NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

JOINT OPERATIONS CENTER TACTICAL ASSAULT KIT (JOCTAK): EVOLUTION TOWARD SCALABLE MULTILATERAL SOF C4I

by

Daniel W. Bandy, Jay D. Parsons, Aaron L. Goldan,
and Eric A. Mitchell

December 2018

Thesis Advisor:	Leo J. Blanken
Co-Advisors:	Alex Bordetsky
	Doowan Lee
Second Reader:	Steven J. Mullins

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE JOINT OPERATIONS CENTER TACTICAL ASSAULT KIT (JOCTAK): EVOLUTION TOWARD SCALABLE MULTILATERAL SOF C4I	**5. FUNDING NUMBERS**
6. AUTHOR(S) Daniel W. Bandy, Jay D. Parsons, Aaron L. Goldan, and Eric A. Mitchell	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This project builds upon the NPS Advanced Digital Advisor Partnering Technologies (ADAPT) project, formerly known as the Remote Advise and Assist (RAA) kit. The RAA kit was developed to fill the policy gap that prohibited U.S. forces from accompanying partner forces. ADAPT expands the RAA technology beyond the Direct-Action mission set to all potential mission types. The NPS research team proposes the development of JOCTAK, a unified TAK solution that can aggregate and display critical relevant information from the network of users and sensors. Much like ATAK, JOCTAK has the potential to display mission-specific and sensor information at the individual operator level, but also to aggregate and instantaneously analyze data and information from multiple units and sensors across the operational area. The capability to do so provides an operational level COP that facilitates timely decision making by both the commander, staffs, and tactical elements. In addition to aggregating the numerous flows of information into a single comprehensive system, it repurposes the Remote Advise Assist concept to CWMD operations. An integrated TAK system would allow nuclear and CWMD subject matter experts who are not organic to the DOD, or not physically located in the JOC, to remotely advise and assist U.S. and partner forces in response to a CWMD operation.

14. SUBJECT TERMS Advanced Digital Advisor Partnering Technologies, Joint Operations Center Tactical Assault Kit, commercial-off-the-shelf, Remote Advise and Assist, multi-domain battle, C4ISR, CWMD	**15. NUMBER OF PAGES** 133
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

JOINT OPERATIONS CENTER TACTICAL ASSAULT KIT (JOCTAK): EVOLUTION TOWARD SCALABLE MULTILATERAL SOF C4I

Daniel W. Bandy
Captain, United States Army
BBA, American Intercontinental University, 2004
MBA, California State Polytechnic University-Pomona, 2007

Jay D. Parsons
Major, United States Army
BS, Wichita State University, 2006

Aaron L. Goldan
Lieutenant, United States Navy
BS, University of Utah, 2012

Eric A. Mitchell
Major, United States Army
BA, Lindenwood University, 2006

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN DEFENSE ANALYSIS (IRREGULAR WARFARE)
and
MASTER OF SCIENCE IN DEFENSE ANALYSIS (TERRORIST OPERATIONS & FINANCING)

from the

NAVAL POSTGRADUATE SCHOOL
December 2018

Approved by: Leo J. Blanken
Advisor

Alex Bordetsky
Co-Advisor

Doowan Lee
Co-Advisor

Steven J. Mullins
Second Reader

John J. Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This project builds upon the NPS Advanced Digital Advisor Partnering Technologies (ADAPT) project, formerly known as the Remote Advise and Assist (RAA) kit. The RAA kit was developed to fill the policy gap that prohibited U.S. forces from accompanying partner forces. ADAPT expands the RAA technology beyond the Direct-Action mission set to all potential mission types. The NPS research team proposes the development of JOCTAK, a unified TAK solution that can aggregate and display critical relevant information from the network of users and sensors. Much like ATAK, JOCTAK has the potential to display mission-specific and sensor information at the individual operator level, but also to aggregate and instantaneously analyze data and information from multiple units and sensors across the operational area. The capability to do so provides an operational level COP that facilitates timely decision making by both the commander, staffs, and tactical elements. In addition to aggregating the numerous flows of information into a single comprehensive system, it repurposes the Remote Advise Assist concept to CWMD operations. An integrated TAK system would allow nuclear and CWMD subject matter experts who are not organic to the DOD, or not physically located in the JOC, to remotely advise and assist U.S. and partner forces in response to a CWMD operation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

ADA	air defense artillery
ADAPT	Advanced Digital Advisor Partnering Technology
ADP	Army Doctrine Publication
AFB	Air Force Base
AFRL	Air Force Research Labs
ARAM	adaptable radiation aerial monitor
ARL	Army Research Lab
ATAK	Android tactical assault kit
BGAN	Broadband Global Area Network
C2	command and control
C4I	command, control, communications, computers, and intelligence
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAARNG	California Army National Guard
CACTF	Combined Arms Combat Training Facility
CASEVAC	casualty evacuation
CBRN	chemical, biological, radiological, and nuclear
CENETIX	Center for Network Innovation and Experimentation
CIV	civilian
CJSOTF-I	Combined Joint Special Operations Task Force Iraq
COCOM	Unified Combatant Commands
COP	common operating picture
CoT	cursor on target
COTS	commercial-off-the-shelf
CST	Civil Support Team
CTTSO	Combatting Terrorism Technical Support Office
CWMD	countering weapons of mass destruction
DACAS	digitally aided close air support
DARPA	Defense Advanced Research Projects Agency
DLI	detection, location, and identification
DOD	Department of Defense
DPRK	Democratic People’s Republic of Korea
DTRA	Defense Threat Reduction Agency

FLOT	forward line of troops
GFC	Ground Force Commander
GPS	Global Positioning System
GRG	grid reference graphics
HAZMAT	hazardous material
HQ	headquarters
IGW	internet gateways
INMARSAT	international maritime satellite
IP	Internet Protocol
ISIS	Islamic State in Iraq and Syria
ISOF	Iraqi Special Operations Forces
ISP	internet service provider
ISR	intelligence, surveillance, and reconnaissance
JEM	Joint Effects Model
JIFX	Joint Interagency Field Experimentation Program
JIIM	joint, interagency, intergovernmental, and multinational
JOC	joint operations center
JOCTAK	joint operations center tactical assault kit
JOEF	Joint Operational Effects Federation
JTAC	Joint Terminal Attack Controller
JTF	joint task force
JWARN	Joint Warning and Reporting System
LBNL	Lawrence Berkeley National Laboratory
LLNL	Lawrence Livermore National Laboratory
LOS	line of sight
MANET	mobile ad hoc network
MCE	Mounted Computing Environment
MDB	Multi-Domain Battle Concept
MFK	Mobile Field Kit
MFK-CBRN	Mobile Field Kit Chemical Biological Radiological Nuclear
MIL	military
MPDS	Man-Portable Radiation Detection System
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
NSW	Naval Special Warfare

