that are focused on in the civilian sector. Therefore, one can expect that much of the work done in the civilian sector cannot necessarily be used directly for military purposes and that targeted research and development in this field will be required to enable effective deployment. This paper explores using Raspberry Pi 3 and the Long-range Radio (LoRa) protocol as an IoT platform for friendly force tracking with the light-weight, industry standard Message Queuing Telemetry Transport (MQTT) publish/subscribe protocol.

Keywords: LoRa, friendly force tracking, MQTT, publish/subscribe

24th ICCRTS Paper 15 Abstract

Evaluating Publish/Subscribe Standards for Situational Awareness using Realistic Radio Models and Emulated Testbed

Frank T. Johnsen and Trude H. Bloebaum Norwegian Defence Research Establishment (FFI) Norway

Norman Jansen Fraunhofer FKIE Germany

Andrew Toth and Kevin S. Chan CCDC Army Research Lab (ARL) USA

Gerome Bovet Armasuisse Switzerland

Marco Manso PARTICLE, Lda. Portugal

There is currently an ongoing initiative to improve the interoperability between nations and other partners during common missions through Federated Mission Networking (FMN). So far, the focus of the standardization and profiling work done in FMN has mostly been on static and deployed networks, where networking resources are stable and plentiful. There is however also a need for interoperability at the tactical edge, between mobile units that have limited and often disrupted communications. In a previous study, we compared different protocols for subscription based distribution of information. We concluded that the WS-Notification standard, which is currently used in NATO, has a too large overhead in lower capacity tactical networks, and that for instance the Message Queuing Telemetry Transport (MQTT) protocol could be used instead.

In this paper, we expand upon those findings by investigating the applicability of MQTT in tactical networks further. Here, we address one of the main shortcomings in the testbed used in our previous experiments by adding in new and more realistic radio models, which allow us to better assess the performance of MQTT in the tactical domain. Furthermore, we also expand our experiments evaluating MQTT for sensor networks (MQTT-SN) as well. The reason for adding MQTT- SN to the experiments is that this protocol is based on UDP rather than TCP.

This work has been performed in the context of the NATO STO/IST-150 «NATO Core Services profiling for Hybrid Tactical Networks» working group.

24th ICCRTS Paper 16 Abstract

A socio-cognitive perspective on implementation and use of smart technology in the Norwegian home guard

Celine R. Karud[a], Frank T. Johnsen[b], and Trude H. Bloebaum[b]

[a]University of Southern Denmark, Denmark

[b]Norwegian Defence Research Establishment (FFI), Kjeller, Norway

The Norwegian Defence Research Establishment (FFI) has developed a communications concept for the Norwe- gian home guard (HV). This concept, called ”SMART” due to the emphasis on smart technologies, has been realized as a technology prototype on the Android platform. The concept includes blue force tracking, observa- tion reports, and chat, and has been tested as an enhancement to the primary communications, which is voice radio. The prototype has been used in several field trials with HV.

This paper presents a qualitative study where the main purpose is to detect potential individual perceived barriers to using the SMART concept, and discuss these from a socio-cognitive perspective. Three semi-structured interviews were carried out with HV personnel. The data material was inductively analyzed and the results presented as ”causal network”. The results show four main interactions that explain potential perceived barriers to adopting the SMART concept in HV. These barriers are discussed from a solution-oriented perspective, and approaches to how the barriers may be overcome are presented. We argue that barriers imposed by technological factors can be mediated by employing appropriate social and organizational measures.

Keywords: Psychology, Situational awareness, Smart technology

24th ICCRTS Paper 17 Abstract

SMART II: Android apps, cloud computing and mobile device management as enablers for efficient operations

Frank T. Johnsen[a] and Ida M. Frøseth[b]

aNorwegian Defence Research Establishment (FFI), Kjeller, Norway
bThe Norwegian Defence University College, Lillehammer, Norway ABSTRACT

”SMART” – pervasive situational awareness at the individual soldier level – was a Concept Development and Experimentation (CD&E) project carried out in Norway during 2016. The concept being tested was the use of smart technology as a cheap and low-complexity platform for collaboration and situational awareness for the Norwegian home guard (HV). SMART included building a prototype based on the Android platform. The prototype was tested in several field trials. In general, the results from the activity strongly indicated that using civilian smart technology yields an operational value. The SMART prototype and concept can provide cheap and low-complexity communications to HV and others who may need this capability. The prototype has since 2016 further evolved, and was used in another CD&E project in 2018, the so-called ”SMART II”. Here, we focused on necessary communication and computing infrastructure support for forces using smart devices to establish their common operational picture. As part of the experiments, we evaluated approaches such as cloud computing and mobile device management (MDM) when deploying and using the software. HV tested the prototype extensively in 2018, with the culmination being its use during the Trident Juncture exercise by one of HV’s rapid response forces. In this paper, we give an overview of our prototype, with emphasis on technology and our experiences with the supporting infrastructure tools.

Keywords: Cloud computing, Mobile device management, Android, Situational awareness

24th ICCRTS Paper 18 Abstract

Uncertainty-Oriented resource selecting method for Agile command and control system

DUANMU Zhu-yun, DING Feng , LI Hao-yu
Science and technology on information systems engineering laboratory,

Nanjing, Jiangsu, 210007, P.R. China

Aimed at building the agile command and control (C2) system, selecting the combination of resources is one of the most important problem. Nowadays, only the fixed value is taken into account and the general values are ignored, which will bring distortion into result. So, it is more meaningful to adopt interval-number. For solving the problem of selecting the combination of resources to build the agile command and control (C2) system, the dynamic attributes of the resources were descripting by interval number. Then, by combing the interval number with the Grey relationship grad theory, the model for selecting the optimal resource of Agile command and control system was constructed. And the weight of each attribute is obtained via using the entropy weight. The similarities between each plan and “the optimal attribute” were calculated by using grey relevance analysis. Lastly, the plan having the maximum similarity was selected. In the instance application, the availability of the method is validated.

24th ICCRTS Paper 19 Abstract

Information Related Capabilities: Targeting Cycle Experimentation and Analysis.

David Connell* and Ahmed Ghanmi

Defence Research Development Canada – Centre for Operational Research and Analysis
Department of National Defence / Government of Canada
Ottawa, ON, K1A 0K2
Canada

* Corresponding Author: david.connell@forces.gc.ca

Abstract. Information and information related capabilities (IRC) play an increasingly critical role in the planning and conduct of military operations. The incorporation of information related capabilities into full spectrum targeting processes are discussed in this paper through the analysis of a series of joint, non- munitions-based experiments. The experiments, based on a real world scenario utilizing current data, are used to support the targeting cycle activities. This paper will describe the targeting (objective, effects, tasks) activities and report on IRC: capability gaps, decision support requirements, Collateral Effects Estimation (CEE) and lessons identified across the strategic, operational and tactical levels. Aspects of information composition and sharing, shared understanding, trust, decision making, risk and assessment associated with the planning and employment of information related capabilities will be presented.

24th ICCRTS Paper 21 Abstract

Training and Evaluating Cyber Analytical Expertise

Regina Joseph, Sibylink
Marieke Klaver, TNO
Judith van de Kuijt, TNO
Diederik van Luijk, National Cyber Security Centre, Netherlands Ministry of Justice and Security

Threats, vulnerabilities, and new forms of attack within the cyber domain develop rapidly. To keep up with and respond to these trends, cyber security professionals must demonstrate reaction velocity, accuracy and a high tolerance for complexity. Publicly available information (PAI) can serve as an important aid to personnel engaged in cyber security analysis. However, evaluation of cyber analytical capacity—a pre-requisite for any measurement of quality or improvement—is still inchoate. This paper covers the concept and design of an initial phase of research begun in October 2018 in The Netherlands and expected to conclude by November 2019 to measure and improve cyber analysis techniques. The research program features a forecasting tournament to record participants' probabilistic estimates on future cyber outcomes based exclusively on PAI knowledge acquisition. The forecasters' predictions are scored using a proper scoring rule (Brier, 1950) in an effort to observe correlations between information gathering and analytical accuracy. Over the course of one year, Dutch public and private sector cyber security professionals receive training in forecasting and open source information extraction; are tasked with making predictions on 50 different events across ten cyber subject matter areas; and are evaluated on their predictive accuracy, calibration, news awareness and bias recognition skills. This phase of research seeks to address whether analysts' predictions are more accurate in certain subjects within the cyber domain than in others and to assess how predictive accuracy in the cyber domain compares to accuracy in other domains in which forecasting tournaments have been organized.

