Call for Papers
Military Cyber Affairs
Winter 2018-2019 Issue
Command and Control of Cyberspace Operations

SUBMISSION DATE: October 1st, 2018

ISSUE ON: Command and Control of Cyberspace Operations

EDITORS: Bobbie Stempfley,
Managing Director, CERT Division
Software Engineering Institute, Carnegie Mellon University
rgs@cert.org

Steve Stone, D. Sc.
Sr. Principal Cyberspace Operations Engineer
The MITRE Corporation
steve.stone@milcyber.org

INTRODUCTION:

As cyberspace is significantly different from the physical domain in the dimensions of time and space, it presents a much more dynamic and complex operational environment for military operations. This complexity may require the military to examine its long-held doctrine for command and control (C2) and decision-making. The challenges facing modern militaries as they adapt to operations in cyberspace include a nascent understanding of the domain and its characteristics; the complex network of participants responsible for the establishment and sustainment of cyberspace; and insufficient strategies to implement agile C2 and decision-making in the face of the complex dynamics presented by this domain.

OBJECTIVE OF THE ISSUE:

In 2015, the Commander of United States Cyber Command stated, “Our traditional command and control and organizational constructs do not enable the speed and agility required to keep pace with change in the cyber domain”.

This issue seeks to present research and analysis of ideas for command and control and organizational constructs that may enable the speed and agility required to keep pace with change in the cyber domain.

RECOMMENDED TOPICS:

- Theories of command and control for cyberspace operations
- Decision making for operations in cyberspace

- How does C2 in the cyberspace domain differ from C2 in other domains (air, land, sea, and space)?
- What are the information requirements for effective C2 and decision making for cyberspace operations?
- How does the private sector and NGO participate in C2 of cyberspace operations?
- What organizational relationships and command authorities best support agile cyberspace operations?
- Is the model of strategic, operational, and tactical levels of warfare and corresponding C2 constructs valid for cyberspace operations?
- How can commanders synchronize operations in cyberspace with operations in the physical domains?
- What are the delineations between intelligence and operations in cyberspace?
- What is the relationship between the structures of the environment and the participants in cyberspace operations?

SUBMISSION PROCEDURE:

Researchers and practitioners are invited to submit papers for this issue on Command and Control of Cyberspace Operations on or before October 1st, 2018. All submissions must be original and may not be under review by another publication. All submitted papers will be reviewed using a double-blind, peer review process.

For publication in MCA:

1. Papers should relate to the conduct of military cyber operations and apply universally to the joint defense community in one of the following areas or a related area: strategy, policy, law, or ethics, operations, or advances in science or technology.

2. Papers should articulate a logical analysis based on a convincing hypothesis that provides a lucid and comprehensible argument for the general public and identifies implications for policy and practice.

3. Papers should include a logical or empirical analysis in support of that hypothesis that is grounded in a study of the research literature.

4. The research design and methodology should conform to professional standards and be clearly described in the paper.

Interested authors should consult the *Military Cyber Affairs* policies located at:

http://scholarcommons.usf.edu/mca/policies.html

Military Cyber Affairs has no rules about the formatting of articles upon initial submission. There are, however, rules governing the formatting of the final submissions located at:

http://scholarcommons.usf.edu/mca/styleguide.html

Papers should be submitted at:

http://scholarcommons.usf.edu/cgi/submit.cgi?context=mca

All inquiries should be addressed to the editors listed above.

Military Cyber Affairs (MCA) is the peer-reviewed professional journal published by the Military Cyber Professionals Association. *Military Cyber Affairs* provides a multi-disciplinary forum for scholarship and discussion of cybersecurity, cyber defense, and cyber operations, and their military implications, drawing from the fields of intelligence, engineering, information technology, law and policy, among others.