PACE	Primary, Alternate, Contingency, and Emergency
PEO C3T	Program Executive Office Command Control Communications-Tactical
PLI	personal location indicator
RaFTS	Radiation Field Training Simulator
R/N	radiation/nuclear
RAA	Remote Advise and Assist
RAP	Radiological Assistance Program
RIID	radioisotope identification devices
RMP	robotic mobility platform
SA	situational awareness
SATCOM	satellite communications
SFOD-A	Special Forces Operational Detachment-Alpha
SME	subject matter expert
SOCCENT	Special Operations Command Central
SOCOM	Special Operations Command
SOF	Special Operations Forces
SOJTF	special operations joint task force
SWaP	size weight and power
TAK	Tactical Assault Kit
TIM	toxic industrial materials
TOC	Tactical Operations Center
UAV	unmanned aerial vehicles
UGV	unmanned ground vehicles
USSOF	United States Special Operations Forces
VIRTUS	Virtual Radiation Training through Ubiety System
WAS	wide area search
WebTAK	web-based TAK
WIC	Weapons Instructor Course
WINTAK	Windows Tactical Assault Kit
WMD	weapons of mass destruction
WMN	wireless mesh network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Many people contributed to the completion of our capstone project either from a content standpoint or during the field experimentation portion. We would like to thank Professors Leo Blanken, Alex Bordetsky, and Doowan Lee for their guidance and mentorship during this process. Their guidance in developing and shaping the experiments was instrumental to our success in writing this thesis.

We would also like to thank Steve Mullins, Eugene Bourakov, and Emma Wendt from the NPS CENETIX Research Center for their mentorship and assistance in designing and executing the experiments. Without their technical expertise and hard work, this work would not have been possible. A special thanks is due to Mike Stevens from the NPS CORE LAB for providing valuable insights throughout the project.

We would also like to thank key members of the NPS Defense Analysis department, COL Michael Richardson, Dr. John Arquilla, and Ms. Jennifer Duncan, for their support and guidance during this lengthy project. Special thanks are also due to the JIFX support team's Scott Ahman and Ashley Dobson. Their tireless efforts in supporting all experimentation at Camp Roberts was pivotal to our group's completing all field experimentation.

We would like to express our sincere appreciation to key members of the 95th Civil Support Team, Major Alex Efros and Sergeant Ricardo Ledesma. They provided much needed technical and tactical expertise for sensor testing and integration during our field experimentation phases. Additional thanks are due to the Lawrence Berkeley National Laboratory's Andrew Haefner, Erika Suzuki, and Ryan Pavlovsky, and the Lawrence Livermore National Laboratory's David Trombino, for their subject matter expertise and assistance.

Lastly, we would like to thank our families for their tireless support and patience throughout this long process. Without their constant support, none of this would have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The escalation of concerns surrounding a nuclear armed North Korea has illuminated the operational scope and size that a military response to a nuclear crisis on the Korean Peninsula would require. Such a massive undertaking would necessitate the involvment of multiple disparate U.S. Special Operations Forces (USSOF) and multinational special operations forces (SOF) partners with various chemical, biological, radiological, and nuclear (CBRN) sensor technologies, all of which operate independently with seperate command, control, communications, computers, and intelligence (C4I) systems. At present, there are no unified joint, interagency, intergovernmental, and multinational (JIIM) C4I solutions capable of responding to a countering weapons of mass destruction (CWMD) crisis on the Korean Peninsula. Current Department of Defense (DOD) and U.S. government C4I systems, networks, and CBRN equipment have limited interconnectivity within the U.S. government and with JIIM partners. To address this gap, a C4I system would have to include numerous situational awareness (SA) and command and control (C2) capabilities that also facilitate the free exchange of critical information and CBRN data among JIIM partners.

The crux of all multinational operations, particularly addressing the Democratic People's Republic of Korea (DPRK) nuclear problem set, is the requirement for an unprecedented level of multinational coordination and information sharing. These threats create the necessity for collaboration among international partners and U.S. JIIM partners. A military CWMD operation on the Korean Peninsula would create specific, nuanced technological challenges that must be overcome. Existing military doctrine outlines the requirement for effective C2 systems and discusses the challenges presented by multinational operations. Army Doctrine Publication (ADP) 6–0, *Mission Command*, describes the need for mission command systems to facilitate the development of a common operational picture that enables collaboration and timely decision-making.[1] This

[1] Department of The Army, *Mission Command,* ADP 6–0 (Washington, DC: Department of the Army, 2014), iv.

requirement for multiple stakeholder involvement becomes more apparent in the context of recent research that identifies 143 U.S. government organizations responsible for counter proliferation alone.[2] In "Preparing for a Crisis," John Lyford identifies a complex network of stakeholders both in the United States and internationally that would be involved in a DPRK CWMD scenario. The number of stakeholders speaks to the need for a solution that encompasses both technical and non-technical JIIM collaboration requirements to facilitate the required joint solutions.[3]

The inability to share information rapidly across domains and among JIIM partners often hampers effectiveness, and it is a critical requirement for a timely and effective CWMD response.[4] The requirement for specialized nuclear and radiological sensors specific for SOF CWMD operations depends not only upon operator-level expertise but also upon near real-time analysis. While there are U.S. units specially trained for CBRN and CWMD response, military action in a potential North Korean scenario would require a greater number of SOF and CBRN forces than are currently available.[5] Similar to the use of the Android tactical assault kit (ATAK) used as an advising platform in Syria and Iraq, the ATAK could facilitate the advising of undertrained forces, or enable conventional forces to participate in the CWMD/CBRN missions on the Korean peninsula. Additionally, fielded CBRN equipment must be able to transmit data, and digitally reach back to headquarters for near-instantaneous analysis and decision making. Existing solutions specific to either mission command or CWMD/CBRN operations are insufficient and the current, dated and proprietary technology available to the United States, or a given systems developer, lacks cross-platform communication through a standard language or file format, forcing ad hoc and limited C4I solutions.

---

[2] Erik J. Stanfield, "Lost in Translation: Lessons from Counterterrorism for a More Proactive Weapons of Mass Destruction Strategy" (master's thesis, Naval Postgraduate School, 2017), 12–13. https://calhoun.nps.edu/handle/10945/55539.

[3] John Lyford et al., "Preparing for a Crisis: Network Coordination to Deal with North Korea's WMD" (master's thesis, Naval Postgraduate School, 2017), 2.

[4] Joint Chiefs of Staff, *Multinational Operations*, JP 3–16 (Washington, DC: Joint Chiefs of Staff, July 16, 2013), I6.

[5] Lyford et al., "Preparing for a Crisis," 2.