24th ICCRTS Paper 22 Abstract

Applying First Principles to Re-Imagine Delivery of the 5th Generation Force

James H.C. Gibson

The pace of change overwhelms the ability to field battlespace ready integrated systems. There is wide-spread recognition that things must change but little agreement on what the change must be. I argue that we need to reframe the problem to ensure that the information technology foundations for C4ISR are an enabler, not a roadblock for the 5th Generation Force.

In this paper I go back to first principles and draw on past work in Network Centric Warfare [1], Information Advantage [2], Command and Control Approaches [3], C2 Agility [4] and the OODA Loop [5] to derive a framing (or paradigm [6]) suitable for holistically engineering the 5th Generation Force.

To my surprise, this results in an inversion of the current approaches. If true, this new approach has significant ramifications, architectural implications, and the power to transform many aspects which currently act as roadblocks to a future state. As a paradigm, the impacts spread across all the themes addressed by the ICCRTS conference.

This paper is intended to provoke discussion and calls for engagement to determine the merit, ramifications and improvements for this approach. An equally valid outcome might prove that this approach is wrong. In this case, the engagement needs to fail fast.

24th ICCRTS Paper 23 Abstract

Calm Interfaces for Integrated C2 Systems

H.-C. Schmitz, A. Cornaggia-Urrigshardt, F. Gσ˙kgσ˙z, S. Kent, K. Wilkinghoff

The concept of calm technology, according to Marc Weiser and John Seely Brown [26] as well as, more recently, Amber Case [3], demands that technology must be robust and unobtrusive. It should require the least amount of human attention possible and make use of the periphery of attention. It should support natural human behaviour and be integrated into established working processes. Technology must enable users to accomplish their essential tasks, which go beyond system interaction, as easily as possible. We investigated Command & Control Information Systems (C2IS) that are integrated into battle tanks and provide the crew with a picture of the current operational situation. The systems enable data exchange within the platoon and the company. However, it seems as if integrated C2IS in use do not reach their full potential as relevant information is not always entered in time and, there- fore, the operational picture is not always complete and up-to-date. One reason for this is that system interaction via the existing GUI, a touchscreen and a keyboard, requires more cognitive effort than can actually be provided, particularly in stressful situations. Following the principles of calm technology, we developed the concept of a distributed, multimodal interface, allowing for both input and output in diverse modalities and via various channels. This also includes other systems in use, such as the tank's periscope. Interaction via a calm interface does not absorb the attention of the operators but instead allows them to interact with the system simultaneously with other tasks. We implemented a prototype and evaluated it with military subject matter experts (SME). Our results indicate the prototype's usefulness and ease of use.

24th ICCRTS Paper 27 Abstract

Implementing a Prototype Reach-back Capability for Decision Support in Multi-domain and Coalition Operations

Adam Brook and Brian Wardman Defence Science and Technology Laboratory (UK)

Kevin Galvin
Thales Research & Technology (UK)

Deryck Arnold
Thales Training & Simulation (UK)

This paper describes experimentation being undertaken by the UK Defence Science and Technology Laboratory (Dstl) supported by Thales UK to develop a prototype simulation-based military decision support capability. The paper looks at: some types of problem which will benefit from a decision support agency; the techniques needed to develop the capability; the challenges in implementing a usable and helpful system; and initial observations about the prototype system. The work describes a simulation reach-back capability supporting the planning and execution of a live-play UK/Coalition joint, multi-agency training event. It builds on the fruits of a number of national and international experimentation and research activities and conceptual systems architectures discussed in this forum in recent years.

The system developed builds on the NATO Allied Command Transformation (ACT) Command and Control (C2) concept architecture for 2030 using cloud computing services with wide area network connectivity to provide reach-back to a decision support centre. Here simulation systems are populated with data to replicate current operational status, etc permitting a number of alternative courses of action to be developed and analysed. The simulation environment offers a number of benefits including the ease with which the decision support results can be shared with the operational user.

24th ICCRTS Paper 29 Abstract

C2 in the Mafia

Marius Vassiliou
Institute for Defense Analyses
mariusvassiliou@gmail.com

Organized crime groups (“mafias”) such as the Sicilian Cosa Nostra, the Calabrian 'Ndrangheta, and others appear to employ effective forms of command and control (C2), well suited to their missions. Studying criminal organizations is difficult because of their inherent secrecy. However, over the years, a body of information has been inferred by various investigators about the nature of such entities. We review some of this knowledge and analyze it through the lens of C2 theory. Most mafias are rigidly hierarchical at the clan level, but the purported hierarchy often overlays a much looser, entrepreneurial, and decentralized de facto network. A form of Mission Command is employed. The shared intent implicit in profit maximization and avoidance of apprehension serves as a fundamental motivator. The de facto allocation of decision rights is broadened by various considerations, including the need to isolate and contain the risk of apprehension, as well as the need for flexibility of action in the face of evolving circumstances. Patterns of interaction and distribution of information are constrained by apprehension risk. Mafias also perform varying degrees of collective C2, to coordinate the activities of various clans within the overall umbrella mafia and contain conflict between them. There is evidence that organizations practicing collective C2 at the appropriate level can outperform those whose clans operate too independently, or conversely are too constrained—and do so with less violence. This is shown, for example, by some cases where the 'Ndrangheta has operated more effectively than the Cosa Nostra in expansion to new territories.

24th ICCRTS Paper 31 Abstract

Ensuring Allies and Coalition Partners Can Leverage C4ISR Technologies to Manage Cyber Risk to Mission

José R. Carreño, George Galdorisi, Paul Shigley

All U.S. security strategies share one thing in common – they call for strengthening U.S. integration with allied and partner nations. The National Defense Strategy goes further, calling for, "strengthening alliances as we attract new partners."

While there are many ways that the United States can strengthen alliances and coalition partnerships, one way is to ensure that forces can be interoperable. For the U.S. Navy, and those we partner with, this involves ensuring that C4ISR technologies enable navies to seamlessly share information.

While policy directives encourage the development of mutually compatible C4ISR technologies, the devil is in the details regarding how the navies of different nations can achieve interoperability. As Dr. David Alberts put it at a previous ICCRTS Symposium, "In today's world, nothing significant can get done outside of a coalition context, but we have been *humbled* by the challenges of devising effective coalition communications."

At the Naval Information Warfare Center Pacific, we have information exchange agreements (IEAs) with almost two dozen nations. These IEAs enable our scientists and engineers to work with their counterparts in laboratories in these nations to co-evolve and develop C4ISR technologies that will enable our navies to work together seamlessly.

We will present our experience as a concept that other Department of Defense (DoD) laboratories may wish to adopt in order to share research and development costs and achieve the kind of interoperability that achieves the NDS goal of strengthening alliances.

