International Technology Alliance
in
Distributed Analytics
& Information Sciences

Biennial Program Plan, 2020

Applicable Period: January 15th, 2020 – September 20th, 2021

Table of Contents

Introduction

DAIS-ITA (International Technology Alliance in Distributed Analytics and Information Sciences) is a collaborative partnership between the U.S. Army and the UK Ministry of Defence which brings together researchers from U.S. Army Research Laboratories (ARL) and UK Defence Science & Technology Laboratory (Dstl) to work alongside a consortium of universities and industrial research laboratories in U.S. and UK. The goal of the alliance is to foster collaborative fundamental research in both nations that will to enable secure dynamic semantically aware distributed analytics for situational understanding in coalition operations. The members of the alliance seek to break down barriers, build relationships, develop mutual understanding and work in partnership to develop technology for the U.S. and UK military.

The consortium is led by IBM, which has major research and development operations in both nations. U.S. members of the consortium are University of California at Los Angeles, University of Massachusetts at Amherst, Pennsylvania State University, Purdue University, Stanford University, Yale University and Raytheon BBN Technologies. UK members of the consortium are Cardiff University, Imperial College London, University of Southampton, University College London, Airbus Group and BAE Systems.

DAIS-ITA consists of three components: The Basic Research Component and two Technology Transition Components, one each for U.S. or UK-led efforts. The Basic Research Component provides for fundamental research, the results of which will be in the public domain. The Technology Transition Components will provide for the application of the fundamental-research results to military, security and commercial applications to foster the best technologies for future defense and security needs.

This document describes the second biennial program plan (BPP) for the DAIS-ITA Basic Research Component and provides an overview of the research work to be undertaken from January 15th, 2020 to January 20th, 2021.

The scope of basic research in the program spans two technical areas: Dynamic Secure Coalition Information Infrastructures (TA-1) and Coalition Distributed Analytics and Situational Understanding (TA-2). TA-1 will perform fundamental underpinning research for enabling distributed, dynamic, secure coalition communication/information infrastructures that support distributed analytics to derive situational understanding. Coalition operations at the tactical edge encounter severe resource constraints and rapid changes in the environment. The research in TA-1 seeks to develop techniques for dynamic, self-configuring services that build services "on-demand," taking into account changing mission needs, context and resource constraints, while seeking to protect coalition information and assets. TA-2 will explore the principles underlying distributed analytics and situational understanding, taking into account the fact that coalition operations involve complex multi-actor situations, have information with a high degree of complexity, needs to be processed in a time-sensitive manner at a high tempo, and are required to align itself with human needs and capabilities.

The outputs of the basic research component of the program will advance the state-of-the-art, develop fundamental knowledge, and provide generalizable results. This fundamental science will be manifested in scientific publications in peer reviewed conferences and journals, books covering subjects in scope of the program, as well as trained researchers. Experimental validation of the research is critical, and any experimentation software will be made available across the Alliance (ideally as open source) and may be integrated into an experimental framework to enable wide-scale experiments to validate inter-disciplinary research.

The research is split into 4 projects, comprised of 2-3 research tasks each, and with the 4 projects spanning two technical areas (TAs):

- Technical Area 1: Dynamic, Secure Coalition Information Infrastructures
  Research is needed to provide the fundamental underpinning research for enabling distributed, dynamic, secure coalition communication/information infrastructures that support distributed analytics to derive situational understanding.
- Technical Area 2: Coalition Distributed Analytics & Situational Understanding
  Multidisciplinary research is needed to provide the fundamental underpinnings for future coalition distributed analytics and situational understanding in the context of ad-hoc coalition operations at the tactical-edge.

These technical areas have associated Technical Area Leader (TAL) roles identified, with Government TALs (GTALs) from both government organizations (ARL and Dstl) as well as Industry TALs (ITALs) and Academic TALs (ATALs). These roles are shown in figure I-1.

This biennial program plan consists of four projects, each of which address issues that cut across both technical areas. From an organizational perspective, project seven and project eight address more issues in TA-1, while projects nine and project ten address more issues in TA-2. The four projects along with the project champions and task leads are shown in figure I-1.

TA1: Dynamic, Secure Coalition Information Infrastructures GTALs (Kevin Chan, John Melrose) A/I TALs (Don Towsley, Mudhakar Srivatsa)		TA2: Coalition Distributed Analytics & Situational Understanding GTALS (Gavin Pearson, Lance Kaplan) A/I TALS (Alun Preece, Dave Braines)	
P7 Policy-enabled Dynamic Infrastructure (Alessandra Russo)	P8 Federated Learning for Coalition Analytics (Shiqiang Wang)	P9 Defending coalitions in adversarial environments (Mani Srivastava)	P10 Ad-hoc Coalition Teams (Roger Whitaker)
Task 7.1: Infrastructure Design and Distributed Control for Dynamic SDC (Liang Ma)	Task 8.1: Distributed Online Learning with Multiple Learners (Mark Herbster)	Task 9.1: Interpretability of Neural Networks in Distributed & Contested Environments under Incomplete Trust (Supriyo Chakraborty)	Task 10.1: Coherence in Coalitions: understanding internal group behavior and dynamics in complex multi-domain environments (Roger Whitaker)
Task 7.2: Federated Policy Learning and Management (Elisa Bertino)	Task 8.2: Agile Analytics Enabled by Decentralized Continuous Learning in Coalitions (Shiqiang Wang)	Task 9.2: Network intelligence from negative ties (Diane Felmlee)	Task 10.2: Learning and Inferencing in Neuro-Symbolic Hybrids for Uncertainty-Aware Human-Machine Situational Understanding (Alun Preece)
	Task 8.3: Cognitive Workflows: Goal Directed Distributed Analytics Using Semantic Vector Spaces (Graham Bent)		Task 10.3: NSPL – A Neural-Symbolic Learning of Generative Policies in Coalition Environments (Alessandra Russo)
Experimentation (Dave Conway-Jones)			

Figure I-1: Summary of projects by technical area

After describing the overall research vision, this BPP document describes each of the projects in more detail.

Research Vision

Coalition operations in the future are going to be highly dynamic events, assisted in their tasks by a conglomerate of sensors, hand-held devices, UAVs, robots, vehicle-mounted machines and backend assets working as a seamless whole with the warfighters conducting the operation. We envision that all of the disparate devices in the coalition, both military-issued and personal assets of the warfighters, along with cloud-based assets when connected, can be combined into a distributed collaborative cooperative intelligent system which assists the operational goals to be achieved faster. We believe that the whole should be bigger than the sum of the parts, and this aggregate should work like a 'distributed brain' working in a coalition context. The goal of our program is to uncover the scientific principles that will let us create such a 'distributed brain' from a collection of devices and information sources. We envision the 'distributed brain' to be a system that provides a self-organizing self-healing predictive analytics capability at the coalition tactical edge, functioning as a whole even when it is isolated from the backend systems, and leveraging the backend systems as and when it finds connectivity.

From an scientific exploration perspective, creating a distributed brain requires that we know how to solve four important problems (a) How can the distributed elements of the brain manage themselves on their own in an unattended manner [autonomicity problem] (b) how can the distributed elements of the brain learn independently when disconnected while share knowledge and make decisions with each other when connected [federated decision making problem]; (c) how can the distributed brain protect itself against bad data and malicious data fed to it [robustness problem] and (d) how can the distributed brain combines human knowledge with the insights learnt from the data it sees in the environment [human-machine federation problem].

While there are other problems/algorithms whose need may be uncovered as we do our research, we want to focus on these four challenges for the immediate phase of our research.

To solve the problem of autonomicity, we propose to invent techniques that can automatically allow different elements of the brain to learn by themselves the rules and policies that allows them to protect themselves, optimize their performance, and avoid faults by observing their state and the environment around them. We assume that each element is capable of retrieving shared knowledge through a central knowledge repository (which can be visualized as a wiki-how that is the controller of the machines, allowing them to share the rules of autonomy with each other, while also providing them with a distributed command and control mechanism. This should result in an approach for federated learning of autonomy policies for distributed command and control.

To solve the problem of federated decision making, we propose an approach where different elements share their learning and decision making with each other to improve the end result. We envision each machine to create a vector representation of the data they are encountering, a vector representation of their environment, and a vector representation of the AI models they have learnt. We also envision them to create a vector representation of the collaborative decision they are making. Each element learns and creates an AI model of its own, shares the AI model with others in the system (using the vector representations), and figures out how to map their vectors to align with the vector representing the overall decision making that has to take place. What we would explore are the different types of vector representations that allow an efficient form of learning in a distributed environment.

To solve the problem of robustness, we propose to study the problem of assigning trust values to models and data received from peers and partners in a distributed environment. We would examine the behavior of the peers in the distributed node with the data they are sending or receiving, examine the amount of data leakage a partner is making through their models and use that to understand whether they are engaged in adversarial behavior. We would also look at the amount of reinforcement of the model's strength that happens as data flows among different nodes and use the positive reinforcement or negative re-enforcement in the network of model and data to understand how much trust to place in each specific node.

To solve the problem of human-machine federation, we propose to explore methods that combine human knowledge (e.g. captured in rules or other symbolic learning methods), with data learnt from distributed sources. We would create techniques that would use this combination to create new integrated models, create artificial agents running off those models, and simulate how those agents would work together with a human to solve a specific problem.

Accordingly, the immediate activities in our research program are:

- *Autonomicity Problem*:

- Infrastructure Design & Distributed Control for Dynamic Software Defined Coalitions
- Federated Policy Learning and Management

- *Federated Decision-Making Problem*:
  - Distributed Online Learning with Multiple Learners
  - Agile Analytics Enabled by Decentralized Continuous Learning in Coalitions
  - Cognitive Workflows: Goal Directed Distributed Analytics Using Semantic Vector Spaces
- *Robustness Problem:*
  - Interpretability of Neural Networks in Distributed & Contested Environments under Incomplete Trust
  - Network intelligence from negative ties
- *Federation of Human and Machine Knowledge:*
  - Learning and Inferencing in Neuro-Symbolic Hybrids for Uncertainty-Aware Human-Machine Situational Understanding Coherence in Coalitions: understanding internal group behavior and dynamics in complex multi-domain environments
  - A Neural-Symbolic Learning of Generative Policies in Coalition Environments

The remainder of this document contains the detailed description of each of the 4 projects and 10 tasks that comprise the BPP20 program.

Project 7: Policy-enabled Dynamic Infrastructure

Project Champion: Alessandra Russo, Imperial College

Email: a.russo@imperial.ac.uk **Phone: +442075948312**

Primary Research Staff	Collaborators
Liang Ma, IBM US	Paul Yu, ARL
Kin K. Leung, Imperial College	Kelvin Marcus, ARL
Leandros Tassiulas, Yale	Sastry Kompella, NRL
Elisa Bertino, Purdue	Jeremy Tucker, DSTL
Alessandra Russo, Imperial College	Gregory Cirincione, ARL
Seraphin Calo, IBM US	John Ingham, DSTL
Andreas Martens, IBM UK	Dinesh Verma, IBM US
Daniel Cunnington, IBM UK	Geeth de Mel, IBM UK
Yaniv Aspis, Imperial College	Mark Law, Imperial College
Sebastian Stein, Southampton	Amani Abu Jabal, Purdue
Konstantinos Poularakis, Yale	Jorge Lobo, Imperial College
Ankush Singla, Purdue	Miguel Rio, UCL
PhD student, Imperial College	
Joao Reis, UCL	
Fan Bi, Southampton	
Tesfay Gebrekidan, Southampton	

Project Summary/Research Issues Addressed

Coalitions require distributed, dynamic, secure coalition communication/information infrastructures that can support distributed analytics to enable situational understanding. Network infrastructures have to be resilient to failures and easily configurable to respond efficiently to changes (e.g., fragmentations) and heterogeneity of the networks, whilst respecting communication and security constraints. Self-configurable mechanisms need to dynamically manage the infrastructure and assets belonging to different parties (or enclaves) in order to respond to

changes in the mission needs, context and resource constraints. Managing different types of resources distributed across coalition infrastructure requires efficient exchanges of resource status information in various enclaves. Such status information exchange is restricted by communication and security constraints as well as network dynamicity. Adaptability is also required at the level of access to information, resources and data, and access control policy decisions need to automatically adapt to respond to changes in the context. For example, in Software Defined Coalitions (SDC) policies are needed to guarantee secure sharing of information among members of different coalition parties. Given the dynamicity of SDC infrastructures and resource constraints such policies cannot be predefined. SDCs policies need to be learned automatically in response to changes in and fragmentation of the SDC infrastructure, and resource availability. The SDC state information is a key contextual information that a policy learner has to take into account when learning information sharing policies, together with decisions for SDC control and resource management. The open research question is how to enable devices (e.g. SDCs controllers) to operate with minimal human intervention in highly dynamic infrastructures whilst maintaining a level of security to guarantee robust distributed analytics.

Whether at the level of network control or information sharing control, advanced policy management systems have to support (network) context-dependent adaptability. In SDC, such systems have to be distributed, able to learn data sharing and communication policies in a federated manner, taking into account data and existing security constraints from different enclaves in an SDC infrastructure. Because of the dynamicity of SDC infrastructures, resource management needs to adapt to respond to network changes (e.g., fragmentation of communication in the network), in order to guarantee the fulfillment of SDC network management objectives. Learning approaches, such as deep reinforcement learning, are needed to control SDC resources in an adaptive and distributed manner at a fine-grained time-scale granularity, to guarantee quick response to network changes and optimization of resources in an SDC network infrastructure. But the notion of optimization of resource management may itself depend on the specific contextual information, mission tactics, security constraints of the parties involved in an MDO. So, attribute-based policies for resource and data management are also needed to determine the best SDC resource management strategy, taking into account security constraints, state of the resources and network infrastructure, as well as tactic multi-domain operations MDO requirements. These policies can be taken into account by the distributed information-exchange decision process among controllers in an SDC infrastructure when adapting to SDC dynamicity.

In the BPP18 program, researchers have identified the inadequacy of a single control plane in terms of reliability/robustness of coalition networks. This project aims to address this problem by exploring a new architecture that allows for primary/backup control planes to respond to network fragmentation as well as delegation of control functions from controllers to nodes insides enclaves to handle dynamicity without causing significant network communication overheads and complexity. However, to be effective, decisions over network control and resource management through exchange of status information among enclaves need to be learned depending on coalition objectives and network dynamics for supporting distributed analytics. In BBP18 symbolic learning techniques have been developed which learn attribute-based policies from data, structured in a tabular form by combining machine learning methods in order to generate policies that are safe generalizations with minimal overfitting. But, in the context of SDC infrastructures for MDO, policies need to be learned in a federated manner using combination of owned data and data from other coalition parties. This project aims to address the second problem of how to learn SDC control and resource management policies that guarantee secure data communication in the context of MDO and highly dynamic network infrastructures.

This project will investigate the above problems in the following two tasks:

- *Infrastructure Design & Distributed Control for Dynamic SDC*, which will undertake research in the areas of 1) network fragmentation, 2) devolution of controllers to handle extreme network dynamics and heterogeneity, 3) distributed multi-agent reinforcement learning (RL) framework for managing SDC resources.
- *Federated Policy Learning and Management*, which will undertake research in 1) federated approach for learning both local and global policies, 2) federated policy management where composition operators for policies learned at local parties will be formalised and investigated, and finally 3) explainability of the learned policies.

Task 7.1: Infrastructure Design and Distributed Control for Dynamic SDC

Primary Research Staff	Collaborators
Liang Ma, IBM US *[Task Lead]*	Paul Yu, ARL
Kin K. Leung, Imperial College	Kelvin Marcus, ARL
Leandros Tassiulas, Yale	Sastry Kompella, NRL
Andreas Martens, IBM UK	Jeremy Tucker, DSTL
PhD student, Imperial College	Miguel Rio, UCL
Sebastian Stein, Southampton	
Konstantinos Poularakis, Yale	
Joao Reis, UCL	
Fan Bi, Southampton	
Tesfay Gebrekidan, Southampton	

Coalitions require a robust network infrastructure to support distributed analytics tasks that is easy to configure, resilient to failures, and agile to coalition policies. Software Defined Coalition (SDC) has been proposed for these requirements. Compared to traditional SDN with a single controller, SDC assets belong to different enclaves (domains), each managed by its controller; efficient status-information exchanges among controllers are required. Furthermore, SDC exhibits high dynamicity, whereas traditional SDN is relatively static. Thus, it is critical for SDC to handle dynamicity efficiently; e.g., fast response to fragmentation, controller disconnections, and new policies. Moreover, coalition network complexity is compounded by node heterogeneity and asymmetry. Efficient integration of network elements running different protocols remains an open issue. Previous DAIS ITA work[2,3,4,5] has recognized the inadequacy of a single control plane in terms of reliability/robustness for coalitions. To address these issues, we plan to investigate a new architecture that *seamlessly stitches control mechanisms together* to provide robustness and efficiency *with reduced overheads and complexity*. This effort will directly address the unsatisfactory reliability, robustness and efficiency of the current SDC control architectures for coalition forces.

Another major challenge for infrastructure robustness is how to manage resources (e.g., communications, computation and learning capability) efficiently. To this end, controllers need to exchange information about resource status in various enclaves. Unfortunately, such exchange is restricted by communication/security constraints and dynamicity. To overcome these challenges, we propose the *embedding techniques from machine learning* (e.g., skip-gram, graph neural networks, etc.) and *deep reinforcement learning* to control SDC resources in adaptively and distributed ways. To resolve the key issue of huge search space for the optimal information-exchange strategy among controllers, a promising approach is to embed network states and potential control actions into vectors such that actions yielding to similar rewards have similar vector embedding. Using these embedded vectors as input, we aim to develop a multi-agent reinforcement-learning framework for distributed information-exchange decisions among controllers. Moreover, the framework can be enhanced using *incremental learning* to adapt to SDC dynamicity. To handle network complexity, the framework can also be improved by leveraging neural networks to proactively learn the latent features that govern the coalition overall performance.

Our work is divided into two inter-dependent subtasks: (7.1.1) Network infrastructure design for dynamic SDC, and (7.1.2) Reinforcement-learning-based frameworks for distributed and adaptive SDC control.

Subtask 7.1.1: Network Infrastructure Design for Dynamic SDC

Handling Network Fragmentation by Primary/Backup Controllers:

Control plane is fragmented when controller(s) and/or control link(s) fail. Multi-control-planes can improve reliability. For example, previous work[1] examines co-existence of distributed and centralized control planes. Work in DAIS ITA[2,3,4,5] proposed reliable architectures where each node dynamically uses one of multiple control planes that are constantly updated. Unfortunately, these techniques are not developed specifically for fragmentation. Particularly, fragmentation may occur infrequently. Otherwise, one may use link-layer and hardware techniques to make the control plane reliable[6]. Therefore, to handle fragmentation, *it is not cost-effective to maintain multi-control-planes constantly updated*. In fact, our experiments demonstrate that multi-control-planes (e.g., OpenDaylight, ONOS, RYU) cause significant synchronization/signaling traffic that increase almost linearly with network size and can be prohibitively large for tactical networks[3,7]. Furthermore, links available as backup (e.g., satellite links) often have a lower data rate than regular links for the control plane. We have not adequately explored these factors.

We aim to propose *a new, efficient architecture to mitigate network fragmentation*, which has not received much attention in DAIS ITA. As in Figure P7-1, each enclave is connected to one primary and one backup controllers. Data flows between enclaves of different technologies can be supported by SDC/MANET gateways[2]. Normally, each enclave is controlled by its primary controller. Primary controllers synchronize status information with each other[8,9,10] through links with sufficient bandwidths on the primary control plane. In Figure P7-2, when fragmentation occurs, each "disconnected" enclave is switched to be controlled by its backup controller until failures are repaired. Backup controllers communicate with each other as well as with operational primary controllers. However, communication links (e.g., satellite links) connecting backup controllers may have limited bandwidth and performance.

[1] S. Vissicchio, L. Cittadini, O. Bonaventure, G.G. Xie and L. Vanbever, On the Co-Existence of Distributed and Centralized Routing Control-Planes, *IEEE Infocom*, 2015.

[2] K. Poularakis, Q. Qin, E. Nahum, M. Rio, L. Tassiulas, Bringing SDN to the Mobile Edge, *DAIS*, 2017

[3] Q. Qin, K. Poularakis, G. Iosifidis, S. Kompella, L. Tassiulas, SDN Controller Placement with Delay-Overhead Balancing in Wireless Edge Networks, *IEEE Transactions on Network and Service Management, vol. 15, no. 4, pp. 1446-1459*, 2018.

[4] G. Li, D. Duan, F. Le, K. Gokarslan and Y.R. Yang, Carbide: Highly Reliable Networks Through Real-Time Multiple Control Plane Composition, *DAIS*, 2019.

[5] K. Poularakis, Q. Qin, K.M. Marcus, K.S. Chan, K.K. Leung, L. Tassiulas, Hybrid SDN Control in Mobile Ad Hoc Networks, *DAIS*, 2019.

[6] J. Liu, Y. Shi, L. Zhao, Y. Cao, W. Sun, and N. Kato, Joint Placement of Controllers and Gateways in SDN-enabled 5G-satellite Integrated Network, in *IEEE Journal on Selected Areas in Communications, vol. 36, no. 2, pp. 221–232*, 2018

[7] Q. Qin, K. Poularakis, G. Iosifidis, L. Tassiulas, SDN Controller Placement at the Edge: Optimizing Delay and Overheads, *IEEE Infocom*, 2018.

[8] Z. Zhang, L. Ma, K.K. Leung, F. Le, S. Kompella and L. Tassiulas, How Advantageous Is It? An Analytical Study of Controller-Assisted Path Construction in Distributed SDN, *IEEE/ACM Transactions on Networking, pp 1-14, doi: 10.1109/TNET.2019.2924616, July*, 2019.

[9] Z. Zhang, L. Ma, K.K. Leung, and Franck Le, "More Is Not Always Better: An Analytical Study of Controller Synchronizations in Distributed SDN," *submitted to IEEE JSAC.*

[10] K. Poularakis, Q. Qin, L. Ma, S. Kompella, K.K. Leung, L. Tassiulas, "Learning the Optimal Synchronization Rates in Distributed SDN Control Architectures," *IEEE Infocom*, 2019.

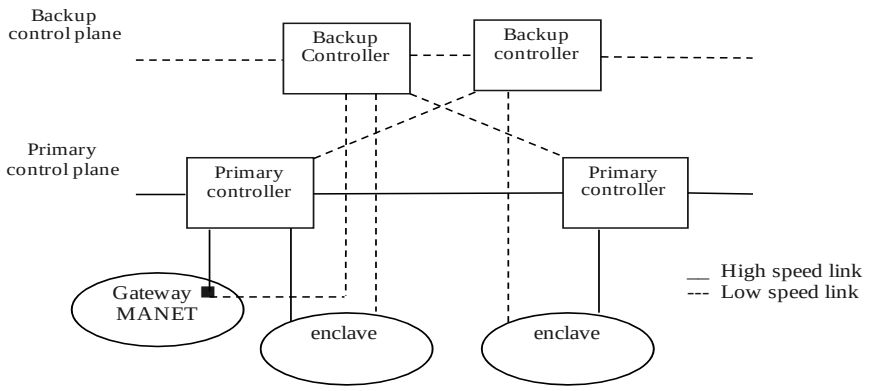


Figure P7-1: Primary/Backup Controllers for Normal Network Operations

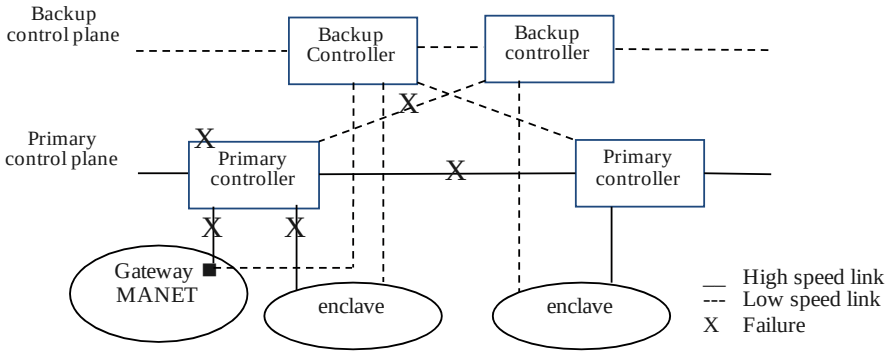


Figure P7-2: Primary/Backup Controllers for Fragmented Network

We plan to examine the following issues:

- Develop cost-efficient mechanisms for tracking enclave conditions (e.g., link quality, connectivity, node mobility, nodes under cyber threat) to determine control switching from the primary controller to the backup and vice versa. To consider scalability and correlations among node/link conditions, recent distributed learning techniques[11] will be extended to track/predict enclave conditions. This can also form the basis for "forcing" fragmentation when the predicted condition/performance is poor.
- To reduce switching time, each backup controller should have basic status information about the corresponding enclave. However, it is inefficient for the primary controller to update the backup constantly with limited bandwidth. Hence, it is important to develop fundamental understanding of when and what status information each primary controller should update the backup for good performance. The issue will be formulated as POMDP and the multi-agent reinforcement-learning framework in Subtask 7.1.2 can be applied here. If this approach remains too complex, the problem will be solved approximately by optimization techniques.

It is worth noting that with severe failures, the infrastructure may fragment into an "agglomeration" of groups of connected enclaves. In that case, each group continues to function with reduced capabilities. The aforementioned issues and solutions for the switching between the primary and backup controllers are applicable to each of these

[11] Tiffany Tuor, Shiqiang Wang, Kin K. Leung, and Bongjun Ko, "Online Collection and Forecasting of Time-Series Data in Large-Scale Distributed Systems," *IEEE ICDCS*, 2019.

enclave groups. When the fragmentation causes disappear, groups of enclaves can re-join to become a larger infrastructure.

Handling Extreme Network Dynamics and Heterogeneity through Devolution of Control:

Besides network fragmentation, other architectural issues exist. First, the primary/backup controllers cannot always react to network events as *fast* as nodes inside enclaves. For instance, it may be impossible for a controller to reroute traffic away from a failed path as quickly as the nodes located close to the source of failure. Moreover, switching to a backup controller would increase further the reaction time[2,5]. Second, frequent network events can trigger an enormous number of resource-reconfiguration requests, which can *paralyze* controller operations. Third, due to heterogeneity of network equipment, controllers can only indirectly control legacy networks by gateway nodes. This results in a degree of *uncertainty* for the outcome of controller decisions.

To address these issues, we propose to *delegate* (or "*devolve*") some of control functions from controllers to nodes inside enclaves, thus revisiting the principle of centralized control of SDC and moving towards a *hybrid architecture*[5]. Functions that require very *time-critical* or *privacy-sensitive* communication between data and control planes such as re-routing information for failed/untrusted paths or locally storing/processing confidential data are candidates for running at the nodes. Yet, less time-critical functions and functions with relaxed privacy requirements can still be performed by the controllers at a *slower timescale*. For example, controllers can periodically compute flow rules that match against suspicious packets in order to realize a firewall function. At a similarly slow timescale, controllers can configure a "network spine" consisting of communication, computing, and storage resources distributed over the network for supporting coalition services. Unlike traditional SDN, however, in our hybrid architecture, nodes with the devolved control capabilities can focus the resources of this spine to those services that are more critical. These decisions will happen at a *faster timescale*. This way, controllers are off-loaded from the task of making "micro-reconfigurations" to fully support faster timescale needs (e.g., in msec), thus enhancing SDC scalability and performance.

The faster timescale is driven, in part, by node mobility and wireless channel fluctuations. The mainstream approach to handle such dynamics is to use a *Mobile Ad-Hoc Network (MANET) protocol* (e.g., OLSR, AODV, etc.), which can provide multi-hop connectivity and allocate resources in a distributed and reconfigurable manner. However, existing MANET protocols focus primarily on communication rather than storage and computation resources and are not designed to support for tactical operations. With the back-end support of controllers in our hybrid architecture, we can overcome these limitations of existing protocols. For example, controllers can selectively announce the list of stored data items and/or suspicious nodes to other nodes. With this information passed by the controllers, nodes can make more intelligent, secure, and data-aware, resource-allocation decisions. We plan to investigate efficient mechanisms for such message passing from controllers to nodes. Techniques that tag packets at the source nodes with encoded routing-path information to affect the decisions of the distributed protocol, such as those in our preliminary work[5], will serve as a starting point of this investigation.

Subtask 7.1.2: Distributed and Adaptive SDC Control and Management

High dynamicity and heterogeneity of SDC impose paramount challenges to resource control/management. Here, we propose to employ learning approaches to proactively learn the underlying principles and adapt to network changes.

Our DAIS-ITA works[12,13,15] have shown the effectiveness of using reinforcement learning (RL) for network resource management. The key advantage of RL is that it does not require the prior knowledge of the environment's dynamics yet can still achieve an adaptive and optimal solution over time. Most existing RL work requires a central entity for collecting network states and computing the optimal information-exchange policy for (enclave) controllers. In battlefields, however, it is preferable if controllers individually decide how to exchange information for resilience and robustness. To this end, we investigate a distributed multi-agent RL framework for managing SDC resources. Depending on coalition objectives, network states can be service load level, resource utilization, etc. The high-level goal is to let each agent (e.g., controller) decide when and what information to exchange (a.k.a. actions) with other

[12] Z. Zhang, L. Ma, K. Leung, L. Tassiulas, and J. Tucker, "Q-placement: Reinforcement-Learning-Based Service Placement in Software-Defined Networks," *IEEE ICDCS*, 2018.

[13] Z. Zhang, L. Ma, K. Poularakis, K. Leung, and L. Wu "DQ Scheduler: Deep Reinforcement Learning Based Controller Synchronization in Distributed SDN," *IEEE ICC, 2019*. (**Best paper award**).

controllers under typical network constraints (e.g., amount of control messages). Such problem is extremely challenging because of exponentially many network state-action combinations and unobservable network states due to communication/protocol issues. Furthermore, SDC dynamicity may change over time, thus complicating the learning process.

We address these challenges by first leveraging the *embedding techniques* in machine learning. This is because efficient embedding can provide low-dimensional representations of network states and candidate actions, which will ease the training process. Moreover, in existing RL work, network states and actions are generally represented by integers or "1-hot" vectors, which cannot capture the intrinsic relations among them. We therefore target to embed each state s and its available actions $\{a_1,a_2,\ldots,a_n\}$ into vectors such that $\|s \oplus a_1\| \approx \|s \oplus a_2\|$ if two actions a_1 and a_2 produce similar reward w.r.t. state s, where $\oplus$ is an operator[14] indicating how s and a_i are related and the norm operation $\|.\|$ is used to evaluate the goodness of a particular action. We plan to employ neural networks to train the relations between states and actions using their corresponding rewards and output the hidden-layer weights as the state/action vector embedding (i.e., as in skip-grams[15] [16] for word/node embedding). Consequently, given a state s, we can reduce the search space for the best actions revealed by the vector representations.

Based on these vector representations, we next develop an efficient multi-agent RL framework. For dynamic SDC, the current states may be unobservable, thus yielding a POMDP problem. For POMDP problems, traditional approaches leverage statistical approaches to compute the belief vectors under Markovian assumptions, which, however, may not be valid for SDC. Therefore, we propose to employ LSTM (long-short term memory) to predict the current network states using past data. Our initial results demonstrate high prediction accuracy of the LSTM-based approach even if the dynamic environment is completely unknown. In this way, the unobservable state problem is converted into a "predictable" state problem, thus easing the learning process for each agent. In addition, we also target on theoretical analysis, aiming to obtain a deep, fundamental understanding as to under what conditions the distributed framework approaches the centralized solution (i.e., only one agent). With such insight, we study how to improve the RL performance when these conditions are not satisfied. Furthermore, training time is crucial for dynamic SDC. To reduce training time, we have built MACS (Multi-Armed Cooperative Synchronization)[17] for a centralized single-agent RL problem. In MACS, each arm is used to compute the value function for the associated action dimension; then the final optimal action is obtained by merging the suggested sub-actions from each arm. For multi-agent RL in dynamic SDC, we propose to extend MACS to tackle distributed problems for military networks.

Additionally, network dynamicity changes over time, for which we plan to use *incremental learning* to enhance our multi-agent RL framework. Specifically, using the newly available data, we continuously train the framework so that it adapts to new data, while retaining the existing knowledge. This capability can help us handle time-varying dynamicity without re-training the model for dynamic SDC.

The above RL framework using vector representations and deep neural networks is also critical to Task 7.2 for federated policy learning and management, due to the generality of the proposed research method for proper state/action representation and multi-agent learning. In addition, as Task 7.1 provides a substrate for efficient policy learning in Task 7.2, we also plan to investigate joint reinforcement learning between Task 7.1 and Task 7.2 to improve the overall performance of the learning framework.

Task 7.2: Federated Policy Learning and Management

Primary Research Staff	Collaborators

[14] One canonical embodiment of $\oplus$ is the vector element-wise sum. We investigate how different operators affect the performance of the reinforcement-learning framework.

[15] S. Rallapalli, L. Ma, M. Srivatsa, A. Swami, H. Kwon, G. Bent, and C. Simpkin, SENSE: Semantically Enhanced Node Sequence Embedding, *submitted to CIKM, 2019.*

[16] [BigData19]

[17] Z. Zhang, L. Ma, K. Poularakis, K. Leung, J. Tucker, and A. Swami, "MACS: Deep Reinforcement Learning based SDN Controller Synchronization Policy Design," *IEEE ICNP, 2019*.

Elisa Bertino, Purdue *[Task Lead]*	Gregory Cirincione, ARL
Ankush Singla, Purdue	John Ingham, Dstl
Alessandra Russo, Imperial College	Dinesh Verma, IBM US
Yaniv Aspis, Imperial College	Geeth de Mel, IBM UK
Seraphin Calo, IBM US	Mark Law, Imperial College
Daniel Cunnington, IBM UK	Jorge Lobo, Imperial College
	Amani Abu Jabal, Purdue

Software Defined Coalitions (SDC) are complex systems, especially when they are dynamic and obtained by the dynamic compositions of resources belonging to different coalition parties. Their deployment in distributed, evolving and fragmented environments increases their management complexity because of security and resource sharing constraints. It is thus critical that their configuration and management be driven by proper policies.

In the context of SDC an important approach for representing and managing policies is represented by attribute-based (AB) policy-based management models and systems (AB-PBMSs). In an AB policy model, policy rules are expressed as conditions against domain-meaningful properties of coalition parties, resources, actions, and environments. This approach simplifies policy administration as policy decisions and recommendations automatically adapt between different contexts based on changes of attribute values. Such a capability is critical to enhance the efficiency in configuring and managing SDC.

For example, decisions concerning the switching between primary and backup controllers can be based on a policy that includes rules with conditions on the security status of the controllers. At run-time the policy automatically suggests the proper switching based on the dynamic evaluation of the security status attribute of the involved controllers.

More in general such an approach is critical to enhance autonomy of coalition parties in the era of multi-domain operation (MDO)[18] involving coalitions. In coalition MDO, coalition parties operating in land, air, sea, cyber will come together to achieve collective goals by sharing multiple viewpoints about emerging situations. Since coalition MDO contains multiple parties and types of resources, approaches to simplify policy specifications and a systematic approach to autonomously adapt policies according to context will be critical.

As part of the BPP18 we have developed the Polisma framework for learning attribute-based policies. Polisma *generates symbolic rules that can be directly enforced by policy enforcement engines (e.g., firewalls, software defined networks), while at the same time providing the ability to use a variety of ML algorithms*. In Polisma (see Figure P7-3) a data mining technique is first used to infer associations between parties and resources in the set of decision examples, such as decisions on resource sharing, and based on these associations a set of rules is generated. In the second step, each constructed rule is generalized based on statistically significant attributes and context information. In the third step, policy domains are analyzed to augment the rules with restrictions as for some application domains (e.g. security) generalization can have undesired consequences. Policies learned by those stages are safe generalizations with minimal overfitting. To improve the completeness of the learned set, Polisma applies a ML classifier to decision examples not covered by the learned rules; it uses the classification result to generate additional

[18] https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

rules in an "ad-hoc" manner. Evaluations on AB information sharing decision datasets, including a real-world dataset[19], show that Polisma is highly accurate[20] and outperforms approaches based only on statistical ML.

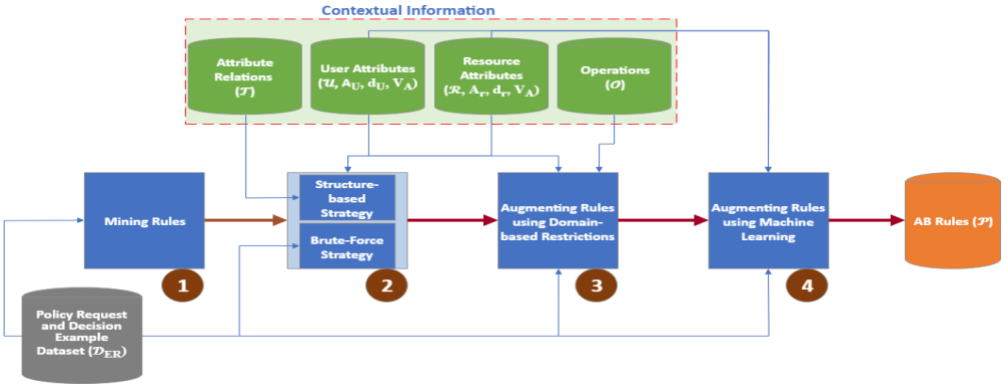


Figure P7-3: The Polisma Framework

However, a limitation of Polisma is that it learns policies of interest to a single party and uses only the data of this party. In coalitions, parties can each have their own datasets and combining these datasets can enhance the learning outcomes. In some cases, coalition members may only share their own local policies but not the data they used to locally learn the policies. As an example, U.S. and UK may have both used their data to determine sharing policies for their resources to be used for an untrusted partner like Kish. In practice, a combination of those cases (i.e., sharing datasets, sharing policies) may occur. *A federated approach is thus required for learning policies from a broad variety of data and knowledge, including raw data, policies expressed as symbolic rules, and ML models*. In what follows we use the term data with such a broader meaning. A challenge is that each party may be willing to only share subsets of their data and/or anonymized versions of their data or even only synthetically generated data. It is therefore critical to develop an AB policy learning framework able to learn from datasets that may be anonymized, or synthetically generated, or missing certain features, while at the same time assuring that each party is able to generate accurate policies.