In a 2016 interview, LTG(R) Tovo, former United States Army Special Operation Command (USASOC) Commander, stated:

> We need a better means to aggregate our data streams and improve the speed and ease with which we synthesize information at the tactical and operational levels. We need a software tool, likely web-based, that aggregates existing feeds into a single interactive interface through which commanders and staffs can plan and execute operations. We also need small, secure, and mobile wireless systems that are capable of accessing and aggregating data stream anywhere a network is available. This includes handheld systems that connect to a networked common operating and intelligence picture and other situational awareness tools. The handheld systems must support ARSOF personnel operating in small, highly dispersed teams within an austere environment, to include denied territory.[6]

A viable solution to this gap exists in the form of currently used SOF technology, especially the Tactical Assault Kit (TAK). At the tactical level, the Android variant of the TAK (ATAK) has proven its ability to provide situational awareness and interoperability among U.S. and partner nation SOF. Our research, spurred by the intesifying nuclear threat the DPRK has posed, has identified gaps within current SOF C4I systems. This research has identified the opportunity to solidify the currently fielded ATAK within tactical-level formations as an SA and command and control (C2) tool for traditional and CBRN operations and scale it for use as a special operations C4I and mission command system. The Tactical Assault Kit (TAK) demonstrate the ability to aggregate and display information and the ATAK's prolific use in SOF operations at the tactical level makes it a logical solution to address this capability gap. The TAK network is adaptable by design, and the system can be expanded from a tactical-level tool to a unified Special Operations Joint Task Force (SOJTF) situational awareness (SA) and mission command system.

By its very nature, the TAK possesses the sort of interoperability and flexibility that will allow it to be easily adapted for use in this capability gap. Our research continued the development of a Joint Operations Center Tactical Assault Kit (JOCTAK), a unified TAK solution that can aggregate and display critical and relevant information from the network

[6] Jeff McKaughan, "Q&A with Lieutenant General Tovo," *Special Operations International,* October 2016, 7–9, https://issuu.com/jeffmckaughan/docs/specops_14-7_final.

of users and sensors. Much like the ATAK, the JOCTAK could display mission-specific and sensor information at the individual operator level but also aggregate and instantaneously analyze data and information from multiple units and sensors across the operational area. This capability could provide a level of understanding that facilitates timely decision-making by commanders, staff, and tactical elements. In addition, to aggregating numerous flows of information into a single, comprehensive system. The inherent technical aspects of CWMD and CBRN operations require the use of specialized sensors and expertise that may reside outside of a tactical military headquarters. An integrated TAK system would allow CBRN subject matter experts (SME) not organic to the DOD or physically located in the joint operations center to remotely advise and assist U.S. and partner forces in real-time during a CWMD operation.

A. CAPSTONE PURPOSE

The purpose of this project is to identify, research, and analyze C2/C4I inefficiencies of SOF operations in a JIIM CWMD environment and to identify possible improvements of interoperability by streamlining and simplifying digital collaboration tools. We continued research and proof of concept experimentation for the development of the Joint Operations Center for the Tactical Assault Kit (JOCTAK), a unified TAK solution that could aggregate and display critical relevant information from a vast network of users and sensors. At the time we began our research, the Combating Terrorism Technical Support Office (CTTSO) had accepted the JOCTAK concept as a capability requirement, and the process for determining its required capabilities had begun.[7] The JOCTAK has the potential to display mission-specific and sensor information from the individual operator level, as well as aggregate and instantaneously analyze data and information from multiple units and sensors across the operational area. The capability to do so would provide an operational-level common operating picture (COP) that facilitates timely decision-making by the commander, staffs, and tactical elements. In addition to aggregating the numerous flows of information into a single comprehensive system, the inherent technical aspects of CWMD and CBRN operations requires the use of specialized sensors and expertise that

[7] Bryan Taylor, personal communication, 24 April 2018.

may reside outside of the headquarters (HQ). An integrated TAK system would allow nuclear and CWMD SMEs that are not organic to the DOD or physically located in the joint operations center (JOC) to remotely advise and assist U.S. and partner forces in real time, during a CWMD operation (Figure 1).

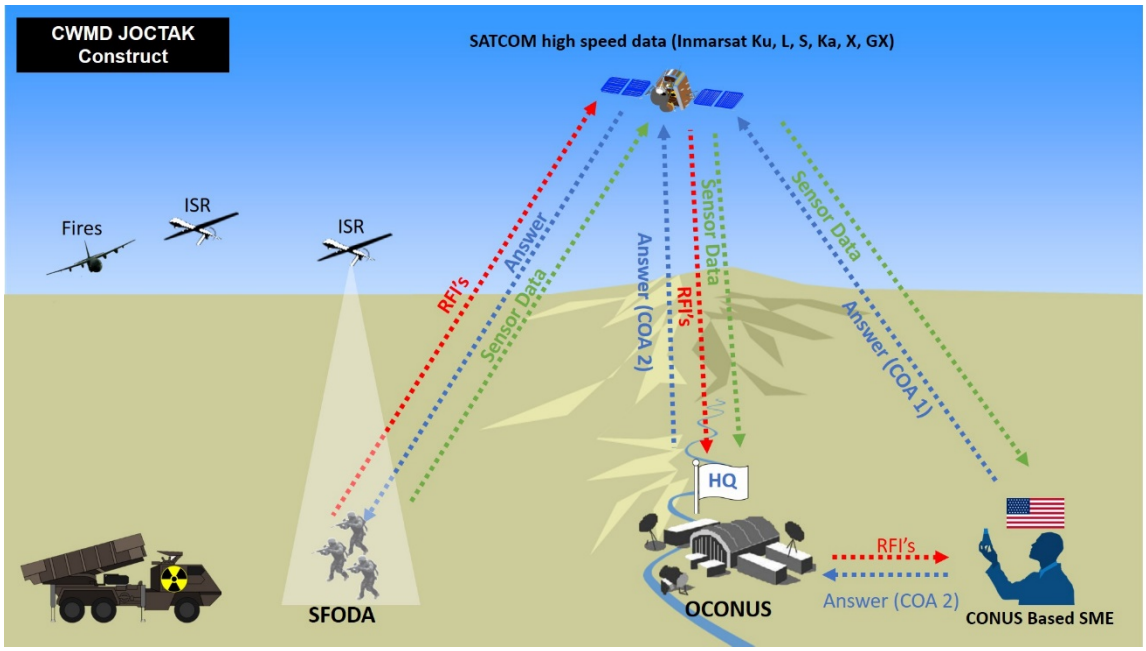

Figure 1. CWMD JOCTAK construct

Given the inherent JIIM nature of CWMD and SOF operations, we identify gaps in two main areas that warrant further research and what we believe would make the most significant impact on operations. First, integrate CBRN sensor capability into existing tactical level C4I technology. Second, develop a comprehensive operational level C4I solution that is dynamic enough to meet the needs of SOF, JIIM, and CWMD operations.

Although multiple CBRN software solutions currently exist, the ATAK's demonstrated effectiveness and capabilities as an SA and tactical-level C2 tool during combat operations have made it the SOF technical solution of choice. The ATAK's status as a program of record within Special Operations Command (SOCOM) and managed by Special Operations Mission Planning Environment will only further promulgate its usage. Therefore, the integration of CBRN-sensor technology into the ATAK warrants further

research with the goal of minimizing the technological burden of warfighters and consolidating sensor data into a single technological solution. This would provide the most comprehensive understanding of the operational environment and apply to all aspects of the mission.

