CALL FOR PAPERS

Armed Forces Communications and Electronics Association (AFCEA), Erie Canal Chapter

C4I and Cyber Conference * Tuesday - Wednesday, June 19 & 20, 2018 * Hotel at Utica Centre, Utica, NY – formerly known as Radisson Hotel

The AFCEA C4I and Cyber conference afternoon workshops will focus on a selected set of specific topics that are directly related to AFRL's Core Technical Competencies. We seek current 'hot-topic' unclassified papers. AFCEA welcomes submissions from government and military service programs, laboratories, academia, and industry. These papers could have been presented elsewhere but they must address current, cutting-edge issues in a compelling manner. Selected papers/authors will have the opportunity to present their ideas during one of the four workshop sessions at the conference this June.

Authors are invited to submit extended abstracts for the topics detailed below that align with the following Core Technical Competencies (CTC):

1. Connectivity & Dissemination
2. Autonomy, C2, & Decision Support
3. Processing & Exploitation
4. Cyber Science & Technology

Important Considerations:

- Electronic submissions can be 3 - 5 pages including figures/graphics. Select one of the focus areas below for consideration. Submissions can include previously published material and/or developed products.
- Submissions should be of sufficient detail and length to permit proper review and evaluation.
- Authors will be notified of acceptance and will be informed as to whether they should prepare a briefing or poster presentation. Notification of format will be provided at time of selection.
- Please indicate on your submission which CTC your paper aligns with.

Deadlines:

- Paper submission deadline: 16 May – **electronic submission to Andrea Gwilt (conference co-chair) - agwilt@srcinc.com**
- Notification of selection: 01 June
- Final briefing or poster submission deadline: 11 June

Connectivity and Dissemination

Building a Seamless Communications Fabric across the C2ISR enterprise

Building a seamless multi-domain communications fabric across the C2ISR enterprise, where the goal is not a single unified network but instead one which appears seamless to the user. The communications environment today consists of a multitude of communications systems designed to meet specific and often discrete needs. This has resulted in "stove pipe" systems which have limited interoperability due to system-unique technical, data, security, and interface standards. We aim to build this fabric through research and development in the following three areas:

Communication Links and Networks

The goal is to provide reliable wideband line of sight and beyond line of sight connectivity. This encompasses both physical and network layer challenges to include waveforms, modulation, and spectrum agility across bands. Key challenges at the physical layer include but are not limited to: propagation in varying environments, spectrum agility, and link survivability. Key challenges at the network layer include but are not limited to: provisioning for unanticipated users & nodes, scalability, and dynamic network topologies. The following cause challenges at both layers: user mobility, timing, interference (non-intentional / intentional), and power constraints.

Secure Multi-Domain Architectures

Data and information across multiple networks and devices must be secured before it is shared. Information resides on different devices & networks where users have varying privileges. The ability to move information across networks and devices from multiple forms of information (e.g., voice, video, text, files) as well as between networks is a necessity. There are two key technical challenges: 1) transfer of information across networks and (2) access requiring trust in users and devices. Currently, this is a mainly manual process which is extremely human intensive.

Mission Responsive Information Exchange

The goal is to timely connect tactical information seamlessly across multiple domains on-demand, at scale, enabling a combat cloud. It includes data from current and future generation aircraft, sensors, and other sources, enabled by gateways, data links, and a distributed server infrastructure. Technologies poised to close these gaps include but are not limited to: 1) cloud computing, 2) information priority and scheduling/distribution, and 3) machine learning.

Autonomy, C2, & Decision Support

Mastering Complexity for Multi-Domain Command & Control

The ability to effectively command & control within a domain is dictated by the complexity of the operating domain. This complexity drives overall operational uncertainty, tempo, and dictates overall manpower requirements. Traditionally, C2 has been considered only for a singular domain, where the complexity has to date been manageable through existing C2 systems & processes. As the AF moves towards Multi-domain operations, this complexity becomes

multiplicative, where each of the singular domains: Air, Space, Cyber, brings with it new operating dimensions in the form of rule-sets, resources, tempo, capabilities, and uncertainties that all must be accounted for, reasoned over, and integrated together in order to achieve a true multi-domain C2 capability. It is this complexity that we seek to master through advancement of key technologies through research and development in the following three areas:

Complex Adaptive Systems - Mastering complexity through composition, orchestration, and distribution of C2 services. C2 systems are inherently complex, comprised of many interconnected system-of-systems spanning people, policy, doctrine, geographic and functionally distributed resources & information, computing, and communication functions. This complexity will only further increase as we seek to move towards true MDC2.