A second limitation of Polisma is that only learns propositional rules (i.e., broadly speaking, rules with no variables). The reason is that such type of rules is suitable for policy enforcement engines. However, propositional rules are only applicable to specific cases and in a coalition setting where contexts are dynamic, high-level properties about the data would allow enforceability of existing policies to new contexts satisfying such properties. Consequently, less propositional policies will be needed to capture the same semantic AB properties. Furthermore, in coalition settings, parties may need to integrate policies with sophisticated reasoners, including causality reasoners, and AI or ML systems. A higher-level representation of policy's conditions would make such integration more feasible. *It is thus critical to learn policies expressed at higher-level logics.*

A third limitation is that Polisma does not support the federated management of policies, by which parties can integrate their own policies to manage shared resources according to mutually agreed criteria. For example, a resource controlled by two different parties can only be accessed by a third party provided that the latter satisfies the policies of both controlling parties. Other policy integration criteria are possible, such as that a policy takes precedence over another in case of conflicts between two policies. *It is thus critical to combine policies, local to each party, according to various criteria*.

Finally, a fourth limitation is that Polisma does not support policy explainability by which humans can understand why certain policies are generated and not others. Such mechanisms are crucial when policies are generated using multiple techniques. *It is thus critical to provide mechanisms for policy generation explanation.*

[19] http://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples

[20] A. A. Jabal, E. Bertino, J. Lobo, M. Law, A. Russo, D. Calo, and D. Verma. Polisma –a Framework for Learning Attribute-based Access Control Policies. *Submitted for Publication* (available from CENSE).

The goals of this task are thus to define approaches to address those shortcomings and to integrate them into a distributed intelligent approach for federated attribute-based policy learning and management.

A major challenge in an AB policy approach is the specification of the AB policies representing the key input for policy enforcement. Since in coalitions we may typically deal with local contexts and situations, the needed detailed knowledge may be lacking. Addressing this challenge requires a distributed intelligence approach to policy learning able to: (i) combine information available at coalition parties about resources to be shared in the SDC (e.g. resource directories, organizational charts, logs, historical data, and local existing policies), controllers, and enclaves; and (ii) use machine learning (ML) to infer AB policies from these combined data.

This task aims to design a distributed intelligent infrastructure for learning and managing coalition AB policies based on data. At a high level our approach consists of two key elements: (a) the use of a federated learning approach by which data and models from different parties in a coalition are combined to enhance the accuracy of the policy learning process; (b) a flexible pipeline able to combine different machine learning (ML) and data mining techniques, and other data analysis techniques.

Our research is organized according to four following subtasks:

Subtask 7.2.1: Federated Policy Learning

The main research issue is that while combining multiple datasets can enhance the policy learning outcome, each dataset may not be very accurate, and this may negatively impact the overall policy learning outcome. It may be that a party can obtain a better policy learning outcome by just using its own local data, which however may be of limited size. Therefore, the question is whether it is better to learn policies by using a larger dataset, which may not be accurate, and miss relevant information, or using a small but accurate dataset. A possible solution to such question is to use a two-layer policy learner (Figure P7-4):

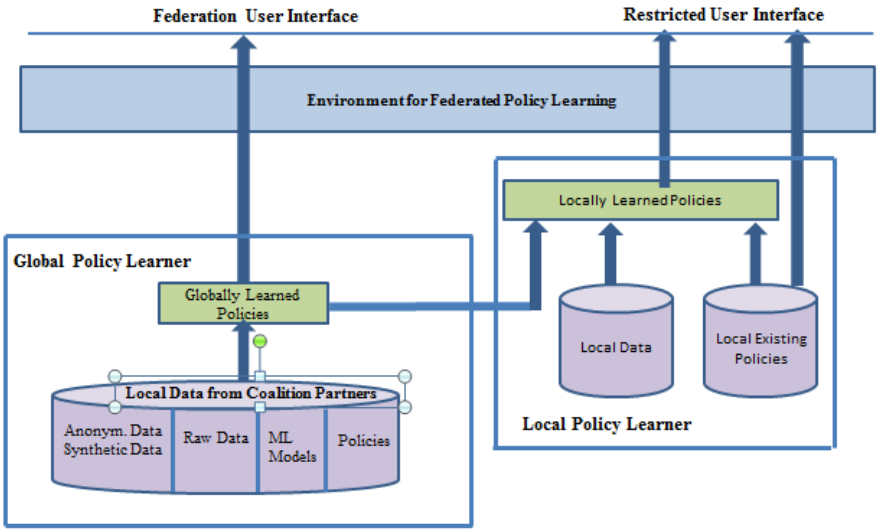


Figure P7-4: The Two-Layer Policy Learner

1) *A global policy learner based on the datasets obtained from different parties*. At this level the learning may be more coarse-grained and not accurate. For this learner, we will consider data anonymized according to various strategies, e.g. k-anonymity, and local differential privacy[21]. In the latter the data provider does not need to trust the data curator with respect to the privacy of its data. We will also consider the cases in which portions of the input data are suppressed either horizontally (i.e., records are suppressed from the party dataset) and/or vertically (i.e., columns are suppressed) and synthetic data are provided. For example, consider an example of historical information on an enclave in a coalition that is provided by a coalition party to other parties in order to allow

[21] Ú.Erlingsson, V. Pihur, A. Korolova. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response. ACM Conference on Computer and Communications Security 2014: 1054-1067

controllers track/predict enclave conditions. An example of vertical suppression is when the field indicating the reconnaissance missions supported by the enclave is removed from all records in the dataset. An example of horizontal suppression is when all records concerning an enclave used in a top-secret mission are removed, where the other records concerning enclaves not used in top secret missions are provided. We will also consider the case in which a party only provides the parameters of a model learned on its own local data. Different approaches need to be combined depending on the specific machine learning algorithm to be used and the type of available datasets. For example, when actual data values are replaced by range values (e.g., value 18 is replaced by interval [10-20]) in k-anonymization, one needs techniques for computing distances between ranges, as distances are required by several ML algorithms. Or one can treat k-anonymized data as uncertain data and provide statistics about the released data, such as the first two moments of the generalized record fields. Ensemble ML techniques can also be used, especially when the input includes both ML models and actual datasets. We will investigate the optimal set of techniques to be used and according to which order. Research issues include the definition of quality metrics for the global policies and anonymization techniques for policies, and how to perform policy learning when some input consists of actual data (possibly anonymized) and/or model, and some input consists of policy rules.

2) *A local policy learner based on the local dataset and the policies obtained from the global learner*. Unlike the global policy learner, the local policy learner has available less data but the data is more precise. It also has available the globally generated policies, although these may be less accurate. The main challenge is how to locally refine the globally generated policies by using the locally more precise and complete data. Another issue is dealing with "conflicts" between the global policies and the local ones. Whether such conflicts arise depends on the local datasets sent to the global learner. For example, suppressing data from a dataset before sending the data to the global learner may bias the data. The proposed approach is based on analyzing the quality of the globally learned policies with respect to the local set of policy decisions and evolving the global policies accordingly. We will extend the ProFact approach[22], developed in the BPP2018, to support such analysis and evolution. We will investigate strategies for conflict resolution based on the "policy need" of each party; for example: (a) a party may be interested in assessing whether its own local policy is correct and in such case when the local policy conflicts with the global policy this indicates that the local policy may need to be revised; or (b) in learning policies for situations it has not yet encountered and in such case the party may adopt the global policy for the situations not covered by its local policy.

Subtask 7.2.2: Learning Policies Expressed in High-Order Logics

We will investigate two approaches and experimentally compare them. (a) The first approach is to replace association rule mining with an inductive learner, e.g. ASG[23] and FastLAS[24] developed in the BPP18. FastLAS, in particular, has been designed to be scalable and to support the selection of the solutions to inductive learning tasks by using application-dependent score functions. The first approach may require modifying the subsequent steps in Polisma (e.g. the step focusing on achieving safe generalization). Depending on the learner used, different approaches may be adopted; for example one could use FastLAS with (AB) specific scoring functions to assign weights to rules in the solution space so that the learning process is guided with the intention of choosing rules that minimize/maximize the score of a solution based on these weights. If FastLAS is used, the second step in the Polisma pipeline would not be required. (b) The second approach is to add a fifth step that applies an inductive learner, i.e., FastLAS, to the policies generated by Polisma. In this case minimal generalizations could be learned that guarantee covering the given propositional policies. Also, in this case domain-specific scoring functions are used to choose among multiple minimal generalizations.

Subtask 7.2.3: Federated Policy Management

The two-layer learner supports an essential function: allowing a party to generate/refine its own policies based on coalition distributed intelligence. As a result, a party may be better equipped when dealing with new situations, events, and contexts. However, in coalitions, most tasks have to be carried out in collaboration. Therefore, we also need

[22] A.A.Jabal et al. ProFact: A Provenance-based Analytics Framework for Access Control Policies, IEEE Transactions on Service Computing, https://ieeexplore.ieee.org/document/8645805

[23] M. Law, A. Russo, E. Bertino, K. Broda, J. Lobo. Representing and Learning Grammars in Answer Set Programming. AAAI 2019: 2919-2928

[24] M. Law, A. Russo, E. Bertino, K. Broda, J. Lobo. FastLAS: Scalable Inductive Logic Programming Incorporating Domain-Specific Optimisation Criteria. Submitted for publication, 2019.

mechanisms by which parties can combine their own local policies (either directly defined by each such party or generated by the two-layer learning process). The mechanism we plan to investigate is based on the definition of a set of algebraic operators for policy compositions; examples of such operators include intersection, union, negation, domain projection. The latter takes a policy and restricts it to be used only for a set of requests (usually a subset of the requests for which the policy was initially specified). Those operators will typically have the closure property and thus can be combined into policy combination (PC) expressions that will be formally defined and for which algebraic properties will be studied. Additional derived operators will be defined such as the precedence operators that given two policies establishes which is the decision/recommendation of one policy has precedence over the other. By using such operators one can provide expressions to deal with conflicts. A semantics will also be defined on the view that a policy can be considered as a function mapping each policy request to a value in the set of possible policy decisions/recommendations.

To deal with conflicts it is important that the elements in such a set be adequately described through an ontology, indicating for example sub-sumption relationships, conflict relationships, and complementarity relationships. We will identify all required relationships and create a simple ontological system by which these decisions/recommendations can be entered into the policy federated management system to be then used in the specification and analysis of PC expressions. For example, consider an example of information sharing decision concerning the sharing of a resource of type *T*, owned by UK, with partner Kish and suppose that there is policy P1 specifying that resources of type *T* can be shared with Kisch; the policy could be expressed as "Resource Type = *T* and Requestor = Kisch, then Share", where Share is the decision recommended by the policy of UK. On the other hand, suppose that U.S. has the policy "Resource Type = T and Requestor =Kisch, then NotShare" where "NotShare" is the decision recommended by US. Now suppose that UK and US have a shared resource of type T, then it is clear that the two policies conflict. However for an automated system to determine that "Share" and "NotShare" are conflicting policy recommendation, one would need to indicate in an ontology, where each node represents a decision, that nodes "Share" and "NotShare" are related by the conflict relationship, and indicate the corresponding conflict resolution, for example that "NotShare" prevails over "Share". Also, the prevalence relationship can be represented in the ontology. Then based on this information, the policy management system can automatically generate the appropriate PC expressions that comply with the conflict resolution indicated in the ontology. As another example, assume that UK has the policy that each primary controller in an SDC must be backed up by two secondary controllers hosted on different servers, whereas US has the policy that each primary controller in an SDC must be backed up by only one secondary controller. Suppose now that UK and US have a controller to be used for a joint mission and thus, they have to agree on a backup policy. In this case the former policy (i.e., backing up on two controllers) "subsumes" the latter (i.e., backing up on one controller). Even though this is not strictly a conflict, it is critical to decide the policy to use. In this case, one can specify that these two policies have a sub-sumption relationship and that the policy to be adopted is the one that subsumes the other and thus the joint policy would be to back up the primary controller on two secondary ones. In addition, as part of this activity we will investigate policy adaptation to different contexts by developing a notion of "policy transferability" and leveraging our past work in BBP18 on learning Answer Set Grammars.

Subtask 7.2.4: Explainability of Policy Learning

Providing explanations about which policies are learned by a system like Polisma is a challenging task because policies are learned according to several steps and using different data. Also, explanations may take different forms, depending on the user preferences. We will explore two complementary mechanisms. The first mechanism is the *policy provenance* which, like a data provenance mechanism, keeps track of all relevant information concerning the lifecycle of a given policy. The provenance information for a policy may include: training datasets from which the policy was learned, context information used for generalizing the policy, learning algorithms used in the policy learning process and all relevant parameters for these algorithms, human actions executed on the policy (e.g., manually removing/adding rules to the policy). The second mechanism is a query mechanism supporting different types of explanation based on the information acquired by the policy provenance mechanism. One interesting type of explanation is based on the counterfactual explanation[25] that has been suggested in different contexts, such as for example to support the "right to explanation" in the General Data Protection Regulation (GDPR) of the EU. An example of a counterfactual explanation is the statement "You were denied a loan because your annual income was $40,000. If your income had been $45,000, you would have been offered a loan". As counter-factual explanations are considered to be quite effective in communicating with human users, these approaches are being investigated in

[25] S. Wachter, B. Mittelstadt, and C. Russell. Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harward Journal of Law & Technology, vol. 31, no. 2, Feb. 2018.

different domain (see[26] for examples). We will explore such an approach and combine it with other approaches for explanation of AI systems[27].

Validation and Experimentation

With the renewed focus on Multi-Domain Operations (MDO) this research has become highly relevant, the algorithms created in this project will aid multiple domains and coalition partners to interoperate in more seamless manner with heterogeneous infrastructure and support distributed analytics whilst respecting communication and security constraints. The proposed methods in both tasks will make use of learning approaches. These techniques will need to be validated to demonstrate the accuracy of their predictions in different SDC scenarios.

In Task 7.1, we will validate the proposed ML approaches by using multiple, similar "vignettes", some of which will be used for training and some for testing. The scenarios will include SDC networks in tactical environments that make used of both network and mobile connections. An example of such scenario will be the Anglova scenario. For demonstration purposes we will use containers to allow algorithms to run on a more lightweight platform such as our testbed of wirelessly-interconnected mobile handheld devices (Android) empowered with SDN control functions we have developed and experimented with in our previous DAIS works[3,5,7]. Commercial exploitation of our testbed will be explored to enable an efficient and highly manageable mobile network infrastructure for dynamic sharing of infrastructure resources among semi-autonomous mobile devices and efficient service delivery.

We will also develop example data to traverse the emulated network. This data may vary according to the vignettes used:

1. Troop deployment – Situational awareness and chat
2. "Kinetic" – Situational awareness and PTT/ROIP
3. Medical Training + medical procedure – Significant data transfers over backhaul that have low priority in training, but high priority when performed for real.
4. "down-time" – Sharepoint traffic, VOIP traffic, and others.

We plan to use these data first in smaller network simulation, e.g., mininet, for quicker validation and then use them on a full-scale validation using EMANE.

Validation of the system needs to compare new capabilities against what's already available:

1. Basic network reachability end-to-end against:
   a. MANET routing, e.g., OLSR
   b. Current SDN, e.g., ONOS, ODL, or Ryu
   c. Theoretical maximum assuming perfect knowledge and instant convergence
2. Resource availability to end nodes against:
   1. Theoretical maximum
   2. Bandwidth consumed

We will also conduct experiments using the scenarios and data considered by the distributed analytic Tasks 8.2 and 8.3 in project 8.

In Task 7.2, our approach to policy generation is also data-driven we will carry out a variety of experiments to validate the accuracy and effectiveness of our approach. These experiments will be conducted on real-world data (e.g. the Amazon datasets, and other publicly available datasets) and data from Task 7.1. Based on the policies relevant for dynamic SDC and data from Task 7.1, we will assess whether our policy learning approaches is able learn the correct policies. We will also, based on scenarios from Task 7.1, determine score functions to be used by FastLAS in order to learn policies that correctly take into account SDC requirements, and investigate our policy adaptation techniques to different contexts.

[26] A. Dhurandhar, P.-Y. Chen, R. Luss, C.-C. Tu, P.-S. Ting, K. Shanmugam, and P. Das. Explanations based on the missing: Towards contrastive explanations with pertinent negatives. NeurIPS 2018.

[27] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi. A survey of methods for explaining black box models. ACM Computing Survey, 2018.

We will evaluate our approaches for learning and managing policies under different metrics, including accuracy, completeness, and robustness in adapting to context changes and will measure their efficiency in terms of computational time. We also evaluate the approaches with respect to usability from the human user point of view. Such evaluation will allow us to determine the type and amount input required from human users and to assess the effectiveness of the policy generation explanations. We will develop a simulation testbed consisting of different agents to showcase to analyze our algorithms with coalitions of different scales. Finally, we will develop scenarios based on the military vignettes, developed at the beginning of the current BPP, and use them in the simulations.

Military and DAIS ITA Relevance

With the renewed focus on Multi-Domain Operations (MDO) this research has become highly relevant. The algorithms created in this project will aid multiple domains and coalition partners to interoperate in a more seamless manner with heterogeneous infrastructure and learn coalition policies using data available at coalition partners.

The relevance of this work is further reinforced by the work done within the NATO FMN (Federated Mission Networking) by the ACT (Allied Command Transformation) in the in following two focus areas of the TIDE (Think-Tank for Information, Decision and Execution Superiority) program:

1. Protected Core Networking: This Focus Area aims at creating a standard network interoperability layer between coalitions, mainly at the Deployed layer. At the moment it is focused on networking only, but the work here can influence future "spirals" to allow for better coalition interoperability both at a fine-grained level of control of the network infrastructure and at a more coarse-grained level of coalition distributed intelligence.
2. Tactical Edge: This Focus Area is aimed at creating a method of interworking at the highly mobile tactical edge where PCN is too heavyweight. The importance here is to allow for a distributed control between coalition partners where a coalition enclave might fragment and be linked by another coalition partner whilst still ensuring secure communications.

The proposed federated policy learning and management framework will also address the MDO coalition needs for dynamically generating coalition policies that ensure secure resource sharing in coalition distributed intelligence. We address this challenge by automatically learning coalition policies in a highly dynamic network infrastructure, using the data available at the coalition partners, whilst ensuring accuracy of the policy learning outcome. The learned policies can then be used to guide coalition tactical decisions. Correct and complete policies are therefore critical for enhancing multi-domain coalition operations when policies need to be generated in a highly dynamic environment with many parties. The proposed federated policy management approach will address this challenge and will enhance autonomous management of coalition infrastructures, thus reducing cognitive load on warfighters in the tactical edge.

The planned demonstration will show the functionalities created from this project at the level of control and management of MDO network infrastructures and learned network infrastructure policies in response to dynamic changes. This demo can be demonstrated at NATO CWIX (Coalition Warrior Interoperability eXploration / eXperimentation / eXamination / eXercise), as previous ITA work has been demonstrated at past CWIX events under transition contracts. Results may also have potential impact into the NATO STO IST-161 which is looking at the Group and Information Centric communications at the Tactical Edge.

Scientific risk of our proposed federated policy learning method is the scalability. Although effective in generating policies that are human-interpretable, the symbolic learners may, in their current form, not be applicable to very large datasets. This risk will be mitigated by (i) using where possible association rule learning algorithms – widely used in many applications – to increase scalability at the cost of generality of the policies learned, and (ii) focusing on learning more coarse-grained types of policies that complement fine-grained policies for network infrastructure management and control generated by multi-agent reinforcement learning methods.

We envisage several potential transitions both within and outside DAIS. Developing a federated policy learning and management capability enables additional transition opportunities that could support future coalition operations. For example, within the Human Machine Teaming (HMT) scenario, future coalition forces will be required to operate in a mixed-autonomy environment where different entities (human or machine) must collaborate effectively. Developing a federated policy learner that is both distributed and capable of expressing learned policy models in human readable language will enable rapid integration of mixed-autonomy systems. This will also apply to Multi Domain Operations (MDO) where systems containing different policy sets must interact.

Also, during operations such as logistical resupply or person of interest tracking, the coalition may be required to integrate with external sensors and networks, such as a local CCTV camera network that have privacy restrictions. A federated policy learning system would not only enable rapid integration but would also ensure privacy over the raw data as this can remain at the edge of the network.

Collaborations, Staff Roles, and Linkages

We plan to conduct collaborative work between Tasks 7.1 and 7.2, in particular on the use of the federated policy learning for learning course-grained (AB) policies on data communication within the context of SDC while fine-grained mechanisms for control and resource management decisions are learned through the proposed multi-agent reinforcement learning. As indicated in the milestones table, this collaborative work will be demonstrated through a joint demo in Q6 of the project with the objective to show the effectiveness and complementarity of the two learning frameworks.

In terms of intra-Alliance collaboration, Task 7.1 is highly related to Task 8.2. We shall explore synergies between resource management using reinforcement-learning techniques, propose in Task 7.1, and algorithmic approaches for dynamic resource allocation that will be developed in Task 8.2. The new properties of continuous learning techniques investigated in this latter task will also shed helpful insights in the way in which we can allow incremental learning in our multi-agent methods.

As we plan also to develop a framework for federated learning of policies that will integrate different forms of symbolic and statistical machine learning, the work in Task 7.2 of this project will be highly related to Task 10.3 in project P10. The seamless combination of neural and symbolic machine learning developed in this latter task will constitute a valuable component in our proposed federated learning framework, in particular when policies for coalition tasks need to be learned from (MDO) data that are not tabular. The federated nature of the framework developed in Task 7.2 of this project will also shed insights on how to develop federated neural-symbolic learning algorithms in Task 10.3 of P10.

Staff Roles

Project P7 has a total of 6 PhD students, 4 allocated to Task 7.1 and 2 to Task 7.2. Of the 4 PhD students allocated to Task 1, 3 are carried forwarded by the previous BBP18 program.

- Fan Bi will be focusing, in Task 7.1, on extending initial work on combining reinforcement learning with mechanism design[28] to the SDC setting by replacing the current reinforcement learning method with linear function approximation with the new deep reinforcement learning techniques developed in Task 7.1. He will also focus on extending initial work on applying mechanism design to coalition setting[29] to the context of SDC in order to incentivise truthful reporting of importance of resources. To make our approach suitable for SDCs we will address its scalability by developing novel polynomial-time algorithms that still preserve the incentive properties.
- Tesfay Gebrekidan will also contribute to the work in Task 7.1, by looking at techniques for detecting and dealing with concept drift and catastrophic changes in the environment (this may occur, for example, as resources are added or removed from the system, as the network becomes fragmented or as entirely new enclaves become available). In these cases, a controller may need to discard some of its existing knowledge and either learn from scratch or employ transfer learning techniques to quickly find new effective policies based on prior knowledge. One technique we will explore will be to store a collection of past policies and quickly select and adapt these based on the current network conditions. Dealing with such dynamism is particularly challenging in the multi-agent setting we consider here, where many agents may simultaneously need to re-learn their policies when catastrophic changes occur.
- Joao Reis will be working, in collaboration with Dr Sebastian Sein, on data-driven neural routing in tactical environments, control plane decisions of an SDC will be determined using a deep neural network approach rather than traditional SDN synchronisation techniques. In a more service-oriented approach to networking

[28] S. Stein, I.A. Moisoiu, M. Ochal, E. Gerding, R. Ganti, T. He, T. La Porta, Strategyproof Reinforcement Learning for Online Resource Allocation. Submitted to AAAI 2020 (currently under review).

[29] F. Bi, S. Stein, E. Gerding, N. Jennings, T. and La Porta, A truthful online mechanism for resource allocation in fog computing. PRICAI 2019: Trends in Artificial Intelligence (pp. 363-376).

simple algorithms such as minimizing statically defined weights to find the shortest network path, are no longer appropriate. Determine optimal routing by using optimization approaches based on multiple metrics is an NP hard for which classical optimization methods would take a long time to converge even for small-scale scenarios. A two-fold solution will be developed: (i) use of a machine learning (ML) approach to mimic optimal, multi-objective routing, without needing explicit human-engineered heuristic-based algorithms, and (ii) use reinforcement learning (RL) to continuously tune the algorithm's model to meet the objectives of maximizing utility within coalition-partner-defined constraints. The second aspect will also relate to the multi-agent reinforcement learning approach developed in Task 7.1 but with focus on routings decisions rather than resource allocation.

We will seek to ensure that our students will continue working closely together across the two tasks and with students on other BPP projects as part of the student cohort. They will participate in periodical conference calls and have mutual visits to ensure steady progress of our research. They will be encouraged to spend time at the different partner institutions during the project and we will investigate opportunities for students to spend time at the IBM Research facilities in both UK and USA.

During the project, we will identify opportunities for collaborative work between team members which will expand on the work described in each respective tasks and leverage upon each other's expertise. Specifically:

- Dr Liang Ma will lead the research activity in Task 7.1, focusing in particular on developing efficient algorithms and frameworks with other team members for the distributed and adaptive SDC control and management using deep neural network and reinforcement learning approaches (subtask 7.1.2). He will also work with the government collaborators on the associated experimentation and transition opportunities.
- Prof. Kin K. Leung and his team will focus on the development of new SDC architecture and control algorithms to handle network fragmentation (Subtask 7.1.1). His team will also participate in the investigation of multi-agent learning techniques for resource management in SDC (Subtask 7.1.2). These two aspects of work will be performed jointly among Imperial College, IBM US and Yale. Kin will work with DSTL and UK industrial partners, including IBM UK, for experimentation and transition opportunities.
- Prof Leandros Tassiulas and his team will bring the expertise network management and will focus on the development of the notion of multiple control modalities to match the volatility of wireless networks in the operational theatre as well as subsequent failures and fragmentation. He will work closely with the rest of the team on the learning approaches that are developed in Subtask 7.1.2 so the novel architecture with multiple modalities is fully integrated in the intelligent network framework.
- Prof. Elisa Bertino, from Purdue University, will bring her expertise in policy-based computer security and attribute-based access control policies, and analytics for edge computing. She will therefore be leading the research in Task 7.2 and in particular lead the work on designing the new framework for federated policy learning and management.
- Prof. Alessandra Russo from Imperial College will bring her expertise in symbolic machine learning as well as in formal reasoning and explanation. She will work in close collaboration with Purdue University, IBM US and IBM UK.
- Dr. Seraphin Calo (IBM US) and Daniel Cunnington (IBM UK) will bring their expertise on systems for policy management, use of AI/ML and analytics in systems management and applications of generative policies.
- Andreas Martens will bring his expertise on the development of experimentations and validations scenarios across the project. In collaboration with Daniel Cunnington, he will work on identifying candidates for further transition and military use. They will jointly work with DSTL colleagues to ensure that emulations of the networks with data communications policies are a close match to future capabilities to ensure that the validation gives accurate results.
- ARL and DSTL collaborators will be collaborating with team members in the project, provide their military domain expertise from U.S. and UK side respectively, provide input during the validation and experimentation phases to guarantee that our developed emulations of policy-enabled dynamic infrastructures are a close match to future capabilities and that the validation gives accurate results. ARL and DSTL collaborators will also help identifying opportunities for transitions to the two countries respectively.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	• Initial ideas and results of tracking mechanisms of enclave condition and performance for the fragmentation architecture (Imperial/IBM US/Yale). • **Deliverable**: Presentation slides or short conference paper
Q1	**Task 2**	• Techniques for Federated Policy Learning and Local Policy Refinement. • **Deliverable**: Scientific paper on the two-layer policy learner and its experimental evaluation.
Q2	**Task 1**	• Design of hybrid cost-efficient/low-overhead architecture for devolution of control to nodes inside enclaves (Yale/IBM US/Imperial/IBM UK). • Embedding strategies for the states and actions in the SDC control and management problem, aiming to improve the model training time (Imperial/IBM US/Yale). • **Deliverable**: Conference paper submissions. Two papers will be led by UCL on (a) deep neural network techniques for control plan management in SDC, (b) two-fold solutions for optimal routing.
Q2	**Task 2**	• Techniques for Learning High-Order Policies. • **Deliverable**: Scientific paper on theoretical and experimental results about symbolic learners for policy learning and approaches for application-dependent solutions scoring.
Q3	**Task 1**	• Detailed control tracking mechanisms for the fragmentation architecture (Imperial/IBM US/Yale). • Based on the state/action embeddings, develop efficient control policies in SDC using different learning approaches (IBM US/Imperial/Yale/IBM UK). • **Deliverables**: (1) Conference paper submission(s) and (2) E&V: AFM demo based on Anglova with added "vignettes" showing different types of data transfer.
Q3	**Task 2**	• Techniques for Federated Policy Management. • **Deliverables**: (1) Scientific paper on theoretical and experimental results about the policy composition algebra and ontology design. (2) E&V: A demo showcasing some functions of the two-layer policy learning tool and the techniques for learning high-order policies.
Q4	**Task 1**	• Detailed mechanisms for dynamic/fine-grained devolution of control to nodes inside enclaves (Yale/IBM US/Imperial/IBM UK). • Formulation of status synchronization mechanisms between primary and backup controllers to tradeoff performance and complexity for the fragmentation architecture; Exploration of possible experimentation and prototype (Imperial/IBM US/Yale/IBM UK). • A truthful mechanism for adaptive SDC control. • **Deliverable**: Conference paper submission(s), paper in AI journal (e.g., JAIR, AIJ, JAAMAS) lead by Southampton on truthful mechanism design in dynamic SDC settings.
Q4	**Task 2**	• Explanation Techniques for Policy Generation.

Research Milestones		
Due	**Task**	**Description**
		• **Deliverable**: Scientific paper reporting the architecture of the policy lineage system and the design of the explanation query mechanism. Results of an end user evaluation will also be included.
Q5	**Task 1**	• Incremental learning methods that are specifically designed for the highly dynamic SDC scenario (IBM US/Imperial/Yale). • **Deliverable**: Conference paper submission.
Q5	**Task 2**	• Design of an Integrated System for Federated Learning and Management. • **Deliverable**: Report on the system architecture and analysis of system deployment approaches in coalition settings, including coalition edge computing settings.
Q6	**Task 1**	• Detailed synchronization mechanisms between primary and backup controllers and tradeoff results of performance vs. complexity for the fragmentation architecture (Imperial/IBM US/Yale). • Multi-agent reinforcement learning algorithms that are robust to concept drift and catastrophic changes. Joint integrated Demonstration between Task 7.1 and Task 7.2 (Imperial/IBM). • **Deliverables**: Paper at AAAI/IJCAI/AAMAS (Southampton) or similar conference on dealing with catastrophic changes in cooperative multi-agent reinforcement learning settings. • Demonstration policy-enabled SDC in military scenario.
Q6	**Task 2**	• Joint integrated Demonstration between Task 7.1 and Task 7.2 (Imperial/IBM). • **Deliverable**: Demonstration policy-enabled SDC in military scenario.

Project 8: Federated Learning for Coalition Analytics

Project Champion: Shiqiang Wang, IBM US

Email: wangshiq@us.ibm.com **Phone: +1-914-945-1772**

Primary Research Staff	Collaborators
Caroline Rublein (PGR), PSU	Ananthram Swami, ARL
Chris Simpkin (PGR), Cardiff	Changchang Liu, IBM US
Don Towsley, UMass	Dave Conway-Jones, IBM UK
Graham Bent, IBM UK	Douglas Summers-Stay, ARL
Hanlin Lu (PGR), PSU	Geeth De Mel, IBM UK
Ian Taylor, Cardiff	Gerard Rinkus, Purdue
Kaushik Roy, Purdue	Hannah Richardson, Dstl
Kevin Chan, ARL	Heesung Kwon, ARL
Kin K. Leung, Imperial	Konstantinos Poularakis, Yale
Krishna Reddy Kesari (PGR), Purdue	Olwen Worthington, Dstl
Laura D'Arcy (PGR), Cardiff	Padraig Corcoran, Cardiff
Leandros Tassiulas, Yale	Raghu K Ganti, IBM US
Liang Ma, IBM US	Ting He, PSU
Mark Herbster, UCL	Tom La Porta, PSU
Nirmit Desai, IBM US	Victor Valls, Yale
Richard Tomsett, IBM UK	Wei-Han Lee, IBM US
Shiqiang Wang, IBM US	Henry Jamieson, Dstl
Stephen Pasteris (PDR), UCL	
Tiffany Tuor (PGR), Imperial	

Yuang Jiang (PGR), Yale	
Yu-Zhen (Janice) Chen (PGR), UMass	
Declan Millar, IBM UK	

Project Summary/Research Issues Addressed

Future military operations will greatly benefit from distributed analytics services available at the tactical edge. Such analytics services encompass a variety of classification and inference tasks, with examples including classifying groups as friend or foe, identifying improvised explosive devices (IEDs), etc. As shown in Figure P8-1, these analytics applications will collect multiple types of mission-related data from various sources, ranging from the physical environment (e.g., sensor measurements, images captured by cameras) to the operational infrastructure (e.g., bandwidth and topological characteristics of the networked system). The challenges of enabling distributed analytics in coalition environments include: 1) data that are necessary for analytics applications may not be shareable across coalition boundaries due to intermittent network connection, communication bandwidth limitation, and privacy concerns; 2) it is difficult to describe analytics services from different coalition members using a single language and optimize these services for the best performance towards the overall goal of the coalition.

In Project 8, we address the above challenges and develop technologies for enabling distributed analytics in military coalitions. Our focus includes how to learn the best actions in dynamic coalition networks in an online and federated manner with limited information exchange across coalition boundaries, as well as how to utilize resources/services across the coalition to perform the required analytics tasks. This project aligns with the ultimate goal of DAIS ITA is to investigate the basic science that will enable the creation of a distributed cognitive computer system (or distributed brain[30]) that can perform analytics on demand across heterogeneous networks of interconnected devices in a military coalition setting operating in synergy with human users providing understanding of dynamic and complex situations involving multiple actors.

[30] D. Verma, G. Bent, and I. Taylor, “Towards a distributed federated brain architecture using cognitive iot devices,” in 9th International Conference on Advanced Cognitive Technologies and Applications (COGNITIVE 17), 2017.

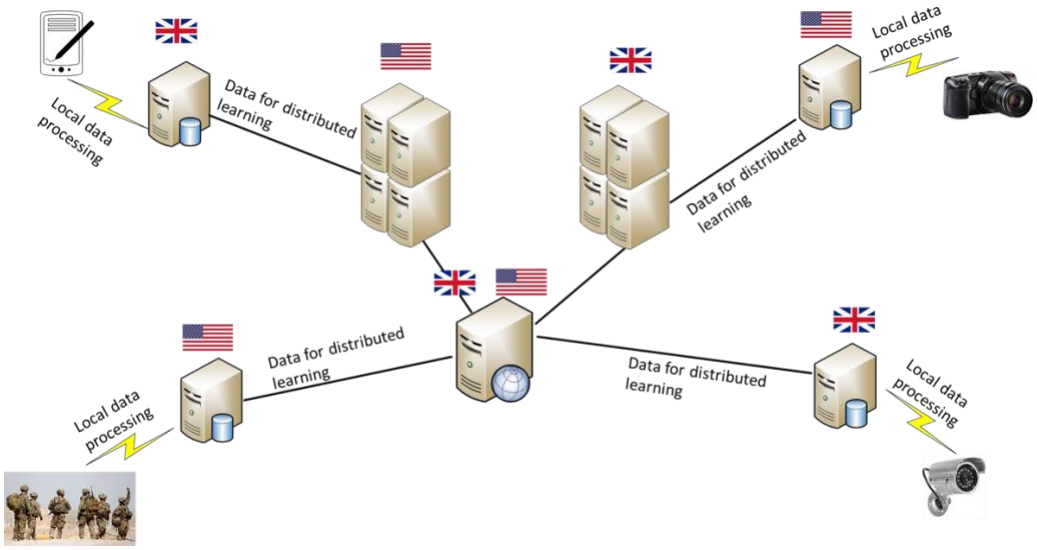


Figure P8-1: Distributed analytics for processing data from dispersed sources.

The project is divided into three tasks:

- In Task 8.1, the goal is to develop distributed online learning algorithms for multiple learners with performance guarantees, understand how software defined coalition (SDC) resource allocation and dynamics affect such algorithms, and develop efficient and robust learner placement and communication-resource allocation algorithms.
- In Task 8.2, we focus on decentralized continuous learning where the goal is to perform a joint analytics task involving members across coalition boundaries without the need of sharing sensitive information (such as raw data). We develop fundamental characterization and algorithms for adaptively updating the analytics in decentralized, dynamic, and uncertain coalition environments.
- In Task 8.3, the goal is to extend the work undertaken in BPP '18 into the construction of distributed cognitive workflows, i.e., distributed workflows that are dynamically created to meet a target goal/intent. The key idea is to construct vectors from a semantic vector space that captures characteristics of services and workflows in a coalition (e.g., obtained via neural embedding such as Word2Vec or Graph/Node2Vec). In principle, this allows one to embed knowledge graphs into a vector embedding.