The same multiplicity and duplication of CBRN systems applies to mission command systems. The JIIM component of CWMD operations demands a software solution flexible enough to adapt and support all missions. Commanders must be able to make timely decisions facilitated by accurate information and input from all relevant stakeholders. If scaled correctly, this collaboration could be enabled through the versatility of the TAK infrastructure. Therefore, the second thrust of our effort is to research and analyze the effectiveness of the TAK infrastructure as an operational level C4I solution. We looked to develop ideas that could enable the seamless transfer of information, collaboration, and interoperability between SOF elements, a joint task force (JTF) HQ, and JIIM stakeholders unrestricted by geography or distance.

Furthermore, the scaled integration of the TAK technologies into SOF CWMD operations allows the continued expansion of the ATAKs use beyond familiar and proven applications. The previous utilization of the ATAK as a Remote Advise and Assist (RAA) tool between Special Forces detachments and Iraqi SOF partners can now be reimagined to a U.S.-based SME advising a Special Forces detachment that is on a mission outside of the continental United States. The technical requirements of CBRN operations could quickly escalate beyond the knowledge depth within the tactical unit or headquarters. For example, analysis of a specific CBRN sensor reading, or the discovery of an unknown device or substance, could be routed directly from a SME to the Special Forces detachment through the TAK software.

B. RESEARCH QUESTIONS

1. How can the expansion of the TAK concept to the joint operational level in the form of a JOCTAK improve the collective planning, mission command, and digital collaboration between JIIM partners during a CWMD operation?

2. How can the TAK-compatible CBRN sensors, and CBRN plug-ins, improve the RAA capability among operators, technical specialists, and mission command during a CWMD scenario?

3. What are the necessary CWMD sensor components and TAK plug-in software designs for meeting future JIIM mission sets?

C. OBJECTIVES

The objective of this research is to test a proof of concept by demonstrating the feasibility of expanding the TAK network to act as an operational-level C4I mission command system for CWMD operations and provide feedback to the development of a JOCTAK by focusing on the following:

1. Demonstrate, as a proof of concept, the feasibility of expanding the ATAK from a tactical-level capability to an operational-level C4I mission command system for CWMD operations.

2. Envision how USSOF would work with partners in a CWMD scenario, connecting them through a federated TAK infrastructure.

3. Identify end user requirements for the JOCTAK.

D. SCOPE

This research followed a ground-up approach to improve the effectiveness of SOF units conducting CWMD operations through testing of tactical-level CWMD sensor technology and its integration into the TAK infrastructure. The usefulness of tactical level units in a CWMD environment is predicated on their ability to detect, locate, and efficiently identify radiological material.[8] Coordinating the sensory information in near real-time from multiple tactical level units/sensors is required for efficient large-scale CWMD mission sets as well as the ability to perform RAA to tactical elements from CWMD SMEs in a timely manner. Once incorporated into the TAK, these technologies provide the groundwork for use as a comprehensive operational-level JOC technology suite providing the SA tools necessary for JIIM operations against weapons of mass destruction (WMD) threats.

E. ORGANIZATION OF THESIS

Chapter II reviews significant background information, guiding doctrine, and familiarization with the TAK and its previous use. Chapter III discusses the application of the TAK system applied as a CWMD C4I system and includes a series of vignettes that illustrate the added value to both the tactical level warfighter and the operational level command. Chapter IV details the iterative experimentation process we performed to identify capability gaps in the ATAK system to determine what needs to be done to develop and expand use of the TAK to the joint operations center. Chapter IV also contains our recommendations for the development of the JOCTAK. Chapter V is our conclusion and discusses findings regarding our research questions in the context of the overall framework of CWMD JIIM C4I solutions.

[8] Alex Bordestsky, personal communication, May 2018.

II. LITERATURE REVIEW

In August 2016, a presidential memorandum transferred the DOD CWMD "integrating and synchronizing" efforts from U.S. Strategic Command to the U.S. Special Operations Command.[9] Today, joint warfighting concepts are still transitioning from traditional to nontraditional threats. This change in focus addresses current and future operational environments. The traditional threat, the Cold War peer-to-peer battlefield scenario, focused primarily on the air-land battle concept and combined arms maneuver warfare. The new, nontraditional environment is characterized by threats from multiple domains, including the evolution of traditional weaponry and the emergence of cyber threats. Additionally, the new environment needs to account for growing nontraditional threats from non-state actors as well as smaller belligerent nation-states such as Iran and, most recently, North Korea.

Threats posed by North Korea, China, and Russia are at levels not experienced since the height of the arms race between world superpowers during the Cold War.[10] Fortunately, the gravity of these threats is understood and efforts to quell them persist. The 2017 National Security Strategy identified the threat and defense against nuclear, chemical, radiological, and biological WMD as a top priority. "Building on decades of initiatives, we will augment measures to secure, eliminate, and prevent the spread of WMD and related materials, their delivery systems, technologies, and knowledge to reduce the chance that

[9] President Obama's amendment of the Defense Secretary's 2005 directive designating U.S. Strategic Command the lead command for "integrating and synchronizing DoD in combating WMD," which changed the lead command to U.S. Special Operations Command. Donald H. Rumsfeld, "Designation of Responsibilities for Combating Weapons of Mass Destruction to Commander, U.S. Strategic Command" (Washington, DC: Office of the Secretary of Defense, 2005); Under Secretary of Defense for Policy, *DoD Countering Weapons of Mass Destruction*, DoD Policy Directive 2060.02 (Washington, DC: Under Secretary of Defense for Policy), 10.

[10] William J. Perry, "Twitter Post," January 3, 2018, https://twitter.com/secdef19/status/948774922884562944?lang=en.

they might fall into the hands of hostile actors. We will hold state and non-state actors accountable for the use of WMD."[11]

Recent actions by state actors challenge international norms of nuclear and other types of WMD proliferation and aggression. For example, for more than two decades North Korea has continued its pursuit of nuclear weapons despite promises to the contrary. According to a March 2018 Foreign Policy Report, "Pyongyang's nuclear weapons and missile programs are far more advanced than at any previous time."[12] While discussing recent developments of the North Korean regime's nuclear program, United Nations Secretary-General António Guterres explained that they have "broken the global norm against nuclear test explosions" calling it "profoundly destabilizing for regional and international security."[13] While recent U.S. diplomacy efforts appear to have silenced ongoing progress, recent reports indicate the North Korean regime is likely to continue its efforts despite sanctions and the U.S. North Korean summit.[14]

Terrorist organizations and illicit actors also represent a significant WMD threat to the United States. In addition to the United States, eight other countries possess nuclear weapons, and as many as 12 maintain stockpiles of chemical and biological weapons and possible delivery systems.[15] The interconnectivity of today's world means that non-conforming countries with nuclear programs represent threats not only from their regimes but also risk proliferation of the world's most destructive weapons to transnational terrorist organizations around the globe.[16] Terrorist organizations and hostile governments'

---

[11] White House, *United States National Security Strategy 2017* (Washington, DC: U.S. Government Printing Office, December 18, 2017), 8, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[12] Robbie Gramer and Emily Tamkin, "Decades of U.S. Diplomacy with North Korea: A Timeline," *Foreign Policy* (March 12, 2018), https://foreignpolicy.com/2018/03/12/a-timeline-of-u-s-negotiations-talks-with-north-korea-trump-kim-jong-un-pyongyang-nuclear-weapons-diplomacy-asia-security/.

