Semantically Managed Autonomous and Resilient Tactical Networking (SMARTNET) and Hybrid C2 operations

Kevin Chan, Kelvin Marcus, Gregory Judd and Peter Boyd

December 7, 2018

Semantically Managed Autonomous and Resilient Tactical Networking (SMARTNET) and Hybrid C2 operations

Kevin Chan, Kelvin Marcus, US Army Research Laboratory, Adelphi, MD
Gregory Judd, Peter Boyd, Defence Science and Technology Group, Edinburgh, SA Australia

Multi domain battle asserts that future operations will occur over more than one domain of sea, air, land, space, and cyber. This is in response to a projected complexity of the operational environment coupled with a sophisticated adversary. In order to maintain battle space dominance future militaries will have to execute command and control across these multiple domains.

Conceptually, we consider multi-domain operations as a multiplex network, where we have several network layers, each node possibly belonging to one or more of the network layers. Each network layer maintaining its own logical topology. For each layer, there exist dynamics of the network or the environment in which the network exists. Additionally, there are interconnections between the network layers, representing linkages between the various network layers. For example, we have a tactical network of tactical radios. Based on the physical terrain, the radios establish a network with a topology generated by the routing protocol (e.g., OSPF, OLSR). This network is supported by a squad of UAVs, providing sensing of an area of interest. A subset of the UAVs have tactical radios that can communicate with the terrestrial network when in range. The UAVs and terrestrial communications network are responsible for coordinating communications of sensing back to the battalion FOB.

NATO SAS-143 is developing theory for hybrid C2 operations, establishing models and concepts for operations over multiple domains, hybrid operations involving human and artificial intelligence agents, and operations in the presence of an active, adaptive adversary. To help validate these developing concepts there is a need for a tactical network experimentation platform, such as the one being developed under the collaborative SMARTNET program described below.

The US Army Research Laboratory (ARL) and Australia’s Defence Science and Technology Group (DST) are collaborating on a project called Semantically Managed and Autonomous Tactical Networks (SMARTNET). The purpose of this collaboration is to develop a proof-of-concept system that will autonomously prioritize, transform and control tactical C4ISR information. The benefits of this endeavor will be: more resilient tactical networks, improved ability to cope with the increased complexity of the environment, and more efficient information dissemination. Ultimately, this will provide enhanced situation awareness to the tactical edge user. The proof-of-concept system will reside as a middleware on a tactical node, between the tactical radio and other networked services (e.g., battle management systems). This middleware will leverage understanding of various environmental and platform contexts (e.g., mission, tactical node, operating environment, network) to optimize the amount of, and rate that, information is put onto the network.

SMARTNET as a concept has the goal of enhancing the efficiently and robustness of tactical networked communications by being more prudent in what information is sent out in the network. The goal is to develop a middleware that resides between the tactical radio and any networked applications (e.g., battle management system). This middleware will consist of three modules to perform prioritize, control, and transform operations on the information. The choice of middleware based on an open architecture approach rather than full redesign of applications or hardware is to promote flexibility in a variety of multi domain settings and scenarios. To achieve this, we expect that SMARTNET will be deployed on a subset of key tactical nodes.

We briefly describe the functions within each of the modules, each of which perform specific operations on the information. Figure 1 illustrates the SMARTNET concept.