Task 8.1: Distributed Online Learning with Multiple Learners

Primary Research Staff	Collaborators
Don Towsley, UMass	Ananthram Swami, ARL
Liang Ma, IBM US	Henry Jamieson, Dstl
Mark Herbster, UCL *[Task Lead]*	Kevin Chan, ARL
Richard Tomsett, IBM UK	Shiqiang Wang, IBM US
Stephen Pasteris (PDR), UCL	

Yu-Zhen (Janice) Chen (PGR), UMass	

Data used for distributed analytics in military coalitions may come in streams, and each datum must be quickly reacted to when received. *Online learning* addresses such streaming data problems.

The problem of machine learning in a centralized environment, where all data is collected in advance and is available to a single learner is well-studied. However, *tactical* military coalition settings present new challenges. In the tactical setting there may be *multiple* uncoordinated data streams generated at different locations, partially restricted per coalition policies, and impossible to collect at a single site due to lack of resources. Moreover, different software defined coalitions (SDCs) may want to perform *multiple* different tasks and each such task can be further complicated by the dynamics of the environment in the form of bandwidth fluctuations, and sensors and processors going up and down. Hence, the goal of this research is to develop algorithms for *multiple* learners processing *multiple* simultaneous data streams for *multiple* tasks in a constrained coalition environment. More precisely this research includes the following goals:

1. Develop distributed online learning algorithms for multiple learners with performance guarantees.
2. Understand how SDC resource allocation and dynamics affect such algorithms.
3. Develop learner placement and communication-resource allocation algorithms, and other techniques for making online learning robust to failures, time varying resources, as well as adversarial manipulation of data streams.

Our proposed research falls into three threads. The first regards distributed online learning in a coalition environment in the absence of resource constraints. The second accounts for, possibly, time-varying resource constraints, while the third focuses on robustifying online learning through learner placement and communication resource allocation.

Subtask 8.1.1: Distributed online learning

We present our vision for distributed online learning in a coalition environment. We begin with a single learner model and then describe extension(s) to a novel multi-learner scenario.

Single Learner Model: Consider an online algorithm whose goal is to learn a linear function[31] in an *adversarial* setting. The algorithm sequentially receives data $(x_1, y_1), \ldots, (x_T, y_T)$. The goal is to learn a hypothesis vector w such that given an observation x, y is predicted by $\hat{y} = w \cdot x$. One approach to quantifying performance is to make statistical assumptions on the data and then prove a convergence rate. By contrast, we model the learning problem as a game, *without statistical assumptions on the data*. At first glance, it seems impossible to prove performance guarantees without assumptions on the data. For example, consider an intelligent adversary with knowledge of the learning algorithm who can corrupt the data stream arbitrarily. The adversary can force any algorithm to perform arbitrarily bad. However, if the adversary can only corrupt a limited number of data points, or alternately the data is subjected to minor statistical noise, the *regret model* in online learning can provide nontrivial guarantees[32, 33].

At time $t = 1, \ldots, T$, the learner receives example $x_t \in \Re^n$ and then predicts $\hat{y}_t$ incurring loss $(\hat{y}_t - y_t)^2$. The goal is to predict with minimal loss. However, given that data may be generated by an adversary, our aim is instead to predict with small *regret*. That is, to guarantee that the learner incurs small loss if there exists some linear predictor with small loss and low complexity.

Formally, we wish to prove

[31] For simplicity and compactness of notation in our presentation we restrict ourselves to linear models, and square loss. More generally we will extend to nonlinear functions as well as strongly convex loss functions.

[32] Cesa-Bianchi, Nicolò and Gábor Lugosi. "Prediction, learning, and games." (2006).

[33] Herbster, Mark and Manfred K. Warmuth. "Tracking the Best Linear Predictor." Journal of Machine Learning Research 1 (2001): 281-309.

$$R(T,u) = \sum_{t=1}^{T}(y_t - \hat{y}_t)^2 - \sum_{t=1}^{T}(y_t - u \cdot x_t)^2 \leq Complexity(u), \quad \forall u \in \Re^n \qquad (\mathbf{1})$$

where e.g.,[34] *Complexity(u)* = $O(\|u\|^2)$. $R(T,u)$ is the *regret*, the performance of our algorithm minus the performance of linear predictor u. We aim to bound the "regret" of not knowing the optimal predictor in advance. Such bounds are very general and with additional assumptions can be converted either to batch convergence guarantees or generalization error guarantees[35]. Such a regret bound generalizes to

$$\sum_{t=1}^{T}(y_t - \hat{y}_t)^2 - \sum_{t=1}^{T}(y_t - u_t \cdot x_t)^2 \leq Complexity(u_1, u_2, \dots, u_T),\ u_t \in \Re^n, i = 1, \dots, T \qquad (\mathbf{2})$$

where for example *Complexity*$(u_1, u_2, \dots, u_T)$ = $O(\sum_{t=1}^{T-1}\|u_t - u_{t+1}\|^2)$ models the complexity of a distribution changing gradually over time. As another example, if we only have a few distinct distributions which repeat, a natural alternative measure is $Complexity(u_1, u_2, \dots, u_T) = O(|\cup_{t=1}^{T} u_t|)$. Both model nonstationary cases; we will focus on the 2nd complexity measure.

Before describing the network version of this model, we introduce our network infrastructure model.

SDC Enclave Model: The network consists of a set of (possibly overlapping) interconnected enclaves belonging to different coalition partners. Associated with each enclave is a controller that performs resource allocation and interacts with other enclave controllers. Last, edges connecting two enclaves have bandwidth and coalition constraints.

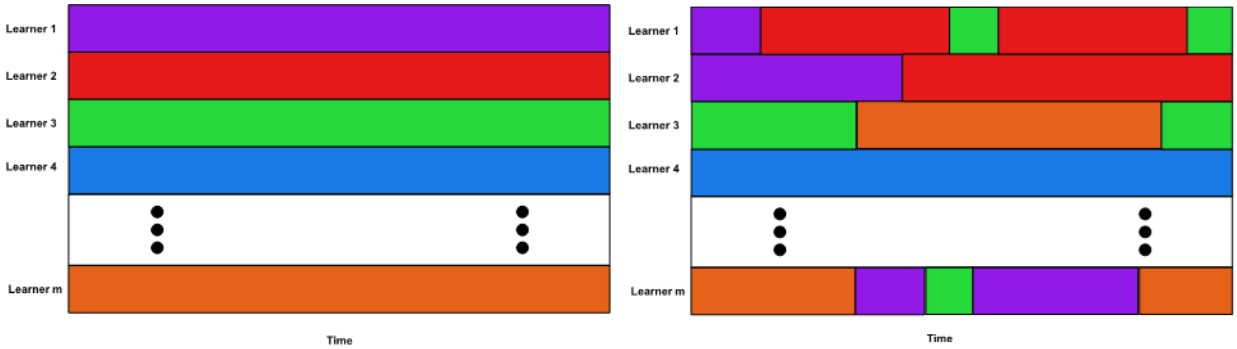


Figure P8-2: Illustrating the multi-learner multi-modal learning model. Left: There are m learners and m independent data streams with one mode (color) per stream, thus no benefit in sharing information. Right: There are m learners and m dependent data streams, each with possibly multiple modes. The modes may be shared between streams. Now, there is a benefit of sharing information between learners.

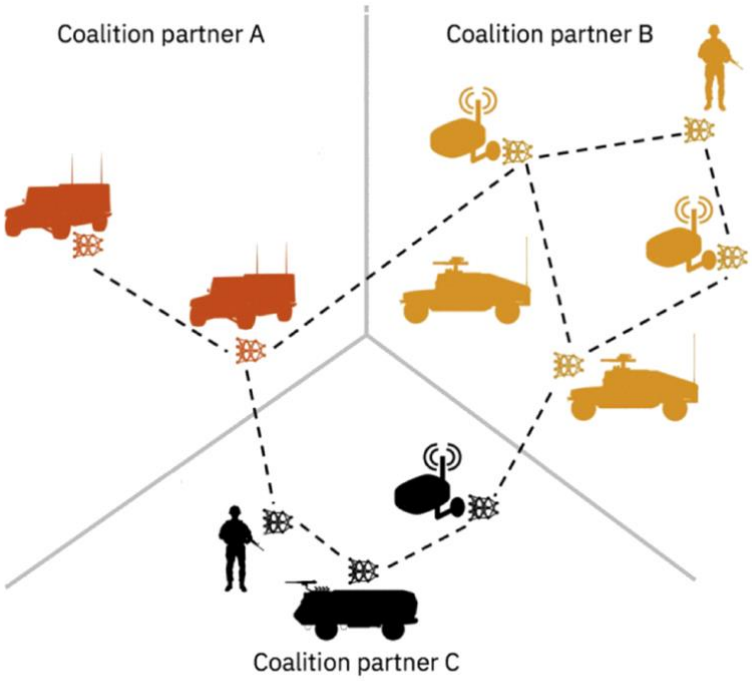
[34] For simplicity, we have suppressed a number of terms in Complexity(.). See e.g., [Cesa-Bianchi, Nicolò, Philip M. Long and Manfred K. Warmuth. "Worst-case quadratic loss bounds for prediction using linear functions and gradient descent." IEEE transactions on neural networks 7 3 (1996): 604-19, Theorem IV.3] for full details.

[35] Cavallanti, Giovanni, Nicolò Cesa-Bianchi and Claudio Gentile. "Linear Algorithms for Online Multitask Classification." COLT (2008).

Multi-Learner Multi-Modal *Learning* Model: The following figures illustrate the network learning model. We have *m* learners and *S modes*. Each learner corresponds to a row in the figures and each "modality" to a color. In Figure P8-2a each learner's data stream corresponds to a single mode, i.e., it is well-predicted by a single linear predictor $u \in \Re^n$. In Figure P8-2b, each learner faces a data stream with multiple modes (colors) but modes may be shared across learners; thus learners 1 & 2 share the red mode but learners 2 & 3 do not share any mode. Learners face the problem that they do not know when modes begin or end. Our goal is to develop algorithms that exploit multi-modal data-streams with multiple learners.

To illustrate this in terms of a practical scenario, consider a reconnaissance squad, in which squad members may be well-separated or clustered. In the first scenario the warfighters are well-separated and each faces its own independent visual recognition problem. In the second scenario the squad is not geographically separated and there are a series of spatially and temporally intermixed visual recognition tasks.

We also need to model how learners interact (i.e., share information). For example, in the above squad scenario, some pairs of warfighters might not be able to communicate, i.e., they may be too distant from one another or alternately belong to different coalition partners. We model learner communications by a graph where vertices are learners and edges represent communication paths. Associated with each edge (path) are bandwidth, latency, etc. The absence of an edge may be due to the lack of a path between learners or due to a policy decision by one or more coalition partners. Moreover, bandwidth may also be reduced due to coalition policy decisions. This, we denote as the **Learner Graph,** which may change over time.



The figure illustrates a learner graph (communication network). A **coalition** between the red, blue and black groups. Communication between the learners may occur directly when there is an edge between them. In the typical case, there will be limited inter-group edges. Although not shown in the figure, an edge may have bandwidth and latency constraints. As time progresses and warfighters move, the connectivity may change due to relative proximity.

Figure P8-3: Illustrating the multi-learner communication model.

We propose the following research:

1. **Centralized Control in a Coalition Environment:** The initial goal is to develop efficient algorithms, that exploit multi-modal data streams across multiple learners belonging to potentially different coalition partners. Each learner's data stream will be routed to a master algorithm that combines the data and routes

predictions/actions of each individual learner. The frequency at which data is delivered from a learner may be affected by coalition policies. We will develop performance guarantees on the *regret.*

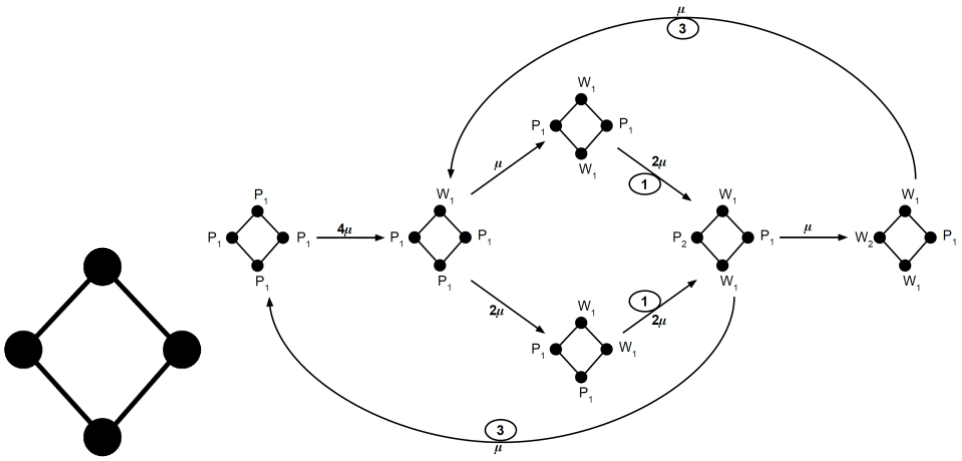
2. **Time Complexity:** The goal here is to improve the time-complexity of the control algorithm through development of approximations.
3. **Decentralized Control in a Coalition Environment:** We will account for restrictions on how learners communicate. These restrictions will be modeled by communication constraints on the *Learner Graph*. This is to meet restrictions on information sharing in a coalition environment.

Subtask 8.1.2: Interactions between SDC infrastructure and distributed online learning

The bounds derived in the previous section do not account for dynamics and randomness present in the infrastructure. Now we consider regret as a function of time, $R'(t,u)$, $t > 0$ rather than the number of iterations ($R(t,u), t = 1,2, \ldots$, and derive bounds and convergence rates for this quantity. If each iteration takes exactly τ time, $R'(t,u) = R(t/\tau, u)$. Using results from the first thread, we will account for variabilities in processing and communication times. In the case of centralized learning, the time to complete an iteration is the sum of a processing time and the additional time needed to collect results from other learners. Consider a baseline where communication delays are independent and identical exponentially distributed. If the m online learners report results to each other after every iteration (completely connected learner graph), each iteration will take $O(\log m)$ time. Hence $R'(t,u) \approx R(\frac{t}{\log m}, u)$. In the case of decentralized learning, the structure of the learner graph also affects $R'(t,u)$. For example, if the learner graph is k-regular, each iteration takes $O(\log k)$ time when communication times are exponentially distributed and $R'(t,u) \approx R(\frac{t}{\log mk}, u)$. The goal of this subtask is to extend regret bounds from the first thread, $R(t,u)$, to account for randomness in the infrastructure, $R'(t,u)$, that then will be used to provide insight on how to design learner graphs that minimize regret. We will leverage results from previous work[36], which studies how processing time variability affects convergence rate for the parameter server computing model. A previous result that maximizes convergence rate for a similar model subject to communication constraints was also devised[37]. However, the existing work neither accounts for randomness encountered in tactical military environments nor coalition constraints, e.g., rate at which data is allowed to be transferred from a learner belonging to one coalition enclave to a learner belonging to a different coalition enclave. Furthermore, neither work considers on-line learning.

[36] G. Neglia, G. Calbi, D. Towsley, G. Vardoyan. "The Role of Network Topology for Distributed Machine Learning," INFOCOM'19, 2019.

[37] S. Wang, T. Tuor, T. Salonidis, K.K. Leung, C. Makaya, T. He, K. Chan. "When edge meets learning: Adaptive control for resource-constrained distributed machine learning," INFOCOM'18, 2018.



(a) (b)

Figure P8-4: Markovian analysis of online learning

We propose the following.

1. **Markovian online learning model.** We model the learning process as a continuous time Markov chain (CTMC) describing the behavior of the online learners as a function of connectivity and allocated resources. Figure P8-4a illustrates a simple four-node learner graph, and Figure P8-4b the associated Markov chain. State P_i denotes a learner processing i steps ahead of the slowest learner and W_i a learner waiting for results from its neighbors while i steps ahead of the slowest learner. Here service times are exponentially distributed with mean $1/\mu$. This CTMC extends to larger systems and can be used to derive average times for learners to complete iterations.
2. **Mean field approximations.** The above approach provides insight for small problems but will not scale. We will explore mean field approximations as a means to study large systems. We will theoretically investigate connectivity patterns for online learners using this approach. Learner heterogeneity and coalition constraints will be handled by introducing multiple classes of learners and adding ODEs for each class.
3. **Learner-focused models.** Another approach is to model the behavior of individual learners. Prior to executing an iteration, a learner requires inputs from k other learners. The iteration consists of processing followed by a communication step where the learner waits to hear from all k learners. Denote the time between iterations as a *cycle time*. The rates at which inputs arrive are functions of cycle times of neighboring learners. If learners are homogenous, this results in a fixed-point problem with average cycle time as the unknown. Learner heterogeneity and coalition constraints are handled as in **2)** above. We will investigate the accuracy of this approach and sensitivity of average cycle time to various system parameters. We conjecture that, as m increases, average cycle time predictions will become more accurate. We will analyze the asymptotics as the number of learners approaches infinity.

Subtask 8.1.3: Robustness against adversaries and network dynamics

To enable efficient and reliable learning, learners need to receive data from their sources, and communicate with other learners. For centralized control, data streams at different learners are shared; while for distributed control, model parameters are constantly exchanged and updated. As such, we explore how to optimally place learners and allocate communication resources so that the online learning framework provides a required level of robustness against system dynamics, e.g., link/node failures, untrustworthy links, evolving policies, etc. Specifically, Figure P8-5 illustrates the logical structure of the multi-learner multi-modal learning problem, where data sources, $\{D_i\}$, are distributed across the entire network ($D_i \in V$) and each D_i associates with one learner. One approach to improve robustness is to associate multiple learners to each data source, e.g., D_4 (Figure P8-5) associates with two learners l_4 and l_4' (e.g., primary and backup). Let φ denote the maximum number of potential failed/untrustworthy links, under which the required communication is guaranteed for a set of learners. Let $V' \subset V$ be the set of nodes that can act as

learners (e.g., with sufficient computing capabilities). Our objective is to find the set of learners L with $L \subset V'$ and $|L| = n$ (n is the total budget) that maximizes φ.

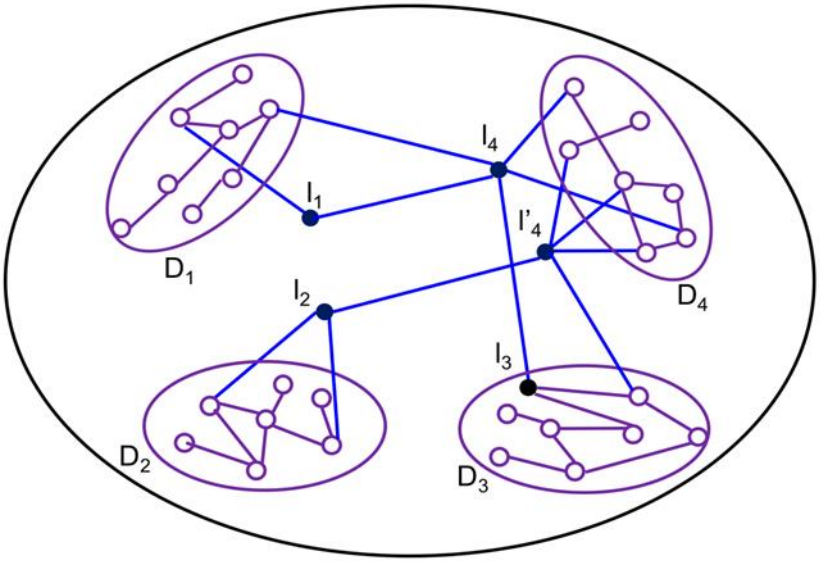


Figure P8-5: Robustness of distributed learning (primary and backup learners l_i and l'_1 associate with data cluster D_i).

This problem is challenging as multiple learners handling the same data source can operate in one of three ways: (i) they all process the same data; (ii) they divide the data from the source among them; (iii) one acts as primary and the rest as backups. For the first, we propose to locate the bottleneck that determines the value of φ, thus identifying critical subnetworks. Next, we investigate how learner redundancy affects the value of φ. We then apply these results to design efficient learner selection algorithms. For the second case, we examine an approach where multiple learners associated with a data source divide the data between them. Such a division will be dynamic to reflect changes in processing and communication resources. We will exploit results on multipath transport control[38] and stream processing[39] for this setting, where we will introduce data controllers to run at each learner that focus on efficient and fair use of communication and processing resources, and will account for variations in the cost of data streamed from the data sources.

Last, we will explore the benefits of a primary-backup approach in providing robustness. We will develop learner placement and communication allocation algorithms for this approach.

Finally, if the value of φ corresponding to the optimal placement still cannot meet the coalition needs, we then explore how to jointly place learners and add highly reliable links (i.e., can always be utilized) to the network at the minimum cost so that the robustness requirement is satisfied. The challenge in this problem is that there are two types of links in the network (highly reliable links and links that may become unusable); therefore, simple edge-connectivity from the network graphical perspective cannot describe it, thus requiring a novel and efficient solution.

Coalition policy constraints: In the above task description we have stated that we will account for restrictions placed on connectivity and bandwidth between enclaves belonging to different coalition partners that may be due to policy constraints. In order to capture these restrictions properly and accurately, we will work with the task 7.1 (belonging to P7), as they have a major focus on coalition policy. This will be facilitated with the presence of one of our PIs, Liang Ma, who is also the lead of task 7.1.

[38] Key, P. Massoulie, L., Towsley, D. "Path selection and multipath congestion control," Proceedings of INFOCOM'07, May 2007.

[39] Zhao, H., Xia, C.H., Liu, Z., Towsley, D. "A Unified Modeling Framework for Distributed Resource Allocation of General Fork and Join Processing Networks", Proceedings of 2010 ACM Sigmetrics, New York, NY, June 14-18, 2010.

Task 8.2: Agile Analytics Enabled by Decentralized Continuous Learning in Coalitions

Primary Research Staff	Collaborators
Caroline Rublein (PGR), PSU	Ananthram Swami, ARL
Graham Bent, IBM UK	Changchang Liu, IBM US
Kevin Chan, ARL	Dave Conway-Jones, IBM UK
Hanlin Lu (PGR), PSU	Geeth De Mel, IBM UK
Kin K. Leung, Imperial	Hannah Richardson, Dstl
Leandros Tassiulas, Yale	Heesung Kwon, ARL
Shiqiang Wang, IBM US *[Task Lead]*	Konstantinos Poularakis, Yale
Tiffany Tuor (PGR), Imperial	Ting He, PSU
Yuang Jiang (PGR), Yale	Tom La Porta, PSU
Declan Millar, IBM UK	Victor Valls, Yale
	Wei-Han Lee, IBM US

Analytics services analyze real-time data collected *by multiple nodes in a decentralized manner* and provide a result. The *analytics result* can be in various forms, such as recommended actions to take in the tactical operation, resource-allocation decisions for the infrastructure (e.g., SDC slice), and artificial intelligence (AI) and machine learning (ML) models tailored to real-time tactical conditions. As the environment changes over time, many analytics services must *learn* such changes and provide results that are suitable for the current condition. Situation-awareness applications are examples of such analytics services.

To enable such agile analytics in military coalitions, there are several challenges ahead:

1. High uncertainty in the availability of computation and data resources of other coalition partners, which can significantly affect the capability of analytics services;
2. High dynamics in the computation and network infrastructure across coalition boundaries, which affects who can participate in the analytics task;
3. Potential mismatch of data representation among different coalition members, which causes that some data may be used jointly in an analytics task while others cannot be jointly used;
4. Sharing raw data across coalition infrastructure is often prohibited due to security concerns and bandwidth limitation.

This work focuses on decentralized learning mechanisms that form the basis of agile analytics adapted to the changing tactical environment over time. We assume that the analytics service (code) is available at multiple nodes. Our method only exchanges the analytics results among participating nodes, without exchanging the raw data, which hence addresses Challenge 4 above. With the goal of providing real-time data-driven decentralized analytics, we

propose the new concept of *decentralized continuous learning* (DCL) and its mechanisms that address Challenges 1 to 3 above.

We note that DCL includes *federated learning* but is broader than the original federated learning concept and incorporates scenarios with dynamically connected nodes, uncertainty in data usefulness/correctness, and incremental learning to capture dynamic changes in the data. Our team has a strong research record in federated learning for resource-scarce environments during the IPP and BPP18[40, 41, 42, 43, 44, 45, 46, 47, 48]. Our work in this task is also complement to Task 8.1, as our focus here is primarily on non-convex objectives (models) such as those involving neural networks.

Conceptually, we would like to highlight that the "learning" we consider here is *not* restricted to model training for ML but applies to a wide range of data-driven analytics tasks that provide *stateful analytics results depending on the data observed in real time*.

This task includes two subtasks. Subtask 8.2.1 focuses on fundamental aspects of DCL for coalitions; Subtask 8.2.2 extends DCL to dynamic coalition services and networks.

Subtask 8.2.1: Fundamentals of Decentralized Continuous Learning (DCL) for Coalitions

Mathematical Modeling and Fundamental Characterization

We consider a wide class of data-analytics tasks as the *analytics service* that can be abstracted as an optimization problem, where the goal is to find an *analytics result* that minimizes an *analytics loss*. The analytics result is described as a vector of numbers, representing the decision or result obtained from the analytics. The analytics loss is an objective function that the analytics service tries to minimize. Each node can have its own definition of analytics loss, which can depend on the data collected at the node, and the overall objective is to minimize an aggregation (such as sum or average) of analytics losses provided by different nodes. The nodes have different levels of processing and communication capabilities and can belong to different coalition members.

We consider the DCL approach for obtaining the optimal analytics result. In this approach, each node performs one step of local computation (i.e., gradient descent), then synchronizes the intermediate analytics result with other participating nodes. The synchronization can be performed either through a single node or in a peer-to-peer manner. After repeating this *iterative learning process* for multiple rounds, the global analytics result converges to the optimal value, where the optimal result can be different when involving different subsets of nodes. As shown in our previous

[40] P. Han, S. Wang, K. K. Leung, "Adaptive gradient sparsification for communication-efficient federated learning," submitted to IEEE INFOCOM 2020, https://dais-ita.org/node/3970

[41] Y. Jiang, S. Wang, B. J. Ko, W.-H. Lee, L. Tassiulas, "Model pruning enables efficient federated learning on edge devices," AFM 2019, https://dais-ita.org/node/3967

[42] W.-H. Lee, B. J. Ko, S. Wang, C. Liu, K. K. Leung, "Exact incremental and decremental learning for LS-SVM," in IEEE International Conference on Image Processing (ICIP), Sept. 2019.

[43] T. Tuor, S. Wang, T. Salonidis, B. J. Ko, and K. K. Leung, "Demo abstract: distributed machine learning at resource-limited edge nodes," in IEEE INFOCOM, Apr. 2018.

[44] T. Tuor, S. Wang, K. K. Leung, and K. Chan, "Distributed machine learning in coalition environments: overview of techniques," in International Conference on Information Fusion (FUSION), Jul. 2018.

[45] T. Tuor, S. Wang, K. K. Leung, B. J. Ko, "Online collection and forecasting of resource utilization in large-scale distributed systems," in IEEE International Conference on Distributed Computing Systems (ICDCS), Jul. 2019.

[46] T. Tuor, S. Wang, C. Liu, B. J. Ko, K. K. Leung, "Efficient and robust federated learning with diverse tasks and data", submitted to IEEE INFOCOM 2020, https://dais-ita.org/node/3971

[47] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "When edge meets learning: adaptive control for resource-constrained distributed machine learning," in IEEE INFOCOM, Apr. 2018.

[48] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205 – 1221, Jun. 2019.

work[49, 50], there exists an optimal trade-off between computation and communication that yields the fastest learning convergence. Compared to traditional distributed optimization approaches, DCL has the following benefits: 1) a usable result is often available after a few rounds of iterations, while the result becomes closer to the optimal if running for more iterations, 2) convergence of gradient can be guaranteed even for non-convex loss functions[51].

In BPP20, we plan to extend our previous work to understand the effects of uncertainty and dynamics in the coalition network. We plan to derive a mathematical model capturing the effect of nodes joining and leaving over time as well as local loss functions (which can be data-dependent) of each node changing over time. The model will be used as a basis for dynamically configuring the learning task in the decentralized setting (e.g., adjusting the update step size, controlling which nodes to participate in the learning) in other parts of this subtask.

The resource model we consider throughout this task is one that includes nodes from multiple coalition members. The available resource and connectivity among nodes can be heterogeneous and vary over time, where the variation can be due to dynamic resource allocation provided by the SDC. The heterogeneity can be caused by coalition resource sharing policies; for example, a coalition member may have more access to its own resource compared to other coalition member's resource. Dynamically changing data sharing policies in the coalition are explicitly modeled by connecting and disconnecting nodes for a particular analytics service depending on whether the current policy allows the degree of information sharing required by the service.

Adaptive Continuous Learning in Decentralized Setting

Analytics services need to capture both long-term conditions that persist throughout the coalition operation and short-term dynamics that can change frequently over time. In such situations, recomputing the analytics results entirely due to minor changes in the loss function is undesirable and wastes resources. Especially when the loss function is data-dependent, computing the entire loss function for a given (current) analytics result during the iterative solution process can consume significant computation resources on the local node. Formally, we consider that the *local* loss function $f(w)$ is decomposable into a sum of K separate loss functions $f_1(w)$, $f_2(w)$,… $f_k(w)$,… , $f_K(w)$, where each $f_k(w)$ corresponds to the loss on a subset of data available at the local node, which is often the case when the analytics is used to train/update a machine learning model, for instance. Here, w stands for the analytics result. When $f_k(w)$ changes for a particular k, it is desirable to update the analytics result (i.e., w) *without querying the other loss functions* $f_l(w)$ with $l \neq k$. We also note that sometimes querying other loss functions is not possible at all, for example when the nodes providing those loss functions become unavailable, or data that define those loss functions have been deleted.

A straightforward approach is to only include updates involving the loss functions corresponding to new/changed data in the iterative learning process. However, this will cause the analytics to forget the old data. To see this, we consider model training as an example, if we deploy a pre-trained image-classification model to a drone, and if the drone's view is highly repetitive, the model in the drone is going to forget the infrequently seen objects as the drone trains this model with new data, which is undesirable. The technique of *continuous learning* is to prevent such forgetting from happening. Our earlier work has shown that for certain types of linear problems, exact continuous learning is possible[52]. For general classes of *non-linear* problems, however, only approximate approaches exist in the literature, including: penalizing forgetting using regularization[53] and re-using a subset of data (loss functions) that has

[49] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "When edge meets learning: adaptive control for resource-constrained distributed machine learning," in IEEE INFOCOM, Apr. 2018.

[50] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205 – 1221, Jun. 2019.

[51] P. Jiang, G. Agrawal, "A linear speedup analysis of distributed deep learning with sparse and quantized communication," in Advances in Neural Information Processing Systems, pp. 2525-2536. 2018.

[52] W.-H. Lee, B. J. Ko, S. Wang, C. Liu, K. K. Leung, "Exact incremental and decremental learning for LS-SVM," in IEEE International Conference on Image Processing (ICIP), Sept. 2019.

[53] P. Dhar, R. V. Singh, K.-C. Peng, Z. Wu, R. Chellappa, "Learning without memorizing," in IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 5138-5146.

not changed (i.e., *subsampling* the original data)[54]. None of these approaches address the decentralized learning setting nor do they provide any performance guarantee.

In this subtask, we propose to study continuous learning in the decentralized setting. We will first focus on how to apply existing regularization and subsampling techniques for non-linear problems in the decentralized case with data (or equivalently, loss functions) located at different nodes. Then, with the goal of developing efficient continuous learning techniques for non-linear loss functions, we will investigate the use a model to *approximate* the unchanged (non-linear) loss functions, so that these loss functions are still considered in the learning process without the exact data defining the loss functions. Computing the approximate loss function is much faster than evaluating the exact loss function. Each node computes its approximate loss function on its own, and the collection of approximate loss functions of all nodes will be involved in DCL. We will identify in what conditions (e.g., characteristics of the analytics logic or the loss functions) such approximation is possible, and what is the effect of the approximation error to the overall learning process thus leading to a theoretical performance result. We will also study the forgetting and remembering behavior of deep neural networks (DNN) when learning on incremental and dynamically changing data. For example, one of our initial experiments found that although DNNs forget catastrophically (rapidly) when some classes of data disappear, they also remember rapidly when the data comes back again after some time. We will build on such experimental findings to develop mathematical models that explain such behavior, which will ultimately lead to efficient continuous learning algorithms for DNN. This loss function approximation is particularly useful in the coalition setting where the exact loss function may not be revealed to other coalition members.

Subtask 8.2.2: Decentralized Continuous Learning for Coalition Services

Decentralized Continuous Learning in Dynamic and Uncertain Environments

The analytics results obtained from continuous learning change over time due to dynamic changes in the data and the loss functions defined on the data. In addition, intentional or unintentional fragmentation of the coalition network can cause the analytics results learned over subsets of nodes to become out-of-sync from time to time. Considering such dynamics and uncertainties of continuous learning in the coalition environment, we will study *how to support different variants/versions of analytics results*.

Dynamic partitioning of the network causes analytics to be obtained with only a random subset of nodes. It is therefore useful to study how to ensure that the analytics results computed on random data subsets capture the global characteristics of the coalition operation. When out-of-sync analytics results "meet", how should we merge these results to best optimize the aggregated loss function of all nodes? The solution to this problem is two-fold: a) we may need to adapt the iterative learning process according to how asynchronous the parameter updates are, b) we may need to find out appropriate "versions" of analytics results to merge because some results may be more overfitted to a specific group of nodes than others. We plan to develop a solution that jointly considers both a) and b).

Our solution will be inspired by methodologies used in our existing work[55, 56, 57]. However, we note that this problem is much more complex and difficult than the existing problems we have studied, because the involvement of mobile nodes and different versions of analytics results gives a much bigger decision space, and new algorithmic techniques need to be developed to solve this problem. The main idea of our solution is that our algorithm tracks multiple versions of analytics results at each node. When nodes meet after being out-of-sync for a while, the algorithm compares the distance of analytics results at different nodes against a threshold, and the results are merged at a version where the distance is not too big. The threshold is designed to guarantee a certain degree of optimality in the learning convergence rate.

[54] S.-A. Rebuffi, A. Kolesnikov, G. Sperl, C. H. Lampert, "iCaRL: incremental classifier and representation learning," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017, pp. 2001-2010.

[55] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "When edge meets learning: adaptive control for resource-constrained distributed machine learning," in IEEE INFOCOM, Apr. 2018.

[56] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205 – 1221, Jun. 2019.

[57] P. Han, S. Wang, K. K. Leung, "Adaptive gradient sparsification for communication-efficient federated learning," submitted to IEEE INFOCOM 2020, https://dais-ita.org/node/3970

In the more general case where different nodes' analytics results (e.g., parameters of ML models) may locate in different vector spaces, which can happen when different nodes use DNN models with different architectures for instance, merging by averaging the analytics results will not be possible. To tackle this issue, we study the following:

- We develop an approach where each node shares a summary of its data instead of analytics results. This extends our work in BPP18 where we devised the concept of robust coreset[58]. The main idea of coreset is that a small subset of data (e.g., at node A) is shared with another node (e.g., node B), so that node B can learn directly on the coreset data without interacting with node A. Compared to sharing all the raw data at node A with node B, sharing the coreset has the benefit of significantly reducing the computation overhead and avoiding leaking sensitive information across coalition boundaries. In BPP20, we plan to extend our work in BPP18 and develop a *joint dimensionality reduction, quantization, and coreset construction algorithm*, for the efficient decentralized learning by sharing a small amount of data in coalition environments.
- When sharing analytics results (model parameters) is desired, we consider the case where each node trains a small model on its own. Then, the small models from multiple nodes are collected and an ensemble of these models is built for further use. While seemingly simple, the challenge here is to determine how small each node's individual model should be so that the ensemble model remains within a desired size for efficient execution. We will focus on applying model pruning techniques to DNN models so that the model size can be reduced even after training. We will compare the performance of this ensemble approach with the more well-studied model averaging approach.

Continuous Learning for Coalition Resource Allocation

Decentralized continuous learning can be coupled with online resource allocation in the tactical infrastructure system in two ways: 1) the analytics service can be a resource-allocation service where the analytics result shows how resources should be allocated based on data of resource availability collected at different nodes; 2) the analytics service can be the training of models used for assisting the resource-allocation process for competing demands.

Our previous work[59] has addressed aspect 2) of this problem where a prediction model of resource usage can be learned in a distributed manner where usage figures of a potentially large number of resource types are represented by multi-dimensional time series. Similar prediction models can be used in tactical operations to *emulate* what resources will be needed for complex tactical situations at a future point of time, thereby providing efficient and proactive resource allocation that traditional optimization-based allocation techniques cannot provide.

In BPP20, we plan to link both 1) and 2) above together; namely, jointly training the resource demand model and applying the model for efficient resource allocation. By jointly predicting the resource demands and availability over time, coalition forces can utilize their limited infrastructure resources more efficiently, when compared with the current resource-allocation approaches that can be viewed as static techniques without considering the time and spatial dynamics of resource demands and usage behaviors. Distributed analytics applications for situation awareness and surveillance by mobile/static sensors can benefit from such advanced resource provisioning mechanisms. Despite the potential advantages, the challenging and interesting part of this problem is that it includes two distributed optimization problems that are coupled with each other, capturing the temporal and spatial resource dynamics[60]. We will provide analysis and solutions to show how DCL can solve this coupled problem. The benefit of applying DCL to resource allocation is that different coalition forces can learn the situation across coalition boundaries without leaking sensitive information, so that resource allocation decisions can be more operation-specific compared to conventional methods based on optimization techniques, with the goal of optimizing the overall objective of the coalition operation.