[13] Antonio Guterres, "Opening Remarks at Press Encounter," United Nations Secretary-General, September 5, 2017, https://www.un.org/sg/en/content/sg/speeches/2017-09-05/secretary-generals-press-encounter.

[14] Gramer and Tamkin, "Decades of U.S. Diplomacy with North Korea."

[15] "Nuclear Weapons: Who Has What at a Glance," Arms Control Association, accessed August 10, 2018, https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

[16] White House, United States National Security Strategy 2017, 8.

willingness to employ some type of WMDs both against their people and abroad exacerbates the risk. The Syrian government is a demonstrable case in point.[17] In addition to the continued risk of WMD use against its own population, the fractured state of the Syrian government and the presence of terrorist organizations on its soil risk the spread of these weapons and chemicals to other terrorist organizations around the world.

In addition to smaller belligerent powers, other near-peer states continue their efforts to mitigate U.S. interests around the globe and continue development of nuclear armaments and military advancements. The 2017 U.S. National Security Strategy identifies this and warns that, "China and Russia want to shape a world antithetical to U.S. values and interests ... [China's] nuclear arsenal is growing and diversifying." While, "Russia aims to weaken U.S. influence in the world and is investing in new military capabilities, including nuclear systems that remain the most significant existential threat to the United States."[18] The threat that these powers represent risks not only to U.S. national interests but also to the safety of the people in surrounding regions. Nuclear technologies and hostile governments threaten Eastern Europe in a manner similar to the threat posed by North Korea to countries throughout the South China Sea as well as South Korea and Japan.

A. THE OPERATIONAL ENVIRONMENT

We determined that any proposed solutions needed to be grounded in the realities of the current operational environment. Because of this we took into consideration the DoD mission command, and CWMD doctrine, as it guides and constrains our uses and implementation of solutions as well as the multi-domain nature of the environment its self.

1. Doctrine

Much of the existing CWMD doctrine is based on countering and addressing a near-peer enemy and the concept of mutually assured destruction in the event of a nuclear incident. This doctrine and the accompanying mindset are dated in that they have

---

[17] "Statement by the NATO Secretary General on the Actions against the Syrian Regime's Chemical Weapons Facilities and Capabilities," NATO, accessed August 22, 2018, http://www.nato.int/cps/en/natohq/news_153661.htm.

[18] White House, United States National Security Strategy 2017, 25.

foundations set in an environment that is pre-internet, where there was a much lower level of interconnectivity and less anonymity.

a. The Multi-Domain Environment

From an operational environment perspective, the U.S. Army, the U.S. Marine Corps, and the DOD are taking notice about how the current CWMD problem set differs from Cold War-era doctrine. In a March 2017 Multi-Domain Battle (MDB) concept paper written by COL Bill Dries, strategist at the Air Staff's Concept Division, indicates that all military services and U.S. government agencies are encouraging the DOD to "think, plan, and operate with a multi-domain approach."[19] Currently, we operate in five domains: maritime, air, land, space, and cyber. Moreover, it is these five domains that the U.S. military uses to define the requirements of the future force, to conduct planning, and to carry out joint operations.[20] While the multi-domain approach to battle is not a new concept, a near-peer adversary's ability to undermine our advantages is a recent development that threatens the United States and its allies and partners. For example, an effective cyber-attack, such as the one conducted against the Ukrainian power grid in December 2016, could disrupt the U.S. network architecture long enough for a state-level actor, such as North Korea or Russia, to seize the initiative. By using technology to its advantage, an adversary can now wage a multi-domain attack that is difficult to detect, attribute to a particular actor, and defend against; thus, reducing our military advantage and threatening national security.[21] To counter these asymmetrical challenges that would deny us "operational access, basing, communications, and freedom of action," we must accelerate the adoption and application of the MDB concept.[22]

An August 2017 paper co-authored by GEN Robert B. Brown and GEN David G. Perkins expanded upon the MDB topics discussed by COL Dries. They contend that to be

---

[19] William Dries, "Some New, Some Old, All Necessary: The Multi-Domain Imperative," War on the Rocks, March 27, 2017, https://warontherocks.com/2017/03/some-new-some-old-all-necessary-the-multi-domain-imperative/.

[20] Dries.

[21] Dries.

[22] Dries.

prepared for the next war, the U.S. military "must effectively innovate and adapt concepts, equipment, and training … where integration into joint and multinational forces is a prerequisite for victory. To get there, we must establish a clear path to prepare the force for the fight tonight, tomorrow, and in the future."[23] The battle tonight and in the next five years will require the U.S. military to "employ existing forces, capabilities, and operational designs" while simultaneously "moving concept to doctrine in a way that guides technologically advanced weapons, systems, and modernized facilities with which to train."[24] The battle tomorrow, from 2022 to 2030, will require moving beyond our current capabilities in order to project our power globally and assure allies. The authors highlight that this requires a multi-domain task force that "will strike critical enemy targets with a combination of lethal and non-lethal means … protect friendly forces and critical nodes."[25]

b. Mission Command Doctrine

In a multi-domain environment, it is incumbent upon a joint force to operate efficiently and effectively. The accomplishment of the mission and command and control or mission command is facilitated by mission command systems. Our primary focus is increasing mission command and C2 functions while developing a common operational picture at the JTF level. It is essential to understand the principles of the mission command and CWMD/CBRN tactics techniques and procedures, in both unilateral and multinational scenarios.

Joint military and Army doctrine define mission command as a philosophy and a warfighting function; but, ultimately, it is a commander's authority to lead, enable, and conduct operations. More specifically, through the mission command warfighting function, C2 of forces is enabled through mission command systems. These systems (personnel, networks, information systems, processes and procedures, and facilities and equipment)

---

[23] Robert B. Brown and David G. Perkins, "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight," War on the Rocks, August 18, 2018, https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/.

[24] Brown and Perkins.

[25] Brown and Perkins.

facilitate the development of a common operational picture and enable collaboration.[26] These systems provide commanders the information necessary to make critical decisions to apply forces and enablers in support of operations.

Multinational operations present numerous information challenges that commanders must overcome to conduct operations successfully. While information sharing is a critical aspect of multinational operations, the inability to do so hampers effectiveness. JP 3–16 discusses international standardization and interoperability as an essential part of cooperation and mission success. Although interoperability and standardization pertain to other areas of military operations such as doctrine, procedures, and training, they are most frequently identified with communications and technology. The ability of multinational partners to communicate and share information and intelligence in a timely matter can often determine the success of operations.[27] The U.S. Army recognizes this, and despite significant efforts toward resolution, technical interoperability remains a significant challenge in the conduct of multinational operations. The U.S. Army's Program Executive Office for Command Control and Communications-Tactical (PEO C3T) is working toward not only transforming U.S. C4I systems that prioritize interoperability but also assisting coalition partners. One venue PEO C3T utilizes to determine interoperability requirements is during the conduct of multinational warfighting exercises. These exercises represent not only an evaluation opportunity for new U.S. systems but also the testing of interoperability with partner systems. The Director of Communications and Congressional Affairs for PEO C3T, Paul Mehney, describes the lack of a single coalition network or standard as a longstanding issue. Each coalition partner has its requirements, baselines, and standards to meet its unique network requirements, missions, and capabilities.[28]

---

[26] Department of the Army, *Mission Command*, ADP 6–0 (Washington, DC: Department of the Army, 2014), iv.