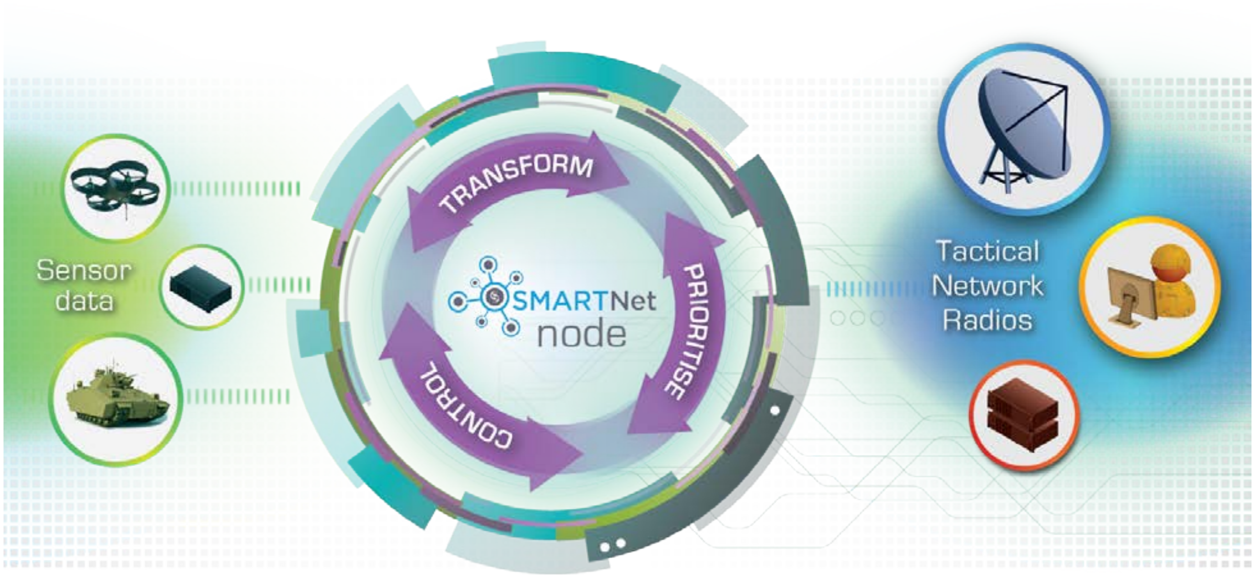

Figure 1: SMARTNET Concept that processes sensor data through Prioritize, Transform and Control modules to manage the information put on tactical networks.

Prioritization: To maximize efficiency of information on the network, we can choose to order the transmission of the information based on perceived importance relative to the mission. One may also consider freshness of information as a means to prioritize the information, for example network intrusion alerts over than periodic health monitoring reports.

Transform: Tactical networks often experience extremely low bandwidths and unreliable connectivity. In order to maximize achievable shared situation awareness, we consider transformation of the sensor data, particularly through compression to reduce the strain on the tactical networks. Transformation of data may also include functions to enhance the security and or privacy of the data.

Control: The information can also be controlled in terms of how frequently information is sent out from each node. For example, position information may require more frequent updates when in contact as opposed to within base operations where dynamics are not as great.