24th ICCRTS Paper 33 Abstract

Experimental Evaluation of a Command and Control – Simulation Interoperation Standard in a Coalition Environment

J. Mark Pullen
C4I & Cyber Center George Mason University

4400 University Drive Fairfax, VA 22030, USA mpullen@c4i.gmu.edu

Brian Wardman
Defence Science and Technology Laboratory, UK Ministry of Defence Portsdown West,
Portsdown Hill Road
Fareham, Hants, UK PO17 6AD bwardman@dstl.gov.uk

James Ruth Trideum Corporation 1000 S. 4th Street, Suite C Leavenworth KS 66048, USA
jruth@trideum.com

The NATO Modelling and Simulation Group (MSG) Technical Activity 145 and SISO Product Development Group for the C2-Simulation Interoperation (C2SIM) have been working together to standardize and operationalize a new capability, which has been described in previous ICCRTS papers by the authors. SISO anticipates balloting the standard late in 2019. This paper reports on an experimental evaluation of the new C2SIM standard that has been undertaken by MSG-145 in preparation for the balloting process. The paper describes the experiment design and its rationale, and includes experimental results.

The planned evaluation involves experimental application of systems that implement the SISO draft C2SIM standard. Software systems from France, Germany, Italy, New Zealand, the UK and the USA interoperated. Evaluation was performed in phases, over a three-month period:

- Experimental application done independently by six national teams, exploring use cases they have been developing since the beginning of MSG-145. A corollary benefit of this phase is that the implementations have been confirmed as operational and the users familiar with them.
- Detailed validation testing of all information flows in the coalition of C2SIM systems in conjunction with NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXcercise (CWIX) 2019, via an Internet Virtual Private Network (VPN).
- Experimental use in a small-scale coalition military distributed mission planning exercise. This includes experimental evaluation of the cyber emulation capability described in a 2018 ICCRTS paper.

24th ICCRTS Paper 35 Abstract

Mobile Tactical Forces:
Experiments on Multi-broker Messaging Middleware in a Coalition Setting

Marco Manso and Barbara Guerra PARTICLE, Lda. PORTUGAL

Kevin Chan and Andrew Toth Army Research Lab (ARL) USA

Ret.Col. Fernando Freire Portuguese Army PORTUGAL

Norman Jansen Fraunhofer FKIE, GERMANY

Trude H. Bloebaum and Frank T. Johnsen Norwegian Defence Research Establishment (FFI) NORWAY

The environment in which tactical forces operate is characterized by disconnected intermittent connectivity and limited bandwidth (DIL). This environment significantly constrains the application of widely used technologies. These characteristics require that technology and standards need to be carefully selected and that appropriate profiles are set. The NATO IST-150 research group is tackling this challenge by analysing standards and technologies appropriate for tactical networks, obtaining promising results with the Message Queue Telemetry Transport (MQTT).

As a result of the NATO IST-150 activities, this paper presents the application and evaluation of MQTT technologies in the context of a three nation coalition setting (i.e., federated-based setup) – specifically NOR (Norway), Portugal (PRT) and the United States of America (USA) – supporting information exchange between brokers, while preserving the Nations' ownership (and control) over its resources.

Using a simplified version of the Blue Force Tracking (BTF) service, the experiment demonstrates the MQTT ability to propagate messages across the whole coalition. Moreover, the experiment results show a high-reliability and low latency in delivering messages (including between coalition brokers).

The North Atlantic Treaty Organization (NATO) places a high priority in achieving technical interoperability between Allied forces, including at the tactical edge, in which IST-150 findings and recommendations will provide valuable inputs.

24th ICCRTS Paper 36 Abstract

Mission Command when waging cyber operations

LtCol Anders Josefsson
E-mail: anders.josefsson@fhs.se Swedish Defence University, Sweden

LTG (R) Joseph Anderson
E-mail: joea9516@gmail.com
Former Deputy Chief of Staff, G-3/5/7, United States Army

Dr Arne Norlander
E-mail: arne.norlander@gmail.com Swedish Defence University, Sweden

CDR Björn Marcusson
E-mail: bjorn.marcusson@fhs.se Swedish Defence University, Sweden

The conditions for military operations have changed due to many things and the cyber-related challenges associated with these conditions require more attention. Many cyber activities are conducted under other circumstances than conventional war that is called the grey zone between peace and war. The objective of this paper is to explore the conditions for mission command when conducting cyber operations. The distinction between war and peace has blurred and adversaries, both state and non-state, threaten the stability in many western countries. Mission command can be seen both as a philosophy and as a method. The fundamental principles for mission command as a philosophy are trust, intent focus, initiative and common ground. This paper discusses if the conditions for Mission Command have changed and are applicable while conducting different types of cyberspace operations and that offensive and defensive cyber operations imply different conditions for Mission Command. The conclusion is that Mission Command as a philosophy is still relevant, but it has to be supported by a comprehensive Command and Control (C2)-Method that is flexible and able to vary between Direct Control and Mission type Control. The C2 Method should be complemented with a dynamic and adaptive control policy for different types of cyber actions. The paper also suggests a holistic model for Dynamic Command that considers both the situations need for action and the Mission Systems C2-needs.

24th ICCRTS Paper 38 Abstract

"Reading the mind of the enemy" through an enhanced multi-domain Commander's Critical Information Re- quirements (CCIR) process

Lt Gen (Ret) Gilles Desclaux[1], Dr. Damien Marion[1] and Pr. Bernard Claverie[2]

[1] Thales Raytheon Systems, Massy-Palaiseau, France

[2] Engineering University for Cognitive Sciences, ENSC Bordeaux, France gdesclaux@ensc.fr

\

CCIRs are information requirements identified by commanders during the planning phases as being critical to facilitate their key decisions and to secure their desired strategy. In the context of increasing complexity, speed and deluge of data which characterize modern warfare, events can occur simultaneously in multiple do- mains and quickly overwhelm the Decision Cycle for operators.

For such situations, we have designed a comprehensive CCIR Process augmented by new technologies which will offer a solid performance level to ensure timely and relevant sense making and responses. We have named it "ANTICIPE". ANTICIPE stands for Augmented Near real Time Instrument for Critical Information Process Experiment.

The innovative idea is to break down a CCIR into 2 sub-levels of information, so called triggers and cues (or Weak Signals), which are linked by rules defined during the planning process. This CCIR Space constitutes an ontology which will be used as mining architecture.

ANTICIPE captures data from all available sources in the operational HQ (documents, chat, mail, Voice Communication System, C4I notifications, open sources) while trans- forming those data into knowledge artefacts. At this stage, mining is done autonomously and a Cues Appearance Data Base is implemented.

Based on a crisis scenario, the concept paper will showcase the comprehensive work- flow through which information sources are processed to discover critical information. It will introduce and discuss the various adaptive HMIs, based on Cognitive technologies. It will especially focus on the various multi-domain ones, data transparency functions and associated confidence measures.

24th ICCRTS Paper 40 Abstract

Networked information transfer strategies for Multi-domain Command and Control

Kevin S. Chan*[a], Gregory B. Judd[b], Claudia M. Szabo[c], Vanja Radenovic[b], Peter Boyd[b], Kelvin Marcus[a]

[a]US Army Research Laboratory, 2800 Powder Mill Road, Adelphi, MD 20783

[b]Defence Science and Technology Group, Third Ave, Edinburgh SA 5111 Australia

[c]Centre for Distributed Technologies, University of Adelaide, Australia

Successful Multi-domain Command and Control (C2) depends on the coordinated exchange of information across information domains. Achieving this coordination across highly dynamic single domain tactical edge network environments is already highly challenging. During Multi-domain operations, the volume of information will be immense making the delivery of the correct information to the correct entities within mission constraints and requirements even more difficult. This will require extensive transformation and filtering of the information exchanged and extensive coordination of the scheduling of information disseminated within and across operational domains. Domains must also be able to coordinate the priority of information shared when intra-domain networking resources may be even more limited than those between domains. Another big challenge is dealing with the policies that each domain has in place. Gathered information will be in multiple formats, collected at different frequencies, with different security classification, and broadly disbursed both physically and logically. The information may need translation or pre-processing prior to sending out of a domain border and this must be done without compromising the achievement of both the sending and receiving domain's mission goals. In terms of the concept of C2 Agility, we propose that these challenges require at least a Collaborative C2 maturity level, at least in regard to the C2 of shared networked resources. In order to meet these challenges within a single domain, we have developed an approach called SMARTNet which seeks to maximize the utility of limited tactical network resources through the prioritization, transformation and control of networked information. This paper will discuss how this approach can be extended to help solve the additional Multi-domain challenges described above.