Key challenges include but are not limited to 1) Composable C2 systems-of-systems to enable rapid evaluation, integration, and orchestration of new C2 capabilities into existing and new architectures and/or systems; 2) Distributed planning, execution, and assessment capabilities to provide a resilient C2 platform for contested operations and environments; 3) Machine-to-machine and machine-to-human workflows and analytics to achieve mission-optimized and adaptive C2-of-C2 capabilities driven by real-time data and intelligent systems for the identification, creation, and composition of C2 capabilities on demand; 4) Scalable information representation & modeling techniques for information & data exchange; and 5) Verifiable adaptive system-of-system composition, provenance, and explainability.

Complex Effects Analysis - Controlling and executing complex effects at speed and scale. Multi-domain operations presents new opportunities for developing and executing complex effects chains that are highly synchronized across domains, continuously adapting to the battlespace, and layered to maximize overall effect. However, to achieve such complexity requires new tools and capabilities for realizing seamless effects generation, planning, and execution across domains.

Key challenges of imposing complexity on the adversary through deployment of multi-domain effects chains is the ability to 1) Characterize, predict, and assess their effect (how to measure the complexity that is imposed); 2) Synthesize, de-conflict, and layer complex effects packages (how to package effects); 3) Present & analyze integrated effects (how to understand the plans that were generated). Additional areas of interest include but are not limited to force readiness and presentation of forces and computation models for representing intent, mission objectives, plans, resource, and outcomes.

Machine Intelligence - Harnessing the speed and scale of machines to exponentially increase human capacity to command & control in an increasingly complex battlespace. The complexity of MD operations will quickly exceed human capacity and will require machine reasoning to augment the human decision maker across all stages of the C2 Monitor, Assess, Plan, and Execute (MAPE) cycle. Foundational to realizing future C2 intelligent systems is the development of machine reasoning and learning systems for decision making and multi-agent systems for the coordination and planning of distributed agents across Air, Space, and Cyber in the presence of incomplete information and operation in uncertain and contested environments.

Key challenges include but are not limited to: 1) Plan analytics for the recommendation, adaptation, and synthesis of plans and courses of actions; 2) Generalized planning techniques,

including but not limited to game-theoretic approaches and machine learning and multi-agent systems for large-scale battle management and operational strategy and tactics development; 3) C2 analytics for predicting and recommendation of new C2 workflows, system composition, and information exchange; 4) Distributed multi-agent, multi-objective planning capabilities to include planning with attrition, degraded communication, & planning in the presence of an active adversary; 5) Operationalizing Machine Learning to support algorithm deployment, human feedback, online model updates, and learning capabilities shared across multi-security boundaries for developing mission-tailored learning capabilities across C2 functions.

Processing and Exploitation

Extreme Computing

Information is growing at an explosive rate, which is currently estimated to be about 3600 PetaBytes per day! This alarming growth rate requires new approaches to be able to store, process and analyze this unprecedented influx of data. The additional forcing function for an operational environment is that this level of computing must occur within mission-required timescales. Extreme Computing technologies, including neuromorphic computing, nano-computing, quantum computing, high performance embedded computing, and machine learning, offer enormous potential towards meeting these needs.

Additionally, Multi-Domain Command and Control (MDC2) requires the ability to collect, process, and distribute data for actionable intelligence, requiring investments in Extreme Computing technologies.

Advances in computing technologies will not come from a single technology, rather Extreme Computing will only be achieved by the careful integration across a variety of disparate technology solutions.

Contributions/papers include, but are not limited to, academic and operational advancements to be able to store, process and analyze the enormous influx of data now available for multi-domain command & control.

Neuromorphic Computing and Machine Learning: These technologies offer huge improvements in SWaP, will enable game-changing autonomy and data-to-decision capabilities that directly support the AF Future Operating Concept vision of providing the warfighter with technological superiority for decades to come.

Quantum Computing and Quantum Networking: "The USAF must develop in-house expertise in both quantum algorithm development and quantum hardware architecture development in order to take advantage of new advances in quantum computing technologies as they become available." [ACC/ST]

High Performance Embedded Computing: Low SWaP focused on high performance ruggedized embedded computing that supports flexible architectures, upstream exploitation, sensor agnostic and heterogeneous data processing. Discovering, prototyping, & demonstrating high-impact, game-changing high-performance computing technologies to the warfighter.