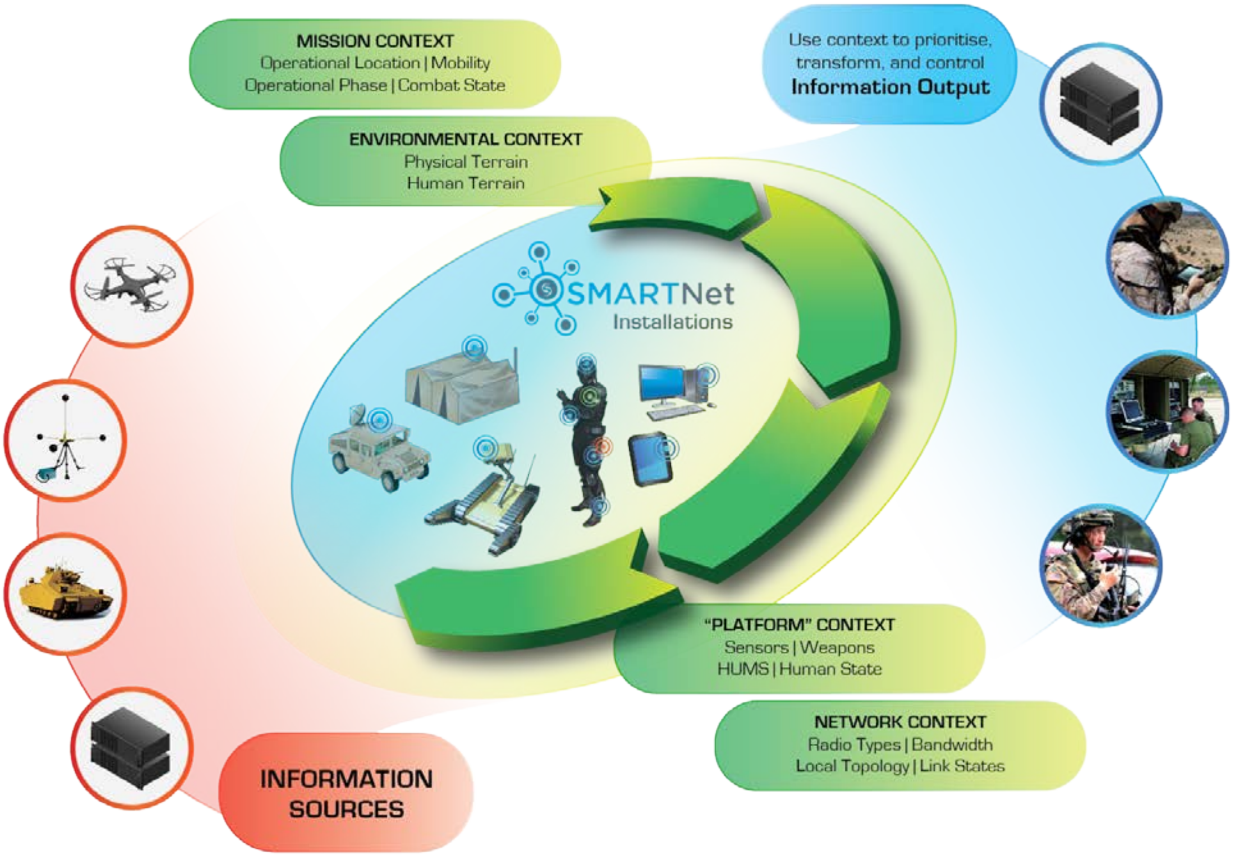

Figure 2. Overall SMARTNET environment, which includes information sources and various environmental contexts. Each node will use this information to autonomously determine efficient use of the tactical network.

The implications of SMARTNET on hybrid operations or hybrid C2 is clear. The experimental platform will provide a validation environment to test out new hybrid Multi-domain C2 and information management concepts. Based on, for example, emerging concepts such as the US Army’s framework for Multi-domain Battle. It will allow help define a C2 architecture where a capability such as SMARTNET can provide a gateway to the inter-domain communications.

Further, the anticipated flexible deployment capability of SMARTNET could allow for deployment on a wide set of tactical nodes.[1]