24th ICCRTS Paper 42 Abstract

Effective and efficient command and control:

A concept method for inquiring the impact of visual representation on order quality

Ulrik Spak, PhD, Swedish Defence University

E-mail: ulrik.spak@fhs.se

What is effective and efficient command and control (C2)? One way of answering this question is to measure the quality of products generated within the C2-process. The main product from the C2- system, in purpose of directing and coordinating the execution system, is undoubtedly the order. One might think that the quality of orders directly correlates to effects generated in the operational environment. However, because of the unforeseeable and unavoidable events in the operational environment, such a causal relation is not necessary true. This paper presents a concept method for experimentally testing relations between order quality and outcomes, by using a simulated microworld in which such events are controlled.

One particular aspect of order quality is the representation of the actual tasks and goals. This work propose an approach that connects to earlier work on operational pictures as a requisite for situation awareness in general and mission understanding in particular. Further, this paper suggests that orders could be adapted to the situation at hand by complementing the textual order with visualizations of military tasks and goals. This line of investigation owns its specific timeliness to the escalating focus on, and need for, mission command in multi-domain C2 in a context of both military and civil defence.

24th ICCRTS Paper 45 Abstract

Tsunami of Smallsat Mega-Constellations: C2 implications

Tim Grant

Retired But Active Researcher (R-BAR) Benschop, The Netherlands
Tel: +31 (0)638 193 749

tim.grant.work@gmail.com

Command & Control (C2) is crucially dependent on the underlying communications infrastructure. This infrastructure may be wired and/or wireless, but until the opening of the space age it was exclusively terrestrial. Communication satellites in geostationary orbit revolutionised long-distance strategic communication, but have limited bandwidth, long latency times, and require bulky and expensive user terminals.

In the coming five to ten years, several commercial organisations will be launching mega-constellations consisting of hundreds or thousands of small satellites in low earth orbit. While some of these mega-constellations are aimed at earth observation, navigation and positioning, and meterology, the great majority will provide global broadband communications to low-cost user terminals and IoT devices. For example, OneWeb won FCC approval in June 2017 to operate 720 smallsats in K_u band, with an option to add another 1980 satellites. In a second FCC filing, they propose a 2560-satellite constellation using V-band. SpaceX is seeking authorisation to operate their Starlink constellation of 4425 broadband satellites using K_a and K_u bands. Other constellations are planned by ViaSat, Boeing, LeoSat, O3b Networks, and Theia Holdings. This concept paper considers the implications of this imminent “tsunami of smallsats” for C2 in military and emergency management operations.

24th ICCRTS Paper 46 Abstract

Sensor C2 in a future operational environment - A suggestion for an experimental study[6]

Mats Carlerby, PhD*
Swedish Defence University, Science of Command and Control and Military Technology Division, Stockholm, Sweden

Björn J.E. Johansson, PhD
Linköping University, Department of Computer and Information Science Linköping, Sweden

In a future and data-intensive operating environment, threats can be assumed to vary considerably. One example of such threats is missiles that can achieve speeds of Mach 5 or above. To handle this type of threat alone, it implies at least two things. First, that a suitable operational picture is provided that take account for future long-distance threats. Second, it is likely that it will be even more important to be able to collect, filter, process and understand relevant data to make priorities and make proper decisions under short time conditions. Third, when considering threats by cyberwarfare, these can be considered as conducted in the speed of light. This will probably suppose an efficient and dynamic C2 of available and different types of sensors, from directly controlled to sensors guided by AI, on a future battlefield. In this paper, we propose an experimental study to investigate from which level of sensor C2 (centralised, decentralised, or a combination thereof) seems sufficient to be able to in time respond to threats in a geographically and by information enlarged operating environment.

24th ICCRTS Paper 47 Abstract

Massage the message:
Modularising software for influence operation detection in social media

Arild Bergh, Ph. D.

Norwegian Defence Research Establishment (FFI) Kjeller, Norway

Over the past few years social media has become a key battleground in influence operations between actors who are in covert or overt conflict [1]. At the same time social media has never been more pervasive. Many of the 2 billion active Facebook users read news selected by automated software routines and many powerful state leaders bypass diplomatic channels to directly present their thoughts through Twitter. Influence operations have been undertaken by smaller and larger terrorist organisations as well as nation states and major upheavals in domestic politics appear to have been the target of small and cheap, but widely distributed, influence operations.

This article discusses a potential technical approach to detect influence operations in social media. The key goals and issues that have influenced the design of the proposed technical solution are discussed. A brief outline of potential architectural solutions that will facilitate heterogeneous data input while providing distributed situational awareness is examined in some detail.

24th ICCRTS Paper 48 Abstract

Command and Control Interoperability Middleware Architecture

Anderson Ferreira, Manoel Pedro Sá, Tomás de A. T. Botelho

Centro de Análise de Sistemas Navais (CASNAV),
Praça Barão de Ladário, s/no - Ilha das Cobras, Rua da Ponte, Ed. no 23 do AMRJ Centro – Rio de Janeiro – RJ – Brasil – CEP 20091-000

Agility, the basis for modern military operations, is a way of dealing with the combined effects of complexity and uncertainty. Modern military operations require precise and timely information shared on a secure and need-to-know basis. Distributed Command and Control (C2) exchanges from a Country's Forces and its Allies require interoperability among Information Systems (IS). In Brazil, these concepts were met by the Command and Control Interoperability project (INTERC2), started as a joint program between Brazil's Ministry of Defense (MD) and Brazilian Armed Forces to achieve C2 Interoperability among C2 Information Systems (C2IS).

According to the Brazilian Ministry of Defense Joint Operations Doctrine, the INTERC2 project built a Service Oriented Architecture (SOA) IS middleware wholly based on the Multilateral Interoperability Programme (MIP) Information Model (MIM), adopted by NATO. Its architecture is based on the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), and it exchanges messages using the Alternate Development and Exchange Method (ADEM) specification.

Adopting MIM was essential to create a common rich object representation. Although the middleware could be considered modest in its beginning to help achieve an elementary shared situational awareness, it is evolving at an increasing pace to incorporate new functionalities such as target lists.

This paper presents the IS middleware architecture, the technological and operational challenges the project team overcame and its Communication Interface, showing the main technologies used in its construction. It also describes a newer version of the middleware developed to allow interoperability between simulation systems.

24th ICCRTS Paper 49 Abstract

Platforms for Assessment of Content Prioritization in C3I GIS Systems

James Michaelis
U.S. Army Research Laboratory, Adelphi MD 20783, USA
james.r.michaelis2.civ@mail.mil

Military C3I (Command, Control, Communications and Intelligence) operations at the tactical level have come to rely upon Geographic Information Systems (GIS), which commonly offer functionality to display geotagged units of information such as imaging feeds and personnel reports. Management of In- formation Objects within military GIS applications presents a number of known research challenges tied both to selection of mission-appropriate information and management of Soldier attention. Towards supporting content filtering and pri- oritization within tactical networks, methods based on the estimated Value of In- formation specific to mission and environmental context have demonstrated prior benefit (e.g., in conservation of bandwidth). By contrast, limited research has been conducted to-date on Soldier interaction with VoI-based content filtering in GIS applications, including assessment of its impact on Situational Awareness. This paper presents foundational work being applied towards studying Soldier interaction with VoI-enhanced GIS applications, covering the design of a sup- porting experimental platform based on the Android Tactical Assault Kit (ATAK).