[27] Joint Chiefs of Staff, *Multinational Operations*, JP 3–16 (Washington, DC: Joint Chiefs of Staff, 2013), I-6.

[28] Paul D. Mehney, "U.S. Army Marches Toward Coalition Interoperability," *Signals*, March 2018.

c. CWMD Doctrine

As operations and challenges increasingly overlap multiple domains, issues involving WMD and CBRN threats require more JIIM resources, and the need for effective command and control of forces, interoperability, and a common operational picture becomes necessary. JIIM collaboration and the involvement of numerous other organizations create unique challenges for obtaining accurate situational awareness of the operational environment.[29] ADP 6–0, *Mission Command*, identifies the development of a shared understanding as a critical task but defining challenge for commanders, staffs, and forces in the conduct of operations.[30] Networks and information systems are critical components of this because they are the primary means by which commanders leverage connectivity to control forces, apply assets, and share their understanding of the situation to higher echelons of command for strategic decision-making.

2. Evolution of the TAK

a. What Is The TAK?

The Tactical Assault Kit (TAK) is a tactical software solution that facilitates situational awareness (SA) and command and control (C2) through Global Positioning System (GPS) and associated map data. The TAK displays user-defined mission-specific information using military standard iconography, and live-data streams. It does this by incorporating Cursor on Target (CoT) data format standards that allow communication and data dissemination across multiple communication substrates. The TAK is currently a program of record managed by the U.S. Special Operation Command, and is under constant development by industry and defense research labs, to meet end-user requirements.[31]

In 2010, Air Force Research Labs (AFRL), Army Research Lab (ARL), The Defense Advanced Research Projects Agency (DARPA), in conjunction with industry research partners, began developing a SA tool based on the Android platform of mobile

---

[29] Joint Chiefs of Staff, "Multinational Operations (JP 3–16)," I-6.

[30] Department of the Army, *Mission Command*, 3.

[31] "Home," TAK, accessed August 23, 2018, https://takmaps.com/.

devices to meet the variety of end-user size, weight, and power requirements (SWaP).[32] The tactical-level Android variant of the TAK, ATAK (Android Tactical Assault Kit), quickly gained popularity within the special operations community, and feedback along with mission-specific requirements drove the development of additional capabilities. Open-source coding allows significant input from the tech community to meet additional need requirements through extensions known as plug-ins. Since its inception, the ATAK's focus on end-user capability has produced more than 90 plug-ins developed by partner organizations to meet specific requirements. These additional applications include video, chat, causality evacuation (CASEVAC), Call for Fire, Digitally Aided Close Air Support (DACAS) 9 Line, and intelligence, surveillance, and reconnaissance (ISR) sensor control.[33]

Tactical-level SA is not a new idea; it was the focus of the Army's Land and Net Warrior programs. However, a significant difference between those programs and the ATAK is the ATAK's readily available coding, which has enabled a vast network of developers to contribute solutions. The software's availability, compared to a proprietary system, has allowed the constant development of the ATAK and the TAK network to meet a variety of demands as well as be continuously upgraded to account for evolving technologies and hardware platforms. The ATAK's utility is also its ability to communicate across multiple communication substrates and among multiple other programs and systems. The TAK's network ability to receive and transmit multiple simple and complex message and data formats facilitates its communication with the various technologies found on today's battlefield. This is accomplished by directly programming the enabling technologies' messaging format during plug-in development or by utilizing multiple file format languages organic to the TAK, particularly the Cursor on Target coding, language, and message routing concepts. According to the MITRE Corporation:

> The Cursor-On-Target (CoT) data strategy centers on the use of a "common language" for tactical systems that is critical in communicating much

[32] Kyle Usbeck et al., "Improving Situation Awareness with the Android Team Awareness Kit (ATAK)," ed. Edward M. Carapezza, 2015, 5, https://doi.org/10.1117/12.2180014.

[33] Josh Sterling, "TAK LSE Brief," Milsuite (PowerPoint, USSOCOM 2018 TAK Working Group, Pinehurst, North Carolina, August 13, 2018), https://www.milsuite.mil/books/groups/2018-tak-off-site.

> needed time sensitive position information. Analogous to functioning acceptably in foreign countries, while only learning a few important words of the native language, CoT starts with a focus on a particular set of important common information on the battlefield. This is seen as a time sensitive position or the "What, When, and Where" (W3) of a specific event. The proof of concept prototype also allows for structured special purpose extensions.[34]

The continuous demand for the ATAKs and its flexibility to adapt to user-specific requirements led to the expansion of the TAK network to include Windows (WinTAK), web-based (WebTAK), and civilian (ATAK-Civ) versions.[35]

- WinTAK is a Windows operating system TAK-variant developed in conjunction with the ATAK to provide similar functionality on a PC or Windows platform.

- ATAK-Civ was developed for use on the Android platform to meet U.S. federal, state, local, and first responder requirements.

- WebTAK is a server-hosted version of the TAK available for use through a web browser.

The continued interest and easily accessible development solutions of the TAK network have resulted in a robust capability that continues to gain traction within the defense and related communities. Its low cost of entry and evolving software infrastructure adapts to changing technology, and hardware requirements make it a solution likely to endure.

---

[34] Michael J. Kristan et al., "Cursor-on-Target Message Router User's Guide," MITRE Corporation, 2009, 2.1, https://www.mitre.org/sites/default/files/pdf/09_4937.pdf.

[35] The naming convention and nomenclature of the ATAK has changed numerous times since its original development. Originally named the Android Team awareness kit (ATAK) was changed to the Android Tactical Assault Kit (ATAK) after the development of a military use version. To better clarify, the two Android versions are now referred to as ATAK-MIL and ATAK-CIV. This distinction was made to emphasis the use of the civilian version by domestic law enforcement and other U.S. government agencies and that it lacks certain combat related features. Typically, the system is referred to only as ATAK or by the slang terms Civ-TAK and Mil-TAK. For the purpose of this paper unless otherwise and specifically annotated the use of ATAK applies to either version. Similarly our use of the term TAK is describing the whole network or versions, platforms, and capabilities.

b. The TAK's Contribution to RAA

The evolution of remote, advise and assist (RAA) technology began in late 2014 with the development of Virtual Accompany Kits by Special Operations Command Central (SOCCENT). Initial efforts for virtual technology were motivated by U.S. policy restrictions limiting U.S. Special Operations Forces (USSOF) from accompanying and being physically present with Iraqi Special Operations Forces (ISOF) in the battle against Islamic State in Iraq and Syria (ISIS). At the request of Special Forces detachments in Iraq, SOCCENT J3 Operations Technology Directorate assisted in the development and filling of initial requirements. The first generation of Virtual Accompany Kits consisted of Samsung smartphones preloaded with the International Traffic in Arms Regulation-compliant version of the ATAK, MyTrax. The Iraq domestic cellular network and a Broadband Global Area Network (BGAN) satellite communications node facilitated connectivity and data flow.[36] This first phase, or prototype—Virtual Accompany Kits—and their role in immediate battlefield successes paved the way for increased development and refinement of the RAA concept. They enabled USSOF to maintain SA and advise and assist partner tactical units despite our physically remote presence.