In addition, we will investigate resource allocation for distributed analytics tasks in a coalition environment using distributed bidding-type approaches, where we plan to primarily focus on analytics tasks (image and video tasks) that can be decomposed (e.g., layers of a CNN) or done in stages. We will then extend this work to include online

[58] H. Lu, M.-J. Li, T. He, S. Wang, V. Narayanan, K. Chan, "Robust Coreset Construction for Distributed Machine Learning," in IEEE Global Communications Conference (GLOBECOM), Dec. 2019.

[59] T. Tuor, S. Wang, K. K. Leung, B. J. Ko, "Online collection and forecasting of resource utilization in large-scale distributed systems," in IEEE International Conference on Distributed Computing Systems (ICDCS), Jul. 2019.

[60] J. Wang et al., "Spatiotemporal Modeling and Prediction in Cellular Networks: A Big Data Enabled Deep Learning Approach," in IEEE INFOCOM 2017.

algorithms, analytics tasks beyond video and imagery, and include learning aspects so that clients learn to pick servers that are better suited to meet their needs.

A potential risk in our research is the lack of military network datasets available for our work. We will take two steps to mitigate this risk: 1) We develop our algorithms with a combination of theoretical analysis and experimental validation; the theoretical analysis does not depend on specific datasets. 2) We will work closely with government collaborators to identify suitable datasets for experimental validation.

Task 8.3: Cognitive Workflows: Goal Directed Distributed Analytics Using Semantic Vector Spaces

Primary Research Staff	Collaborators
Chris Simpkin (PGR), Cardiff	Douglas Summers-Stay, ARL
Graham Bent, IBM UK *[Task Lead]*	Gerard Rinkus, Purdue
Ian Taylor, Cardiff	Olwen Worthington, Dstl
Kaushik Roy, Purdue	Padraig Corcoran, Cardiff
Krishna Reddy Kesari (PGR), Purdue	Raghu K Ganti, IBM US
Laura D'Arcy (PGR), Cardiff	Richard Tomsett, IBM UK
Nirmit Desai, IBM US	
Declan Millar, IBM UK	

Automatic service composition in mobile and pervasive computing faces many challenges due to the complex and highly dynamic nature of the environment. Common approaches consider service composition as a decision problem whose solution is usually addressed from optimization perspectives which are not feasible in practice due to: the intractability of the problem; limited computational resources of smart devices; service host's mobility; and time constraints for constructing composition plans. During BPP '18, we considered the challenge from the perspective of an interacting network of **Cognitive Services** that can self-discover other services with which they need to interact (including data services, network services, policy and security services) and can self-organize into appropriate service workflows to achieve the user requirements. This was achieved by exploiting the properties of Vector Symbolic Architectures (VSA)[61,62,63]. Whilst we have demonstrated the potential of the VSA representation for decentralized composition of predefined workflows, BPP '18 has highlighted a number of open questions that still need to be

[61] T. A. Plate, Distributed representations and nested compositional structure. University of Toronto, Department of Computer Science, 1994.

[62] P. Kanerva, "Hyperdimensional computing: An introduction to computing in distributed representation with high-dimensional random vectors." Cognitive Computation, vol. 1, no. 2, 2009, pp. 139–159.

[63] T. A. Plate, Holographic Reduced Representation: Distributed Representation for Cognitive Structures. Stanford, CA, USA: CSLI Publications, 2003.

resolved if the goal of 'Instinctive Analytics' is to be achieved. Our work to date is summarized in a series of connected papers[64, 65, 66, 67] .

In this task we propose to extend the concept to **Cognitive Workflows**, in which the workflow is dynamically created to achieve the specified goals or intent; thereby enabling true instinctive analytics, as shown in Figure P8-6.

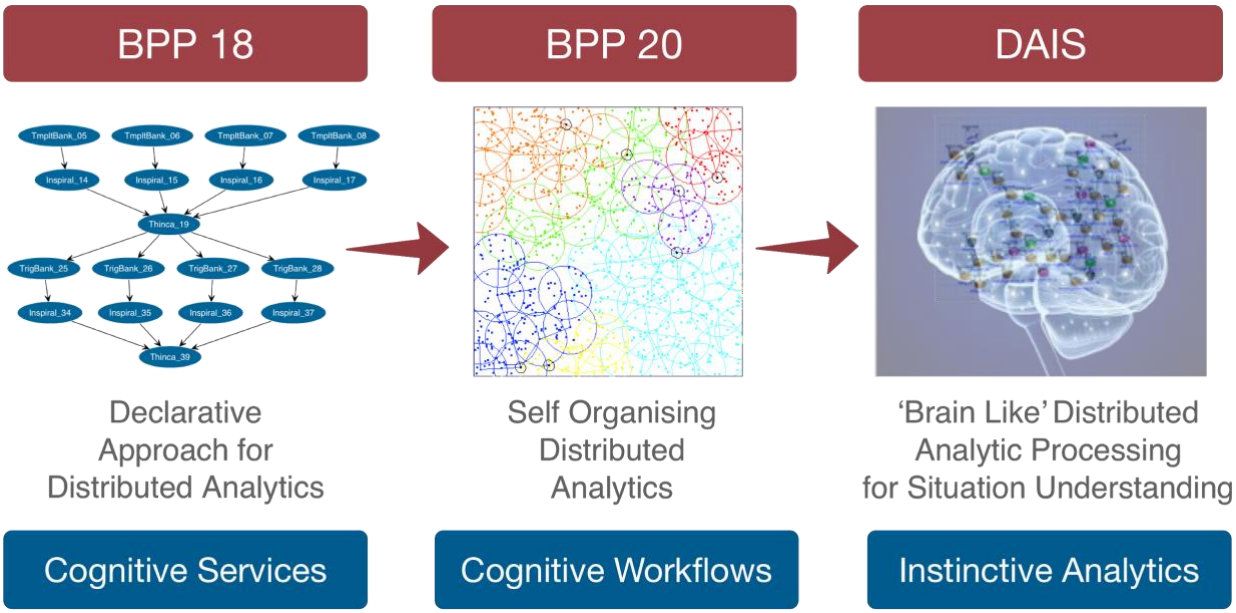


Figure P8-6: Cognitive workflows.

In other words, given a goal, how would we construct a workflow to fulfil that goal?

To realize the vision of cognitive workflows we propose to investigate the mathematical properties of **Semantic Vector Spaces** (SVS) and how these vector spaces can be combined with the VSA representation. SVS's have been demonstrated to be capable of inferring and/or deducing chains of reasoning that can connect a premise to a conclusion in a very natural **cognitive** sense. This is achieved through a sequence of vector operations in the SVS. Our hypothesis is that SVS's combined with the VSA representation can be used to construct cognitive workflows. In the coalition setting SVS's representing similar concepts but constructed independently can be aligned through a process of vector mapping. Our proposed research will specifically focus on issues of aligning SVS's created by different coalition partners so that complementary services and workflows owned by other coalition partners to achieve specific goals can be identified.

To achieve this, we have identified three fundamental research challenges:

1. **Semantic Vector Space for Cognitive Workflow:** How to exploit the mathematical properties of SVS's, such that the chains of reasoning describe the workflow needed to achieve a desired goal and how the SVS from different coalition partners can be aligned via learned mappings.

64 C. Simpkin, I. Taylor, G. A. Bent, G. de Mel, and R. K. Ganti, "A scalable vector symbolic architecture approach for decentralized workflows."

65 C. Simpkin, I. Taylor, D. Harborne, G. Bent, A. Preece, and R. K. Ganti, "Dynamic distributed orchestration of node-red iot workflows using a vector symbolic architecture," 11 2018, pp. 52–63.

66 C. Simpkin, I. Taylor, G. A. Bent, G. de Mel, S. Rallapalli, L. Ma, and M. Srivatsa, "Constructing distributed time-critical applications using cognitive enabled services," Future Generation Computer Systems, vol. 100, pp. 70–85, 2019.

67 C. Simpkin, I. Taylor, D. Harbourne, G. A. Bent, R. K. Ganti, "Efficient Orchestration of Node-RED IoT Workflows Using a Vector Symbolic Architecture", Special Issue Future Generation Computer Systems, 2019 (Under Review)

2. **Distributed Cognitive Workflow:** How the topology of SVS can be exploited such that they can be distributed across edge network environments and how chains of reasoning can be performed in a decentralized setting.
3. **Edge Efficient Cognitive Workflows:** How future cognitive services and cognitive workflows based on combining SVS's and VSA representations can be efficiently implemented in extremely low power neuromorphic processing devices, specifically Spiking Neural network (SNN) devices potentially using sparse vector representations in our VSA representation.

To fully exploit the properties of a VSA representation, what is needed is a method of constructing an SVS in which the services are semantically self-describing not only in terms of their interface parameterization and service description but also by their structural identity in terms of the graph structure of the workflow in which they connect[68]. SVS representations provide a number of desirable properties that can be exploited and that are particularly **relevant to the coalition context**. Using learned word embeddings as a motivating example, it has been demonstrated that SVS's constructed in different languages and using different text corpus can be mapped onto each other such that words with similar semantic meaning in the different vector spaces can be identified[69]. SVS's, in the case of learning word embeddings, also support arithmetic operations on the resulting word vectors to achieve results like: *czech+currency=koruna* which prove to be instinctively correct. Summers-Stay et al., at ARL, have also shown that by embedding a knowledge graph into an SVS, it is possible to perform inference over a body of knowledge that can handle ambiguity, association, analogy, and abduction naturally as part of the process[70,71]. The work has also demonstrated a way of discovering chains of reasoning connecting a premise to a conclusion directly in a real valued SVS is described. Such chains of reasoning are similar to the chains of reasoning that humans would perform on the same data. We have demonstrated that a similar approach can be performed in an equivalent VSA vector space of large binary vectors.

Analogously, our ultimate goal is to learn SVS representation of services to build workflows via vector compositions. To do so, we not only need to capture the functionality of the service, but also the (a) workflow graph (may have loops, self-loops i.e. non DAG based); (b) composability of services; (c) security, policy restrictions from coalition partners and (d) cost of invoking the service, thus requiring a scheme that goes much beyond known vector learning algorithms. In this context, the knowledge graph can be considered as the graph of known workflow transitions and the resulting chains of reasoning are the possible workflows required to achieve the desired goal (premise to conclusion). These may include novel workflow compositions.

In BPP '18 one of the other main goals of Project 4.2 was to explore the possibility that the brain-inspired computing models that underpin the VSA representation could be represented in fundamentally different ways to today's processing architectures and specifically using a non-Von Neumann architecture such as a neuromorphic processor. An extension to this work is to determine how the mathematical operations required to construct semantic vector spaces and VSA operations can be represented in ways that can support implementation in SNNs and other potential low power neuromorphic processing devices.

The proposed high-risk program of work to achieve these challenging objectives will be undertaken in three subtasks.

Subtask 8.3.1: Mathematical Properties of Semantic Vector Spaces for Cognitive Workflow

The objective of Subtask 8.3.1 is to address our first challenge by undertaking fundamental research into the mathematical properties of SVS's that might be exploited to achieve the goal of cognitive workflows. To do this we

[68] S.Rallapali, L. Ma, M. Srivatsa, A. Swami, H. Kwon, G. Bent, "SANE: Semantically Augmented Node Embeddings", ICLR 2019 (Under Review).

[69] S.Jensen, "Word and Phrase Translation with Word2Vec"2018, ,https://arxiv.org/pdf/1705.03127.pdf

[70] D. Summers-Stay, D. Li, P. Sutor, A. Raglin "Query Answering by Deductive and Analogical Reasoning in a Semantic Vector Space", ACS Poster Collection (2018) 1–13

[71] D. Summers-Stay "Deductive and Analogical Reasoning on a Semantically Embedded Knowledge Graph". In: Everitt T., Goertzel B., Potapov A. (eds) Artificial General Intelligence. AGI 2017. Lecture Notes in Computer Science, vol 10414. Springer, Cham

propose to investigate how complex workflows can be represented as a functional composition where each service essentially is treated as a mapping of input to output i.e. *f*: Input → Output. In the case of linear workflows the workflow is then the composite function i.e. If W is the linear chain of services S1, S2, S3 that are respectively represented by the transfer functions *f*, *g*, and *h* with suitably chosen domains and codomains, then $W = f \circ (g \circ h)$. In the case of complex workflows the services may have multiple inputs and outputs and this results in similarly complex e.g. of the form $W = i \circ (h \circ f, g \circ f)$. The basic research will investigate how from different functional compositions of varying complexity it is possible to construct SVS's and the types of mathematical operation that can then be performed in these vector spaces.

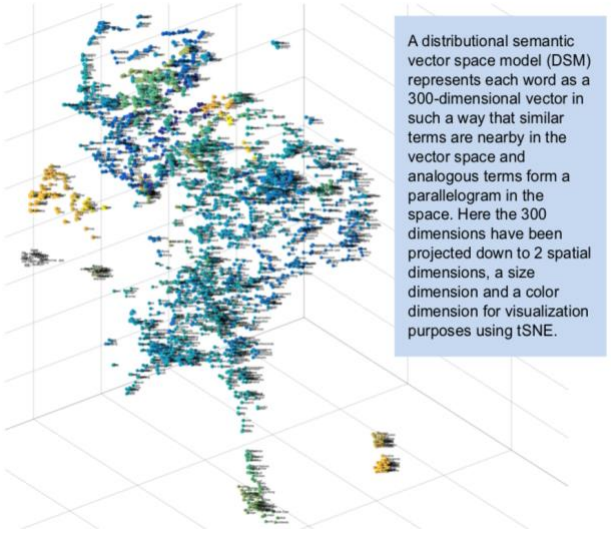


Figure P8-7: Illustration of vector space model.

In the case of linear compositions, we propose to initially investigate constructing SVS's using shallow neural networks, such as the skip-gram model of Word2Vec.The proposed approach for discovering the chains of reasoning in the vector space of functions would then be similar to that developed by our research collaborator Doug Summers-Stay[72] for word embeddings as illustrated above. In the case of more complex functional compositions representing splitting and merging of service workflows, other approaches for learning the vector space e.g. Structure2Vec[73] may be more appropriate and we propose to investigate these other potential solutions. Importantly the vector embedding needs to capture the goal of the workflow in addition to the workflow steps that are required to achieve the goal. This is required to ensure that different workflow configurations that can achieve the same goal are discoverable. This property of neural embedding is currently not supported in state-of-art solutions. Having constructed the required SVS we propose to assess its capability to perform inference, handle ambiguity, association, analogy, and abduction and how these mechanisms can be used to discover novel functional/workflow compositions that achieve desired goals.

We also propose to investigate how the SVS's from different coalition partners can be aligned either via learned mappings or using novel approaches based on identifying similar chains of reasoning in the different vector spaces. This is analogous to the learning of mappings between word embedding vector spaces constructed from different languages but in a sparse vector space. The goal is to learn the mapping matrix between services and workflows from different coalition partners using the minimum number of shared workflow examples. To achieve this objective we therefore propose to investigate the possibility that we can extend the current BPP '18 work which is investigating

[72] D. Summers-Stay "Deductive and Analogical Reasoning on a Semantically Embedded Knowledge Graph". In: Everitt T., Goertzel B., Potapov A. (eds) Artificial General Intelligence. AGI 2017. Lecture Notes in Computer Science, vol 10414. Springer, Cham

[73] H. Dai, B. Dai, L. Song, "Discriminative Embeddings of Latent Variable Models for Structured Data", arXiv:1603.05629v4 [cs.LG] 26 Sep 2016

how to generate directed acyclic graphs (DAGs) using deep reinforcement learning, specifically deep Q-learning the vector mapping in sparse reward environments[74], to the challenge of generating novel functional/workflow compositions by leveraging the properties of SVS's. We note that the work being undertaken in Task 8.1 is investigating a similar goal of learning a linear function in an adversarial setting without any statistical assumptions on the data and we propose to collaborate with Task 8.1 to determine how continuous online learning can be used.

Subtask 8.3.2: Distributed Cognitive Workflows

The objective of Subtask 8.3.2 is to address our second challenge of how cognitive workflows can operate in edge network environments in a fully decentralized manner and specifically in a coalition setting where the services are owned by different partners.

The fundamental research challenge is to determine, from the topology of an SVS, how the vector space itself can be distributed across edge network environments. Our hypothesis is that the local topology of any service essentially describes the service and that by storing a portion of the SVS local to each service it will be possible to follow the chains of reasoning across distributed services (i.e. goal directed workflow composition) can be performed in the decentralized setting. We also propose to investigate how the topological structure of the vector space can be exploited using deep reinforcement learning in sparse reward environments to determine 'next best step' transitions towards a specified goal.

A stretch goal of this subtask will be to determine if it is possible to learn the local structure of an SVS in the decentralized setting. We propose to investigate if it is possible to locally construct the SVS from the local portion of the workflow/functional compositions in which it is represented and how much of the local workflow structure is required to do this. Our proposed approach is based on the concept that a services description is based not only on its individual functional capability but also on the workflow context in which it is invoked (i.e. which services it connects to (i.e. its logical neighbors) and in turn which services they connect with. Over time the service description (i.e. its location in the SVS) evolves depending on the workflow contexts in which it has, or potentially could have been invoked. This task is performed in parallel by the distributed services operating across the network. We will investigate strategies for obtaining the necessary information from passive monitoring of the network vector traffic. The impact on network bandwidth to perform these operations will be established.

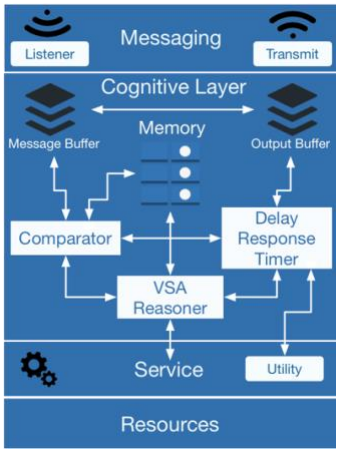


Figure P8-8: Cognitive service wrapper.

In BPP '18 we developed the concept of a cognitive service wrapper (illustrated in Figure P8-8) that could be added to real world services to provide an abstraction layer between the semantic vectors and the underlying service and resources. The cognitive layer listens to the symbolic vectors that are being exchanged between the services and responds appropriately where there is a match with its own local service vector. We propose to investigate how the

[74] L. D'Arcy, et al, "Deep Q-Learning for Directed Acyclic Graph Generation", ICLR, 2019.

concept can be extended to support the distributed construction of the SCS. The subtask will also seek to leverage the decentralized continuous learning algorithms being developed in Task 8.2 and we will investigate how the semantic vector representation can be used for resource description and to control the workflows required to implement the distributed learning tasks.

Subtask 8.3.3: Edge Efficient Cognitive Workflows

In Subtask 8.3.3 we propose to extend our BPP investigations into non Von Neumann implementation of VSA's by exploring how the operations that are required to construct the SVS and the VSA representation of services and workflows can be implemented as neuromorphic circuits and specifically to the possibility to construct the distributed SVS using SNNs and to learn the mappings between SVS's constructed by different coalition partners. The task links closely with Subtasks 8.3.1 and 8.3.2.

In the context of Subtask 8.3.1 the fundamental research challenge is to investigate how the required VSA mathematical operations of binding and superposition together with the operations required to construct SVS's and to perform the chains of reasoning can be performed using the sparse vector representations which are better suited to these types of non Von Neumann processing. We propose to determine how the orthogonality properties required for the binding operations and unbinding operations can be preserved in the sparse representation and also determine theoretical bounds on the number of sparse vectors that can be combined dependent on vector dimension and sparsity.

To address the challenge of learning the SVS representations and cross vector space mappings, we propose to explore bio-plausible SNN training methodologies for enabling energy-efficient neuromorphic computing in edge devices with on-chip learning capability. SNNs can be trained in an unsupervised manner using Spike Timing Dependent Plasticity (STDP) based local learning rules[75], which has been experimentally observed in the rat hippocampal neurons[76]. STDP-based learning has hitherto been demonstrated for fully connected[77] and convolutional SNNs[78,79,80,81,82,83,84,85,86] that are only a few layers deep. This approach is therefore applicable to learning shallow

[75] Song, S., Miller, K.D. and Abbott, L.F., 2000. Competitive Hebbian learning through spike-timing-dependent synaptic plasticity. Nature neuroscience, 3(9), p.919.

[76] Bi, G.Q. and Poo, M.M., 1998. Synaptic modifications in cultured hippocampal neurons: dependence on spike timing, synaptic strength, and postsynaptic cell type. Journal of neuroscience, 18(24), pp.10464-10472.

[77] Diehl, P.U. and Cook, M., 2015. Unsupervised learning of digit recognition using spike-timing-dependent plasticity. Frontiers in computational neuroscience, 9, p.99.

[78] Masquelier, T. and Thorpe, S.J., 2007. Unsupervised learning of visual features through spike timing dependent plasticity. PLoS computational biology, 3(2), p.e31.

[79] Tavanaei, A. and Maida, A.S., 2017, May. Multi-layer unsupervised learning in a spiking convolutional neural network. In 2017 International Joint Conference on Neural Networks (IJCNN) (pp. 2023-2030). IEEE.

[80] Tavanaei, A., Kirby, Z., and Maida, A. S., 2018. Training spiking convnets by stdp and gradient descent. In 2018 International Joint Conference on Neural Networks (IJCNN) (Rio de Janeiro, Brazil), 1–8.

[81] Ferré, P., Mamalet, F. and Thorpe, S.J., 2018. Unsupervised Feature Learning with Winner-Takes-All Based STDP. Frontiers in computational neuroscience, 12, p.24.

[82] Kheradpisheh, S. R., Ganjtabesh, M., Thorpe, S. J., and Masquelier, T., 2018. Stdp-based spiking deep convolutional neural networks for object recognition. Neural Networks 99, 56–67.

[83] Lee, C., Srinivasan, G., Panda, P., and Roy, K., 2018. Deep spiking convolutional neural network trained with unsupervised spike timing dependent plasticity. IEEE Transactions on Cognitive and Developmental Systems, 1–1 doi:10.1109/TCDS.2018.2833071.

[84] Srinivasan, G., Panda, P. and Roy, K., 2018. STDP-based Unsupervised Feature Learning using Convolution-over-time in Spiking Neural Networks for Energy-Efficient Neuromorphic Computing. J. Emerg. Technol. Comput. Syst. 14, 4, Article 44.

[85] Thiele, J.C., Bichler, O. and Dupret, A., 2018. Event-based, timescale invariant unsupervised online deep learning with STDP. Frontiers in Computational Neuroscience, 12, p.46.

[86] Mozafari, M., Ganjtabesh, M., Nowzari-Dalini, A., Thorpe, S.J. and Masquelier, T., 2018. Combining STDP and Reward-Modulated STDP in Deep Convolutional Spiking Neural Networks for Digit Recognition. arXiv preprint arXiv:1804.00227.

neural networks, such as the skip-gram model of Word2Vec, a variant of which we propose to investigate as a mechanism to learn the required SVS.

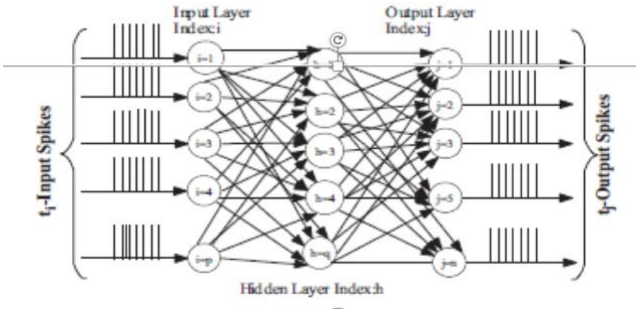


Figure P8-9: Spiking neural network.

In the context of Subtask 8.3.2 we will investigate how the cognitive service wrapper concept could be implemented in an SNN architecture and what type of energy efficiencies can be gained. We will also investigate how communication between future distributed SNN based cognitive services can be achieved using the VSA as a communications protocol.

Validation and Experimentation

Task 8.1

We will validate our ideas through a combination of theoretical analysis, numerical computations based on the models developed to account for learner infrastructure interactions, and simulation of different learner algorithms and robustness enhancing algorithms in the face of failures and time varying resource availability. The latter will reflect radio channel fluctuations, movement of warfighters, etc.

We will evaluate our robustness-related algorithms through simulation in practical coalition scenarios with the following objectives: (i) given a learning task such as target detection by a recon squad, identify critical links/subnetworks that determine network robustness in military settings; (ii) select a set of learners (e.g., soldiers, UAV, etc.) optimally w.r.t. a distributed learning goal; (iii) add reliable links (e.g., soldier radios) for the sake of overall robustness. Although we will focus primarily on coalitions consisting of two partners, we will also consider scenarios with three or more. Coalition aspects will show up in terms of different models being learned by different partners, on coalition dependent bandwidth constraints, and coalition dependent learner graph connectivity. Furthermore, to get more realistic results in large-scale battlefield scenario, we will implement our algorithms in the EMANE/CORE emulation platform together with real deployable systems (e.g., consisting of sensors and other mobile devices). All of this will culminate in a demo at AFM 2021 demonstrating the progress made, with an in-progress demo at AFM 2020.

Task 8.2

In addition to theoretically evaluating our algorithms' performance where possible, we will conduct extensive experiments to validate our proposed algorithms by considering two specific analytics applications: 1) visual analytics for detecting/classifying images containing specific objects, 2) continuous resource allocation for distributed analytics (e.g., handling surveillance images for situation awareness) SDC slice in coalition networks as mentioned in Subtask 8.2.2. We will work closely with ARL and Dstl collaborators to identify suitable datasets for these applications and evaluate the performance of our proposed algorithms using these datasets.

Our algorithms will be evaluated first in a simulated decentralized system with real datasets, then on our experimentation platform developed in BPP18 that includes a large-scale emulation system[87] and a smaller-scale

[87] D. Conway-Jones, T. Tuor, S. Wang, K. K. Leung, "Demonstration of federated learning in a resource-constrained networked environment," in IEEE International Conference on Smart Computing (SMARTCOMP), 2019.

Raspberry Pi system[88, 89]. We plan to further extend our experimentation platform by working closely with Projects 1, 3, 4, and 5 to develop a common edge network emulation environment within which decentralized continuous learning can be implemented. We will make use of CORE/EMANE wireless models to represent typical coalition networks with a representative decentralized continuous learning task, where we will work with ARL and Dstl collaborators to ensure that proper network models and learning tasks are used.

First, each individual research outcome (algorithm) will be evaluated separately. Then, a coherent system including a collection of the algorithms developed in this task will be developed, evaluated, and demonstrated. We will further identify transition opportunities of our algorithms and system to real military applications.

Task 8.3

In support of Subtasks 1 and 2 we initially propose to generate functional compositions from a variety of non-service workflow sources (e.g. different mathematical formulations of the same function) We will also potentially leverage datasets from MyExperiment[90] and the common workflow language repository[91]. We then propose to validate the results for scientific workflows generated using the Pegasus workflow generator[92]. We will use the Node-RED Library[93] of workflows for the evaluation of actual IoT service workflows. In support of Subtask 8.3.3, we will use a number of simulation tools for representing and evaluating the required spiking neural network neuromorphic circuits these include PyTorch[94], Brian Spiking Neural Network Simulator[95] and bespoke simulation tools developed by Purdue and IBM.

We propose to use our existing CORE/EMANE models, together with the network models developed to support Tasks 8.1 and 8.2, to demonstrate how the enhanced such new computing models might be applied across a coalition network and the types of inter-process communication that would be required to support such models.

Military and DAIS ITA Relevance

The US Department of Defense's (DoD) Artificial Intelligence (AI) Strategy directs the DoD to accelerate the adoption of AI and the creation of a force fit for our time. In addition, multi-domain operations[96] is a recent operating concept published by the U.S. Army TRADOC, where active involvement of multiple domains to perform highly coordinated activities is being promoted. To accomplish these goals, agile analytics enabled by the joint use of resources and exchange of information across domains is necessary. This project addresses the key aspects towards achieving these goals.

More specifically, Task 8.1 presents a general framework in which we have a network of learners where each learner processes its own individual data streams and needs to make predictions. For example, the learner(s) may correspond to image classification systems, which filter and assess video streams for potential threats that soldiers receive from their bodycams. These learners communicate over a network with a limited unreliable communication capacity along each link sharing information to other nearby learners. It is natural to assume that the video streams from nearby soldiers would help an individual soldier assess threats in their immediate environment. But given the potentially limited communications links rather than transmitting video streams a natural alternative is to transmit

[88] Y. Jiang, S. Wang, B. J. Ko, W.-H. Lee, L. Tassiulas, "Model pruning enables efficient federated learning on edge devices," AFM 2019, https://dais-ita.org/node/3967

[89] T. Tuor, S. Wang, T. Salonidis, B. J. Ko, and K. K. Leung, "Demo abstract: distributed machine learning at resource-limited edge nodes," in IEEE INFOCOM, Apr. 2018.

[90] MyExperiment. https://www.myexperiment.org

[91] The common workflow language. https://github.com/common-workflow-language/common-workflow-language

[92] The Pegasus Workflow Generator. https://confluence.pegasus.isi.edu/display/pegasus/WorkflowGenerator

[93] Node-Red Library https://flows.nodered.org/?type=node&num_pages=2

[94] Pytorch. https://pytorch.org

[95] Brian Spiking Neural Network Simulator - http://briansimulator.org

[96] https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

some subset of the individual learner's model parameters. The purpose of this research is then to determine how to do this efficiently and optimally. However, the scope of research is general in its applicability. Thus, we are not just limited to networked bodycam image classification; other natural applications include protection from multi-pronged network attacks, inducing cooperative control for a variety of Intelligence, Surveillance & Reconnaissance (ISR) tasks.

Task 8.2 focuses on providing agile analytics to tactical coalitions and addresses how continuous learning can be enabled between coalition partners' assets and services. Continuous learning is supported by the resources provided in SDC slices, where each slice exists for a small amount of time. Our validation and experimentation will focus on *improving situational awareness and decision-making*, which is one of the key technologies for future coalition operations. Analytics applied to perception tasks such as imagery analysis can extract useful information from raw data and equip coalition leaders with increased situational awareness. It can generate and help commanders explore new options so that they can select courses of action that best achieve mission outcomes, minimizing risks to both deployed coalition forces and civilians. The recent joint US-UK Defence Innovation Board meeting, conducted to explore major areas of co-operation between the nations and ensure military capabilities into the future, specifically identified this as a key area for cooperative research effort.

In Task 8.3, the research effort is aligned with army coalition operation challenges: (i) develop situational understanding using coalition services in a distributed environment and (ii) agile service composition, positioning and execution in dynamic resource constrained coalition environments. The effectiveness of future military coalition operations (combat or humanitarian) will increasingly depend on the agility in which new services and functionality can be discovered and rapidly deployed in distributed coalition environments. Our research will further develop the foundations for achieving these objectives through a combination cognitively enabled services and cognitive workflow that will increasingly rely on non Von Neumann processing to realize the vision of "Instinctive Analytics" in the DAIS concept of a "Distributed Federated Brain". We have already identified a number of transition opportunities for the BPP'18 research and for proposed research from this task. These can be found on CENSE at https://dais-ita.org/node/3974.

The experimentation and demonstration platform developed throughout this project will be used as a basis for transition opportunities and further exploration for applied military research. One potential transition work would be taking the demonstration system a stage further and getting the demonstration system working on military radios in a lab setting to further prove the suitability of the research.

Collaborations, Staff Rotations, and Linkages

Project 7 is investigating policy-enabled dynamic infrastructure for efficient management of the networked computing system across coalition members. The computation and communication resources provided by Project 7 in the form of an SDC slice will be leveraged by Project 8 to run distributed analytics. Conversely, distributed analytics services can be applied for further improving resource allocation (8.2.2) or describing and allocating resources for complex tasks using cognitive workflows (task 8.3). Linkage between Projects 7 and 8 will be facilitated by Kin Leung (Imperial) and Leandros Tassiulas (Yale) who are working on both projects.

Within Project 8, the concept of learner graphs developed in task 8.1 can serve as a theoretical foundation for capturing the effect of communication resource constraints. We will explore whether the same or similar model (or any other insights obtained in the research) is applicable to decentralized continuous learning studied in task 8.2. Tasks 8.1 and 8.2 complement each other in the sense that task 8.1 primarily focuses on linear models and task 8.2 focuses on more general non-linear models such as deep neural networks. Task 8.3 introduces vector representations of coalition analytic services, including finger printing of machine learning models to facilitate model search and ranking; this technique can be used describe the analytics services (in the form of learning) developed in task 8.1 and 8.2 as well as resource demands considered in task 8.2. Conversely, the decentralized learning technique developed in task 8.2 can be applied to task 8.3 as a way of learning the semantic vectors.

Project 9 studies defense mechanisms against attacks to neural networks and graph models. Project 8 can benefit from these studies to improve the robustness of learning. In addition, the federated learning mechanisms developed in Project 8 can be used to facilitate network intelligence in Project 9.

The ad-hoc teaming and group behavior research in Project 10 can provide further input to decentralized learning in Project 8 so that the learning occurs in the best interest of the coalition. The learning mechanisms devised in Project 8 can in turn be applied to the specific applications for situational awareness and policy generation in Project 10.

Investigators and students of P8 will participate in regular conference calls and have mutual visits for multiple times every year to ensure steady progress of our research.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	• Development of Markov models accounting for infrastructure interactions with online learning. (UMass, UCL) • Output: Tech report (UMass, UCL)
Q1	**Task 2**	• Identify requirements and basic building blocks of the mathematical modelling of DCL (IBM US, Yale, IBM UK, Imperial). • Develop an initial method of applying existing continuous learning techniques to the decentralized setting (Imperial, IBM US). • Initial experimental investigation of DCL with dynamic node connectivity (Yale, IBM US, IBM UK). • Initial description of an experimentation scenario (IBM UK, IBM US, Imperial, Yale). • Identify possible techniques for dimensionality reduction (PSU, IBM US). • Initial formulation of resource allocation for distributed analytics tasks using distributed bidding-type approaches (PSU, IBM UK) • Output: Slides, short write-ups
Q1	**Task 3**	• Report on initial investigation into mapping workflows into a Semantic Vector Space. **(Cardiff**, IBM US, IBM UK, IBM US, ARL) • Report on initial Investigation into VSA representation in SNN's (**IBM US**, Purdue, Cardiff, IBM UK, Dstl)
Q2	**Task 1**	• Regret-bounded learning in the multi-learner model with centralized control. (UCL, UMass) • Development of mean-field models for infrastructure interactions with online learning. (UMass, UCL) • Quantify network capacity in tolerating failures and adversaries (IBM US, UMass, UCL) • Output: Papers (all) and Simulation Experiments (IBM UK, all)
Q2	**Task 2**	• Develop a mathematical model to capture the performance of DCL (IBM US, Yale, IBM UK, Imperial). • Conduct experiments of applying existing continuous learning techniques to the decentralized setting (Imperial, IBM UK, IBM US). • Develop an initial mechanism to capture different versions of analytics results for DCL with dynamic node connectivity (Yale, IBM US, IBM UK). • Develop an initial experimentation platform to support the algorithms developed in this task (IBM UK, IBM US). • Analyze the performance of combining dimensionality reduction techniques with coreset-based cardinality reduction techniques (PSU, IBM US). • Experimental study of analytics task decomposition (PSU, IBM UK). • Output: Long and short papers summarizing work in progress submitted to AFM. Early work in progress demo prototype.

Research Milestones		
Due	**Task**	**Description**
Q2	**Task 3**	• Journal/conference Paper on Theoretical basis for Semantic Vector Space Representation of **linear workflows.** (**Cardiff**, IBM UK, IBM US, ARL) • Journal/conference paper on VSA representation of workflows using sparse vectors and their representation in SNNs. (**Purdue**, IBM US, IBM UK, Dstl)
Q3	**Task 1**	• Development of mean-field models for infrastructure interactions with online learning. (UMass, UCL). • Efficient learner placement algorithm and primary/backup learner association for online learning under the required robustness level against failures and adversaries. (IBM US, UMass, UCL) • Develop initial demonstration showing the effectiveness of online learning with dynamic infrastructure (IBM UK, all). • Output: Tech Report (UMass, IBM US, UCL) and a demo (IBM UK, all) at AFM 2020
Q3	**Task 2**	• Finalize the mathematical model to capture the performance of DCL and conduct experiments (IBM US, IBM UK, Yale, Imperial). • Develop enhanced approaches for continuous learning in the decentralized setting, using improved loss function approximators, and run further experiments with new approaches (Imperial, IBM US, IBM UK). • Formulate the problem of dynamic (optimal) control of DCL with dynamic node connectivity (Yale, IBM US, IBM UK). • Formulate the problem of optimally configuring the multi-dimensional data reduction pipeline (PSU, IBM US). • Algorithms for resource allocation of decomposable analytics tasks (PSU, IBM UK). • Develop initial demonstration showing the capability of decentralized continuous learning with dynamic connection of nodes (IBM UK, IBM US, Imperial, Yale). • Output: Submit an external paper on the mathematical model of DCL. Submit an external paper on continuous learning in the decentralized setting. Slides, short write-ups, AFM demo prototype.
Q3	**Task 3**	• Journal/conference paper on the theoretical basis for decentralized construction of novel **linear workflows** based on user specified goals. (**Cardiff**, IBM UK, IBM US, ARL). • Fall Meeting Paper and validation via demonstration of goal directed cognitive **linear workflow** composition at the network edge (**IBM UK,** Cardiff, IBM US, ARL). • Fall Meeting Paper and validation by demonstration of SNN VSA representation of workflows using sparse vectors in SNNs (**IBM US**, Purdue, IBM UK, Dstl).
Q4	**Task 1**	• Regret-bounded learning in the multi-learner model under two types of complexities (UCL, UMass). • Output: Paper (UCL, UMass) and Simulation Experiments (IBM UK, all).