24th ICCRTS Paper 51 Abstract

MEAP 2: An Update to MEAP for Streaming Data

Darius E. Jefferson II
CCDC - Army Research Lab, RDRL-CII-B 2800 Powder Mill Rd, Adelphi, MD 20783
darius.e.jefferson.ctr@mail.mil

Andre V. Harrison
CCDC -Army Research Lab, RDRL-CII-B 2800 Powder Mill Rd, Adelphi, MD 20783
andre.v.harrison2.civ@mail.mil

Mark S. Dennison
CCDC -Army Research Lab, RDRL-CII-B 2800 Powder Mill Rd, Adelphi, MD 20783
mark.s.dennison.civ@mail.mil

The Moving Ensemble Analysis Pipeline (MEAP) is an open-source Python program designed to analyze cardiovascular signals obtained from body-worn sensors. Its main purpose is to calculate cardiovascular features whose values have physiologically-interpretable meanings. The value of these features can then be further analyzed in order to estimate one's physiological or psychological state. They could also be used to develop machine learning algorithms to estimate the current physiological or psychological state of a person. One of the natural applications of this software is the enhancement of command and control (C2) capabilities within the modern battlefield as a human-focused element of the Internet of Battlefield Things (IoBT), where the tasking and allocation of human assets can be improved by knowing the soldiers' current state. However, there were several limitations in the original version of MEAP. MEAP was designed to be used as a lab tool and as such many of its functions required human intervention. Also, MEAP can only read from pre-recorded sensor data in the AcqKnowledge or MATLAB formats. These problems prevented the original system from ever being useful in an IoBT environment, where transferrable data could be lost or degraded and where data would be streamed instead of being pre- recorded. In order to solve these issues, a new version of MEAP (MEAP 2) was developed. This paper presents an overview of the original MEAP, its background and purpose, and then discusses objectives for MEAP 2, the current progress on those objectives, and future applications for the software.

24th ICCRTS Paper 52 Abstract

C4ISTAR Evolving the C2 Brazilian Army Doctrine- A Tactical Case Study at Amazonian Scenario

Nina Machado Figueira[1] Victor Bramigk[2]
Gustavo Claudio Couto Karl[3] André Pierre Mattei[4] Márcio Cardoso Borzino[5] Marlos Mendonça Corrêa[6] Giancarlo Niedermeier Belmonte[7]

Nowadays the state-of-the art of military thought is directed to joint operations and Network Centric Warfare (NCW). The NCW has improved situational awareness at every level of the decision-making chain. In this scenario, the need to integrate the existing Decision Support Systems, which are known as stands for Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance (C4ISTAR), has arisen. This work presents an environmental monitoring application for the automatic generation of geointelligence data to track gunshot activity. So, the main purpose of these missions is the target acquisition. It is proposed the use of an Unmanned Aerial Vehicle (UAV), which gather data from a Sound Sensor Network (SSN) and process it through Mission Oriented Sensors Array (MOSA). MOSA accomplishes mission management, providing processed and ready-to-use information in real time, done in embedded data processing engines. The MOSA modeled for this application integrates information from a SSN, used for direction of arrival estimation of a gunshot in surveillance mission. The link between UAV and the Ground Control Station uses a Software Defined Radio (SDR) for communication. Then, this array is integrated with In-Flight Awareness Augmentation System (IFA2S) to improve safety during the flight. The main contributions of this paper are the concepts, models, functional architecture and a proposal of a new tactic geointelligence system composed by reconfigurable sensors.

[1] Brazilian Army Officers Improvement Academy, Rio de Janeiro, Brazil - nina.figueira@eb.mil.br
[2] Brazilian Army Technological Center, Rio de Janeiro, Brazil - bramigk.victor@eb.mil.br
[3] Digital Convergence and Mechatronics Center of Reference in Innovative, Santa Catarina, Brazil - gkc@certi.org.br
[4] SENAI Institute of Innovation for Embedded Systems, Santa Catarina, Brazil - andre.mattei@sc.senai.br
[5] Brazilian Army Technological Center, Rio de Janeiro, Brazil – borzino.angelo@eb.mil.br
[6] Brazilian Army Technological Center, Rio de Janeiro, Brazil – marlos.mc@gmail.com
[7] Brazilian Army Officers Improvement Academy, Rio de Janeiro, Brazil – belmonte.giancarlo@eb.mil.br

24th ICCRTS Paper 53 Abstract

C4ISTAR in Brazilian border security – a proposal of a Mobile Surveillance Network to integrate Brazilian Army Defense System.

Nina Machado Figueira
Brazilian Army Officers Improvement Academy
nina.figueira@eb.mil.br

Ângelo Márcio Cardoso Ribeiro Borzino Brazilian Army Technology Center
borzino.angelo@eb.mil.br

Marlos de Mendonça Corrêa Brazilian Army Technology Center
mendonca.correa@eb.mil.br

This work proposes a Mobile Surveillance Network (MSN) which aims to leverage from Network Centric Warfare (NCW) concept to improve the situational awareness. The NCW has improved situational awareness at every level of the decision-making chain. Command, Control, Communications, Computer, Information/Intelligence, Surveillance and Targeting (C4ISTAR) is shaping the Brazilian Military Doctrine and Military Systems Conception. This proposal aims to be used in forest environment, but it could be used in urban areas, if the algorithms are properly adjusted. It is proposed the use of a fleet of Unmanned Aerial Vehicles (UAV) for direction of arrival estimation of a gunshot in surveillance mission carried on urban or jungle environments. This is accomplished by adding acoustic detection capability to an UAV, which is coordinated through Mission Oriented Sensors Array (MOSA). MOSA accomplishes mission management, providing processed and ready-to-use information in real time, done in embedded data processing engines. MOSA has a central role in this system, acting distributed. This demand robust communication, which is achieved using a MANET waveform in a Software Defined Radio (SDR) for communication among the UAV.

24th ICCRTS Paper 54 Abstract

Automated information extraction to facilitate comprehension across text difficulty levels

Erin Zaroukian
US CCDC Army Research Laboratory 2800 Powder Mill Road Adelphi, MD 20783-1138

Information extraction (IE) pipelines are designed with the end goal of pointing human decision makers toward relevant information within large collections. While research often focuses on the internal computational metrics of the pipeline itself (e.g., F scores), designing the presentation of the output of the pipeline for optimal end user understanding should be a goal. Previous work addressing this goal demonstrated poorer comprehension of text for problem solving when that text was presented with markup from an existing IE pipeline versus plain text, suggesting that this IE pipeline was not well suited for extracting and presenting information to end users. A follow-up study that used markup designed to be maximally accurate and task relevant no longer showed a disadvantage for comprehension with markup, but still failed to show a meaningful advantage. Further investigation into the difficulty of the text showed that text difficultly did not seem to affect performance. Text difficulty, however, is multidimensional and hard to assess, so further testing is required to learn which elements and degrees of text difficulty (e.g., quantity, sparsity of relevant information, degree of dependence between elements) may be relevant and how specific types of markup might facilitate comprehension for different degrees and types of text difficulty.

24th ICCRTS Paper 55 Abstract

Information Sharing Patterns in Action Teams: Understanding Cognitive Interactions in Dynamic Environments

Steven J. Mullins

Naval Postgraduate School Monterey, CA 808-341-7877

sjmullin@nps.edu

The use of teams to help achieve organizational goals is a ubiquitous phenomenon in today's workplace. Teams comprise interdependent members who coordinate their work through a process of interactions to share information with each other. These interactions are fundamental to building and updating situation awareness and cognition of the team's task progress and its dynamic environment. Timely, accurate, properly shared information is critical in order to accomplish team tasks, especially in action teams who perform complex or time sensitive tasks and operate interdependently, such as aircrews, naval ship crews, special operations forces, and coast guard boarding teams.