As interest continued to grow in 2015 and funding was secured, the Naval Postgraduate School began testing myriad commercial off-the-shelf (COTS) products focused on improving the operability of the system. Phase two prototypes included upgrades and incorporation of equipment inherently designed to increase integration with each other. The Android-based smartphones now contained integrated satellite on-the-move capability, on-the-move mapping solutions, and a commercial laser range finder that significantly expanded the end-user range data flow and functionality.[37] The Special Operational Detachment-Alphas (SFOD-A) and Combined Joint Special Operations Task Force- Iraq (CJSOTF-I), newly capable of reliably tracking ISOF partner positions, were able to develop and share a common operational picture of the battlefield. This clarity

---

[36] Christopher Thielenhaus, Pat Traeger, and Eric Roles, "Reaching Forward in the War against the Islamic State," *PRISM: A Journal of the Center for Complex Operations* 6, no. 3 (2016): 100.

[37] Christopher Thielenhaus and Eric Roles, "Virtual Accompany Kits Return to Baghdad: A View from the Front Lines," *Special Warfare* 30, no. 2 (2017): 27.

provided the ability to provide operational fires and needed support through reliable two-way communication during operations against ISIS, resulting in the successful integration of these RAA kits into the CJSOTF-I (Figure 2).

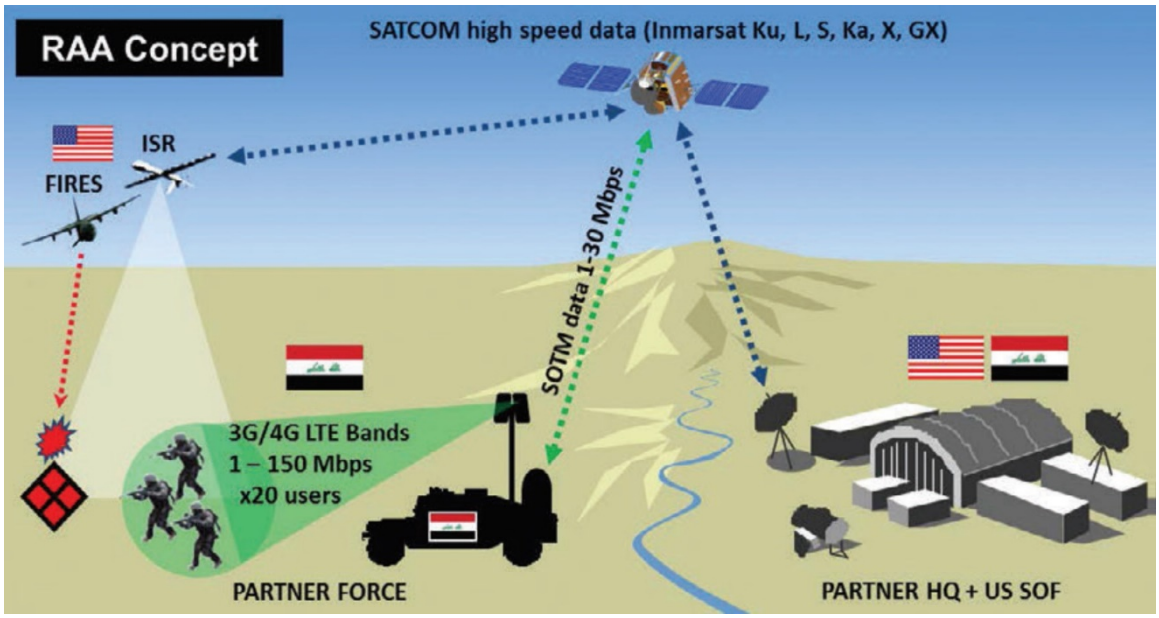

Figure 2. RAA concept[38]

The ATAK's flexibility to adapt to user-specific requirements has led to its continued adoption by multiple U.S. government agencies at the federal and state levels, as well as numerous foreign militaries. Most notably, the ATAK was used to provide C2 to over 2300 officers and agents from nine different militaries and federal, state, and local law enforcement agencies during the 2017 presidential inauguration.[39] In the aftermath of Hurricane Harvey, Air Force Special Tactics Squadrons, the National Guard, and other first responders utilized the ATAK to coordinate emergency recovery efforts.[40] These use-case

[38] Source: Thielenhaus and Roles, 28.

[39] Michael Ferriter and Phil Schupp, *ADAPT Team Inauguration Trip Report* (Herndon, VA: Interagency Joint Operations Center Herndon, VA and Monterey, CA: Naval Postgraduate School, January 2017), 10.

[40] Ryan Conroy, "Special Tactics Saves Lives in Hurricane Harvey Aftermath," U.S. Air Force, August 31, 2017, https://www.af.mil/News/Article-Display/Article/1297004/special-tactics-saves-lives-in-hurricane-harvey-aftermath/.

scenarios represent the TAK network's ability to adapt to large-scale network demands over vast geographic areas as well as meet information and diverse support requirements.

3. Other C4I Systems for Mission Command

a. U.S. Army C4I

When evaluating C4I systems, there are four areas to consider: the method of data transmission (i.e., radio, internet service provider [ISP], cellular, satellite communications [SATCOM]); the hardware required to run the applications; the software applications themselves; and the ability to integrate additional resources, sensors, and capabilities depending on the problem set.

The method of data transmission is both a strength and a weakness regarding current programs used by the DoD. Programs like Warfighter Information Network-Tactical, which now encompasses a multitude of network types, still suffer the shortfalls that affect other U.S. systems in a JIIM environment.[41] These shortfalls are twofold. First, it is difficult to share the same COP with partner nations due to the classification levels of the networks used. Some systems try to mitigate this shortfall, with various chat programs and joint blue force tracking. Unfortunately, these systems often suffer from a lack of use on both sides. Partner and allied nation forces are reluctant to populate the COP with their own unit positions when U.S. units do not trust the less restrictive system with U.S. blue force positions and information. The second is the restricted bandwidth that is a result of remote or austere conditions where the DoD often operates. Many of the newer C4I systems have the capability to function across multiple substrates, circumventing the bottleneck of classified communications by using a shared network.