Research Milestones		
Due	**Task**	**Description**
Q4	**Task 2**	• Develop algorithms to solve the dynamic (optimal) control problem of DCL with dynamic node connectivity (Yale, IBM US, IBM UK). • Formulate the problem of jointly training the resource demand model and applying the model for efficient resource allocation (Imperial, IBM US, IBM UK). • Develop initial algorithms for near-optimally configuring the multi-dimensional data reduction pipeline (PSU, IBM US). • Develop initial online algorithms for resource allocation (PSU, IBM UK). • Output: Slides, short write-ups.
Q4	**Task 3**	• Journal/conference paper on the theoretical basis for Semantic Vector Space Representation of **Complex Workflows.** (**Cardiff**, IBM UK, IBM US, ARL). • Journal/conference paper SNN Representation of Semantic Vector Space for **linear workflows** (**Purdue**, IBM US, IBM UK, Dstl).
Q5	**Task 1**	• Experiment and evaluations in real military and civilian network traces. (IBM UK, all). • Output: Tech Report (all)
Q5	**Task 2**	• Run experiments of dynamic (optimal) control of DCL with dynamic node connectivity (Yale, IBM UK, IBM US). • Develop algorithms for jointly training the resource demand model and applying the model for efficient resource allocation (Imperial, IBM US, IBM UK). • Enhance the experimentation platform with new algorithms and more realistic military scenarios (IBM UK, IBM US, Imperial, Yale). • Evaluate the initial algorithms for configuring the multi-dimensional data reduction pipeline in terms of their efficiency and performance in supporting simple machine learning models to identify gaps and possible areas of improvement (PSU, IBM US). • Evaluate online resource allocation algorithms with realistic analytics tasks (PSU, IBM UK). • Output: Submit external paper on dynamic control of DCL with dynamic node connectivity. Full demo prototype.
Q5	**Task 3**	• Journal/conference paper on the theoretical basis for decentralized construction of novel **complex workflows** based on user specified goals. (**Cardiff**, IBM UK, IBM US, ARL). • Journal/conference paper on mapping semantic vector spaces from different coalition partners. (**Cardiff**, IBM UK, IBM US, ARL).
Q6	**Task 1**	• Development of learner-focused models accounting for infrastructure interactions with online learning. (UMass, UCL). • Network conditions and algorithms for adding a small number of reliable links to enable the robustness of distributed learning. (IBM US, UMass, UCL). • Multi-learner model under limited communication resources. (UCL, UMass).

Research Milestones		
Due	**Task**	**Description**
		• Develop full demonstration of online learning with dynamic infrastructure, with an option of plugging in non-linear learning models developed in Task 8.2 (IBM UK, all). • Output: Paper (all), Simulation Experiments (IBM UK, all) as a demo at AFM 2021 as well as the Paper above.
Q6	**Task 2**	• Run experiments of jointly training the resource demand model and applying the model for efficient resource allocation (Imperial, IBM US, IBM UK). • Run further experiments of dynamic (optimal) control of DCL with dynamic node connectivity in realistic military coalition scenarios and integrate the algorithm into the experimentation platform (Yale, IBM UK, IBM US). • Enhance the algorithms for configuring the multi-dimensional data reduction pipeline based on findings in the initial evaluations and evaluate the enhanced algorithms in terms of their efficiency and performance in supporting both simple and complex machine learning models (PSU, IBM US). • Extend online resource allocation algorithms to support server selection and a broader range of analytics tasks (PSU, IBM UK). • Develop full demonstration of decentralized continuous learning with dynamic connection of nodes, where one application is to learn the semantic vectors developed in Task 8.3 is considered as an application (IBM UK, IBM US, Imperial, Yale). • Output: Submit external paper on jointly training the resource demand model and applying the model for efficient resource allocation. Submit external paper on optimized configuration of multi-dimensional data reduction pipeline. Long and short papers reporting final results submitted to AFM. AFM demo.
Q6	**Task 3**	• Journal/conference paper on Decentralized Cognitive Service Composition using SNN's (**Purdue**, IBM US, IBM UK, Dstl). • Fall meeting paper and validation by demonstration of Decentralized Cognitive Service Composition using SNN's (**IBM US** + all). • Fall meeting paper and validation via demonstration of goal directed cognitive **complex workflow** composition at the network edge, where the target application represented by the workflow is an analytics service developed in Task 8.1 or 8.2 (**IBM UK** + all).

Project 9: Defending coalitions in adversarial environments

Project Champion: Mani Srivastava, UCLA Email: mbs@ucla.edu Phone: +1-310-496-6587	
Primary Research Staff	**Collaborators**
Alun Preece, Cardiff	Alistair Nottle, Airbus
Cassie McMillan, Penn State	Cheryl Giammanco, ARL
Dave Braines, IBM UK	Dave Marshall, Cardiff
Diane Felmlee, Penn State	Faiz Sayyid, DSTL
James Ashford, Cardiff	Gavin Pearson, DSTL
Jeya Vikranth Jeyakumar, UCLA	Harrison Taylor, Cardiff
Lauren Hudson, Cardiff	Luis Garcia, UCLA
Liam Hiley, Cardiff	Mark Hall, Airbus
Liam Turner, Cardiff	Prudhvi Gurram, ARL
Mani Srivastava, UCLA	Raghuveer Rao, ARL
Mudhakar Srivatsa, IBM US	Rhodri Morris, Cardiff
Richard Tomsett, IBM UK	Santiago Quintana, Airbus
Roger Whitaker, Cardiff	Scott Gartner, Penn State
Supriyo Chakraborty, IBM US	Simon Julier, UCL
	Vedran Galetic, Airbus
	Yulia Hicks, Cardiff

Project Summary/Research Issues Addressed

For coalitions to be effective it is essential that a reliable working relationship among partners in a coalition be maintained despite differences and attacks on cohesion and analytics by external and internal adversaries. Since multidomain military operations involve teams of humans and artificial agents, defending coalition present challenges that span the two, and currently there exist significant gaps on both sides. Deep learning models that are increasingly at the core of analytics are particularly vulnerable to a variety of attacks, both during learning and inferencing, and methods to make their predictions as well as the explanation of their predictions robust to adversaries are lacking. Similarly, network relationships are at the core of partnerships in a coalition, and currently a proper understanding of

how adversarial actions disrupt these relationships and what measures are effective at detecting and countering them is lacking. Seeking to explore and understand these problems, the goal of this project is to assure collective intelligence in a coalition even in the presence of various forms of adversarial activities in digital, sensor, and social domains. The project is composed of two tasks that together address the aforementioned research challenges.

The first task ("Interpretability of Neural Networks in Distributed & Contested Environments under Incomplete Trust") undertakes the challenge of assuring that the results of distributed analytics in a coalition are robust to attacks -- both attacks on training data using which models used in analysis are learnt and on sensory and other inputs to those models using which predictions, decisions, and explanations are made. In particular, the task focuses on how explanations accompanying the output of machine-learning based analytics can be done robustly with quantified uncertainty so as to provide a sound basis to detect and mitigate adversarial actions.

The second task ("Network intelligence from negative ties") undertakes the challenge of ensuring the stability of the coalition under adversarial attacks that are aimed at reducing trust and enhancing competition. The task has as its objectives understanding how conflict and co-operation within a social network lead to stability or instability and developing new methods to capture both content and context of interactions enabling enhanced prediction of spread of conflict within a group.

Task 9.1: Interpretability of Neural Networks in Distributed & Contested Environments under Incomplete Trust

Primary Research Staff	Collaborators
Supriyo Chakraborty, IBM US *[Task Lead]*	Alistair Nottle, Airbus
Alun Preece, Cardiff	Dave Marshall, Cardiff
Mani Srivastava, UCLA	Faiz Sayyid, DSTL
Richard Tomsett, IBM UK	Harrison Taylor, Cardiff
Jeya Vikranth Jeyakumar, UCLA	Luis Garcia, UCLA
Liam Hiley, Cardiff	Mark Hall, Airbus
	Pridhvi Gurram, ARL
	Raghuveer Rao, ARL
	Santiago Quintana, Airbus
	Simon Julier, UCL
	Vedran Galetic, Airbus
	Yulia Hicks, Cardiff

Strategic advantage of a coalition military mission, often measured in terms of quicker identification and exploitation of opportunities, is contingent upon technology-driven autonomy and agility of decision making within the command hierarchy. As such, deep learning models, owing to their superior performance on a variety of tactical

tasks, are increasingly being deployed as part of a complex human-machine hybrid network for data-driven situational understanding (SU) – a key requirement for effective decision making[97]. However, successful decision making based on SU produced by machines depends not only on the quality of inferences but also providing, as warranted, the human decision-maker with adequate explanations to establish trust and collaboration[98, 99].

The success of deep learning models can be primarily attributed to their ability to progressively represent input data as a sequence of abstract non-linear features suitable for a given learning task. These features, while allowing the model to approximate any computable function over the inputs, are not readily human-explainable -- leading to opacity of the models.

Interpretability techniques are designed to discern the decision process of neural networks and provide insights into their inner workings. They broadly fall into three categories[100]: *(a) Sensitivity analysis* – shows how a small change to the inputs affects the classification score for the output of interest; *(b) Signal methods* – isolate input patterns that stimulate neuron activation in higher layer[101]; and finally *(c) Attribution methods* – assign importance to input dimensions by decomposing the mass of an output neuron into contributions from individual input dimensions. While the past couple of years have seen significant strides in the design of interpretability mechanisms, they are still limited in terms of their resilience to various sources of uncertainty inherent in model training and deployment[102], and also unreliable, producing inconsistent explanations for the same model decision[103].

In this task, we address the research challenge of assurance of distributed learning by creating robust interpretability mechanisms, specifically for distributed learning environments in coalition settings characterized by (i) multiplicity of agents with possibly adversarial objectives, (ii) sharing multi-modal data for information fusion, (iii) under information flow constraints that necessarily control the extent of sharing between partners.

Each of these factors contributes to additional uncertainty in -- (i) training data acquisition (e.g., due to data poisoning attacks, data sharing constraints); (ii) model training (e.g., due to model poisoning attacks); (iii) deployment and inference (e.g., due to black/white-box evasion attacks) -- and introduce challenges in developing robust interpretability mechanisms.

Technical Approach

To develop interpretable machine learning algorithms under uncertainty conditions we identify several key challenges arising from the coalition context and broadly group them as (i) Interpretability under adversarial uncertainty; (ii) Interpretability in a distributed learning setting under incomplete knowledge of training data. Our research proposal is divided into two inter-linked sub-tasks corresponding to these challenges.

97 M. R. Endsley, “Towards a Theory of Situation Awareness in Dynamic Systems”, in *Human Factors: The Journal of the Human Factors and Ergonomics Society, pp 32-64 (37), 1995.*

98 "Why Should I Trust You?": Explaining the Predictions of Any Classifier,” M. Ribeiro, S. Singh, and C. Guestrin, in *KDD, 2016.*

99 Z. Lipton. "The mythos of model interpretability." *arXiv preprint arXiv:1606.03490* 2016.

100 “The (Un)reliability of Saliency Methods”, P. Kindermans, S. Hooker, J. Adebayo, M. Alber, K, Schutt, S. Dahne, D. Erhan, and B. Kim, *in NeurIPS, 2017.*

101 “The Building Blocks of Interpretability”, C. Olah, A. Satyanarayan, I. Johnson, S. Carter, L. Schubert, K. Ye, and A. Mordvintsev, in *distill.pub, 2018.*

102 “The (Un)reliability of Saliency Methods”, P. Kindermans, S. Hooker, J. Adebayo, M. Alber, K, Schutt, S. Dahne, D. Erhan, and B. Kim, *in NeurIPS, 2017.*

103 “Sanity Checks for Saliency Metrics”, D. Harborne, R. Tomsett, S. Chakraborty, P. Gurram, A. Preece, 2019. (*Under Submission). https://dais-ita.org/node/3823*

Subtask 9.1.1: Interpretability under adversarial uncertainty

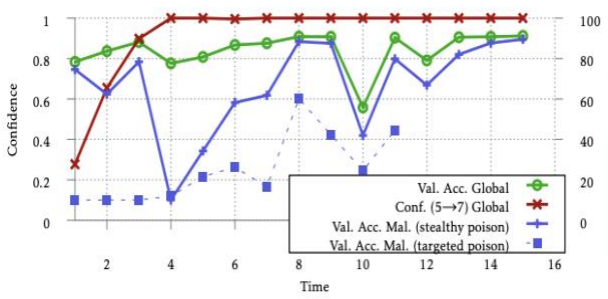


Figure P9-1a

Figure P9-1b

Figure P9-1a shows the success rate of the targeted model poisoning attack while preserving the accuracy of the model[104]. Figure P9-1b shows black-box adversarial examples generated using GenAttack against the Inceptionv3 model for $L_{\{\infty\}} = 0.05$[105].

Adversarial attacks on deep learning-based systems are executed by adding norm-constrained structured noise to the data either at training time (poisoning attacks) or during inference time (evasion attacks) to elicit untargeted/targeted misclassification on selected samples of the test dataset. In a coalition setting, adversarial attacks can originate from both coalition members as well as external sources. In BPP18, we proposed digital domain adversarial attacks, during both model training and inference, for an adversary with limited information and black-box access to the model (see Figure P9-1). Successful and robust adversarial attacks have also been executed on physical systems[106, 107]. The robustness of these attacks imply that environmental changes do not automatically reduce the effectiveness of the attacks.

A robust interpretability mechanism should be able to identify the uncertainty due to the above attacks and present them as part of the explanation. Consequently, robust interpretability mechanisms can also detect adversarial manipulations and indicate inconsistencies in the model output. Below we present challenges and solution approaches for developing robust interpretability mechanisms under digital and physical space attacks.

1.a. Interpretability under digital domain attacks

Our experimental observations, from using state-of-the-art interpretability techniques with adversarial inputs, is that the existing techniques are not sensitive enough to identify the adversarial perturbations (see Figure P9-2) and produce saliency maps that are either inconsistent with the model decision or extremely noisy[108, 109]. In fact, saliency techniques have been shown to be vulnerable to simple translation and image scalings[110].

[104] "Analyzing Federated Learning Through an Adversarial Lens", A. Bhagoji, S. Chakraborty, P. Mittal, S. Calo, in *ICML, 2019.*

[105] "GenAttack: Practical Black-box Attacks with Gradient-Free Optimization", M. Alzantot, Y. Sharma, S. Chakraborty, H. Zhang, C. Hsieh, M. Srivastava, in *ACM GECCO, 2019.*

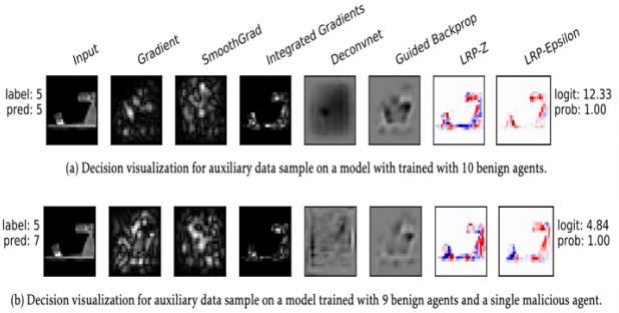
[106] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, "Robust Physical-World Attacks on Deep Learning Visual Classification", *in CVPR, 2018.*

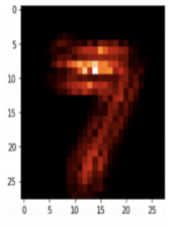
[107] "Fooling automated surveillance cameras: adversarial patches to attack person detection," S. Thys, W. V. Ranst, T. Goedeme, *arXiv preprint*, arXiv:1904.08653, 2019.

[108] "Why the Failure? How Adversarial Examples can Provide Insights for Interpretable Machine Learning", R. Tomsett, A. Widdicombe, T. Xing, S. Chakraborty, S. Julier, P. Gurram, R. Rao, M. Srivastava, in *IEEE FUSION, 2018.*

[109] "Analyzing Federated Learning Through an Adversarial Lens", A. Bhagoji, S. Chakraborty, P. Mittal, S. Calo, in *ICML, 2019.*

[110] "The (Un)reliability of Saliency Methods", P. Kindermans, S. Hooker, J. Adebayo, M. Alber, K, Schutt, S. Dahne, D. Erhan, and B. Kim, *in NeurIPS, 2017.*





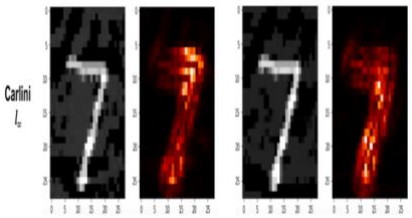


Figure P9-2a ***Figure P9-2b*** ***Figure P9-2c***

Figure P9-2a Output of interpretability techniques on benign and poisoned data samples[111]. Figure P9-2b Saliency map for accurate classification of MNIST digit '7'. Figure P9-2c Saliency maps for "7" misclassified as "6' (left) and "8" (right) under CW attack[112]. The saliency maps are not sharp and do not explain the model output.

Recently, Tao[113] introduced a novel interpretability mechanism by identifying bi-directional correspondence between attributes and internal neurons to identify neurons critical for individual attributes. They showed that their interpretability mechanism is robust and can detect adversarial examples better than state-of-the-art *feature squeezing* based detector[114]. However, a recent attack by Carlini[115] has exposed vulnerability in the adversarial detector proposed in[116].

Initial Solution Approach: In spite of the vulnerability to adversarial attacks, we are motivated by the key idea[117] that models should be encouraged (via explicit regularization) to learn features that are human explainable. This would not only lead to better interpretability, but also to better model generalization.

An important facet of human experience is our ability to break down what we observe and interact with, along characteristic lines. Visual scenes consist of separate objects, which may have different poses and identities within their category. In natural language, the syntax and semantics of a sentence can often be separated from one another. This is the idea of learning disentangled factors of variation. We propose to use disentangled learning[118, 119], to establish bi-directional correspondence between human-understandable features and disentangled factors, for enhanced interpretability. In addition, our hypothesis is that any adversarial perturbation would be more detectable when projected over the disentangled factors of variation in the latent space making the interpretability mechanism more robust to adversarial attacks.

1.b. Interpretability under physical domain attacks

Physical systems are increasingly adopting deep learning models for safety-critical missions. Hence, explaining the decision made by the models becomes extremely important. However, robust visual adversarial perturbations

111 "Analyzing Federated Learning Through an Adversarial Lens", A. Bhagoji, S. Chakraborty, P. Mittal, S. Calo, in *ICML, 2019.*

112 "Why the Failure? How Adversarial Examples can Provide Insights for Interpretable Machine Learning", R. Tomsett, A. Widdicombe, T. Xing, S. Chakraborty, S. Julier, P. Gurram, R. Rao, M. Srivastava, in *IEEE FUSION, 2018.*

113 "Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples", G. Tao, S. Ma, Y. Liu, X. Zhang, in *NeurIPS, 2018.*

114 "Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks", W. Xu, D. Evans, Y. Qi, in NDSS, 2018.

115 "Is AmI (Attacks Meet Interpretability) Robust to Adversarial Examples", N. Carlini, *arXiv preprint, arXiv:1902.02322, 2019.*

116 "Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples", G. Tao, S. Ma, Y. Liu, X. Zhang, in *NeurIPS, 2018.*

117 "Attacks Meet Interpretability: Attribute-steered Detection of Adversarial Samples", G. Tao, S. Ma, Y. Liu, X. Zhang, in *NeurIPS, 2018.*

118 "Challenging Common Assumptions in the Unsupervised Learning of Disentangled Representations," F. Locatello, S. Bauer, M. Lucic, G. Ratsch, S. Gelly, B. Scholkopf, O. Bachem, in *ICML, 2019.*

119 "Learning Disentangled Representation: From Perception to Control", https://sites.google.com/view/disentanglenips2017

under varying environmental conditions--including viewpoints--have been shown to achieve high targeted misclassification rates[120, 121]. Any interpretability mechanism has to be robust to these physical space attacks.

Initial Solution Approach: We observe that missions of interest are often monitored using multiple modality sensors. To enhance interpretability, we propose to leverage the complementary nature of the multi-modal data to train an ensemble of models, one for each modality. Under the assumption that an adversary does not simultaneously perform a correlated attack across all the different modalities, we will exploit the consistency of explanations, one for each model, to explain the ensemble decision while possibly also identifying the domain corresponding to the adversarial perturbation. Integrating interpretability of decisions being made in the digital space will facilitate a semantic understanding[122] and cohesiveness between the components of a learning-enabled physical system and vice versa.

As part of this subtask,

1. We will combine disentangled learning together with bi-directional attribution maps (between features and neuron activation patterns) to create novel robust interpretability mechanism under digital domain attacks.

2. Combine complementary multi-modal data/embeddings to train models and use consensus among the ensemble of explanations to create robust interpretability under physical space attacks.

Subtask 9.1.2: Interpretability as assurance under incomplete training information

A coalition setting is often characterized by *information flow constraints* that control the sharing of sensitive data between members. In this setting, federated learning, for instance, allows members to collaborate and iteratively train a global model without sharing raw training data[123]. Each member can independently use the global model for decision making but has incomplete knowledge of the data used for training the model. Furthermore, in the absence of complete knowledge of the training data, the decision maker might not fully trust the trained model and its output. An *explanation of the global model output, therefore, is also an assurance about the correctness of model behavior*. The need for assurance also places constraints on the suitability of an interpretability mechanism used for generating the explanation. While attribution-based saliency maps or signal methods can provide insights into the model decision, they are inadequate for providing assurance. The reason is that these interpretability methods use the trained model weights to arrive at an explanation. The decision maker might not fully trust the trained model and by extension any explanation based on the model.

One possible explanation that could provide assurance is the subset of training data samples that most influenced the model output. However, the identified training samples, if shared, could end up violating the data sharing constraints within a coalition, presenting an interesting conundrum: *how do we provide interpretability in a coalition setting without violating data sharing constraints of its members?* Furthermore, the same set of model parameters could have been modified by different coalition members through distinct and unrelated set of training data samples. *How do we represent this uncertainty in the explanation for the decision maker?* We outline these problems and possible approaches in the subsections below.

2.a. Generating explanations under information flow constraints

Providing the training data context as part of an explanation, for a particular model output, can provide assurance to the decision maker especially if the subset of training examples is *close* to the test sample under some norm-based distance.

[120] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, "Robust Physical-World Attacks on Deep Learning Visual Classification", *in CVPR, 2018.*

[121] "Fooling automated surveillance cameras: adversarial patches to attack person detection," S. Thys, W. V. Ranst, T. Goedeme, *arXiv preprint,* arXiv:1904.08653, 2019.

[122] "Semantic Adversarial Deep Learning," Dreossi, T., Jha, S. and Seshia, S.A., *in International Conference on Computer Aided Verification,* 2018.

[123] "Federated Learning: Strategies for Improving Communication Efficiency", J. Konecny, H. B. McMahan, F. X. Yu, P. Richtarik, A. TheerthaSuresh, D. Bacon, *arXiv preprint arXiv:1610.05492,* 2017.

Initial Solution Approach: At every coalition member, we would use *influence functions* to identify the set of relevant training samples. For a given test point, influence functions quantify the change in model output for a small change in training sample[124]. Thus, one can compute the influence due to every training data sample on a given test point, sort the samples in order of their influence score, and identify the ones that are the most responsible for the model prediction. However, sharing the relevant raw data samples with the decision maker as part of the explanation, can violate the data sharing constraints. To address this problem, we will generate layer-wise activation maps of the relevant training data samples and use the activation maps as proxy for the raw data. The non-linearity of neurons (resulting in many-to-one mapping of data to activation maps) guarantee that the activation map cannot be used to reconstruct the original data. Each member uses the global model to generate activation maps and shares them with the decision maker. The decision maker will in turn compute activation maps for its local dataset and identify images whose representations are closest (w.r.t a chosen distance metric, e.g., SVCCA[125]) to the activation maps received from the other members. The closest images would form the explanation set for the given test point.

2.b. Representing uncertainty in an explanation

The distributed nature of the coalition setting presents unique challenges in terms of generating training samples-based explanation. For a given test sample, every member identifies the most influential training data samples from its own local dataset and using the method outlined above shares the corresponding activation maps. The decision maker needs to prune the received set to find the most likely set of training examples as explanation. In addition, an adversary could also synthesize poisoned samples to maximize the influence scores for a given test prediction. These poisoned samples would increase the uncertainty of the explanation set.

Initial Solution Approach: The uncertainty in the explanation stems from the number of activation maps received from the coalition members and the many-to-one mapping between data and their activation maps (due to non-linearity in the global model). We draw equivalence between finding the most relevant explanation from the collection of activation maps and the Deep k-nearest neighbors (DkNN) problem presented in[126] and propose to use the DkNN mechanism to compute similarity scores between activation maps. In addition, we will also explore different distance metrics in the feature space (e.g., SVCCA, norm-based, Wasserstein, KL-divergence) to identify the most relevant set of training data samples, at the decision maker, that are representative of the received activation maps.

As part of this subtask,

1. We will leverage influence functions to approximate the effect of training samples on a model output and exploit latent space representation similarities to create explanation in a distributed setting under incomplete knowledge of training data and information flow constraints.

2. Quantify the uncertainty in explanations generated in distributed learning environments under information flow constraints.

Task 9.2: Network intelligence from negative ties

Primary Research Staff	Collaborators
Diane Felmlee, Penn State *[Task Lead]*	Cheryl Giammanco, ARL
Roger Whitaker, Cardiff	Gavin Pearson, DSTL

[124] "Understanding Black-Box Predictions via Influence Functions", P. Koh, P. Liang, *in ICML, 2017.*

[125] "SVCCA: Singular Vector Canonical Correlation Analysis for Deep Learning Dynamics and Interpretability", M. Raghu, J. Gilmer, J. Yosinski, J. Dickstein, *in NeurIPS, 2017.*

[126] "Deep k-Nearest Neighbors: Towards Confident, Interpretable and Robust Deep Learning", N. Papernot, P. McDaniel, *arXiv preprint*, arXiv:1803.04765, 2019.

Dave Braines, IBM UK	Rhodri Morris, Cardiff
Mudhakar Srivatsa, IBM US	Scott Gartner, Penn State
Cassie McMillan, Penn State	
Liam Turner, Cardiff	
James Ashford, Cardiff	
Lauren Hudson, Cardiff	

Network structure represents a vital component in wide-ranging aspects of multi-domain operations[127]. One expectation of multi-domain operations is that adversaries will expand the battlefield and behave to *"create stand-off by separating U.S. and partners politically"*. Partnerships are highly dependent on diverse forms of networks, and the ability to disrupt, or defend against disruption, can be aided by deep knowledge from these networks, especially in the case of unconventional warfare and information warfare where the aim is *"to fracture alliances and win without fighting"*. This is particularly salient for coalitions – where negativity is created and used to disrupt networks so that the support on which a coalition is based becomes diminished.

This task builds on our previous work on network motifs, in which we demonstrated the value of examining local network structure. We continue to examine elements of network structure but expand our focus beyond motifs. We now consider wider aspects of networks, including negative ties, in support of multi-domain operations and coalitions where actors are distributed across complex social and organizational structures.

We focus on a radically *new form of network representation* to better understand conflict situations – involving the so-called *negative tie*. These ties are novel because they tend to be excluded from current representations of social networks, but they are critically important in conflict situations. Generally social networks use ties (edges) to represent positive relationships, with the lack of ties otherwise. This leaves open the status that exists between unconnected parties – is a tie absent because two parties actively conflict, or is it because they don't know each other? In other cases, directly aggressive, conflictual connections among actors tend to be given short shrift, with the bulk of analyses focused around positive interchanges. Negative ties resolve these dilemmas and potentially enrich the basis for analysis and provide a promising perspective for social network research.

This white paper focuses on enhancing network intelligence using negative ties, with a view to being able to better *understand*, *detect* and *counter* the activities of adversaries in networks that underpin coalitions. It allows us to assess how distributed interventions by adversaries generate disruption across networks. This can lead to wider de-stabilization. We focus on:

- *The potential for assessing disruption through modeling negative, conflictual ties:* understanding how local characteristics of negative ties relate to global properties of networks, enabling inferences to be made when networks are partially observable.
- *Temporal characteristics of network behavior:* using novel neural-inspired approaches to determine the stability of social network ties among positive and negative interactions between nodes.
- *The diffusion of conflict in multi-domain networks:* the application of new AI/ML techniques to provide enhanced prediction of the spread of negative, conflictual social ties and communications.

Our premise is that future adversaries will be nation states that engage in deliberate activity ahead of open conflict to disrupt human networks that underpin the stability and politics of coalitions. The scope for drawing inferences from the behavior of adversarial states based on data is currently limited, due to the relatively recent adoption of activity such as unconventional warfare. However, alongside other data sources on human behavior, *terrorism* creates a lens through which we can learn about the anarchy that states may be seeking to create: we propose using terrorism as a proxy for possible state-sponsored behavior by adversaries who seek to disrupt, posture and carry

[127] https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

out unlikely acts often through subversive manipulation beyond the boundaries of their territory. Recent attacks (e.g., Salisbury in the UK) are examples of this behavior.

Our research focuses on understanding specific questions that arise in this context. In particular we propose a layered approach, moving from *structural* (1) to *temporal* (2) to *predictive* (3) analyses, as framed by the following questions:

1. How do cooperative and (positive) conflictual (negative) links in human networks enable the network to retain coherence? Can structural components distinguish between these two types of ties? Can predictions be made from local features that give forewarning of changes to the overall network?
2. Can we take networks of humans, possibly extended to other actors such as machines, and better understand how interactions in the temporal domain emerge to create negative ties? Can "neural" representations of human actors be exploited to characterize and detect regularity, under or over representation concerning interactions?
3. How can AI/ML predict the spread of negative, conflictual exchanges in complex networks? Can deep learning techniques distinguish between positive and negative interactions? Can such an approach be used to identify and predict the attacker and the defender?

Technical Approach

Research will be largely data-driven, using representations of network behavior pertaining to conflict among actors as well as disruption by actors at the group-level.

Subtask 9.2.1: The role of negative ties in local and global structures

Goal: to understand how negative (e.g., conflictual) ties within networks interact with positive (e.g., cooperative) ties to provide overall stability or instability

The bulk of research on social networks focuses on positive network ties, such as those of friendship, and information exchange. Only recently have researchers begun to examine the "dark side" of human interaction where negative ties emerge and represent different forms of interpersonal conflict, intolerance and abuse. More research in this area is necessary because such ties rarely exist in isolation. Wider impact to the underlying population is likely as compound effects are reinforced through social means, leading to potential propagation of negativity and fracture of the population. Consequently, negative ties represent an important "tool" at the disposal of an adversary for undermining the population that an opponent represents.

Therefore, it is important to understand the interplay between local structures involving negative ties, and the overall global structure that may result from dynamic interactions. This is not well understood but remains particularly important – for example interventions to promote negative ties in a foreign population are potentially valuable to an adversarial state. Furthermore, this dark side of networks is ripe for disruption by an adversary, due to secondary actions taken by actors in response to embedded negative ties.

Building on our prior work that considers the structural patterns of positive, affective interactions[128] and the harmful ties that connect terrorist groups[129, 130, 131], one of the key questions we address concerns the extent to which the local structure of positive and negative linked networks differ. For example, positive and negative networks are likely to exhibit varied patterns of dyad, triad, and tetrad motifs, that is, statistically overrepresented sub-graph patterns. Individuals may be more likely to reciprocate the bonds of friendship, as opposed to those that are defined

[128] Felmlee, Diane, McMillan, Cassie, Towsley, Don, and Roger Whitaker (2018). Dyads, triads, and tetrads: Uncovering the local structure of social groups through network motifs. *The International Social Network Association for Network Analysis Sunbelt Conference Utrecht, Netherlands.*

[129] McMillan, Cassie, Felmlee, Diane and Dave Braines (2019). Dynamic patterns of terrorist networks: A Comparison of common structures among terrorist group ties. *Journal of Quantitative Criminology: Special Issue on Terrorism*.

[130] Verma, Dinesh, Yalagadda, Rithvik, Gartner, Scott, Felmlee, Diane, and Dave Braines (2019). Understanding Patterns of Terrorism in India Using AI Machine Learning.

[131] Turner, L. D., Colombo, G. B., Whitaker, R. M., & Felmlee, D. (2017). Parameterising the dynamics of inter-group conflict from real world data. In *2017 IEEE SmartWorld 2017* IEEE.

by conflict. Negative tie networks also may not demonstrate common patterns of triad transitivity closure that characterizes positive networks. The enemy of my enemy may not be my enemy, but could be my ally instead.

More broadly, we ask: Can network structural components distinguish positive links between actors from those that are negative? Do networks develop unique "signatures," that can be identified by a combination of patterns among negative and positive links? To what extent do positive versus negative ties reinforce stability or instability? We will use statistical models, including Exponential Random Graph Models, to examine the components of networks and change over time. Relevant datasets include data on online aggression and military interventions. The outcome of this subtask concerns establishing the value of including negative ties in social network modeling. This is fundamental research of widespread applicability.

Subtask 9.2.2: Temporal characteristics of negative ties

Goal: To understand how latent temporal network signatures can be characterized and used to identify distinct patterns of behavior relating to negative ties.

Particularly in large-scale networks, assessing the temporal interaction between actors, both human and machine, can be difficult. However, this can be of fundamental value in network intelligence, particularly if it leaves a signature that is indicative of change, such as the formation of a negative tie. We focus on this issue and bring a fresh perspective. In particular, we consider re-conceptualizing networks as collections of individuals that can be thought of as "neurons" that "spike" when specific actions occur[132]. This leads to a spike-train representation of activity for each actor that can be combined and assessed collectively with the spike-trains of others.

Techniques from neuroscience are particularly useful for enhancing data analysis in "spike-train" form[133]. In this field a fundamental challenge is to determine synchronicity between the firing of neurons so that relationships can be established between different elements under varied conditions. This translates well to behavior between human (and potentially other) actors - analysis techniques can be exploited and enhanced accordingly. For example, neural analysis techniques were successfully extended by the authors[134] to analyze interactions between individuals in groups, based on new measures of periodicity between interactions[135].

We seek to further extend the "neural" spike-train representation of behavior for the detection and characterization of latent temporal characteristics, in particular focusing on the interaction between adversarial (i.e., negatively tied) individuals. We will further extend existing techniques[136, 137] for negative tie characterization, looking at aspects such as automatic parameterization (e.g., resolution of discrete event time windows) so that patterns can be rapidly established in large networks without human intervention, for rapid deployment and analysis.

We aim to establish useful features that rapidly characterize changes in interaction between network actors. The results will enable us to extrapolate features on which further artificial intelligence can capitalize, in support of Subtask 9.2.3. The work will allow us to understand how distributed entities in the network are functioning and provide distinctive signatures (a form of "motif"), considerably extending developments in BPP18 T6.2 through an alternative approach.

[132] Williams, M. J., Whitaker, R. M., & Allen, S. M. (2016). There and back again: Detecting regularity in human encounter communities. IEEE Transactions on Mobile Computing, 16(6), 1744-1757.

[133] Kreuz, T., Chicharro, D., Andrzejak, R. G., Haas, J. S., & Abarbanel, H. D. (2009). Measuring multiple spike train synchrony. Journal of neuroscience methods, 183(2), 287-299.

[134] Williams, M. J., Whitaker, R. M., & Allen, S. M. (2012). Decentralised detection of periodic encounter communities in opportunistic networks. *Ad Hoc Networks*, *10*(8), 1544-1556.

[135] Williams, M. J., Whitaker, R. M., & Allen, S. M. (2012). Measuring individual regularity in human visiting patterns. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing* (pp. 117-122). IEEE.

[136] Kreuz, T., Chicharro, D., Andrzejak, R. G., Haas, J. S., & Abarbanel, H. D. (2009). Measuring multiple spike train synchrony. Journal of neuroscience methods, 183(2), 287-299.

[137] Williams, M. J., Whitaker, R. M., & Allen, S. M. (2016). There and back again: Detecting regularity in human encounter communities. IEEE Transactions on Mobile Computing, 16(6), 1744-1757.

Subtask 9.2.3: AI for Learning Spread of Conflicts on Complex Social Networks

Goal: To harness AI models to predict the spread of conflicts on complex social networks

Being able to predict how negative ties spread in large and complex social networks is a critical but currently non-existent capability, because negative ties tend to be absent from social network analysis. Our prior work in NS-CTA studied spatiotemporal spread of events using social network data[138] (e.g., shortage of gas after hurricane Sandy). Other work focused on information spread on social networks[139], [140]. However, they do not address spread of conflicting views on complex social networks with both positive and negative ties. In particular, state-of-the-art models are not adequately equipped to answer the following question: *when a conflict arises, who will participate and on which side of the conflict?*

In this subtask we will look to build AI/ML capabilities taking into account multiple layers - structural metrics (Subtask 9.2.1), temporal characterizations (Subtask 9.2.2) as well as potential content of interactions between the parties themselves. Traditional approaches treat text documents as monologues (e.g., Universal sentence embeddings and BERT[141]) and often fail to account for the multi-party nature of conversations that occur in groups. While the former captures the sequential nature of text (using recurrent neural networks and transformers) in a monologue, it is insufficient to model the sequential nature of multi-party conversations. An independent body of work focuses on learning graph embeddings and applying graph convolutions[142] that capture the multi-party nature of networks; our prior work in DAIS ITA developed neural embeddings for graphs with textual annotations[143]; however, these approaches do not account for the sequential nature of conversations that arises in the spread of conflicts.