However, a clear understanding of the interaction processes by which action team members share information remains elusive. Information sharing interactions are the foundation of cognition and contribute to team success or failure, which can be fatal in some situations. Organizations like the military depend upon action teams to accomplish tasks with high reliability. However, incidents like the shoot down of Blackhawks in Iraq (Snook, 2002), the Vincennes shoot down of the Iranian jetliner, or recent naval ship collisions suggest the need to explore the possible ramifications of a relationship between action team information sharing patterns and performance failures. Despite a robust body of research, existing analytical approaches do not fully address the nature of momentary member interactions in the context of team cognition.

24th ICCRTS Paper 56 Abstract

An initial assessment of the Endeavour Space dimensions☆

Björn J.E. Johansson, PhD*
Swedish Defence Research Agency, Department of C4ISR, Linköping, Sweden

Oscar Bjurling, Jacob Weilandt
Linköping University, Linköping, Sweden

David S. Alberts, PhD
Institute for Defence Analyses, Alexandria, VA

Mats Carlerby, PhD
Swedish Defence University, Science of Command and Control and Military Technology Division, Stockholm, Sweden

C2 agility theory postulates that no single approach to C2 is appropriate for all kinds of endeavours, and that being C2 agile implies having the ability to select the appropriate C2 approach for a certain mission or endeavour. The Endeavour Space is a central concept in C2 agility theory as it is used as the basis for determining an appropriate C2 approach for endeavours based on their location in this space. Johansson, Carlerby, and Alberts proposed the following three dimensions for the Endeavour Space: dynamics, tractability, and dependencies. This paper reports an initial attempt to assess how humans perceive these dimensions when presented with problems that are tailored to reflect different degrees of dynamics, tractability, and dependencies. A set of experiments using the ELICIT (Experimental Laboratory for Investigating Collaboration, Information-sharing and Trust) platform was conducted. ELICIT scenarios were created to represent different regions of the Endeavour Space. In addition, a prototype self-assessment instrument was designed, developed, and tested in the study, to capture how study participants experienced the Endeavour Space dimensions. Eight teams consisting of seven participants took part in the study. No significant differences in perceived complexity could be found between the scenarios. However, all Endeavour Space dimensions indicated correlational relationships with perceived difficulty, and most of them correlated with ELICIT performance.

24th ICCRTS Paper 58 Abstract

The Consistency of Visual Search Models on High Dynamic Range and Tone-Mapped Images

Andre V. Harrison
U.S. Army CCDC - Army Research Lab, FCDD-RLC-IB 2800 Powder Mill Rd, Adelphi, MD 20783
andre.v.harrison2.civ@mail.mil

Michael A. Green
U.S. Army CCDC - Army Research Lab, FCDD-RLC-IB 2800 Powder Mill Rd, Adelphi, MD 20783
michael.a.green85.ctr@mail.mil

Chou P. Hung
U.S. Army CCDC - Army Research Lab, FCDD-RLH-FC 7101 Mulberry Point Rd, Aberdeen PG, MD 21005 chou.p.hung.civ@mail.mil

Adrienne J. Raglin
U.S. Army CCDC - Army Research Lab, FCDD-RLC-IB 2800 Powder Mill Rd, Adelphi, MD 20783
adrienne.raglin2.civ@mail.mil

Tone mapping operators (TMO) are compression algorithms that compress the bit depth of high dynamic range (HDR) images in such a way that when the tone mapped version of the HDR image is shown on a low dynamic range screen, large portions of the image don't appear over/under-exposed. But the process of reducing the bit-depth of an image often alters the appearance of the image due to the loss of information and the introduction of artifacts, changing the gaze patterns when people look at those tone mapped images. Saliency-based TMOs aim to compress the bit-depth of an HDR image while trying to keep the most salient locations in the HDR image salient after tone mapping. However, these models don't ensure that the saliency model used is actually able to predict eye gaze in HDR environments accurately and assess how eye gaze is influenced by artifacts introduced into the image by the compression process. In this paper, we evaluate a suite of saliency models against 8 well-known TMOs and the original HDR image to see how well each saliency model can predict the change in eye gaze when different TMOs are applied. By doing this, we can establish a firm basis on which to develop a saliency-influenced tone mapping model to both compress HDR images and influence attention within the tone-mapped image. If TMOs can selectively choose what to emphasize or de-emphasize in a tone-mapped image based on saliency results, then saliency-based TMOs can be used to effectively direct attention even in complex environments.

24th ICCRTS Paper 61 Abstract

Modelling Multi-Domain C2 with network synchronisation: a cyber based use-case

Author: Alexander C. Kalloniatis,
Defence Science and Technology Group,
24 Scherger Drive, Canberra Airport, 2600, Australia

alex.kalloniatis@dst.defence.gov.au

Cyber operations in the Defence context will invariably be required in combinations with other military capabilities, each in their own distinct physical and information environments, creating the circumstances for Multi-Domain Operations and a need for requisite C2. In this paper I adapt a mathematical model for synchronisation of decision-making cycles on networks, a representation I have presented over several previous ICCRTS, to formulate this problem. Multiple organisations, including an operational-level joint headquarters, an air operations centre, a cyber threat analysis centre, an ICT infrastructure management organisation, and a non-government agency interact in a context where tactical air assets are deployed, humanitarian assistance is underway, and a requirement for defensive cyber operations is triggered. Each of these five organisations are modelled using caricature heterogeneous network designs, and each operates on quite different time-scales given the technical challenges they face in their separate domains. The baseline form of the model incorporates sparse links between the various organisations, and is tuned to exhibit synchronised decision-making in the absence of 'cyber disruption'. Using stochastic noise, I then represent the impact of a cyber-attack. I explore the role of added links through the presence and interactions of assistant autonomous agents in improving the capacity of the collective to achieve synchronised decision-making.

24th ICCRTS Paper 62 Abstract

Data Collection and Research in CDXs
- Command and Control, Cyber Situational Awareness and Intelligence Perspectives on Cyber Defense

Magdalena Granåsen[a], Gazmend Huskaj[c,e], Stefan Varga[b,d]

[a] FOI Swedish Defence Research Agency, SE-164 90 Stockholm, Sweden
[b] KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[c] Swedish Defence University, Box 278 05, SE-115 93, Stockholm, Sweden
[d] Swedish Armed Forces Headquarters, SE-107 85 Stockholm, Sweden
[e] University of Skövde, Box 408 05, SE-541 28, Skövde, Sweden

The annual cyber defense exercise Locked Shields is the world's largest unclassified defensive exercise. The exercise participants form "blue teams" that are tasked to defend their critical infrastructure against an attacking "red team." The blue teams are scored based on how well they keep their essential system functions running and the extent to which they manage to assess and report what they are exposed to. During Locked Shields 2019, 24 blue teams from 30 countries participated in a two-day exercise. The case study presented in this paper focuses on one of the blue teams. The team consisted of around 60 people from governmental institutions as well as private companies. The objective of this paper is to explore the possibilities to collect meaningful data for research on Command and Control, C^2, Cyber Situational Awareness, CSA, and Intelligence in conjunction with an inter-organizational cyber defense team during a cyber defense exercise. During preparations preceding the exercise, the research team observed the development of strategy, coordination structures and organization in the temporarily formed team as it prepared to solve the highly challenging exercise tasks. During the exercise, data collection included questionnaires, observations, team communication logs, reporting from the blue to the white team and performance scores. The data collection sought to satisfy needs within three research themes - 1) command and control, C^2, 2) cyber situational awareness, and 3) intelligence. A review of the dataset showed that the data is well suited for further analysis. The paper presents initial results as well as an outline of how the different types of data collected contribute to research within the three research themes.