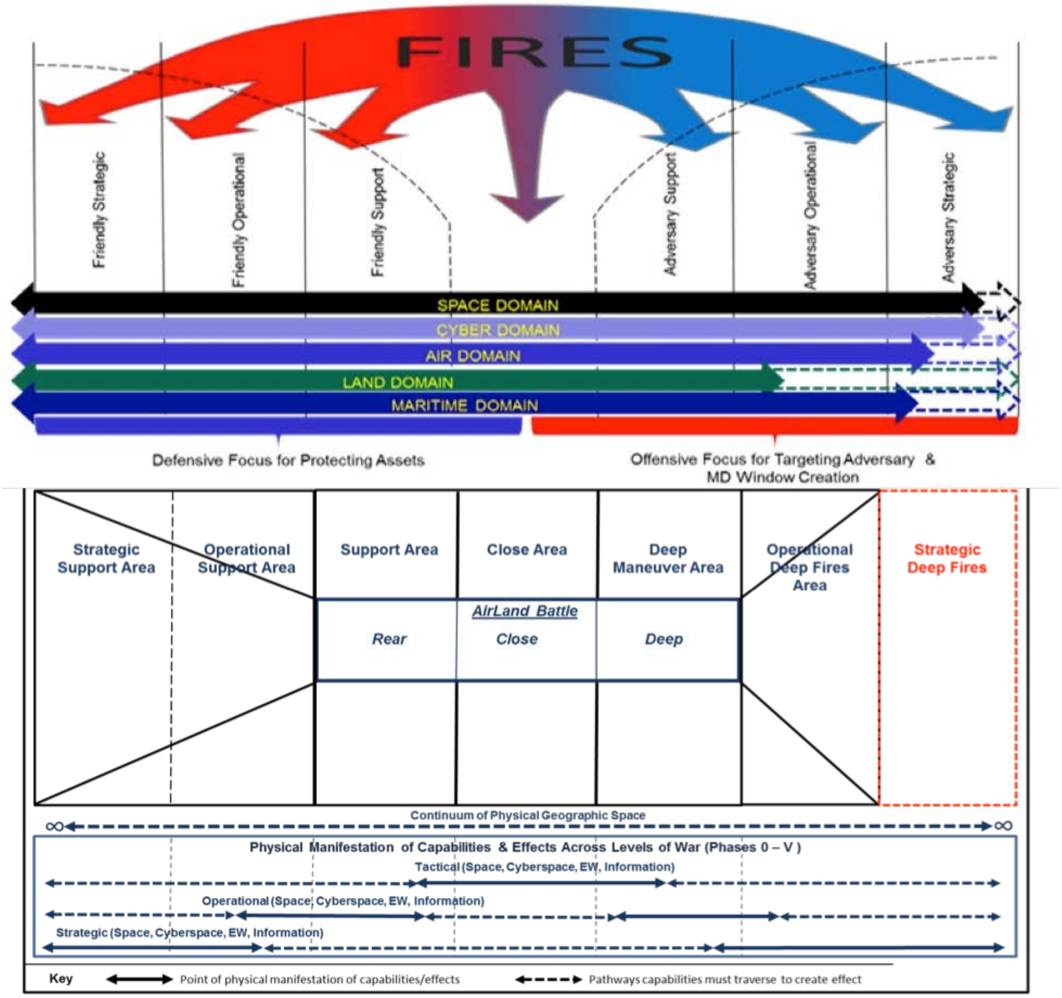
FIRES
Friendly Strategic
Friendly Operational
Friendly Support
Adversary Support
Adversary Operational
Adversary Strategic
SPACE DOMAIN
CYBER DOMAIN
AIR DOMAIN
LAND DOMAIN
MARITIME DOMAIN
Defensive Focus for Protecting Assets
Offensive Focus for Targeting Adversary & MD Window Creation
Strategic Support Area
Operational Support Area
Support Area
Close Area
Deep Maneuver Area
Operational Deep Fires Area
Strategic Deep Fires
AirLand Battle
Rear
Close
Deep
Continuum of Physical Geographic Space
∞
∞
Physical Manifestation of Capabilities & Effects Across Levels of War (Phases 0 – V)
Tactical (Space, Cyberspace, EW, Information)
Operational (Space, Cyberspace, EW, Information)
Strategic (Space, Cyberspace, EW, Information)
Key
Point of physical manifestation of capabilities/effects
Pathways capabilities must traverse to create effect

Figure 3. The Army's Battlefield framework for multidomain battle[1].

For the validation of SMARTNET and its utility to tactical environments, after developing the concept and the middleware, we will identify multiple use-cases and networked applications at different scales and dynamics. A position location information (PLI) of blue forces is proposed as the initial proof of concept for SMARTNET. Future uses cases include red force tracking (RFT) and mass medical telepresence. These examples require a greater amount of network resources along with greater expected dynamics. With these proof of concept shown in network emulation (e.g., ARL's network science emulation laboratory) and simulation environments, we also plan various field experiments, located both in the US and AUS.

[1] https://breakingdefense.com/2018/05/generals-worry-us-may-lose-in-start-of-next-war-is-multi-domain-the-answer/