Cyber Science & Technology

Imposing Defensive Cyber Outcomes (Ideas, concepts and technologies for negating adversaries' actions in cyberspace)

> *"The Department of Defense must work with its interagency partners, the private sector, and allied and partner nations to deter and if necessary defeat a cyberattack of significant consequence on the U.S. homeland and U.S. interests. The Defense Department must develop its intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyberattacks before they can impact U.S. interests. Consistent with all applicable laws and policies, DoD requires granular, detailed, predictive, and actionable intelligence about global networks and systems, adversary capabilities, and malware brokers and markets. To defend the nation, DoD must build partnerships with other agencies of the government to prepare to conduct combined cyber operations to deter and if necessary defeat aggression in cyberspace….During heightened tensions or outright hostilities, DoD must be able to provide the President with a wide range of options for managing conflict escalation. If directed, DoD should be able to use cyber operations to disrupt an adversary's command and control network…DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property"*
>
> - [DoD Cyber Strategy (2015), P.14]

> *"Major powers…have a significant and growing ability to hold U.S. critical infrastructure at risk via cyber attack, and an increasing potential to also use cyber to thwart U.S. military responses to any such attacks. This emerging situation threatens to place the United States in an untenable strategic position. Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. The U.S. military itself has a deep and extensive dependence on information technology as well, creating a massive attack surface."*
>
> - [Defense Science Board Task Force on Cyber Deterrence, 2017]

The Air Force will be operating in a cyber environment where it will always be outnumbered and out resourced by its numerous potential adversaries. Mission success will depend on deterring adversaries from engaging AF assets, and assuring critical strategic and tactical weapon systems:

- **Plan and Conduct Tailored Deterrence Campaigns**: The U.S. cyber deterrence posture must be "tailored" to cope with the range of potential attacks that could be conducted by each potential adversary. And it must do so in contexts ranging from peacetime to "gray zone" conflicts to crisis to war. Clearly, for U.S. cyber deterrence (as with deterrence more broadly), one size will not fit all. Through the employment of multiple defensive elements we seek to **deter** adversaries by increasing their level of effort required to achieve their objectives. It is helpful to refer to the Defense

Science Board's Six-Tier adversarial model which depicts the resources and motivations of attackers, ranging from script kiddies to criminal enterprises to nation states.

- **Create a Cyber-Resilient Infrastructure:** The DoD must devote urgent and sustained attention to boosting the cyber resilience of select U.S. systems (cyber, nuclear, non-nuclear) and supporting critical infrastructure in order to ensure that the United States can credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber-attacks. In effect, DoD must create a cyber-resilient infrastructure for U.S. military forces to underwrite deterrence of major attacks by major powers.

    - Challenges we face include developing: 1) technologies to protect our embedded systems from cyber-attacks; 2) technologies that allow our systems to be adaptable, resilient, and survivable; 3) robust, open architectures solutions that provide flexibility for affordable development, upgrade, and adaptation throughout the weapon system life cycle.

- **Enhance Foundational Capabilities**: In addition to the measures outlined above, the Department of Defense and the broader U.S. Government must pursue several different types of capabilities, such as enhancing cyber attribution, the broad cyber resilience of the joint force, and innovative technologies that can enhance the cyber security of the most vital U.S. critical infrastructure. Further, attribution may allow us to further deter adversaries by imposing consequences through prosecution or other sanctions. Without attribution, the U.S. is unable to execute internationally lawful actions to contain or shunt adversarial cyber-attacks, nor is it able to do so within meaningful timeframes.

With these thoughts in mind, we would like to hear your suggestions/advice on working these problems. Potential solutions should focus on the science and technology of deterring our potential cyber adversary, adapting to attacks during mission operations, or providing robust attribution capabilities within meaningful timeframes.

AFCEA Erie Canal Chapter contacts:

Rick Lockridge, Erie Canal President, richard.lockridge@radiancetech.com

Andrea Belmont-Gwilt, Conference Chair, agwilt@srcinc.com

Dawn Rava-Crofoot, Erie Canal Secretary, dawn.rava-crofoot@axenterprize.com

Gene Blackburn, Conference staff, eugene@blackburncny.net

Joe Turczyn, Air Force AFCEA Rep, joseph.turczyn@us.af.mil