24th ICCRTS Paper 65 Abstract

Disinformation in the Cyber Domain: Detection, Impact, and Counter-Strategies

Ritu Gill
Defence R&D Canada, Canada
Ritu.Gill@drdc-rddc.gc.ca

Judith van de Kuijt
Netherlands Organization for Applied Scientific Research TNO, Netherlands
judith.vandekuijt@tno.nl

Magnus Rosell
Swedish Defence Research Agency, Sweden
magnus.rosell@foi.se

Ronnie Johansson
Swedish Defence Research Agency, Sweden
ronnie.johansson@foi.se

The authors examined disinformation via social media and its impact on target audiences by conducting interviews with Canadian Armed Forces and Royal Netherlands Army subject matter experts. Given the pervasiveness and effectiveness of disinformation employed by adversaries, particularly during major national events such as elections, the EU-Ukraine Association Agreement, and the Malaysian Airlines Flight 17, this study assessed several aspects of disinformation including i) how target audiences are vulnerable to disinformation, ii) which activities are affected by disinformation, iii) what are the indicators of disinformation, and iv) how to foster resilience to disinformation in the military and society. Qualitative analyses of results indicated that in order to effectively counter disinformation the focus needs to be on identifying the military's core strategic narrative and reinforcing the larger narrative in all communications rather than continuously allocating valuable resources to actively refute all disinformation. Tactical messages that are disseminated should be focused on supporting the larger strategic narrative. In order to foster resilience to disinformation for target audiences, inoculation is key; inoculation can be attained through education as part of pre-deployment training for military, as well as public service announcements via traditional formats and through social media for the public, particularly during critical events such as national elections. Manually working with identified indicators of disinformation to monitor ongoing disinformation campaigns is a tedious and resource intensive task in the presence of fast flowing information in multiple social media channels. The authors discuss how such indicators can be leveraged for automated detection of disinformation.

24th ICCRTS Paper 67 Abstract

Countering Risk to Mission Through A Cyber Hardening Framework

Rosalie McQuaid[1]*, Deb Bodeau[1], Patricia Carbone[1], Anurag Dwivedi[3], Dan Fitzpatrick[1], Joanne Fitzpatrick[1], Richard Graubart[1],

Ryan Kelly[3], Alexander Ly[3], Robert Lychev[2], Jeremy Mineweaser[2] * Corresponding Author

[1] The MITRE Corporation
[2] MIT Lincoln Laboratory
[3] Johns Hopkins University Applied Physics Laboratory

We propose a cyber mission resilience framework that could enable stakeholders to evaluate and enhance the resilience of existing and future national defense weapon systems. Stakeholders can experimentally validate the framework through mission-focused analysis and experimentation. Interested partners can help refine the framework by applying it to a wide variety of missions and system

24th ICCRTS Paper 68 Abstract

Management of Deployment Stress in The Cyber Age Topic

C van't Wout
CSIR, South Africa
;CvtWout@csir.co.za

H. Pieterse
CSIR, South Africa;
Hpieterse@csir.co.za)

S.V. Ball
CSIR, South Africa;
sball@csir.co.za)

Council for Scientific and Industrial Research PO Box 395, Pretoria, 0001
info@csir.co.za

An overview of the literature on military-related stress confirms that stress remains part of the deployed soldier's life, whether it relates to concerns about his family back home, the nature of the military environment, accumulated stress, combat stress, or traumatic stress. All stress related to deployment is discussed under the umbrella term "deployment stress". Since the identification of combat-related stress more than a century ago, a debate has emerged on whether psychological debriefing should be done or not. This paper circumvents the debate on whether debriefing works or not by proposing a comprehensive process of utilising information technology to assist the deployed soldier to manage stress and to provide a tool for health care professionals and military commanders to identify psychological risks and consequently enable timeous intervention. The discussion starts by defining stress in the context of the military,

National Defence Force, with specific reference to the challenges and limitations of the current process, including a debate on whether psychological debriefing should be done or not. These challenges have underscored the need to develop alternative stress management tools for the operational environment in the cyber domain, to augment current procedures. This chapter will therefore propose a model of user requirements for the development of a psychological health protection system for operational forces where software applications (tools) can be merged on a secure internet-based platform as a stress management tool for operations to minimise the risks related to deployment stress.

24th ICCRTS Paper 69 Abstract

DEVELOPING CYBER WARFARE CAPABILITIES AS AN INTEGRAL PART OF COMMAND AND CONTROL

MR MPHAHLELA THABA
Council for Scientific and Industrial Research, South Africa
Jthaba@csir.co.za

DR JABU MTSWENI
Council for Scientific and Industrial Research, South Africa
Jmtsweni@csir.co.za

MRS MIRRIAM MOLEKOA
Council for Scientific and Industrial Research, South Africa
Mmolekoa@csir.co.za

MS AVUYA MXOLI
Council for Scientific and Industrial Research, South Africa
Amxoli@csir.co.za

The rapidly changing nature of the modern battlespace presents vast amounts of challenges to the modern Commander. Cyberspace has been identified as the fifth domain of war by North Atlantic Treaty Organisations (NATO) in addition to Land, Sea, Air and Space. The nature of this domain is such that it co-exists with all the traditional domains, and can never be isolated or treated separately from them. The speed at which the modern Commander requires to make decisions in the cyberspace is expected to evolve to multiples quicker than the decision-making cycle time in the other domains. This implies that Command and Control (C2) in its traditional sense, by form i.e. structure, and function will need to take into consideration this evolution. The fourth industrial revolution (4IR) presents a whole new dimension of challenges to the battlespace. These could either be advantageous to the Commander's ability to accomplish a mission, or could present the opposing force with an added advantage, which the Commander will have to attend to. This paper deals with the approach to developing cyber warfare capabilities, and how this should be an integral part of the overall military capability available to the Commander. It defines cyber warfare capability as a military capability, and proposes elements critical to develop this capability. The functional attributes for the cyber warfare capabilities as defined in the paper, are based on the National Institute for Standards and Technology (NIST) framework that focuses on five pillars: (1) Identify, (2) Protect, (3) Detect, (4) Respond and (5) Recover. In this framework, the aspects of Attack could be added in the Protect pillar. The paper will conclude by proposing the lifecycle through which cyber warfare capabilities should be managed. It will further recommend possible amendments to traditional C2 functions, including structures supporting the Commander for successful accomplishment of a mission.

24th ICCRTS Paper 70 Abstract

A Method to Model a Digital Network Supporting Mission Type Orders for Command and Control in a Contested Environment

Craig M. Bleile
Navy Warfare Development Command, N00S, Bldg. O-27, Norfolk, VA 23511
craig.bleile@navy.mil

With the emergence of network-centric warfare (NCW), the US Department of Defense (DOD) has made strides in moving from traditional hierarchal organizational structures to edge-based organization for warfighting. However, the command and control method is supported by link-based battle networks requiring the edge nodes to both feed and pull from the network to create a cohesive picture for shared battlespace awareness.i This has created a network that exchanges large volumes of data, very often of a redundant natureii. As the amount of data transmitted is proportional to emissions in the electromagnetic spectrum, this creates signals that may be proportionally exploited for targeting, creating risk to force. This paper proposes a method to model an edge organization using mission-type orders to understand the required information exchange requirements (IERs) in a contested environment to explore controlling that risk.

24th ICCRTS Paper 71 Abstract

Microservice API design to support C2 semantic integration

Andrew Zschorn[1]
andrew.zschorn@dst.defence.gov.au

Hing-Wah Kwok[1]
hing-wah.kwok@dst.defence.gov.au

Wolfgang Mayer[2]
wolfgang.mayer@unisa.edu.au

[1] Joint and Operations Analysis Division, Defence Science and Technology Group Australia
[2] University of South Australia, Adelaide

Operational Headquarters (HQ) need to maintain situation awareness and command and control (C2) in an increasing variety of operations. As the operational focus of HQ changes over time, so too do the information requirements of HQ staff. C2 and decision support systems need to be highly flexible to support this level of information variety. Achieving 5th Generation HQ capabilities will place higher still demands for organizational agility, which must be supported by agile information systems. We use the term agile semantic integration for the process of timely deployment of new information sources into operational HQ, such that it is amenable to human and machine reasoning, and integrated with existing HQ information sources. We propose a microservices architecture, and review technology implementation choices for information access and integration, focusing in particular on Application Programming Interface design, and the agility and maintainability of the system.