Our work will attempt a *first-of-a-kind model* that combines graph convolutions with sequential models in an attempt to embed text into a high dimensional space that simultaneously captures the content of the text as well as the context of who (in the social network sense) is responsible for this text. We will begin with simple neural architectures that attempt a simple late fusion of output from sentence embedding and graph embedding and evolve them into richer models where the recurrent and the graph convolution units are closely interleaved. By leveraging deep learning techniques that combine graph convolutions with recurrent neural networks we will predictively model the spread of positive/negative ties. We will evaluate the efficacy of our approach in the context of cyberaggression, wherein our prior work[144] gathered a comprehensive dataset that can be used to capture negative ties.

Finally, spanning all three subtasks we plan to research, define and evaluate techniques for communicating the complex results of the previously defined analyses to human users. This will directly yield *"…a meta-heuristic framework mapping a comprehensive typology to different representation frames and modelling methods*" and is, to the best of our knowledge, an open research question. The focus on the typology for interchanges with human users will enable more precise communication of the combined results of our analyses and will support insight by the human analysts trying to make sense of the coalition situation to take appropriate action. The communication of information will be multi-modal, spanning linguistic as well as visual renderings.

[138] Ganti, M. Srivatsa and T. Abdelzaher. (2013). Spatiotemporal Spread of Events in Social Networks: A Gas Shortage Case Study. In MILCOM 2013.

[139] C. Budak, T. Georgiou, D. Agrawal and A. El Abbadi. (2013). GeoScope: Online Detection of Geo-Correlated Information Trends in Social Networks. In VLDB 2013.

[140] H. Sanchez and S. Kumar (2012). Twitter Bullying Detection. In NSDI 2012.

[141] J. Devlin, M-W. Chang, K. Lee and K. Toutanova. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In NAACL 2019.

[142] Z. Wu, S. Pan, F. Chen. G. Long. C. Zhang and P.S. Yu. (2019). A Comprehensive Survey on Graph Neural Networks. https://arxiv.org/pdf/1901.00596.pdf

[143] S. Rallapalli, L. Ma, M. Srivatsa, I. Taylor and G. Bent. (2019). SANE: Semantically Augmented Node Embeddings. Under submission. https://dais-ita.org/node/2301

[144] Felmlee, D., DellaPosta, D., Inara Rodis, P., and Matthew, S. (2019). Cyber Aggression on Social Media: A Quasi-Experimental Study of Policy on Sexist and Racist Messages. The meeting of the American Sociological Association, New York, NY.

The development of a formal meta-model to support the metrics and models of results will help both individual analysts, as well as coalition groups of analysts seeking to work together to unambiguously share appropriate information in a consistent format. The meta-model will support communication between human and machine agents using the same representation. The meta-model will also support the potential for machine-assistance in processing results, for example: summarizing or fusing across large sets of results or data.

Validation and Experimentation

Task 9.1

Following is the list of associated tools and datasets we plan on using for experimentation and validating use cases for various tasks.

***Experimental tools and datasets*:** We will evaluate the interpretable methods that have been implemented in the iNNvestigate toolbox[145] across the uncertain contexts presented in both the subtasks. The Adversarial Robustness Toolbox[146] and the CleverHans repository[147] will act as benchmark frameworks for evaluating the robustness of our interpretability mechanisms. They provide a comprehensive set of adversarial attacks, defenses, as well as robustness metrics to establish baseline comparisons for our approaches. The experimentation will be performed on standard evaluation datasets in this context such as the CIFAR-10 and ImageNet datasets.

***Validation Use Cases*:** Establishing a ground truth would necessitate transparency into the latent space of the associated models--the very problem interpretability mechanisms are attempting to address. Hence, we validate our approaches using representative use cases.

1. *Experimentation with human participants:* We will utilize a service such as the Amazon mTurk marketplace to facilitate the human evaluation of explanation quality (while adhering to MODREC and HRPO procedures and approvals for human-derived data use).
2. *Robust interpretability:* We will test the robustness of the developed interpretability mechanisms to detect and identify adversarial examples generated by digital adversarial attack techniques developed in the previous BPP as well as ones in ART and CleverHans libraries.
3. *Multi-modal robustness and enhanced interpretability*: We will leveraging existing multi-modal datasets such as (i) the crowd-funded dataset http://crowdsignals.io (large set of rich longitudinal mobile and sensor data recorded from a demographically diverse cohort), (ii) the CASAS dataset http://ailab.wsu.edu/casas/datasets/ (a multimodal longitudinal sensor dataset capturing complex events corresponding to activities of daily living), and (iii) our own multimodal UK traffic dataset which includes video imagery and natural language.
4. *Interpretability as assurance:* We will validate the use of interpretability as assurance mechanism by creating distributed framework of agents with access to local data, enforcing information flow constraints under coalition setting, and quantifying the change in uncertainty.

Task 9.2

We will undertake validation experiments using several approaches:

Network Analyses of Data

We will use several datasets to test and validate our algorithms, such as enemies in military disputes, aggressors and trolls in online data, terrorists (dark ties), and the absence of positive ties. These datasets will enable us to draw

[145] "iNNvestigate neural networks!", Alber, M., Lapuschkin, S., Seegerer, P., Hägele, M., Schütt, K.T., Montavon, G., Samek, W., Müller, K.R., Dähne, S., Kindermans, P.J., in *Journal of Machine Learning Research, 2019.*

[146] "Adversarial Robustness Toolbox v0.10.0", Nicolae, M.I., Sinn, M., Tran, M.N., Buesser, B., Rawat, A., Wistuba, M., Zantedeschi, V., Barcado, N., Chen, B., Ludwig, H., Mollow, I., Edwards, B., in *CoRR,* 2018.

[147] "Technical Report on the CleverHans v2. 1.0 Adversarial Examples Library", Papernot, N., Faghri, F., Carlini, N., Goodfellow, I., Feinman, R., Kurakin, A., Xie, C., Sharma, Y., Brown, T., Roy, A. and Matyasko, A., *arXiv preprint arXiv:1610.00768,* 2016.

conclusions regarding the unique structure, and dynamic nature of negative (or absent) ties, as compared to positive links.

- Terrorist networks[148]
- Online Aggression[149]
- Military intervention in disputes between nations[150]
- DAIS-ITA authorship networks from the Science Library[151]
- Data from the Cardiff University Crime and Security Research Institute, involving interaction of "groups" through social media.

Alternative forms of temporal analysis based on neural-models

In subtask 9.2.2 we will use complementary data shared with subtasks 9.2.1 and 9.2.3 to experiment with neural-inspired "spike train" models of interaction taking into account the extent of negativity in the tie. This will work closely with other subtasks in i) establishing the structure of negative ties (subtask 9.2.1); ii) establishing features that support prediction (subtask 9.2.3). We will support large datasets using supercomputing facilities (Supercomputing Wales).

AI and Deep Learning

For subtask 9.2.3 we will use data from our previous work[152] repurposed to explore the basis for negative ties. The data will be used to train AI and ML models in the context of a network with both positive and negative ties. We seek to quantify and validate the rate of spread of conflicting information, predict whether an entity will be for/against the factoid and identify key entities responsible for the spread. We will study the influence of negative ties (subtask 9.2.1) and temporal dynamics of behavior (subtask 9.2.2) on the spread of conflicting information.

We will consult regularly with government colleagues regarding additional possible data and our validation and experimental procedures.

Military and DAIS ITA Relevance

Being able to defend coalitions in adversarial environments is key to DAIS ITA goals of exploiting heterogeneous distributed coalition data and analytics for situational understanding during military operations. With coalitions consisting of both human and AI agents, defending coalitions naturally involves assuring the integrity of coalition analytics (focus of Task 9.1) as well as behaviors (focus of Task 9.2) in the presence of both internal and external adversarial actions. Below we describe the military and DAIS ITA relevance of both of the tasks that compose this project.

Task 9.1

The research proposed under Task 9.1 aligns with ARL's Artificial Intelligence & Machine Learning and Human-Agent Teaming Essential Research Areas, targeted at addressing gaps in the coalition context related to **Operationalizing Artificial Intelligence for Multi-Domain Operations** (specifically the challenge of complex human-machine hybrid network for data-driven situational understanding) as well as **Federated Artificial Intelligence for Multi-Domain Operations** (specifically the areas of *AI and ML with Highly Heterogeneous Data* and *Adversarial AI and ML in Contested Deceptive Environment*).

148 John Jay & ARTIS Transnational Terrorism Database (JJATT). 2009. (http://doitapps.jjay.cuny.edu/jjatt/data.php)

149 Felmlee Aggression Data (2019)

150 Correlates of War (http://www.correlatesofwar.org/data-sets)

151 http://sl.dais-ita.org/science-library

152 S. Rallapalli, L. Ma, M. Srivatsa, I. Taylor and G. Bent. (2019). SANE: Semantically Augmented Node Embeddings. Under submission. https://dais-ita.org/node/2301

The importance of interpretability of ML agents in military operations can be understood by considering Endsley's Situational Understanding (SU) and Situational Awareness (SA) model[153]. SU is extremely important in new warfighting concepts, such as the Internet of Battlefield Things (IoBT) in which the battlefield is populated by a coalition of multiple agents[154] and machines. In such a coalition setting of MDO, SU must be formed at two levels: within each coalition partner, and amongst all the coalition partners, and it is essential that partners be able to rely on assets contributed by other partners. Hence, ML models and agents must provide a suitable level of explanation for their outputs so that the military decision-makers can make reliable and informed decisions. The distributed setting of the MDO also provides adversaries with opportunities to interrupt the coalition operations. Robust interpretability mechanisms can help detect such adversarial attacks.

We anticipate opportunities for the interpretability research in this task to be fast-tracked to transition via Cardiff's Crime and Security Research Institute and its strategic relationships with several UK police forces and UK Government departments. We have already sought engagement with the open-source community through release of prototype software[155, 156], and will continue with this path. Finally, commercial transition opportunities will be explored by the industry partners through product offerings (IBM AIX-360 cloud services, processes at Airbus).

Task 9.2

Analyzing negative ties can enable new insights into the dynamics of tactical coalition networks in complex multi-domain operations. Negative ties align with how populations fracture and evolve towards conflict or become perturbed and disrupted through third party manipulation, e.g. from an adversary state.

Awareness of the structure of successful coalition networks can be used to better plan and subsequently monitor partner interaction. Positive network patterns may indicate healthy interconnections between disparate coalition enclaves. Negative interactions could specify sources of conflict; types of subgraph structures (e.g., imbalanced triads and/or tetrads) could indicate inefficient, and potentially stressful interconnections, or passive negativity through lack of connection.

Understanding the dynamics of external groups in conflict, insurgency and peacekeeping also has direct military relevance. The closed and subversive nature of such networks means building knowledge from observation of sub-structures is highly valuable. In a coalition setting this enables shared understanding of a common threat, enhancing military intelligence. For example, negative ties may be particularly good at highlighting latent conflicts for dominance within local power structures, enabling the coalition to understand the likelihood of local groups consenting to, or resisting, the coalition mission. Such knowledge supports "campaign authority"[157], empowering coalition forces to better understand the complex social structures in their operating environment and thereby act in a way to earn the consent of local factions and the wider population.

Useful scenarios include:

- determining good structures for tactical military coalition networks
- identifying features of coalition networks exhibiting successful or unsuccessful interaction
- interactions between humans and autonomous systems
- understanding adversarial networks such as terrorist cells

The techniques and methods that emerge from this task will support new technical capabilities, e.g. for generating good or bad examples of network structures, real-time detection of significant network changes, or

[153] M. R. Endsley, "Towards a Theory of Situation Awareness in Dynamic Systems", in *Human Factors: The Journal of the Human Factors and Ergonomics Society, pp 32-64 (37), 1995.*

[154] "The internet of battle things", Kott, A., Swami, A., and West, B., Computer, 49(12):70–75, 2016.

[155] "Sensegen: A Deep Learning Architecture for Synthetic Sensor Data Generation", Alzantot, M., Chakraborty, S. and Srivastava, M., in *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2017.

[156] "Deep Residual Neural Networks for Audio Spoofing Detection," Alzantot, M., Wang, Z. and Srivastava, M.B, *arXiv preprint arXiv:1907.00501*, 2019.

[157] From UK Land Operations Doctrine https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf

capabilities to infer wider network structures from partial observations. The underlying algorithmic work to enable these capabilities will be made available as open source software.

Collaborations, Staff Rotations, and Linkages

This project has close synergies with Project 10 leading to several collaboration opportunities. One example of such a linkage is with the human-agent teaming subtask of Task 10.2 led by Braines on integrating symbolic reasoning and sub-symbolic learning techniques. Specifically, robust interpretability of deep learning models under Task 9.1 can allow better human machine coordination and enhanced reasoning over semantically meaningful concepts, while the meta-heuristic framework under Task 9.2 relates to human-agent teaming as well. Additionally, Task 9.2 also has significant synergies with Task 10.1 led by Whitaker on coalition group behavior. Furthermore, the research Task 9.1 under Robust interpretability in the distributed learning setup has linkages with TA1 Task 8.2 on Federated Learning. We have closely collaborated with members of the team (IBM UK, Imperial College) in BPP18 and will continue to work together.

Beyond the ITA, researchers from Task 9.2 plan to identify potential collaboration(s) with a the newly formed STRONG[158] (Strengthening Teamwork for Robust Operations in Novel Groups) research program. For example, in understanding how knowledge of the impact of negative ties could be applied to monitoring and improvement of heterogeneous human-machine teams. Potential knowledge exchange through collaboration with key researchers, or participation in the annual Summer Innovation Summit events.

The project team will also engage in multiple forms of staff rotation to foster team wide collaboration. The rotation activities will include inviting PhD students for industry summer internships at IBM US and IBM UK; short duration academic visits between team members; and, visits to ARL facilities.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	• Propose NN architecture for robust interpretability that leverages the notion of disentangled learning for human-understandable features in the latent space. • **Deliverable**: *research paper(s), and performance on baseline datasets/models.*
Q1	**Task 2**	• Determine formal representations of networks exhibiting negative ties and metrics expressing differences in higher-order connectivity in comparison to networks with homogeneous ties. • **Deliverable**: *external conference paper(s).*
Q2	**Task 1**	• Evaluate the interpretability mechanism over suite of adversarial attacks for strength of detectability, and design framework for physical space attacks including adversarial patches. • **Deliverable**: *performance results for adversarial evaluation of interpretability mechanism, and attack success rate of physical space attacks.*
Q2	**Task 2**	• Methods that combine analysis of the structure of networks (e.g. motifs) with "neural" spike-train representations to examine regularity and anomalies. • **Deliverable**: *external conference/journal paper.*
Q3	**Task 1**	• Adapt exploitation of multi-modal embeddings for robust interpretability under physical space attacks.

158 https://www.arl.army.mil/www/default.cfm?page=3501

Research Milestones		
Due	**Task**	**Description**
		• **Deliverable**: *paper with framework, and code/implementation details.*
Q3	**Task 2**	• Machine learning models to predict the evolution of cooperation and conflict within social networks using features from Q1 and Q2. • **Deliverable**: *external conference/workshop paper(s).*
Q4	**Task 1**	• Create distributed framework for generating influence function-based activation-map representations of training data. Generate explanations for a federated learning setup. • **Deliverable**: *technical report containing performance of the proposed approach, and results of an Amazon mTurk based study on the quality of the generated explanation.*
Q4	**Task 2**	• The relationship between local and global network characteristics in terms of negative ties. • **Deliverable**: *external conference/journal paper(s).*
Q5	**Task 1**	• Representing uncertainty in explanation in the context of distributed and contested environments. • **Deliverable**: *paper with experimental results and code/implementation details.*
Q5	**Task 2**	• Determine how global features of complex, edge-bipartite networks can be predicted using local substructures and temporal features. • A formal meta-model to support the cohesion of the metrics and methodologies adopted. • **Deliverable**: *technical report/conference paper.*
Q6	**Task 1**	• Open source public release of research-grade of software, models, tools and algorithms, with documentation. • **Deliverable**: *consolidation and release of open source materials.*
Q6	**Task 2**	• Open source code will accompany deliverables where appropriate. • **Deliverable**: *Organization and release of relevant open source materials; Search algorithms for uncovering negative online content.*

Project 10: Ad-hoc Coalition Teams

Project Champion: Roger Whitaker, Cardiff University Email: whitakerrm@cardiff.ac.uk Phone: +44 (0)29 2087 6999	
Primary Research Staff	**Collaborators**
Roger Whitaker, Cardiff University	Dr Cheryl Giammanco, ARL
Liam Turner, Cardiff University	Dr Malgorzata Turalska, ARL
Rhodri Morris, Cardiff University	Wafi Bedwei, Cardiff
Nirmit Desai, IBM US	James Ashford, Cardiff
Geeth de Mel, IBM UK	Gualtiero (Walter) Colombo, Cardiff
Yarrow Dunham, Yale	Peter Houghton, Dstl
PDR, Yale	Eunjin (Ellie) Lee, IBM UK
Alun Preece, Cardiff	Lan Hoang, IBM UK
Angelika Kimmig, Cardiff	Jonathan Lenchner, IBM US
Marc Roig-Vilamala, Cardiff	Yunfeng Zhang, IBM US
Sam Vente, Cardiff	Vedran Galetic, Airbus
Dave Braines, IBM UK	Mark Hall, Airbus
Supriyo Chakraborty, IBM US	Alistair Nottle, Airbus
Mani Srivastava, UCLA	Santiago Quintana, Airbus
Tianwei Xing, UCLA	Erik Blasch, AFRL
Alessandra Russo, Imperial	Jonathan Bakdash, ARL
Mark Law, Imperial	Lance Kaplan, ARL
Elisa Bertino, Purdue	Chris Willis, BAE
Ankush Singla, Purdue	Federico Cerutti, Brescia / Cardiff
Daniel Cunnington, IBM UK	Sayyid Faiz, Dstl

Seraphin Calo, IBM US	Sam Hepenstal, Dstl
Sukankana Chakraborty, Southampton	Gavin Pearson, Dstl
	Paul Sullivan, Intelpoint Inc
	Murat Sensoy, Ozyegin / Cardiff
	Simon Julier, UCL
	Luis Garcia, UCLA
	Brian Rivera, ARL
	John Melrose, DSTL
	Dinesh Verma, IBM US
	Graham White, IBM UK
	Geeth de Mel, IBM UK
	Jorge Lobo, Imperial
	Sebastian Stein, Southampton

Project Summary/Research Issues Addressed

Ad-hoc coalition teams are fundamental to agile interoperability between joint forces, which may span nations and domains. This is critical to fulfilling complex coalition tasks including situational understanding. Project 10 will advance the required capabilities for flexible coalition teams to function while taking into account the increasing need for machine and human interoperation. In this scenario, intelligence – both machine and human – is distributed, requiring context aware learning and organizational mechanisms that allow parties from different domains to function with synchronicity across complex coalition tasks. This has significant implications for human and machine interactions and ultimately governs the capabilities at the coalition's disposal.

However, currently there is a knowledge gap on how to compose teams with diverse human and machine components for optimal interoperability in the coalition and multi-domain context. In this project we pursue the *organization*, *integration* and *autonomy* of both human and machine agents to fulfill coalition objectives pertaining to multi-domain scenarios with context and situational awareness. The project takes a holistic view that considers a spectrum of agency from human actions through to machine components, where there is a need for interpretability of autonomous actions. The tasks address this as follows:

- In Task 10.1 we focus on understanding the function and operation of *coalition-based groups* in terms of their coherence and ability to make effective decisions. Increasingly in future, the agents aligned with groups may not only be human – therefore we consider the potential psychological implications for coalition subgroups when the advanced capabilities of autonomous agents may inadvertently feedback into the human coalition and cause disruption on human actors.
- In Task 10.2 we address the need to rapidly integrate machine analytic components in a way which (1) is aware of uncertainties; (2) exploits synergies; and (3) supports human decision makers. Our objective is to achieve a step change in free-flowing composition of uncertainty-aware human-agent and agent-agent

information analytics. The approach goes beyond the traditional hierarchical architecture and ensures that humans will be seen as "other agents" in a computational multi-agent setting.

- In Task 10.3 we explore how to enable coalition systems and devices to operate with minimal human intervention in highly heterogeneous, and dynamic contexts whilst maintaining a level of security, to guarantee robust distributed analytics. We propose a novel approach for neural-symbolic learning of generative policies that are context aware. The approach will use a new policy generation architecture and learning paradigm to learn, from multi-modal data, policies that are human-interpretable. The "plug-and-play'' characteristics of our approach will facilitate a natural extension to coalition-based distributed intelligence.

Task 10.1: Coherence in Coalitions: understanding internal group behavior and dynamics in complex multi-domain environments

Primary Research Staff	Collaborators
Rhodri Morris, Cardiff University	Dr Cheryl Giammanco, ARL
Liam Turner, Cardiff University	Dr Malgorzata Turalska, ARL
Roger Whitaker, Cardiff University *[Task Lead]*	Alun Preece, Cardiff University
Nirmit Desai, IBM US	Wafi Bedwei, Cardiff University
Geeth de Mel, IBM UK	James Ashford, Cardiff University
Yarrow Dunham, Yale	Gualtiero (Walter) Colombo, Cardiff Uni
Academic Post-Doctoral Researcher, Yale	Peter Houghton, Dstl
Sukankana Chakraborty, Southampton	Eunjin (Ellie) Lee, IBM UK
	Lan Hoang, IBM US
	Jonathan Lenchner, IBM US
	Yunfeng Zhang, IBM US
	Sebastian Stein, Southampton

In this task we focus on understanding the function and operation of *coalition-based groups* in terms of their coherence and ability to make effective decisions. *We formalize a* coalition-based group *to be composed of sub-groups that join forces to accomplish a common goal against an adversary*. This is a general definition – the sub-groups may represent different elements of a country's forces and government (land, air, sea, cyberspace, or economic and political policy) or sub-groups could be allied national military (e.g., US and UK). We refer to a coalition-based group as "*a coalition"* or "*joint forces".*

The importance of how coalition-based groups function has been heighted by *multi-domain operations*[159] (MDO) and the *fusion doctrine*[160], which both recognize that future battles will not be fought on a single battlefield. The increased fluidity between domains requires new levels of convergence, which are not just technological. More domains with greater fusion *necessitate effective coalition-based groups* that make objective decisions without impediment. Thus, it becomes centrally important to understand how "internal" sub-groups interact, relate and cooperate to fulfill a wider mission. However, this is complex – humans are heavily disposed to working in groups[161] from a psychological perspective. This *in-group bias* can be valuable against adversaries but may also yield potential problems when groups need to work together.

This task examines how coalition-based groups may structure, fracture or strengthen based on their in-group disposition. Increasingly in future, agents aligned with groups may not only be human – therefore we consider the potential psychological implications for coalition subgroups when the advanced capabilities of autonomous agents may inadvertently feedback into the human coalition and cause disruption on human actors.

We study coalition operations as a *cognitive coordination problem*, where failure occurs when subgroups could achieve a more effective coalition but fail to do so because of behaviors that impede interactions and contributions to decision-making. Coalitions that cannot resolve this are susceptible to destabilization by adversaries. In this context we focus on specific questions:

- *Understanding group-based tensions underlying coalition operations:* How do coalition members reconcile multiple identities and affiliations? How is cognitive dissonance potentially manifested in group-decision making, based on alternative views or beliefs accrued from different affiliations? How can coalitions engage the strength of subgroups without suffering from internal conflicts that are driven by in-group bias?
- *The structure and dynamics of coalitions for information sharing:* What are the tradeoffs between accuracy and speed of decision-making in hierarchies? What are the effects of information exchange at various levels of coalition structure on the ability of individual groups to perform assigned tasks and on collective performance of coalition forces? Is there an optimal placement, role and behavior of liaison officers across the coalition? What is the impact of informal structures in coalitions?
- *Implications for human-agent teaming in support of multiple domains:* What are the psychological and information implications for a future human-agent team when agents function to support broader coalition objectives (e.g., across multiple domains)? Can domain-specific human teams be given greater awareness of "unknown unknowns" (e.g., threats from other domains) and how can this be mitigated through information provided to sub-groups?

Outcome expected: fundamental insights that support the operational integrity of coalitions functioning in complex multiple domains: i) insights into how humans may be incentivized to structure and coordinate decision-making in a coalition context; ii) developing best practices for coalition organization in respect of information sharing; iii) understanding the relationship between human and machine-based agent teaming and effect on internal coalition functioning.

Technical Approach

Our hypothesis is that *understanding both human and technological capabilities and organization in support of coalition-based groups will lead to long-term strategic advantage.* Our methodological approach is two-fold: firstly to explore and translate the "static" theory underlying meaningful dynamic scenarios, based on computational modeling; secondly through computational experimentation with machine learning, to observe the implications for human agent-based teaming when agents extend their objectives to multiple domains. We explore this using three subtasks.

159 https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

160 National Security Capability Review, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf

161 Whitaker, R. M., Felmlee, D., Verma, D. C., Preece, A., & Williams, G. R. (2017, May). From evolution to revolution: understanding mutability in large and disruptive human groups. In Next-Generation Analyst V (Vol. 10207, p. 1020703). International Society for Optics and Photonics.

Subtask 10.1.1: Understanding group-based tensions underlying coalition operations

Goal: Determine the implications of group-based psychological theory on the dynamics of coalitions through simulation-based modeling.

Using generative computational modeling and building on substantial findings from BPP18 T6.1, we will consider: i) the psychological effects on individual actors as a consequence of coalitions; ii) the collective effects of individuals on how coalitions function. Critical considerations are *in-group bias*, *identity* and *cognitive dissonance*, which form the focus in this subtask and were initially explored in BPP18.

In-group bias[162],[163] is a fundamental human disposition that gives rise to potential internal adversarial behavior between subgroups, despite being part of the same coalition. Building on previous findings[164], we extend agent-based modeling to explore multiple layers of in-group bias that are generated when social identifications intersect with organizational structure. We will base this in hypothetical but meaningful scenarios that align with input from Military Advisors. Coalitions mean that subgroup members have almost inherently divided loyalties to some degree - policies or incentives that coordinate those loyalties become very important.

We will consider the role of individual *identity based on groups* in shaping the disposition and behavioral characteristics of actors. Group-based identity provides powerful influence over individuals[165]. Work on superordinate identities[166] becomes highly relevant. We will employ adaptations of economic games where individuals are forced to make decisions factoring in their psychological dispositions as a consequence of their coalition and sub-group identities[167],[168]. We will introduce new utility and reward functions that structure how actors value their individual-level priorities versus sub-group or coalition level priorities. We seek to understand how the individual reconciles the tensions induced from multiple identities, how this is reinforced, and how this influences a coalition's coherence and ability to function, including the issue of internal competition.

In addition to this, we recognize that often individuals with predisposed loyalties may prove detrimental to coalition efforts (for instance, impede the process of information sharing – related to Subtask 10.1.2) as a consequence of their internal conflicts. Specifically, these individuals may actively influence other individuals within their social neighborhood to prioritize their own sub-group targets over the coalition goals. To deal with such cases, we will extend previous work[169] to identify ways to effectively incentivize predisposed individuals with bias towards any particular sub-group to re-adjust their self-goals (and priorities) to align them with the coalition objectives with the aim of containing any conflict that may arise within the coalition. This work will also explore cases where adversarial actors actively attempt to impede coalition goals by exploiting the sub-group affiliations and loyalties of coalition members.

In terms of cognitive dissonance, as top-down decisions or policies are implemented, they impose behavior on sub-group members. This will be at odds with the beliefs of a given sub-group in some cases, such as those with a restricted rather than multi-domain perspective. Having to behave in line with that policy can create dissonance, which functions to bring agent beliefs in line with the implemented policies. But is the resulting belief revision in the interests of the coalition? On the one hand, shared beliefs across the coalition create unity and cohesion. On the other hand a diversity of views can be valuable as a hedge against "groupthink". How should these interests be balanced? Different

[162] Dunham, Y. (2018). Mere membership. *Trends in cognitive sciences*, *22*(9), 780-793.

[163] Hewstone, M., Rubin, M., & Willis, H. (2002). Intergroup bias. *Annual review of psychology*, *53*(1), 575-604.

[164] Whitaker, R. M., Colombo, G. B., & Rand, D. G. (2018). Indirect reciprocity and the evolution of prejudicial groups. *Nature Scientific reports*, *8*(1), 13247.

[165] Hogg, M. A. (2006). Social identity theory. *Contemporary social psychological theories*, *13*, 111-1369.

[166] Gaertner, S. L., Dovidio, J. F., Anastasio, P. A., Bachman, B. A., & Rust, M. C. (1993). The common ingroup identity model: Recategorization and the reduction of intergroup bias. *European review of social psychology*, *4*(1), 1-26.

[167] Bedewi,W., Whitaker R.M., Colombo, G.B., Allen, S.M., Dunham, Y. Modelling stereotyping in cooperation systems, *11th International Conference on Computational Collective Intelligence, to appear.*

[168] Whitaker, R.M., Dunham, Y et al. The evolution of Identity Fusion, https://dais-ita.org/node/3723

[169] Chakraborty, S., Stein, S., Brede, M., Restocchi, V., Swami, A. and de Mel, G. (2019) Competitive influence maximisation using voting dynamics. Workshop on Social Influence held in conjunction with the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.

organizational structures could potentially support achieving the optimal balance, for example if some sub-groups do not have behaviors imposed on them in the same way as other sub-groups.

To progress we will generalize our work[170] on the coevolution of networks and cognitive dissonance. We will use coalition structures (shared with Subtask 10.1.2) and extend modeling to multi-domains, for example by allowing increased dimensionality on the issues over which convictions are held. Our aim is to gain a new understanding of how dissonance coexists with coalition structures, while increasing the dimensionality of the problem space, consistent with multiple domains. Aligned with this, we will introduce specific metrics assessing important issues such as "groupthink". Our modeling of cognitive dissonance also supports Subtask 10.1.3 and the framework to assess human-agent teams when agents align with multiple domains, beyond the human "users".

Subtask 10.1.2: The impact of structure and dynamics of Coalitions for information sharing

Goal: To understand how coalition organization, in terms of formal and informal structures, impact on the coherence and dynamics of coalition operations for information sharing.

We focus on discovering optimal conditions for coalition information sharing. Specifically, we investigate information exchange between coalition forces and impact of network structure and multiple chains of command on decision synchronization, force agility and mission effectiveness. This is at the heart of *command and control (C2)*[171] - military hierarchical structure poses unique challenges to communication and decision-making, where traditional top-down structure is contrasted with the fast-moving situational awareness[172]. *Efficiency of communication and decision-making in top-down command-and-control structure* is critical.

We investigate the *impact of alternative organization of teams on efficiency of information sharing and coalition problem solving* using two approaches. Firstly, we simulate interactions between members that exchange information with each other through the network structure of the group[173]. Secondly, we will observe human participation in team-based tasks[174] where the role of team-members and impact of the communication network can be assessed. This involves online experiments where individuals share information to more efficiently and collectively solve complex tasks. Collective exploration of problems can be examined through these two approaches, allowing us to assess the connection between team structure, information flow through the community and efficiency of decision-making. We investigate possible *lateralization* through bridging across coalition sub-structures as well as interconnected hierarchically structured teams.

We also address tensions that are inherent in coalition decision-making, specifically concerning *potential delay induced from hierarchical structures versus the required accuracy of decision-making.* We will consider a gradation of tasks, starting from a decomposable task, which can be accomplished by teams independently, and finishing with a complex task that requires simultaneous input from multiple teams. We will build models of decision-making taking into account the trade-offs between hierarchy (e.g., through command centers), synchronization and propagation of errors.

Finally, we consider *coordination versus adaptation*, by investigating the efficiency of top-down control over team's operations (centralization versus decentralization) against changing problem space. Complexity of assigned tasks, interdependence of tasks assigned to individual teams, accuracy and speed of identifying a solution will be considered. We will also compare the effect of varying level of lateral interactions outside of the command center, in contrast with more hierarchical layouts, in an evolving problem space, such as seen in the context of Subtask 10.1.3.

170 The Coevolution of social networks and cognitive dissonance, https://dais-ita.org/node/3725.

171 Alberts, D. S., & Hayes, R. E. (2006). *Understanding command and control*. Assistant Secretary of Defense (C3I/Command control research program), Washington DC.

172 Alberts, D. S., & Hayes, R. E. (2003). Power to the edge: Command... control... in the information age. Office of the Assistant Secretary of Defense, Washington DC command and control research program (CCRP).

173 Barkoczi, D., & Galesic, M. (2016). Social learning strategies modify the effect of network structure on group performance. *Nature communications*, *7*, 13109.

174 Mason, W., & Watts, D. J. (2012). Collaborative learning in networks. *Proceedings of the National Academy of Sciences*, *109*(3), 764-769.

Subtask 10.1.3: Implications for human-agent teaming in support of multiple domains

Goal: To understand the psychological and information implications for human-agent teaming in coalitions when AI agents function to support broader coalition objectives (e.g., across multiple domains).

Game-playing AI systems that disrupt an adversary are maturing rapidly and will have a radical impact on future coalition C2 abilities: thus to achieve the vision of the distributed coalition intelligence we need to examine how the inclusion of such advanced AI systems within coalitions will impact on the human element of the coalition. We are going to use the example of AI in support of strategic decisions and user-centered design as our way into this problem, particularly with respect to consideration of cognitive dissonance (Subtask 10.1.1) and the role of information sharing (Subtask 10.1.2) between the human and the AI agents. This example will partly build on an existing network-based game[175] that can be used to evaluate AI agents for predicting and countering the behavior of human and AI adversaries that attempt to influence a population (e.g., through messages in cyberspace or targeted interactions with individuals).

Our *human-agent modeling approach* involves setting up four[176] concurrent instances of a network-based game (e.g., by extending weighted voting scenarios and the existing influence game) that hypothetically represent four domains in which a coalition agent is competing against an adversary. We will interconnect the four networks to represent points of dependency and overlap between the domains. Using existing reinforcement learning techniques[177] we will train the coalition agents to make decisions based on single domain knowledge, taking into account time pressures[178] and induced uncertainty/risk[179,180] from partial information[181]. We will then contrast this against an alternative configuration where agents are not restricted to single domain knowledge – instead they are trained assuming exposure to networks representing all the domains, resulting in access to greater diversity of partial information as well as uncertainty.

This approach allows us to assess i) the potential strategic advantage (i.e., performance) from access to multiple domains; ii) the extent to which domain-specific human subgroups have to reconcile decisions that may appear to adversely affect their domain due to issues beyond their domain; iii) the opportunity to support human subgroups through agents being able to classify, contextualize and communicate "unknown unknowns", as represented through risks and responses beyond their domain, as opposed to "known unknowns" within their domain.

Framing human-agent teaming in this way supports *goal-driven coalition information processing*, specifically relating to decisions made in competition with an adversary. We note that agents can potentially provide information to help rationalize the uncertainty for subgroups that are involved from other domains. This will also support human teams in avoiding "surprise" and also relates to the concepts of lateralization between concurrent organizational hierarchies at different levels of command (Subtask 10.1.2). Such agent capability can mitigate well-known human cognitive biases such as in-group bias and cognitive dissonance (Subtask 10.1.1). However, the potential of such human-agent teaming has not been previously explored yet could help clarify principles that support complex multi-domain operations, their unity and coherence in the presence of AI.

175 Restocchi, V., Hill, L., Stein, S., Brede, M., Eshghi, S. (2018). Evaluating Competitive Influence Maximisation Strategies Using an Online Game. https://dais-ita.org/node/2464

176 Four instances are nominally used to represent land, air, sea and cyberspace.

177 https://github.com/openai/multiagent-particle-envs

178 Wai, H. T., Yang, Z., Wang, P. Z., & Hong, M. (2018). Multi-agent reinforcement learning via double averaging primal-dual optimization. In Advances in Neural Information Processing Systems (pp. 9649-9660).

179 Amato, C. (2018, July). Decision-Making Under Uncertainty in Multi-Agent and Multi-Robot Systems: Planning and Learning. In *IJCAI* (pp. 5662-5666).

180 Eriksson, H., & Dimitrakakis, C. (2019). Epistemic Risk-Sensitive Reinforcement Learning. arXiv preprint arXiv:1906.06273.

181 Depeweg, S., Hernández-Lobato, J. M., Doshi-Velez, F., & Udluft, S. (2017). Decomposition of uncertainty in Bayesian deep learning for efficient and risk-sensitive learning. arXiv preprint arXiv:1710.07283.

Task 10.2: Learning and Inferencing in Neuro-Symbolic Hybrids for Uncertainty-Aware Human-Machine Situational Understanding

Primary Research Staff	Collaborators
Alun Preece, Cardiff *[Task Lead]*	Vedran Galetic, Airbus
Angelika Kimmig, Cardiff	Mark Hall, Airbus
Marc Roig-Vilamala, Cardiff	Alistair Nottle, Airbus
Sam Vente, Cardiff	Santiago Quintana, Airbus
Dave Braines, IBM UK	Erik Blasch, AFRL
Supriyo Chakraborty, IBM US	Jonathan Bakdash, ARL
Mani Srivastava, UCLA	Lance Kaplan, ARL
Tianwei Xing, UCLA	Chris Willis, BAE
	Federico Cerutti, Brescia / Cardiff
	Sayyid Faiz, Dstl
	Sam Hepenstal, Dstl
	Gavin Pearson, Dstl
	Alessandra Russo, Imperial
	Paul Sullivan, Intelpoint Inc
	Murat Sensoy, Ozyegin / Cardiff
	Simon Julier, UCL
	Luis Garcia, UCLA

We will advance the capabilities of human-AI collaboration for Coalition Situational Understanding (CSU) by proposing a novel approach where humans, subsymbolic, and symbolic AI-equipped agents collaborate to address complex coalition tasks in support of Multi-Domain Operations (MDO)[182].

