2019-12

Cyber/Radio Frequency Military Deception in Naval Operations

Maule, Randy W.; Fitzpatrick, Christian R.; Balogh, Imre

Monterey, California: Naval Postgraduate School

NPS NRP Executive Summary
Cyber/Radio Frequency Military Deception in Naval Operations
Network Emulation of Signals Intelligence for Marine Air Ground Task Force Training
Report Date: 12/31/19 Project Number (IREF ID): NPS-19-N036-A and NPS-19-M185-A
Naval Postgraduate School Graduate School of Operations and Information Sciences

MONTEREY, CALIFORNIA

CYBER/RADIO FREQUENCY MILITARY DECEPTION IN NAVAL OPERATIONS / NETWORK EMULATION OF SIGNALS INTELLIGENCE FOR MARINE AIR GROUND TASK FORCE TRAINING

Period of Performance: 10/15/2018–12/31/2019

Researchers:
Principal Investigator (PI): Dr. R. William Maule, GSOIS, Information Sciences
Principal Investigator (PI): Dr. Imre L. Balogh, GSOIS, MOVES Institute
Additional Researcher(s): Mr. Christian R. Fitzpatrick, GSOIS, MOVES Institute

Prepared for:
Topic Sponsor Lead Organization(s):
N2/N6 - Information Warfare and HQMC Plans, Policies & Operations (PP&O)
Navy Topic Sponsor Organization: OPNAV N2/N6 TENCAP
Navy Topic Sponsor Name: Mr. Michael E. Corner, michael.corner.ctr@navy.mil, (703) 695-7529
Marine Topic Sponsor Organization: II Marine Expeditionary Force (II MEF)
Marine Topic Sponsor Name: Mr. Jeremy Hoff, jeremy.hoff@usmc.mil, (910) 451-5628

NPS NRP Executive Summary

Cyber/Radio Frequency Military Deception in Naval Operations
Network Emulation of Signals Intelligence for Marine Air Ground Task Force Training
Report Date: 12/31/19 Project Number (IREF ID): NPS-19-N036-A and NPS-19-M185-A
Naval Postgraduate School Graduate School of Operations and Information Sciences

EXECUTIVE SUMMARY

Project Summary

The research integrates two previously discrete projects on cyber and electronic warfare. The Navy project focuses on cyber/radio frequency (RF) for operational military deception (MILDEC), while the Marine Corps project focuses on cyber/RF for Marine Air Ground Task Force (MAGTF) training. The combined projects collectively address next-generation electronic warfare and warfighter training. This report established spectrum models and signal instrumentation for cyber/RF MILDEC and training. Analysis included processes to monitor and assess tactical information, manage RF and communication signals, and manipulate data for cyber effects.

Keywords: *cyber, radio frequency, RF, military deception, MILDEC, signals intelligence, SIGINT, training*

Background

The Department of Defense has been creating new infrastructure to organize cyber and electronic warfare, however, the technologies are not fully realized to manage these new capabilities in terms of infrastructure and specialized warfighter skills. Research is needed to define infrastructure for tactical RF-to-cyber and design warfighter training for operational implementation, and is advanced through four objectives in two use-cases (UC):

- UC 1: Extend Sea Trial research in spectrum and cyber signal management
- UC 1: Model instrumentation for cyber/RF architecture and tactical effects
- UC 2: Define hardware and user-interfaces for training design and development
- UC 2: Define optimal network topology to emulate RF-to-cyberspace models

Findings and Conclusions

The models, workflows, and instrumentation in this research present operational methods, and the analytics provide status for command decision support. Specifically, implementation addresses tactical clouds, data science for real-time assessment, and artificial intelligence (AI) for predictive analytics, sensors assess the radio spectrum, agents measure network traffic, and data science provides visualizations with detailed analysis, while machine learning and AI support execution automation.

In this work, training techniques and technologies for cyber/RF MILDEC were investigated, and scenarios for distributed cyber/RF operations were designed. Signals in the RF physical environment included: Wi-Fi, commercial cellular, ultra-high frequency, very high frequency, and satellite communications. Additionally, nodes were emulated for tactical communications with state and non-state actors, and command operations were evaluated in a congested signals intelligence and cyberspace environment.

NPS NRP Executive Summary

Cyber/Radio Frequency Military Deception in Naval Operations

Network Emulation of Signals Intelligence for Marine Air Ground Task Force Training

Report Date: 12/31/19 Project Number (IREF ID): NPS-19-N036-A and NPS-19-M185-A

Naval Postgraduate School Graduate School of Operations and Information Sciences

Recommendations for Further Research

Future research may extend our models, methods and instruments in specific operational scenarios, and develop the database to automate execution. Additionally, AI and machine learning capabilities may be extended, and training for specific scenarios based on defined operational contexts can be designed and developed.

Acronyms

artificial intelligence	AI
Marine Air Ground Task Force	MAGTF
military deception	MILDEC
Modeling Virtual Environments and Simulation	MOVES
radio frequency	RF
signals intelligence	SIGINT
use-case	UC