24th ICCRTS Paper 72 Abstract

Power Implications within Command and Control Organizations: New Insights through Knowledge Measurement

Dr. Mark E. Nissen
1411 Cunningham Rd, Room 2006, Naval Postgraduate School, Monterey, CA, 93943, USA.
MNissen@nps.edu.

Dr. Shelley P. Gallup
Root Hall, Room 103A, Naval Postgraduate School, Monterey, CA, 93943, USA.
spgallup@nps.edu.

Paul R. Shigley
53560 Hull St, Naval Information Warfare Center Pacific, San Diego, CA, 92152, USA.
paul.shigley@navy.mil

Robert M. Tanner
53560 Hull St, Naval Information Warfare Center Pacific, San Diego, CA, 92152, USA.
robert.m.tanner@navy.mil

The concept *military power* is very clear: One military organization seeks to impose its will upon another, relying on its chosen command and control (C2) approach to plan, conduct, coordinate and refine warfare activities. This reflects power *of* a military organization. Aside from the obvious rank structure, however, the implications of power *within* such organization are tenuous: The concept *organization power* remains ambiguous, resists quantification and continues a longstanding lack of research attention. This applies in particular to the dynamics of organization power within a chosen C2 approach, which require additional theoretic development. The research described in this article builds upon recent C2 work to develop a system for visualizing and measuring dynamic knowledge in the organization. This enables us to interrelate more closely the dynamics of C2 knowledge with organization power, focusing in particular on how power is wielded and perceived in the military organization, and to measure the effects of C2 organization power on military knowledge, action and performance. We illustrate the use and utility of this approach through a measurement example in the C2 organization context. The research makes a theoretic contribution by advancing a coherent approach to dynamic knowledge measurement and by extending our understanding of C2 organization power. As such, it is likely to stimulate considerable thinking, discussion, debate and continued research.

24th ICCRTS Paper 73 Abstract

The Dungeon Effect: The importance of biophilic design to C2 effectiveness in military environments

Irena Ali
irena.ali@dst.defence.gov.au

Keely McKinlay
keely.mckinlay@dst.defence.gov.au

Joint & Operations Analysis Division, Defence Science & Technology Group, Canberra, Australia

Current operating environments require organisations to be agile and innovative, and military organisations are no different. Recent research has highlighted how the physical environment relates to collaboration, innovation and cognitive function. In particular, 19th and 20th century trends in office design that favoured minimalist and utilitarian function have been shown to have negative and detrimental effects on the mental wellbeing of employees. In contrast, using the concept of biophilic design that emphasises human connection with nature has been shown to have productivity and wellbeing enhancing effects on those same employees. In this paper we draw on the findings of the organisational perception study conducted recently in a busy military establishment where the physical working environment emerged as a major concern. The study findings prompted further research into addressing different aspects of the physical working environment as applied to this particular setting. However, we advocate going beyond the study setting and applying principles of biophilic design in other military establishments to not only create restorative and innovative work environment but to enhance cognitive function and positively contribute to C2 in military establishments.

24th ICCRTS Paper 74 Abstract

AUTONOMOUS SYSTEMS AS INTELLIGENT TEAMMATES: SOCIAL PSYCHOLOGICAL IMPLICATIONS

Esther Kox, Msc
esther.kox@tno.nl

Prof. dr. José Kerstholt
jose.kerstholt@tno.nl

Tom Hueting, Msc
tom.hueting@tno.nl

Dr. Jonathan Barnhoorn
jonathan.barnhoorn@tno.nl

Drs. Aletta Eikelboom
aletta.eikelboom@tno.nl

TNO, PO Box 23, 3769 ZG Soesterberg, The Netherlands.

C2 processes will be increasingly affected by automation. Think, for example, of artificial intelligence that supports situation awareness or gives advice on a course of action. Insight into these effects are particularly important as automation evolves from intelligent task support towards an intelligent teammate. To enable effective human-autonomy teamwork, in addition to task-related factors, more knowledge is required on relational aspects. In general, human functioning in teams is largely affected by factors that emanate from an unconscious level. Think, for example, of assumptions regarding level of knowledge of other team members (taskwork), assessment of trust regarding commitment to the task, or assessment of social intent in communication (teamwork). This raises questions whether psychological mechanisms still operate in the same way, when human teams would be complemented by intelligent autonomous systems. Do humans apply the same rules to autonomous systems as they would to fellow humans and can these systems ever fully understand and act on the endless number of implicit social rules and underlying dynamics? We recently started a research programme to experimentally investigate these issues. We use a virtual environment resembling a first-person shooter task. In this task the participant makes decisions together with his buddy (an autonomous system) and by systematically varying various characteristics of the buddy we can investigate their impact on aspects such as acceptance of advice and trust. To date, one experiment has been conducted mainly demonstrating that the quality of the buddy's advice has a significant impact on acceptance and trust. A second experiment is currently being conducted focusing on trust repair. The main research question is to what extent trust repair will be affected by giving an apology and/or an explanation for the incorrect advice. The paper will provide an overview of relevant social-psychological factors on human automation interaction, the first results of our own research and some implications for future C2 processes.

24th ICCRTS Paper 75 Abstract

Automation of IoT based Decision Making with Uncertainty

Somiya Metu[1], Adrienne Raglin[1] Dawn A. Lott[2]

[1]Army Research Laboratory, 2800 Powder Mill Rd, Adelphi, MD, USA 20873

[2]Delaware State University, 1200 N. DuPont Highway, Dover, DE, USA 19901

There is an increased dependence on IoT devices to support teams of humans and agents in a multi- domain battle. There are numerous challenges in the reliance of data from these IoT devices. One critical challenge is the uncertainty related to the devices and data from devices. The uncertainty may significantly affect decision making that relies on this data. In this paper, we use a set of parameters to represent an uncertainty value associated with simulated IoT devices. We discuss Sentry Agents (SAGE), which is a dynamic multi-agent-based framework for system automation. SAGE is used in the construction of various scenarios for decision making involving IoT devices. These scenarios provide a platform to investigate factors that contribute to uncertainty from IoT devices and data when decision tasks are performed.

24th ICCRTS Paper 76 Abstract

The Variety Calculus – an alternative proposition for command & control in a complex world

Dr Gordon Niven* & Lt. Gen. Sir David Capewell

The Defence Science & Technology Laboratory Porton Down
Salisbury SP4 0JQ
UK

Our hypothesis is that the contemporary approach to military operations is not adequately equipped to address the complexity of the modern operating environment. Complex situations are frequently not amenable to the reductive and deterministic thinking on which much current doctrine and methodology are based. Alternative ways of thinking about operations that factor in an understanding of the origins and implications of complexity are therefore required to facilitate the development of new approaches to Command & Control.

The "Variety Calculus" offers such a way of thinking that is a synthesis of concepts originating in Cybernetics and Complexity Science. We propose that the cybernetic concept of "requisite variety" offers an approach to facilitating self-awareness and situational awareness in order to gear the structure and processes of the operating enterprise to the nature of the operating environment.

We equate "variety" with the range of underlying relationships and interactions that combine to create the emergent properties of a complex operating situation. The Law of Requisite Variety implies that this variety must be matched by the operating enterprise to achieve effective understanding and action. This can be addressed by exploiting the recursive levels of organisation that exist in complex situations at different scales of observation to inform organisation and campaign design. It has implications for how internal relationships and activities are configured and conducted and begins to reveal a coherent approach to information, decision making, and the application of all levers of influence in order to deal with complex, emergent and volatile operating environments.