[182] See the military relevance section for more details on the topic of MDO and the relevance to this research activity

Background

Here, we go beyond the traditional hierarchical architecture that sees humans interacting only with symbolic AI-equipped agents that in turn leverage subsymbolic AI for achieving human or super-human abilities on specific tasks. Such a traditional architecture is limited because: (1) it is not always the case that symbolic AI is needed for interaction with humans[183]; (2) there are tasks for which a symbolic AI can support a subsymbolic AI agent[184]; and (3) there are tasks for which humans can support symbolic and/or subsymbolic AI agents[185], hence AI agents need to be equipped with the capabilities to learn and reason about human hierarchies and structures.

Technical approach

Our research questions lay the foundations for this paradigm shift, where humans will be seen as other agents in a multi-agent setting as depicted in Figure P10-1. To achieve this vision, we need to understand how to:

1. enable subsymbolic AI agents to share uncertainty-aware representations of insights and knowledge that can then be communicated to symbolic AI agents;
2. equip symbolic AI agents to learn the uncertainty distribution of causal links from data, while being able to share insights to subsymbolic AI agents;
3. develop symbiotic AI techniques to effectively interact with humans, at first by adapting stereotypical behaviors via continuous learning from human-machine teaming activities.

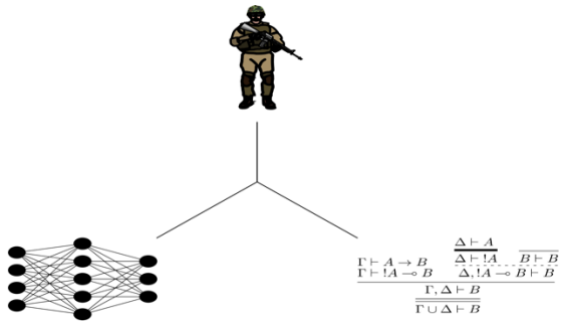


Figure P10-1: A multi-agent non-hierarchical approach to CSU

This task will advance capabilities to contribute to complex coalition tasks in support of MDO[186], where the need for joint and multinational teams and multi-domains is cardinal[187]. It is of paramount importance to provide a coherent view and assessment of operational situations as they happen thus integrating learning and reasoning for CSU in complex, contested environments to inform decision makers at the edge of the network. CSU requires[188] both

183 Ribeiro, Marco Tulio, Sameer Singh, and Carlos Guestrin. "Why should I trust you?: Explaining the predictions of any classifier." Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining. ACM (2016).

184 Jingyi Xu, Zilu Zhang, Tal Friedman, Yitao Liang and Guy Van den Broeck. A Semantic Loss Function for Deep Learning with Symbolic Knowledge, *In Proceedings of the 35th International Conference on Machine Learning (ICML)*, 2018.

185 Phan N, Dou D, Piniewski B, Kil D. A deep learning approach for human behavior prediction with explanations in health social networks: social restricted Boltzmann machine (SRBM+). *Netw Anal Min*. 2016;6:79.

186 Spencer, David K., Stephen Duncan, and Adam Taliaferro. "Operationalizing artificial intelligence for multi-domain operations: a first look." In *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications*, vol. 11006, p. 1100602. International Society for Optics and Photonics, 2019.

187 Training, US Army, and Doctrine Command. "TRADOC Pamphlet 525-3-1 "The US Army in Multi-Domain Operations 2028,"." *Training and Doctrine Command, Ft. Eustis, VA,(6 December 2018), viii–x* (2018).

188 A. Preece, F. Cerutti, D. Braines, S. Chakraborty and M. Srivastava, "Cognitive Computing for Coalition Situational Understanding," in *DAIS 2017 - Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations at IEEE SmartWorldCongress*, 2017.

collective insight—i.e., accurate and deep understanding of a situation derived from uncertain and often sparse data—and collective foresight—i.e. the ability to predict what will happen in the future.

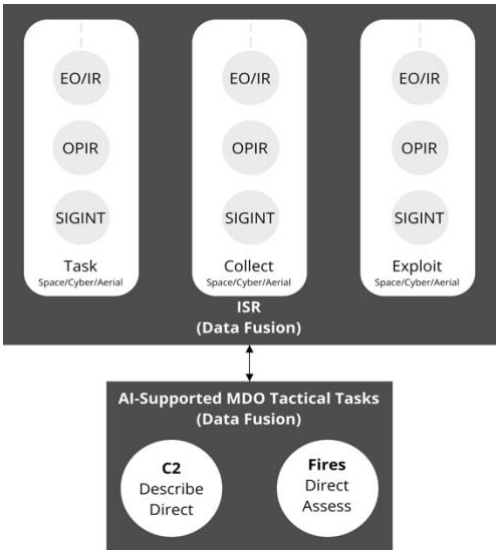


Figure P10-2: Simplified version of the figure from Spencer 2019 (see footnotes). In rectangles symbolic systems; in circles subsymbolic systems; in rounded rectangles hybrid solutions.

CSU depends on human-AI collaboration: machine processes such as AI agents offer powerful affordances in terms of data analytics, but they need to provide levels of assurance (explanation, accountability, transparency) for their outputs, particularly where those outputs are consumed by decision makers without technical training in information science. Current machine learning (ML) approaches are limited in their ability to generate interpretable models (i.e., representations) of the world necessary for CSU[189]. Moreover, these approaches require large volumes of training data and lack the ability to learn from small numbers of examples as people and knowledge representation-based systems do[190]. An ability for domain experts to tell a machine relevant information[191] increases the tempo and granularity of human-AI interactions and the overall responsiveness of the system in meeting mission requirements. We seek to equip coalition machine agents with integrated learning and knowledge representation mechanisms that support CSU while affording assurance (explainability) and an ability to be told key information to mitigate issues with sparse data (tellability).

Such interactions begin to enable both the "Interactivity" and "Autonomy" goals for the DAIS ITA program at the 5-year midway point, as expressed in the original program vision. The proposed research in this task is in the context of rapidly formed coalition teams comprised of human and AI agents, operating at the edge of the network, with limited connectivity, bandwidth and compute resources, in a decision-making role.

[189] B. Lake, T. Ullman, J. Tenenbaum and S. Gershman, "Building Machines That Learn and Think Like People," *Behavioral and Brain Sciences*, pp. 1-101, 2016.

[190] R. Guha, "Towards a model theory for distributed representations," in *2015 AAAI Spring Symposium Series*, 2015.

[191] Note that we do not assume that experts always know all the relevant information, but instead wish to enable the ability to provide such information into the system when it is known, either entirely or in partial form.

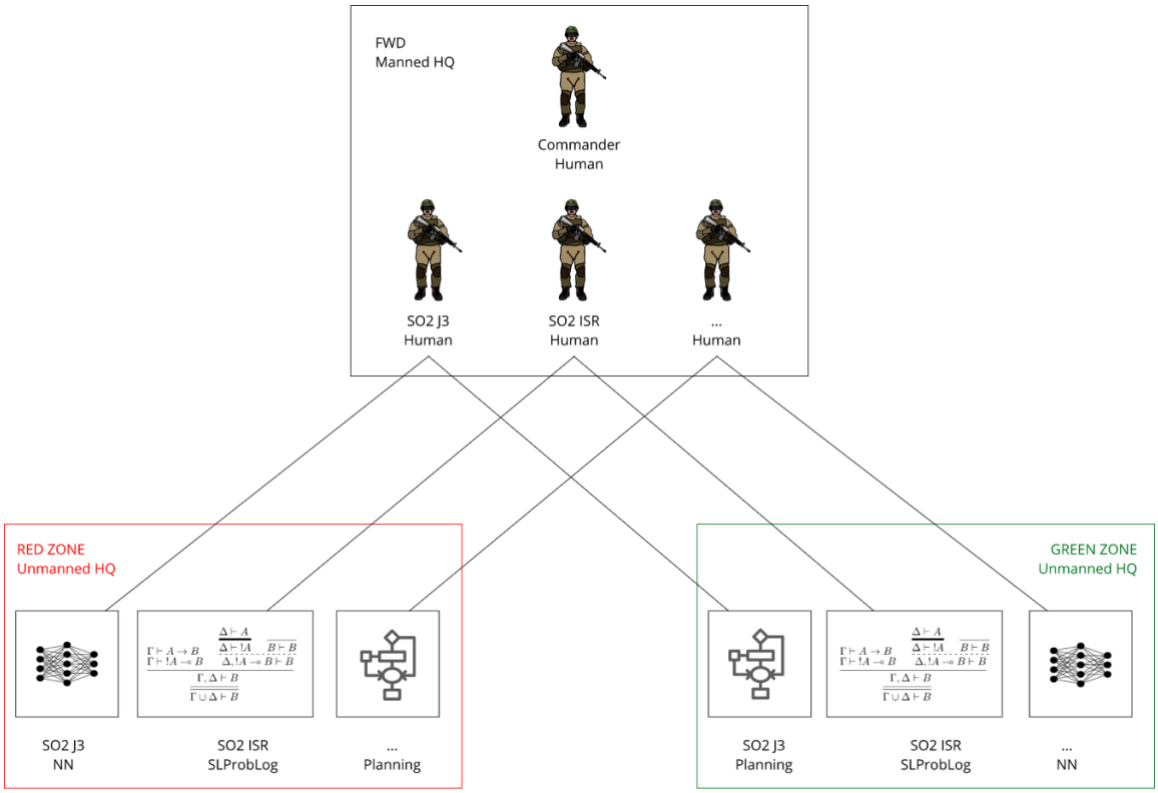


Figure P10-3: Human-Machine Teaming (HMT) in the tactical domain: figure elaborated from Si Pierson et al, 2019 (see footnotes)

Alongside the MDO military context, the research goals fit directly with the Human Machine Teaming (HMT) perspective in the tactical domain vignette within the DAIS-ITA scenario[192] with techniques and capabilities arising from this research being directly relevant to supporting that vignette. The vignette is discussed further in the military relevance section and is summarized in Figure P10-3.

In our earlier research we have built significant foundations for the neuro-symbolic hybrid environment, including multi-agent learning[193], evidential deep learning[194], probabilistic logic programming[195], forward inferencing architectures where the output of a neural network was fed into probabilistic logic engine to detect events with complex spatiotemporal properties[196].

The research proposed in this task directly addresses these challenges and the three explicit subtasks that comprise the technical details are described in detail below.

[192] Full details about the DAIS ITA scenario can be found on CENSE, but for simplicity the reference used throughout this whitepaper is the recent SPIE DCS paper on the topic of the DAIS ITA scenario.

[193] Xing, Tianwei, Sandeep Singh Sandha, Bharathan Balaji, Supriyo Chakraborty, and Mani Srivastava. "Enabling Edge Devices that Learn from Each Other: Cross Modal Training for Activity Recognition." In *Proceedings of the 1st International Workshop on Edge Systems, Analytics and Networking*, pp. 37-42. ACM, 2018.

[194] Sensoy, Murat, Lance Kaplan, and Melih Kandemir. "Evidential deep learning to quantify classification uncertainty." In *Advances in Neural Information Processing Systems*, pp. 3179-3189. 2018.

[195] Cerutti, Federico, Lance Kaplan, Angelika Kimmig, and Murat Şensoy. "Probabilistic Logic Programming with Beta-Distributed Random Variables." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 7769-7776. 2019.

[196] Hu, Zhiting, Xuezhe Ma, Zhengzhong Liu, Eduard Hovy, and Eric Xing. "Harnessing deep neural networks with logic rules." *arXiv preprint arXiv:1603.06318*, 2016.

Subtask 10.2.1: Uncertainty-aware subsymbolic/symbolic reasoning

Goal: Address the challenge of sharing relevant CSU knowledge between coalition partners, by creating a neural architecture that, ideally for any learning task, will force the creation of a semantic graph-embedding representation of CSU knowledge.

Prior works have shown that logic may be distilled into the learning process[197] or by constraining neural network outputs by integrating a probabilistic interpretation of the logic into the semantic loss function[198]. The notion of how well a logical formula is satisfied being incorporated into the semantic loss function has also been applied in the context of learning the logical rules themselves[199]. However, bridging the gap between providing logical assurances for propositional statements and the inferencing prowess of machine learning has not been generalized or scaled to complex applications. We aim to augment the recent result in[200] with a latent representation that can be reused by a symbolic approach as proposed in[201]. The overall aim of this subtask is the combination of logic with machine learning[202, 203] and how to achieve this in a coalition setting.

FigureP10-4: Uncertainty-aware processing, taken from Wang, 2018 (see footnotes).

In[18], and as shown in Figure P10-4, the authors introduced a differentiable (smoothed) maximum satisfiability (MAXSAT) solver that can be integrated into the loop of larger deep learning systems. By integrating this solver into end-to-end learning systems, it is possible to learn the logical structure of challenging problems in a minimally supervised fashion. However, the input to the system must be defined a priori. In this whitepaper we want to address this limitation, exploiting a technique first introduced in[204], where the authors propose an unsupervised architecture combining deep learning and classical planning.

197 Hu, Zhiting, Xuezhe Ma, Zhengzhong Liu, Eduard Hovy, and Eric Xing. "Harnessing deep neural networks with logic rules." *arXiv preprint arXiv:1603.06318* (2016).

198 Xu, Jingyi, Zilu Zhang, Tal Friedman, Yitao Liang, and Guy Van den Broeck. "A semantic loss function for deep learning with symbolic knowledge." *arXiv preprint arXiv:1711.11157*, 2017.

199 Bombara G, Vasile C-I, Penedo F, Yasuoka H, and Belta C. A Decision Tree Approach to Data Classification using Signal Temporal Logic. In Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control (HSCC '16), 1-10. 2016.

200 Wang, Po-Wei, Priya L. Donti, Bryan Wilder, and Zico Kolter. "SATNet: Bridging deep learning and logical reasoning using a differentiable satisfiability solver." *In Proceedings of ICML, 2018.*

201 Asai, Masataro, and Alex Fukunaga. "Classical planning in deep latent space: Bridging the subsymbolic-symbolic boundary." In *Thirty-Second AAAI Conference on Artificial Intelligence*. 2018.

202 Hu, Zhiting, Xuezhe Ma, Zhengzhong Liu, Eduard Hovy, and Eric Xing. "Harnessing deep neural networks with logic rules." *arXiv preprint arXiv:1603.06318* (2016).

203 Xu, Jingyi, Zilu Zhang, Tal Friedman, Yitao Liang, and Guy Van den Broeck. "A semantic loss function for deep learning with symbolic knowledge." *arXiv preprint arXiv:1711.11157*(2017).

204 Asai, Masataro, and Alex Fukunaga. "Classical planning in deep latent space: Bridging the subsymbolic-symbolic boundary." In *Thirty-Second AAAI Conference on Artificial Intelligence*. 2018.

We therefore will:

1. create a propositional state representation of the input of a MAXSAT layer using a Variational Autoencoder that generates a discrete latent vector;
2. adapt this architecture for an arbitrary learning problem, thus forcing the neural network to produce as a by-product the semantic graph-embedding representation that can be interpreted as the input of a MAXSAT problem.

Subtask 10.2.2: Learning and reasoning with uncertainty-aware logic programming

Goal: Address the challenge of generating robust CSU knowledge in contested coalition environments, by creating novel mechanisms for symbolic AI agents to rapidly learn the uncertainty distribution of casual links from (often sparse) data, while being able to share insights to subsymbolic AI agents.

The goal of this subtask is to enable SLProblog[205] to learn uncertainty-aware parameters as well as causal links from partial observations of data. Learning from partial interpretations is a common setting in statistical relational learning, which has so far not yet been studied in its full generality for uncertainty-aware programming languages (cf.[206]). In this task we propose to overcome such a limitation by introducing an estimator that uses an Expectation-Maximization (EM) framework that iteratively maximizes a likelihood function at the end of each timeslot. This posterior belief is then passed as a prior to the next slot allowing incremental processing of data in that window without revisiting data from the past. Following[207], posterior belief will then be derived from the Cramer Rao lower bound: the variance of any unbiased estimator is bounded by the inverse of Fisher information matrix, which measures the amount of information an observable random variable X carries about an unknown parameter.

As per the second enhancement, we will expand on[208], where a differentiable version of ProbLog is used for end-to-end training of a logical layer on top of a neural network. In particular, we will expand on research developed during the BPP18 with learning of early indicators of violence[209].

We therefore will:

1. create a hybrid symbolic/subsymbolic approach to share insights, building on earlier BPP18 research;
2. learn parameters for a SLProbLog program from partial observations using the EM framework.

Subtask 10.2.3: Human-machine system architecture for uncertainty-aware CSU

Goal: Address the challenge of enabling rapid exploitation of adaptive CSU knowledge to inform decision-making across coalitions, by creating system architectures to enable demonstrable synergy between machine and human agents for actionable insight and foresight in a contested environment. Note: this subtask is explicitly focused on the specific subset of human-machine synergies enabled by the results of the previous two subtasks.

Throughout our earlier research into CSU we have identified the need for the agile integration of human and machine agents from across coalition partners into dynamic and responsive teams. We have proposed "Human-Agent Knowledge Fusion" (HAKF) as a capability to support this deep interaction, comprising bi-directional information

[205] Cerutti, Federico, Lance Kaplan, Angelika Kimmig, and Murat Şensoy. "Probabilistic Logic Programming with Beta-Distributed Random Variables." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 7769-7776. 2019.

[206] Fierens, Daan, Guy Van den Broeck, Joris Renkens, Dimitar Shterionov, Bernd Gutmann, Ingo Thon, Gerda Janssens, and Luc De Raedt. "Inference and learning in probabilistic logic programs using weighted Boolean formulas." *Theory and Practice of Logic Programming* 15, no. 3 (2015): 358-401.

[207] Cui, Hang, Tarek Abdelzaher, and Lance Kaplan. "Recursive Truth Estimation of Time-Varying Sensing Data from Online Open Sources." In *2018 14th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 25-34. IEEE, 2018.

[208] Manhaeve, Robin, Sebastijan Dumancic, Angelika Kimmig, Thomas Demeester, and Luc De Raedt. "Deepproblog: Neural probabilistic logic programming." In *Advances in Neural Information Processing Systems*, pp. 3749-3759. 2018.

[209] Vilamala, Marc Roig, Liam Hiley, Yulia Hicks, Alun Preece, and Federico Cerutti. "A Pilot Study on Detecting Violence in Videos Fusing Proxy Models." in *22nd International Conference on Information Fusion (FUSION)*, 2019.

flows of "explainability" and "tellability" thereby enabling meaningful communication between AI and humans[210] as shown in Figure P10-5. During BPP18 this HAKF capability was extended to support "Conversational Explanations"[211], focused so far mainly on the interpretability flow, enabling AI agents to provide explanations of results arising from complex machine/deep learning classifications.

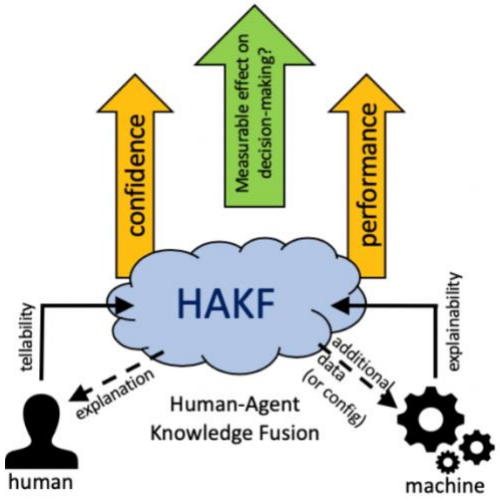


Figure P10-5: Human-Agent Knowledge Fusion for improved confidence and performance in support of better decision-making.

In this subtask we add human interaction to the distributed symbolic/subsymbolic integration from the previous two subtasks. We will establish the minimum set of common language that the various human and AI agents need to master to ensure effective communication for a given task. To support *intuitive machine processable representations* in the context of *dynamic context-aware gathering and information processing services*, we will pay particular attention to the human consumability of machine generated information, especially in the context of conversational interaction. This common language must be capable of conveying uncertainty and the appropriate structures to achieve integration with the subsymbolic layers, as identified in subtasks 10.2.1 and 10.2.2, as well as more traditional semantic features relevant to the domain. We do not limit ourselves to purely linguistic forms; novel visual or diagrammatic notations, or indeed other communication techniques, may be relevant as part of the solution.

We will consider the case of automated negotiations between various autonomous agents, some of which will be humans. At the same time, humans themselves can be the object of a learning task: their own behavior can potentially be nudged in specific directions if the machine agent learns enough about the individual human agent (or human agents in general) to infer the impact of suggestions or changes. In addition, machine agents might need to identify the best fit among the human agents for a given task, with historical data helping them towards this goal. Such symbiotic AI techniques can be used to more effectively interact with the humans, at first by adapting stereotypical behaviors via continuous learning from human-machine interactions.

Such a complex and dynamic hybrid setting is particularly risky and prone to exploitation in a contested environment, hence the need to integrate the uncertainty-aware and probabilistic capabilities from subtasks 10.2.1 and 10.2.2. All of this much be achieved in a tempo that is appropriate to the decision-making task and the involvement of the human users, with machine agents able to support real-time interaction.

We therefore will:

[210] Braines, D., Preece, A., & Harborne, D. (2018). "Multimodal Explanations for AI-based Multisensor Fusion." In NATO SET-262 RSM on Artificial Intelligence for Military Multisensor Fusion Engines in Budapest, Hungary.

[211] Tomsett, R., Braines, D., Harborne, D., Preece, A., & Chakraborty, S. (2018). "Interpretable to Whom? A Role-based Model for Analyzing Interpretable Machine Learning Systems." In ICML Workshop on Human Interpretability in Machine Learning (WHI 2018), Stockholm, Sweden.

1. define novel human-machine system architecture(s) supporting conversational interfaces that can build a model of other interacting agents, irrespective of whether they are humans or machines;
2. create a negotiation protocol for rapidly exchanging CSU knowledge between human and machine coalition agents in contested, uncertain environments.

Task 10.3: NSPL – A Neural-Symbolic Learning of Generative Policies in Coalition Environments

Primary Research Staff	Collaborators
Alessandra Russo, Imperial *[Task Lead]*	Brian Rivera, ARL
Mark Law, Imperial	John Melrose, DSTL
Elisa Bertino, Purdue	Dinesh Verma, IBM US
Ankush Singla, Purdue	Graham White, IBM UK
Daniel Cunnington, IBM UK	Geeth de Mel, IBM UK
Seraphin Calo, IBM US	Jorge Lobo, Imperial

In coalition environments, one of the key challenges is how to support "distributed intelligence" in a secure and context-aware manner. The emphasis here is on autonomous, dynamic adaptation of devices, in response to changes in the (coalition) context in which they operate, whilst maintaining robustness and guarantee optimal decision-making during a distributed coalition intelligence task. For example, in the case of rapidly forming coalition teams that comprise of humans and devices operating at the edge of the network with limited connectivity, devices need to autonomously generate and adapt their policies depending on the contextual information of the ad-hoc human-machine teams and taking also into account any existing security constraints. These policies have to be learnable and interpretable in order to provide useful information for a better coalition situation understanding (CSU). The open research question is how to enable devices (e.g. autonomous agents of an ad-doc team) to operate with minimal human intervention in highly heterogeneous, dynamic and evolving contexts whilst maintaining a level of security to guarantee robust distributed analytics.

Solutions have been proposed ([1]–[4]) for *context-aware learning of policies*. But these approaches assume data to be expressed in a structured form (e.g. csv, tabular). In practice, contextual information is very heterogeneous, ranging from unstructured data, such as images and audio data, to structured data, such as type of devices, trust levels, etc. Furthermore, the nature of the distributed coalition intelligence presupposes such information to be often collected by multiple devices collaborating in a coalition, or ad-hoc human-machine team, mission, depending on security, resource availability, tactical plans. So, *understanding context* requires techniques that are capable of extracting key features from multimodal datasets, and performing this learning process in a federated fashion using data and existing security policy constraints from other coalition members. Features extracted from contextual information should then be used by the devices to dynamically learn context-dependent policies. These policies need to be amenable to analysis and human interpretation in order to facilitate their automated evaluation (to assess when a new learning step is needed) and allow for human inspection over policy-driven decisions. These are crucial aspects of dynamic adaptation, necessary for the process to be robust, optimal and worth of human confidence. The coalition gap is therefore the need to develop context-aware policy learning in a distributed intelligence setting where policies are learned from multi-modal data. The learning method has to be able to combine well-known advantages of "black box" machine learning

approaches for feature extraction from unstructured data with "white box" symbolic learning methods for the computation of interpretable and optimal policies.

Background

Generative policies have been proposed as a method for addressing the open research question of autonomous, dynamic adaptation of coalition systems and devices in a context-aware manner. During BBP18 significant advances have been made on the development of a formal framework for generative policy models that enables autonomous devices to learn and generate context-dependent optimal policies in response to changes in the coalition environment in which they operate. A new class of context-sensitive grammars, called Answer Set Grammars (ASG), has been developed as a generative policy model, and a state-of-the-art symbolic learning system, called ILASP[212] has been used to solve the task of learning generative policy models from given labelled (positive and negative) examples of past decisions, and related contextual information[213].

Also, a new system architecture for generative policies has been developed[214] that seamlessly integrates in autonomous devices policy learning, adaptation, decision and enforcement points. The framework and architecture have been applied in the context of coalition information sharing[215], access control[216] and logistical resupply of coalition forces[217], demonstrating the flexibility of ASG as a generative policy model and the ability to learn symbolically from few examples, whilst explaining the learned outcomes and capturing human-driven policy rules. Complexity results on (i) deciding whether a given policy is accepted or not by the learned generative policy model and (ii) deciding whether a learned generative policy model provides optimal policies in a given context, supported by successful applications of this approach to both synthetically generated datasets[218] and real world datasets (e.g. Amazon data), have demonstrated that ASG and symbolic learning can allow devices to automatically learn context-sensitive generative policy models and instantiate optimal context-dependent policies in response to contextual changes. A recent study[219] has evaluated the performance and suitability of a symbolic learner within the generative policy model architecture for generating policies using real-world datasets, compared to mature statistical learning algorithms. The ASG-based symbolic learner has demonstrated equal if not better performance on small problem sizes whilst being fully explainable. The advantage of this approach, from the point of view of CSU, is that policies instantiated from learned generative policy models are amenable to formal analysis for verification of completeness, correctness, conflict detection and most importantly, they are interpretable by humans for inspection.

[212] Mark Law, Alessandra Russo, and Krysia Broda. Inductive Learning of Answer Set Programs from Noisy Examples. In Advances in Cognitive Systems, 2018. Available online: https://arxiv.org/pdf/1808.08441.pdf

[213] M. Law, A. Russo, B. Elisa, B. Krysia, and L. Jorge, "Representing and learning grammars in answer set programming." In AAAI, 2019. Available online: https://dais-ita.org/node/2512

[214] S. Calo, I. Manotas, G. de Mel, D. Cunnington, M. Law, D. Verma, A. Russo, and E. Bertino, "AGENP: An ASGrammar-based GENerative policy framework," in Policy-Based Autonomic Data Governance. Springer, Sep. 2019, pp. 3–20. Available online: https://daisita.org/node/2483

[215] D. Cunnington, G. White, M. Law, and G. de Mel, "A demonstration of generative policy models in coalition environments," in Advances in Practical Applications of Survivable Agents and Multi-Agent Systems: The PAAMS Collection. Springer International Publishing, 2019, pp.242–245. Available online: https://dais-ita.org/node/3408

[216] S. Calo, D. Verma, S. Chakraborty, E. Bertino, E. Lupu, and G. Cirincione, "Self-generation of access control policies," in Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies, ser. SACMAT '18. New York, NY, USA:ACM, 2018, pp. 39–47. Available online: https://dais-ita.org/node/2187

[217] G. White, J. Ingham, M. Law, and A. Russo, "Using an ASG based generative policy to model human rules," 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Jun. 2019. Available online: https://dais-ita.org/node/3438

[218] G. White, J. Ingham, M. Law, and A. Russo, "Using an ASG based generative policy to model human rules," 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Jun. 2019. Available online: https://dais-ita.org/node/3438

[219] G. White, D. Cunnington, M. Law, A. Russo, and E. Bertino, "A comparison between statistical and symbolic learning approaches for generative policy models". Submitted for review at ICMLA 2019. Available online: https://dais-ita.org/node/3898

Technical Approach

Existing results assumes contextual information to be composed of structured data, with meta-data defined by the policy manager. The approach has thus far focused mainly on text-based data either in string or tabular format. Although somewhat reasonable, this assumption is limited within the context of ad-hoc coalition teams. In coalition environments, devices are equipped with sensors that collect unstructured data (images, audio, video) and need to work together to gain a better understanding of the context and situation in which they operate. These unstructured data are valuable sources of contextual information which need to be taken into account when learning generative policy models, in order to guarantee the generation of best policies for given coalition operations. In this task we advocate that *hybrid machine learning* is more appropriate for automatically learning context-aware generative policy models. This presents different technical challenges related to the coalition environments and to the actual technical development of the machine learning solution.

From the coalition environment point of view the technical challenges are related primarily to resource constraints and low bandwidth between devices. Devices do not have large computational power, so computation at-the-edge for understanding contexts need to be economical from a computational point of view. Communications between devices are unreliable and may have limited bandwidth. It will most of the time be unfeasible to exchange large quantities of data.

Machine learning solutions for extracting contextual information have to be robust in the presence of lack of information or constrained resources. From a research point of view, the main technical challenge is the *integration* of deep machine learning with symbolic learning into a seamless *neural-symbolic learning approach*, in a way that preserves their respective advantages whilst addressing the challenges of a coalition setting. The current AI state-of-the art in hybrid machine learning methods has seen either solutions that harness Deep Neural Network (DNN) architectures with logical constraints (e.g. Logic Tensor Networks[220, 221]) in order to enhance the classification performance of DNN, or pure neural-symbolic architecture engineered specifically to perform reasoning or rule-learning (e.g.[222]). Both methodologies, although applicable to raw data, such as text and images, do not allow interpretability of their learned models.

This task aims to build a *novel neural-symbolic approach for learning policies* that will enable:

1. richer contextual and situational understanding by learning symbolic abstractions from multi-modal sensor data (e.g. imagery, audio, video), which can be used as contextual information for policy learning, in a "*forward propagation fashion*";
2. a "*plug and play*" feature of the architecture that allows the neural component to be replaced by existing federated learning components, to support symbolic policy learning at the edge of an SDC network.
3. decreases in the computational resources required for learning policies from multi-modal datasets, by means of an end-to-end learning style that will exploit the symbolic learning process to harness the neural-symbolic feature abstraction from raw datasets.

In order to achieve the objectives outlined above, we envisage a neural-symbolic architecture composed of two main components: a *neural component* that learns symbolic abstractions from multimodal contextual data and a *symbolic component* that uses these symbolic abstractions to learn context-aware optimal policies from past positive and negative decisions as labelled examples. The integration of these two components will be investigated in two stages. Firstly, a *forward propagation* approach will be developed and evaluated, which will focus on training neural components to classify symbolic abstraction from unstructured datasets. These abstractions will be given to the symbolic learner as contextual information with fixed learned weights, and optimal context-dependent policies will be learned, which will maximise coverage of given labelled examples. In the second stage a *fully integrated end-to-end approach* will be explored in which the learning of symbolic abstractions from raw data will be done together with the learning of symbolic policies, by means of forward and backward propagations through the two neural and

[220] Luciano Serafini, Artur d'Avila Garcez, Logic Tensor Networks: Deep Learning and Logical Reasoning from Data and Knowledge. Available online: https://arxiv.org/abs/1606.04422

[221] Zhiting Hu, Xuezhe Ma, Zhengzhong Liu, Eduard Hovy, Eric Xing , Harnessing Deep Neural Networks with Logic Rules, ACL 2016. Available online: https://arxiv.org/abs/1603.06318

[222] Tim Rocktäschel, Sebastian Riedel. End-to-End Differentiable Proving, NIPS 2017. Available online: https://arxiv.org/pdf/1705.11040.pdf

symbolic components, guided by an appropriately defined notion of a loss function in terms of coverage of labelled examples of past context-aware policy decisions.

Subtask 10.3.1: Hybrid Neural-Symbolic Learning of Generative Policies

The high-level architecture is given in Figure P10-6. We will explore first a simple architecture where structured and unstructured data are given in input as contextual information together with past policy decisions relevant to that context and a generative policy model is learned. One of the key technical challenges will be the identification of the symbolic abstractions that will need to be learned from the contextual information. We will assume on a first instance that these are predefined and given as templates to the architecture. We will then explore if they can be directly learned from the unstructured data. We will use a "plug-and-play' approach in which, depending on the type of unstructured data (images, audio, video), different neural components will be used and where possible pretrained ones. Also, on a first instance, the architecture will be assumed to be a learning system local to the device, making it therefore capable of performing contextual understanding *and* policy learning. The device will be assumed to have full access to the relevant context and associated unstructured data. Through experimentation, the suitability of various neural models and architectures for contextual understanding (e.g. CNNs, Fast R-CNN, LSTM) will be explored. With this approach, the neural components are trained in isolation and at policy learning time their weights remain fixed. At policy generation time, the current contextual situation is passed to the architecture whose trained neural component will extract relevant features that together with the learned generative policy model will lead to the appropriate context-sensitive policy instantiation. The policy generation architecture is shown in Figure P10-8. In this approach re-learning can occur because (i) the generative policy model does not have policies related to the current context (i.e. the model is incomplete), or because the neural classifier is not able to classify relevant features from the current context. In the first case a re-learning of a new generative policy model is triggered, in the latter case the classifier is retrained to classify the new contextual data. We expect the reclassification of the neural component to be faster as it will leverage its pretrained model. In the case of limited computational resources, pruning techniques, to make CNN amenable for deployment at the edge, and/or more "light-weight" machine learning methods (e.g., Random Forest) will be used and trained to learn contextual abstraction. The technical challenges include (i) how to identify the level of feature abstraction required and how to choose which features to abstract to ensure the symbolic learning task can be solved with maximum explainability using the available computational resources; and (ii) how to engineer the symbolic ILASP learning step to support contextual policy learning with contextual features that are uncertain.

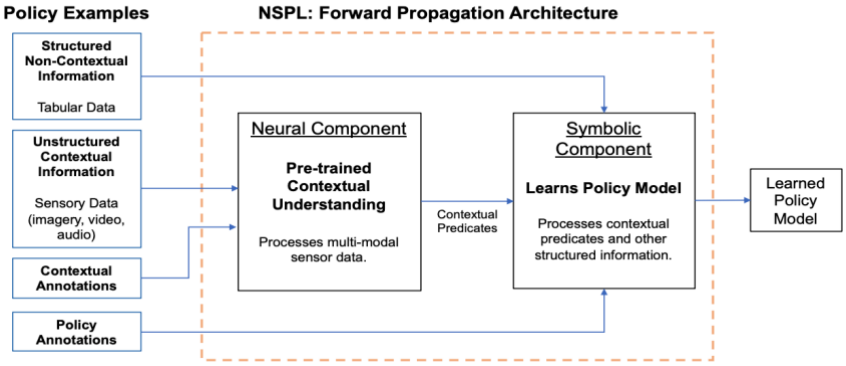


Figure P10-6: Hybrid Neural-Symbolic Learning of Generative Policies

We will evaluate the performance of our hybrid approach versus a pure deep learning approach and also evaluate the impact of using pretrained models when a re-learning step is performed. The "plug-and-play'' characteristic of our approach will facilitate a natural extension to the case of distributed intelligence. This will be realized by extracting the neural component from the device and move it towards external sensors at the edge of the network, enabling federated contextual understanding where symbolic abstractions from unstructured data of different modality can be

shared between coalition partners without sharing the raw contextual data (e.g. a CCTV camera image). The second technical challenge is therefore how to engineer such an extension of our hybrid architecture in a way that take into account environmental constraints such as unreliable or low-bandwidth communication between systems and operational directives such as the requirement to generate a policy within a certain amount of time.

Subtask 10.3.2: End-to-end Neural-Symbolic Learning of Generative Policies

The hybrid aspect of our approach makes it particularly suited for integrating, but in a modular fashion, prior knowledge and symbolic learning during the training phase of the neural component. The second stage of our task will develop and evaluate a *fully integrated* neural-symbolic approach for learning generative policy models, where background knowledge and level of accuracy of the learned policies can be used to improve the learning performance of our neural component through back-propagation. With a fully integrated approach, the neural-symbolic generative policy model would be trained end-end (i.e. using both forward and backward passes over neural and symbolic components) based on labelled examples of policy decisions, as oppose to training each component in isolation. This enables the symbolic learning component to semantically guide the neural network component through back-propagating miss-classified policy examples. The high-level architecture is shown in Figure P10-7.

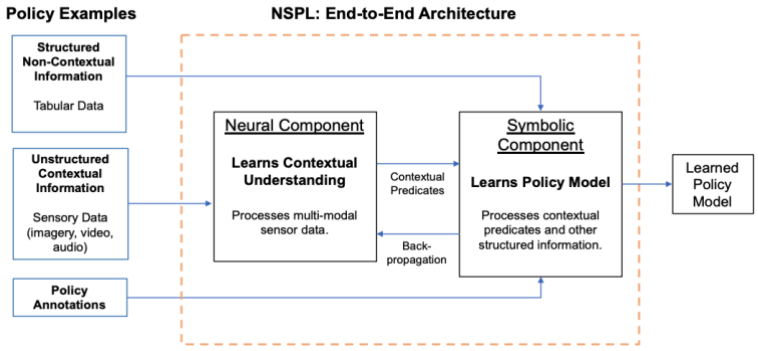


Figure P10-7: Fully Integrated Neural-Symbolic Learning of Generative Policies

In this case, we will concentrate on local autonomous system, where back-propagation can freely occur between the symbolic and neural components based on policy examples. Through experimentation, this integrated approach will be evaluated and compared against the previous *hybrid* neural-symbolic generative policy learner, as well as pure symbolic and pure neural approaches. Our hypothesis is that due to the ability to back-propagate background knowledge and partially learned policies, the performance of the neural component should improve also in the case of fewer contextual data making the *integrated* neural-symbolic approach outperform other methods for learning generative policies. The technical challenge in this case will be how to define a differentiable loss function in terms of coverage of examples for our symbolic learner in a way that it can be backpropagated through the symbolic learner and guide the learning of more accurate policies based on more accurate contextual abstractions generated by the neural component.

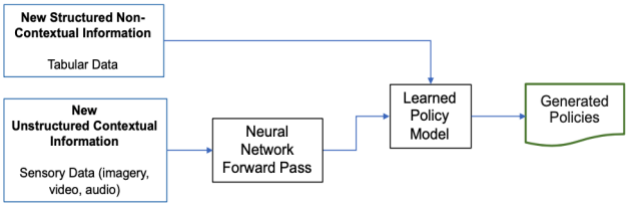


Figure P10-8: Policy Generation

Validation and Experimentation

Task 10.1

Subtask 10.1.1 involves using generative computational modeling approach (see BPP18[223]). This approach translates social and psychological theories for individual-agent decision-making into a computational form (e.g., cognitive dissonance theory, in-group bias), led by Yale and Cardiff. This allows us to consider the group-level effects that are structured in accordance with coalition problems and multiple domains. Extensive simulation will be used, staging the inclusion of complexity, implemented using supercomputing facilities[224]. Scrutiny by sociologists (Dstl) and psychologists (Yale, ARL) will support rigor in model development.

Subtask 10.1.2 involves developing and examining protocols for information sharing while varying the underlying network structures that interconnect the coalition (ARL). This will involve both simulation and human participation. Where appropriate, scenarios will be shared with Subtask 10.1.1, and created with military advice (ARL, Dstl). Human experimentation (ARL, Yale) will be supported by extensive simulation that enables wide-ranging problem parameters to be examined. Metrics for model assessment will be co-developed (ARL, Cardiff, IBM-UK) to ensure that different and diverse forms of optimality are assessed. This is particularly important when assessing trade-offs.

Subtask 10.1.3 will examine how machine-based agents function across multiple domains as opposed to framing decisions based on a single domain only (IBM-US-UK, Cardiff). The implications for human actors in particular coalition subgroups (Subtask 10.1.2) will be assessed, who may observe seemingly counter-intuitive agent decisions, as framed from a domain-focused perspective. Validation will involve metrics that capture different forms of variance, e.g., cognitive friction that subgroups may encounter (Yale, Subtask 10.1.1), and performance against an adversary who adopts heuristic strategies (Cardiff). Structured experiments will build-up from a single domain, adopting a simple game for interaction between the coalition and adversary. Existing reinforcement learning techniques[225] will be engaged (IBM-UK, IBM-US).

Task 10.2

Our validation approach will test whether our research goals have been advanced or achieved: Have we increased the capability to rapidly share CSU knowledge between coalition partners, and can we more rapidly generate the CSU knowledge in contested environments from sparse data sources? Can human agents in the system use this CSU knowledge for decision making and show improved foresight and insight?

We intend to use temporal datasets of simple scalar sensor modalities and, once we have refined our methods, consider time series data of complex modalities. Candidate data sets include:

[223] Whitaker, R. M., Colombo, G. B., & Rand, D. G. (2018). Indirect reciprocity and the evolution of prejudicial groups. *Nature Scientific reports*, *8*(1), 13247.

[224] Whitaker is Director of Supercomputing Wales, a £15M investment in research supercomputing facilities for Wales, UK.

[225] https://github.com/openai/multiagent-particle-envs

- http://crowdsignals.io (large set of rich longitudinal mobile and sensor data recorded from a demographically diverse cohort)
- http://ailab.wsu.edu/casas/datasets/ (a multimodal longitudinal sensor dataset capturing complex events corresponding to activities of daily living)
- Our own multimodal UK traffic dataset[226] (including video imagery and natural language)
- Our own multimodal dataset created for the AFM2019 T5.1 demonstration, and possibly the UCF-Crime dataset[227] that collects publicly shared CCTV videos of violent activities.

In our creation of novel human-machine system architectures we will run experiments to yield measurable "synergistic" outcomes in the uncertainty-aware CSU context (where synergy is an increased team capability when compared to individual agent performance). Such measurements will include the degree to which symbolic/subsymbolic integration has been achieved within the layers of the system, and the degree to which parameters can be learned from partial observations. As a starting point, we will define decision-making tasks and synergy metrics in collaboration with the military advisors (MAs) such that we can then conduct (a) a pilot study with a small group of individuals from our target domain (selected with help from the MAs) to be followed by a study on a proxy task (having characteristics similar to the actual task) involving participants recruited from a wider population, e.g., undergraduate students.

Our experiments will also carefully consider trust of humans in their machine counterpart; cooperation & interoperability of manned/unmanned sensors (including prioritization); effective communication between AI agents and humans in order to make decisions on potential targets.

We therefore plan to measure each of the outcomes from the subtasks, but also bring together each of these into a unified system that can be observed in the context of the overall goal of improved uncertainty-aware CSU.

Task 10.3

The proposed neural-symbolic approach developed in this task will be validated and evaluated with respect to three main metrics: accuracy, training time and explainability. On a first instance, a synthetically generated dataset will be used to validate the accuracy of the symbolic abstraction performed by the neural component and its forward propagation into the symbolic learning component. For this initial task we envisage to use unstructured text and images together with synthetically generated policy outcomes. To identify relevant datasets, we will investigate existing neural-symbolic learning techniques (e.g. DeepProbLog[228], LTN[229], NTP[230]) and related datasets (e.g. PASCAL[231], CLEVR[232], and VisualGenome[233]). Where possible we will use these existing techniques as comparative benchmarks for our architecture. We will also use real-data and simulated data generated in P7 to evaluate the learning of policies for control and management of SDC infrastructures and related security policies. In this case we will compare the accuracy (precision and recall) and computational time of our neural-symbolic learning techniques with respect to pure end-to-end statistical learning, end-to-end symbolic learning, multi-agent reinforcement learning and federated

[226] A. Nottle, D. Harborne, D. Braines, M. Alzantot, S. Quintana-Amate, R. Tomsett, L. Kaplan, M. Srivastava, S. Chakraborty and A. Preece, "Distributed opportunistic sensing and fusion for traffic congestion detection," in DAIS 2017 - Workshop on Distributed Analytics InfraStructure and Algorithms for Multi-Organization Federations at IEEE SmartWorldCongress 2017, 2017.

[227] Sultani W, Chen C, and Shah M. Real-world Anomaly Detection in Surveillance Videos. In IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[228] R. Manhaeve, S. Dumancic, A. Kimmig, T. Demeester, and L. De Raedt, "DeepProbLog: Neural probabilistic logic programming," in Advances in Neural Information Processing Systems, 2018, pp. 3749–3759.

[229] Luciano Serafini, Artur d'Avila Garcez, Logic Tensor Networks: Deep Learning and Logical Reasoning from Data and Knowledge. Available online: https://arxiv.org/abs/1606.04422

[230] Tim Rocktäschel, Sebastian Riedel. End-to-End Differentiable Proving, NIPS 2017. Available online: https://arxiv.org/pdf/1705.11040.pdf

[231] http://host.robots.ox.ac.uk/pascal/VOC/

[232] https://cs.stanford.edu/people/jcjohns/clevr/

[233] http://visualgenome.org

policy learning developed in Tasks 7.1 and Task 7.2. We will also evaluate the approach in the context of CSU using data generated in Task 10.2. Learned policies will be about information sharing conditional to relevant contextual information and situation-aware information. As for the explainability metric, none of the existing neural-symbolic learning techniques that have been proposed in the literature, are capable of supporting neural-symbolic rule learning. So, we will be able only to evaluate our approach against pure symbolic learning methods when the contextual information is structured. We expect, however, the outcomes of the validation of our approach to provide first challenging benchmarking results for the AI community in general.

The second evaluation stage will be based on the end-to-end neural symbolic extension of our approach. We will in particular evaluate (i) the performance of the end-to-end training versus the forward propagation approach, (ii) the impact on accuracy of the distributed context-aware learning, with and without pruning methods in order to accommodate restricted computational power at the edge of the network, and (iii) effectiveness of the neural-symbolic approach on solving policy learning tasks that have been found to be too challenging for pure symbolic learning method[234]. The evaluation will take into account various scenarios: (i) logistical resupply and (ii) ad-hoc human-machine teams. In the logistical resupply scenario, multi-modal sensor data will include CCTV cameras and microphones to capture image and audio-based data respectively and learned policies will be about decisions of safe and secure actions to take (e.g., re-route, deploy ground troops or deploy a surveillance UAV). For training, we will use available datasets that will emulate contextual situations, such as urban CCTV camera where certain objects will indicate the presence of an enemy vehicle, the Urban Sounds: audio samples of varying sounds alongside an accompanying taxonomy[235], open source dataset of live CCTV images and video[236], which combines video and audio data; and tabular structured data Adult Income and Forest Cover[237]. In the scenario of CSU, we will learn policies for data sharing when contextual information is extracted by CSU approaches described in Task 10.2. We will evaluate our approach by assessing the impact that learned policies have on CSU when learned policies are used as constraints on the symbolic inference for CSU.

Military and DAIS ITA Relevance

This project addresses a forward-looking military context that US-UK coalitions face in future. Each task contributed to this effort in a particular way. The approach of Task 10.1 involves i) *internal coalition operation*, ii) the context of *multi-domain operations (MDO)*, and *iii) impact of future game-playing AI systems upon the coalition.*

Coalitions represent a complex organizational structure that co-joins traditionally hierarchical operations. Through Subtasks 10.1.1 and 10.1.2 we aim to support insights into policy and interventions that enable coalitions to function more effectively – in particular being less susceptible to fracturing, such as from dilemmas that are crafted by an adversary to cause friction between multiple coalition forces.

At the individual level, actors in a coalition have to deal with a psychological coexistence between groups, where their identities and allegiance may influence their worldview and potential contributions to Coalition decision-making. Subtask 10.1.1 addresses these social psychological issues relating to humans participating in multiple groups. The generative modeling will provide demonstration of psychological concepts that are evident in a coalition, including the tensions and cognitive dissonance that may emerge and potential mechanisms to manage this.

Subtask 10.1.2 addresses structural issues that can particularly affect the speed and accuracy of decision-making. We expect to demonstrate the differences between information sharing protocols and the effects of *lateralization* through bridging across coalition sub-structures.

Subtask 10.1.3 allows us to consider effects of AI systems on the coalition in supporting multi-domain operations. It examines future tensions and effective operation in human-agent teaming for ad-hoc coalitions using advanced AI systems to resolve complex multi-actor, multi-domain operations, addressing TA2 topics A.1 and A.2

[234] G. White, D. Cunnington, M. Law, A. Russo, and E. Bertino, "A comparison between statistical and symbolic learning approaches for generative policy models". Submitted for review at ICMLA 2019. Available online: https://dais-ita.org/node/3898

[235] https://urbansounddataset.weebly.com/

[236] https://data.london.gov.uk/dataset/tfl-live-traffic-cameras

[237] https://archive.ics.uci.edu/ml/datasets/adult, https://archive.ics.uci.edu/ml/datasets/covertype

from the program announcement. Findings will be available to support briefings and demonstrations, promoting further thinking on how AI and human teaming in a multi-domain context.

Task 10.2 focuses on the context of future military operations - these will span multiple domains and timeframes and require highly agile integrated systems that draw on the strengths of human and AI agents working together. MDO describes how a military force, as part of a joint force operation, must counter and defeat a near-peer adversary capable of contesting in all domains, from competition to armed conflict, in the 2025-2050 timeframe. Such capabilities require constant CSU to ensure adversary activities are understood and countered in effective and proportionate ways. By fusing symbolic and subsymbolic systems with uncertainty-aware mechanisms that more deeply integrate the coalition human-AI teams, we can offer responsive capabilities to inform decision-making and provide wide-ranging CSU in pre-conflict, conflict and post-conflict situations, in a distributed environment.

Task 10.2 will demonstrate exactly these capabilities in the context of the DAIS ITA vignette. For example: an area of potential enemy activity is identified and in response, coalition air platforms drop a large number of autonomous (low size, weight, and power) sensors in the target area in order to monitor the advance of enemy forces. Concurrently with the deployment of the manned Tac HQ A, a second unmanned Tac HQ B is established further forward in the high threat area consisting of 'virtual staff officers'. These are designed to work in cohort with their opposite numbers in the manned HQ and reduce both HQ footprint as well as the workload/threat to human operators. By applying our research in this context, we increase the opportunity for collaboration with other research across DAIS ITA as well as better presenting our research in a manner accessible to military subject matter experts and stakeholders.

Task 10.3 also addresses the requirement that future coalition forces will be exposed to Multi-Domain Operations[238]. Specifically, this task focuses on the information requirements and in order to outperform enemy forces, the coalition needs to efficiently process information quicker and more intelligently. With MDO, the type of contextual information available to coalition forces will be more heterogeneous and highly dynamic, exceeding the information processing capability of a human analyst. Also, operating environments may contain limited computational resources and lack of (or have low) bandwidth communication to high performance computing facilities. Coalition systems and devices may therefore be expected to offer 'edge-of-network' reasoning and decision-making capabilities.

Through Task 10.3, A NSPL will enable coalition forces to learn generative policy models that are capable of taking into account rich, unstructured contextual information from a variety of coalition sensors. This leads to autonomous decision-making capability in MDO where the amount and heterogeneity of contextual information exceeds human ability to analyze. For example, consider a logistical resupply scenario where a convoy must continuously evaluate their current route choice for risk of adversarial compromise. The coalition has access to various sensors collecting unstructured contextual information such as CCTV cameras and structured information such as the current and forecasted weather conditions. The resupply convoy also has a set of potential actions, such as re-routing, or deploying a surveillance UAV to investigate enemy activity. Given that the resupply convoy may have limited bandwidth communication to a back-end datacentre or human operator, with a NSPL, the convoy can autonomously decide its next action and use past decisions to learn optimal policies to enforce in such contextual situations.

Transition opportunities will be pursued in collaboration with ARL and DSTL, such as integration with future logistical operation systems, e.g. NATO Logistics Functional Area Services[239] to enable autonomous decision making in MDO operations. We will explore transition opportunities with ARL on the use of our hybrid learning approach to learn interpretable decision-making policies and device-based security policies within the context of ad-hoc human-machine teams.

Collaborations, Staff Rotations, and Linkages

Task 10.1 has clear relevance and alignment with Tasks 10.2 and 10.3 within Project 10. Linkages and synergies will be explored, particularly concerning the interaction between human and machine systems involving neuro-symbolic interaction (Task 10.2) and the use of generative policies for autonomous agents (Task 10.3). Additionally, there are strong linkages to Task 9.2 (network intelligence from negative ties) based on the use of

[238] U.S. Army. The U.S. Army in Multi-Domain Operations. Nov, 2018. Available online: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

[239] Pecina, Miroslav, and Jan Husak. "Application of the New NATO Logistics System." Land Forces Academy Review 23.2 (2018): 121-127

networks to structure coalition interactions. Indicative staff rotations are planned in alignment with the task research milestones. Regular staff rotation is planned, and this is aligned with deliverables as specified in the Research Milestones for each quarter of the project.

Task 10.2 involves collaborations, staff rotations and linkages with the following projects and organisations:

- P8.3 – The proposed use of SVS for reasoning is complementary to the hybrid approach here and we will continue our regular collaborative (biweekly) meetings with that team.
- P9.1 – Synergy with our subtask 10.2.2 and interpretability in the context of our subtask 10.2.3; ensuring the approach is able to accommodate interpretability. Cardiff students will undertake rotations to IBM UK and US.
- P9.2 – Our subtask 10.2.3 aligns with the WP0026 "meta-heuristic modelling" research. Detailed insights from both can inform creation of compatible interaction models. PSU will rotate to Cardiff in Spring 2021.
- P10.3 – Also considering symbolic/subsymbolic integration, affording strong potential for cross-TA collaboration. Task 10.3 focuses on rule learning, while we focus on parameter learning and uncertainty-awareness. We will align our uncertainty-aware and CSU perspectives with the policy-based perspective in 10.3. Cardiff and Imperial will establish regular cross-task collaborative workshops.

Task 10.3 will leverage research outcomes achieved in the BPP18 Project 2-Task1 in particuar during the evaluation phase in comparing the proposed neural-symbolic learning method with the pure symbolic learning method developed on that project. Task 10.3 will also leverage results and exprience gained in DAIS BBP18 on federated machine learning when extending our approach to distributed context understanding.

Task 10.3 has synergies with Project P7, as the neural-symbolic learning approach developed in this task will complement the federated policy learning framework developed in Task 7.2, and with Task 10.2. The neural-symbolic learning approached developed in Task 10.3 will provide a general-purpose learning architecture and algorithms for generating predictive models from multi-modal data for distributed intelligence. This approach complements the work in Task 10.2, which will focus predominately on a neuro-symbolic hybrid approach that combines learning of situational features with symbolic reasoning in order to support human-machine situational understanding. Our proposed neural-symbolic learning method differs in the use of symbolic learning component. Although the neural component of our architecture will be of the same nature of the neural components used in Task 10.2, our symbolic component will be different: it will be a learning component instead of a symbolic inference component. Again, the plug-and-play nature of our approach will allow our symbolic component to be used as part of the architecture developed in Task 10.2 in order to learn optimal decision-making policies based on information related to current coalition situations. These learned models can be used in the context of a CSU not to replace the human-centric decision making at the edge of the network, but to provide suggestions to the humans of best decisions to take, together with supporting explanations related to current CSU. The symbolic inferencing component developed in Task 10.2 can be integrated into our architecture to support neural-symbolic inference of explanations for recommended decisions based on our learned CSU-driven decision-making policies.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 1**	• Key mechanisms to model coalition member motivations from behavioural and psychological perspectives (Subtask 10.1.1 – *Yale lead* with Cardiff, Dstl and ARL). • Definition of structural considerations in Coalitions and specification of initial metrics relative to information sharing (Subtask 10.1.2 – *ARL lead* with Cardiff and IBM US). • **Deliverable:** Technical report to support publications in Q2-Q6, with the potential to publish at SPIE, or an ITA-organised workshop. • *Cardiff* staff rotation.

Research Milestones		
Due	**Task**	**Description**
Q1	**Task 2**	• Create a hybrid symbolic/subsymbolic approach to share insights, building on earlier BPP18 research. • **Deliverable**: Research paper(s) on the architecture/approach and insights gained (**Cardiff**, ARL, UCLA, IBM UK/US).
Q1	**Task 3**	• Investigation into current neural/symbolic techniques. • **Deliverable**: Survey Report.
Q2	**Task 1**	• Single domain/dimension model for coalition game in an adversarial setting. Proof of concept findings (Subtask 10.1.3 - *IBM US lead* with IBM UK, Dstl, ARL and Cardiff). • **Deliverable:** Conference publication to support modelling of the underlying agent-based coalition game and its representation. • *IBM US* staff rotation.
Q2	**Task 2**	• Propose a propositional state representation of the input of a MAXSAT layer using a Variational Autoencoder that generates a discrete latent vector. • **Deliverable**: Research paper and code/implementation details (**UCLA**, IBM US, Cardiff, ARL, IBM UK) • Define novel human-machine system architecture(s) supporting conversational interfaces that can build a model of other interacting agents, irrespective of whether they are humans or machines; define evaluation tasks/metrics. • **Deliverable**: Research paper and code/implementation details (**IBM UK**, Cardiff, UCLA, IBM US, ARL)
Q2	**Task 3**	• Neural/Symbolic Learner for Generative Policy Models based on forward propagation from neural to symbolic learning components. • **Deliverable**: Paper on algorithm and implementation of neural-symbolic learning with forward propagation.
Q3	**Task 1**	• Information sharing protocols and psychological implications of coalitions - key principles and initial findings. (Subtasks 10.1.1 and 10.1.2 - *Cardiff lead* with Yale and ARL). • **Deliverable:** Conference or Journal publication addressing the psychological and structural implications of sub-group interactions on coalition operations. • *Yale* staff rotation. • Strategies to mitigate conflict within coalitions in the presence of sub-groups by incentivizing predisposed individuals to align their self-goals with those of the coalition. (Subtask 10.1.1 – *Southampton lead* with IBM UK and ARL). • **Deliverable:** Conference or journal publication (e.g., AAMAS or IJCAI) on strategies for mitigating conflicts due to sub-group membership in coalitions.
Q3	**Task 2**	• Within the human-machine system architecture; define a novel negotiation protocol of CSU knowledge between human and machine agents. • **Deliverable:** Paper with protocol description and theoretical assumptions, and demonstrable case studies (**IBM UK**, Cardiff, UCLA, ARL, IBM US)

Research Milestones		
Due	**Task**	**Description**
Q3	**Task 3**	• Demonstration of the use of neural-symbolic learning for learning policies in the context of CSU. • **Deliverable**: Learning of policies for optimal decision-making based on information related to current situation understanding.
Q4	**Task 1**	• In-depth assessment of tensions in coalition information space for human agent teams in real-world scenarios as a result of AI systems. (Subtasks 10.1.2 and 10.1.3 – *IBM UK lead* with ARL, IBM US and Cardiff). • **Deliverable:** Conference or Journal publication assessing the implications of autonomous AI on human coalition operations. • *IBM UK* staff rotation.
Q4	**Task 2**	• Learn parameters for a SLProbLog program from partial observations using the EM framework. • **Deliverable:** Paper with experimental results and code/implementation details (**Cardiff**, ARL, UCLA, IBM US/UK)
Q4	**Task 3**	• Integrated Neural/Symbolic Generative Policy Model performing a forward and backward pass over neural components during learning. • **Deliverable**: Algorithm and implementation of end-to-end neural-symbolic learning,
Q5	**Task 1**	• The implications on inclusion of reinforcement learning in multiple dimensions to support coalition decisions - effects on human teams. Development of a specific scenario applying this to social influence operations (Subtasks 10.1.1 and 10.1.3 – *IBM US lead* with Yale, Dstl, Cardiff and Southampton). • **Deliverables:** Conference or Journal publication examining how machine-based agents function across multiple domains as opposed to framing decisions based on a single domain only. Software demonstrator of network-based influence game that allows AI agents and human decision makers to interact, and jointly compete against human or AI adversaries.
Q5	**Task 2**	• Adapt the evolving architecture for an arbitrary learning problem, thus forcing the neural network to produce as a by-product the semantic graph-embedding representation. **Deliverable:** Paper(s) with experimental results and code/implementation details (**UCLA**, IBM US, Cardiff, IBM UK, ARL) • Run trial to measure effectiveness of the human-machine system architecture on CSU vignettes. **Deliverable:** Paper(s) with experimental results and code/implementation details (**IBM UK**, Cardiff, UCLAs, ARL, IBM US)
Q5	**Task 3**	• Evaluation of Hybrid Neural-Symbolic Learning of policies for information sharing and communication in CSU and ad-hoc human-machine teams. • **Deliverable**: Paper presenting policy learning in ad-hoc teams that uses contextual information generated by current CSU.
Q6	**Task 1**	• In-depth analysis of agent-based models to understand:

Research Milestones		
Due	**Task**	**Description**
		i. psychological factors underlying sub-group and coalition motivations (Subtask 10.1.1 - *Yale lead* with Dstl, ARL and Cardiff). ii. structural dynamics for information sharing for advanced C2 operations (Subtask 10.1.2 – *ARL lead*, IBM US and Dstl). iii. possible interventions (structural and psychological) to support multi-force engagement for cohesive and effective coalition operations in the context of future AI. (Subtasks 10.1.3, 10.1.2 and 10.1.1 – *Cardiff lead* with all partners). • **Deliverable:** Conference or Journal publication(s) presenting the organisational, structural and psychological implications concerning information sharing, organizational structure and collaboration on coalition operations.
Q6	**Task 2**	• Open source public release of research-grade software, models, tools and algorithms, with documentation and tutorial. Focused around the human-machine system architecture, with embedded components for each of the research threads across the 3 subtasks as outlined in the previous quarters. • **Deliverable:** Consolidation and release of open source materials (**IBM-UK**, ARL, Cardiff, Dstl, IBM-US, UCLA)
Q6	**Task 3**	• Open source public release of datasets generated during the project, research- grade software, and tools with related documentation. • **Deliverable**: Consolidation and release of open source materials.

Experimentation

Project Champion: Dave Conway-Jones, IBM UK Email: conway@uk.ibm.com Phone: +44 7802 222 965	
Primary Research Staff	**Collaborators**
Dave Conway-Jones, IBM UK	Andreas Martens, IBM UK
Graham White, IBM UK	Geeth de Mel, IBM UK
Keith Grueneberg, IBM US	Patrick Baker, Dstl
Maroun Touma, IBM US	Paul Sullivan, (c/o ARL)
	Olwen Worthington, Dstl
	Brian Rivera, ARL
	Derek Halpin, Dstl
	James Harryman, Dstl
	James Pritchett, Dstl
	Paul Alderton, Dstl
	Tom Squires, Dstl
	Matthew Cox, Dstl
	Jeremy Tucker, Dstl
	Scott Mastin, ARL
	Sue Toth, ARL

Project Summary

The objective of DAIS ITA experimentation is to enhance the research program by facilitating integrated experimentation and helping researchers to run experiments. This will enable richer interaction between different elements of research to be explored, supporting collaborative inter-disciplinary research, validation of the research (including quantification of the impact of the research) and identification of critical research questions. This will be delivered in conjunction the experimentation and validation material provided in each of the task descriptions for BPP20 and will evolve as needed throughout the program.

This research experimentation will be undertaken in support of the DAIS ITA vision of a coalition collective intelligence: the coalition collection intelligence delivers (at least) (i) the dynamic adaption of secure, resilient

context-aware information systems, (ii) distributed integration & exploitation of coalition data & information across heterogeneous information infrastructures, and (iii) derivation of situational understanding of complex situations by human users synergistically supported by machines. When considering this coalition collective intelligence in the context of experimentation it is important to account for key contextual factors, such as those expressed in MDO (Multi-Domain Operations). For example: by ensuring that capabilities explored in the research, and scenarios built to support experimentation, take into account both competition and conflict, and the critical need to support coalition and cooperative capabilities in a hostile environment where adversaries increasingly seek to isolate and separate.

The research experimentation will represent (at least) (i) high tempo, dynamic, distributed and time sensitive tactical environment (aka task arrival rate, distribution, priority and resource demand), (ii) sensors and other sources of information providing data to users who need situational understanding of the wider world (e.g. threat actor location, status, capabilities, activities and intent), (iii) congested and contested nature of the electro-magnetic environment (including bandwidth constrained and fragmented tactical edge), (iv) coalition context.

The research experimentation is planned to focus on a small number of Coalition Collective Intelligence use cases. Two candidate use cases are outlined below, but we anticipate that up to four such cases could be defined during the initial period of this activity:

a) Understanding of complex multi-actor tactical situations by human users synergistically supported by machines exploiting distributed coalition data & information across heterogeneous information infrastructures;
b) Operations & Management of a dynamic adaptive secure, resilient context-aware information systems responding to high tempo, dynamic, distributed and time sensitive tactical environment (aka task arrival rate, distribution, priority and resource demand) in a congested and contested nature of the electro-magnetic environment utilising the coalition's heterogeneous information infrastructures.

These represent two of the major functional areas which the DAIS ITA research programme aims to support. They need to be enhanced by a more detailed set of capability concepts demonstrating how elements of the research could, if matured into a technical solution, provide benefits to the warfighter and the interaction of research tasks. They will be revisited in consultation with the Military Advisors and other specialists to ensure they are correct for the DAIS ITA research program. For example, in delivering this experimentation work, the second use case could be expanded to show how the operation and management of the information infrastructure would be affected by a denial of service attack via a persistent jamming campaign by the adversary. This broad perspective onto the more unified infrastructure is something which individual tasks are unlikely to be able to undertake but which could be of substantial benefit to the program. This and other more specific cases will be explored and developed through the delivery of this experimentation work (see milestones for details of the proposed process).

The chosen use cases and capability concepts will continue to be assessed throughout the delivery of the experimentation work and refined or expanded when needed.

This experimentation activity is written in a similar manner to a traditional DAIS ITA research task, but with a focus on the methods and mechanisms used to achieve the successful delivery of these research tasks. It is, therefore, generally written in the form of "how", rather than "what"; with the "what" already coming from the BPP20 research tasks. This experimentation work is fundamental science and the development of integrated experiments, demonstrations and scenarios/vignettes can be published in conference proceedings when appropriate, as indicated in the milestones below.

While transition activities are out of scope for the basic science research program (and are therefore not covered in this description, or the milestones below), this experimentation work is well placed to inform potential transition activities in each country. The leads for this experimentation task will therefore also work closely with the transition functions within each country and be encouraged to brief relevant departments or organizations as advised by Dstl and ARL. This work is in addition to existing transition activities, and not intended to replace the potential for researchers to directly pursue transition opportunities, but instead to add the potential to build longer running relationships that could lead to transition, built around the stories and capstone demos that will be developed as part of this task.

Collaborations, Staff Rotations, and Linkages

This experimentation task relates to every other project and task within DAIS ITA, and through the milestones indicated below, links with relevant research within each of the tasks will be identified and established through

connections with specific researchers. The purpose of the experimentation team is to enable the researchers to continue their work unhindered, but to help provide context and links into the experimentation activity with the increased potential for cross project collaboration and experimentation. This may be through the experimentation assisting in the development of assets, or through identification of linkages to other active research that may be mutually beneficial. The experimentation team will also act as a catalyst to bring the military advisors from both Dstl and ARL (and any other organizations) together with researchers through a series of meetings, regular teleconference calls etc. There will be the potential for staff rotations in this work, perhaps most notably for any Military Advisors wishing to more deeply embed into a research organization for short periods, or for researchers to locate at IBM or Dstl/ARL for more exposure to military advisors.

Note that the majority of the resource available for experimentation is in the first year (Q1-4), so the main focus for the Q5-Q7 milestones is the design, build and execution of Capstone Demos that have been informed by the detailed work during Q1-4. These are likely to be based around the two key use cases (Coalition Collective Intelligence; and Coalition Collective Intelligence Operations & Management) outlined earlier, with possible additional use cases added during execution of this work.

The milestones listed below are provided as high-level descriptions of the tasks undertaken, rather than specific measurable outputs such as published papers. This reflects the assistive nature of the work. Certain significant deliverables such as Capstone demos and open source publication are listed and will be delivered in conjunction with research from across the BPP20 program.

Due	Description
Q1	• Organize and host one (or possibly two if logistically required) kick-off workshops with Military Advisors and key DAIS Primary Investigators (PIs) to establish the baseline for this new experimentation thread, building on the two key use cases identified above. • Review previous DAIS research outcomes to harvest any existing or potential assets or reusable components. Also identify any promising research areas that could be progressed towards asset status with the support of the experimentation team. • Establish monthly experimentation calls for the Military Advisors, key PIs and TALs for the duration of BPP20. These are to be run by the experimentation team, but need input from the stakeholder, advisor and researcher community to help ensure the right work is taken forward. • **[This milestone is repeated for all quarters]** Assist DAIS ITA researchers in designing or running experiments and any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.). This may require close coordination with task leads and project champions to ensure that relevant researchers are committed to participating in these kinds of experimentation activities, with the core experimentation team providing guidance and assistance as appropriate.
Q2	• Review and reuse (or redefine, where needed) the DAIS ITA scenario and vignettes, developing any additional details to enable them to be more usable by the program. Ensure that the scenario meets both US and UK requirements, and reflects current perspectives such as MDO.

Due	Description
	• Where possible, identify datasets[240] (either for reuse from elsewhere, or that are required to be developed for DAIS ITA directly) and compile these into a central location[241], along with documentation, for improved access to researchers across the program. • From the asset and capability register created in Q1, identify opportunities for integrated stories or end-to-end demonstrations comprising multiple assets[242]. • **[This milestone is repeated for all future quarters]** Guide DAIS ITA researchers in designing or running experiments and assist with any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.).
Q3	• Consolidate appropriate assets, code, examples and data into the publicly available GitHub repository for DAIS - https://github.com/dais-ita/ (This can be done either by the experimentation team on behalf of researchers, or by researchers directly). • Create standard documentation, example and links to research papers for all assets published to GitHub. For any assets not yet able to be shared publicly, work with the authors to ensure consistency with this approach for eventual publication. • Assist DAIS ITA researchers in designing or running experiments and any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.). This milestone is repeated for all quarters. • Interim demonstration(s) of progress so far, at AFM2020. These may be initial versions of the future Capstone demos or showcasing some of the specific experimental work from assisting other researchers.
Q4	• Integrate key assets and research outcomes into 2-3 key stories, with input from the Military Advisors. Develop these stories into storyboards for "Capstone Demo", taking into account key DAIS aspects (collaborative, distributed, coalition) and US and UK military relevance. Get approval from DAIS leadership to take these Capstone Demo ideas forward for demonstration at AFM 2021. • Repeat Q1 activity, reviewing latest DAIS research to seek candidate assets and outcomes. • Assist DAIS ITA researchers in designing or running experiments and any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.). This milestone is repeated for all quarters.
Q5	• In close coordination with Military Advisors, develop each of the Capstone Demos, create missing datasets, develop descriptions of

[240] Since experience indicates that it will likely be prohibitively expensive to create (or find) highly relevant datasets, it is probable that a collective of loosely related data capable of exercising different research tasks will be gathered, with effort in the scenario and capstone activities to create a plausible narrative to link these where needed.

[241] Whilst desirable, the need for unified datasets must not be on the critical path, and experimentation must be able to proceed with separate more fragmented data.

[242] In this quarter we are therefore driving the possible stories based on the research being done, but in Q4 we then define actual stories, based on this initial assessment, and use these to drive the integration of different research aspects.

Due	Description
	the demos (as conference/workshop papers, or technical reports). These Capstone Demos may integrate specific research in some cases, and in others provide a narrative context into which other research can be more loosely linked. This gives flexibility for working closely and deeply with some researchers, whilst providing less intensive assistance for others. • In some cases, there may be research which has not yet reached implementation. This can still be included in the Capstone Demos, if appropriate, e.g. through simulation or extrapolation. • Iterate through the demo development, ensuring that the focus on telling the fundamental science perspective is maintained. Review regularly with DAIS leadership, Military Advisors and key researchers. • Assist DAIS ITA researchers in designing or running experiments and any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.). This milestone is repeated for all quarters.
Q6	• Deliver Capstone demos at AFM 2021. Update Science Library with detailed descriptions, videos and links to code assets (on GitHub) and relevant papers for each of the Capstone Demos. • Assist DAIS ITA researchers in designing or running experiments and any supporting infrastructure or logistical requirements (e.g. edge devices, cloud infrastructure, HRP processes etc.). This milestone is repeated for all quarters.

Biennial Program Plan (BPP) Budget for Projects and Organizations

This section summarizes the total cost and budget for the activities within the BPP. The funding in the BPP is only for people listed as contributors in the preceding sections. The collaborators listed for a project and tasks are not allocated any Government funds for that project/task. The budgets are for a period of 20 months from January 15, 2020 to September 20, 2021.

The following reflects the Biennial Program Plan BPP Government Share, Private Share, and total cost by organization. Total cost is the cost of research undertaken. Government Share is total cost minus the Private Share, the cost of research shared by the consortium partner. Overall, the Government Share reflects a US-UK split of 50:50.

Biennial Program Plan 2020 (BPP20)			
US Institutions	**BPP Government Share**	**BPP Private Share**	**BPP Total Share**
BBN Raytheon	$0	$0	$0
PSU	$509,066	$86,236	$595,302
Purdue	$723,479	$85,612	$809,091
Stanford	$0	$0	$0
UCLA	$613,902	$0	$613,902
UMASS	$362,662	$36,266	$398,928
Yale	$731,708	$95,455	$827,163
IBM US	$3,725,850	$638,883	$4,364,734
US Totals	**$6,666,667**	**$942,453**	**$7,609,120**
UK Institutions	**BPP Government Share**	**BPP Private Share**	**BPP Total Share**
Airbus	$21,200	$0	$21,200
BAE	$21,200	$0	$21,200
Cardiff	$1,189,866	$0	$1,189,866
Imperial	$1,006,708	$111,860	$1,118,568
Southampton	$280,874	$0	$280,874
Univ College London	$307,103	$0	$307,103
IBM UK	$3,839,715	$675,680	$4,515,396
UK Totals	**$6,666,666**	**$787,540**	**$7,454,207**
US+UK Totals	**$13,333,333**	**$1,729,993**	**$15,063,327**
*BPP20 POP of January 15, 2020 to September 20, 2021			

Overall, the Government Share reflects a US-UK split of 50:50. The Academic Portion represents 51% of the Government Funding without Program Administration. The Program Administration represents 15% of the total Government Funding.

Govt Share	US	UK	Total	Percent
Universities	$2,940,817	$2,784,718	$5,725,535	**51%**
Industries	$2,681,925	$2,856,809	$5,538,734	**49%**
Total Technical	**$5,582,742**	**$5,641,527**	**$11,224,269**	**85%**
Management	$1,043,925	$1,025,139	$2,069,065	**15%**
Total	**$6,666,667**	**$6,666,666**	**$13,333,333**	

The parentage of academic share of research in each country exceeds the 40% required in the contract.

The split of Government funds is 50:50 in each country.

The percentage of Government share across technical areas is approximately 50:50 with 53.0% for TA-1 and 47.0% for TA-2

(end of document)