The next C4I system area of concern faced by the DoD is hardware and software. The military, in general, is fond of proprietary solutions vice COTS solutions. This creates the problem of proprietary hardware and software that does not adapt to keep pace with technology. It constrains the user to specific platforms and software packages provided by

---

[41] Mark Pomerleau, "Here's What the Army's Tactical Network for the Future Will Look Like," C4ISRNET, October 3, 2017, https://www.c4isrnet.com/it-networks/2017/10/02/heres-what-the-armys-tactical-network-for-the-future-will-look-like/.

the company contracted for the initial solution. This is also problematic because many of these systems are not designed to interface with other C4I systems, which may have different manufacturers. The systems are also not always designed to link together to form a cohesive COP. That must be done external to the system by someone on a watch floor or in a JOC/Tactical Operations Center (TOC). Ideally, these systems would allow for upgrades to hardware and software in the same manner as a conventional home computer. Users can replace components or the hardware entirely and still run the same software, or upgrade both, and move their data over to a new system. There is cross-platform compatibility across versions, and it is easy to install additional software/plug-ins that allow added functionality depending on the desired use case.

The U.S. Army has taken initial steps to alleviate this problem by contracting with Systemic Inc. for its SITAWARE suite of C2 programs, which will soon form the foundation of the Army's Mounted Computing Environment (MCE).[42]

(1) SITAWARE

SITAWARE, a commercial system currently in use by Danish, Swedish, and Spanish forces, does come close to meeting these requirements.[43] The DoD recognized the success of this system and, in early 2018, the Army decided to use Systemic's SITAWARE C2 suite, "as the backbone of its developing Mounted Computing Environment (MCE)."[44]

SITAWARE addresses the need to have a common C2 system and messaging structure from the tactical to the operational level, including a shared COP.[45] The system can be used over almost any communications equipment it is plugged into, whether it be radio, cellular, or ISP. Furthermore, the system is designed so that the data packets are very

---

[42] Giles Ebbutt, "US Army Expands Use of SitaWare" (Jane's by IHS Markit, February 9, 2018), 1, http://www.janes.com/article/77780/us-army-expands-use-of-sitaware.

[43] Giles Ebbutt, "Integrated Command and Control from Joint Headquarters to the Tactical Edge," *IHS Jane's International Defence Review*, 47, May 2014: 2–3, http://www.janes360.com/images/assets/724/38724/Systematic_reprint.pdf.

[44] Ebbutt, "US Army Expands Use of SitaWare," 1.

[45] Personal communication with Jeff Flachman, Senior Manager, Defense Sales Systematic Inc., July 20, 2018.

small, approximately 3 to 10 bytes, which allows for more robust communication on low-bandwidth networks or in austere environments with limited connectivity that might result in packet loss.[46]

While SITAWARE allows for partial solutions by providing basic data transfer of COP and communication information from tactical units to mid-level and finally operational-level HQs, it falls short when integrating sensor information, including outside inputs into the overall COP, or allowing the reach back to SMEs.[47] The capacity exists for the SITAWARE network to transfer data from any type of sensor or piece of equipment that can be connected to a field radio; however, it does not fuse the information provided by the equipment into the overall COP. SITAWARE comes close to being an ideal solution but falls short simply due to the nature of its origin; it is a contracted system from a single supplier.[48]

(2) Joint Operational Level CBRN/CWMD C4I Systems

The current guidance for joint operations concerning countering weapons of mass destruction, Joint Publication 3–40, *Countering Weapons of Mass Destruction,* makes no mention of the systems used for C2, C4, or C4ISR.[49] This is not surprising, since it provides strategic, or at best, operational-level guidance. At the tactical level, the current CBRN/CWMD systems outlined in the latest update—October 31, 2013—to the ATP 3–11.36, *Multi-Service Tactics, Techniques and Procedures for Chemical, Biological, Radiological, and Nuclear Aspects of Command and Control*, are often specific to one portion of the C4ISR structure. Because of this, the systems lack interconnectivity to a unified operating system that is accessible from both the operational and tactical levels. In a CBRN scenario that requires multiple sensors, "many CBRN agent detector and alarm arrays operate as independent units; therefore, when a CBRN attack is detected, only those

---

[46] Flachman.

[47] Flachman.

[48] Ebbutt, "Integrated Command,"1-6.

[49] Joint Chiefs of Staff, *Countering Weapons of Mass Destruction*, JP 3–40 (Washington, DC: Joint Chiefs of Staff, 2014).

personnel in the immediate vicinity hear the alarm. Adjacent units need to be notified by radio, wire communications, audible means, or verbal means."[50]

Furthermore, many of the current CBRN/CWMD C4I systems communicate using classified methods, which inhibit JIIM interoperability and complicate coordination among JIIM units. Following are brief descriptions that show the reactive mindset inherent in most of these systems. These systems are designed primarily for use at the operational level; there is little to no integration with tactical level units.

JWARN: Joint Warning and Reporting System

> The JWARN primarily provides an integrated early warning capability, an IM system, and a capability to analyze the OE. It provides the capability to query and disseminate critical, time-sensitive CBRN defense information throughout the OE to enhance overall force protection. There are five primary mission essential functions performed by JWARN: SA, warning, reporting, hazard prediction; and "basic" battle management analysis. The JWARN implements these functionalities to provide an enhanced CBRN defense capability for the warfighter.[51]

JEM: Joint Effects Model

> The JEM provides a single, DOD-approved methodology and model that provides a common representation of CBRN hazard areas and effects resulting from CBRN weapons and TIM. Operationally, JEM supports operational and crisis action planning to mitigate the effects of WMD, to include weapons with CBRN payloads and accidental TIM releases. Additionally, JEM assists DOD components and allied or coalition forces by providing CBRN and TIM hazard predictions and effects to the warfighter during and after an incident. Analytically, JEM assists DOD components and allied or coalition forces to train jointly develop doctrine and tactics; and assess warfighting, technology, material development proposals, and force structure. The JEM is interoperable with selected command, control, communications, computers, and intelligence (C4I) systems. Software applications on those C4I systems (JWARN) use JEM to provide an enhanced prediction of hazard areas to provide a detailed warning to U.S. forces within those areas. Operational effects systems on those C4I systems (JOEF) uses JEM to predict hazard areas. JEM may also

---

[50] Joint Chiefs of Staff, *Operations in Chemical, Biological, Radiological, and Nuclear Environments*, JP 3–11 (Washington, DC: Joint Chiefs of Staff, 2013), F-5.

[51] Joint Chiefs of Staff, F-2.

be operated as a stand-alone application that is not interfaced or networked with a C4I system.[52]

JOEF: Joint Operational Effects Federation

> The JOEF "provides automated decision support tools that enable the joint force commander to more effectively and efficiently assess risk and allocate scarce resources in preparation for and during operations involving CBRN and [toxic industrial materials] (TIM) hazards."[53]

(3) Tactical-Level CBRN Systems

In terms of a dedicated CBRN response unit, the U.S. Army National Guard has Stationed Weapons of Mass Destruction Civil Support Teams (CTS) in all 50 states.[54] In the event of a chemical, biological, radiological, nuclear, or high-yield explosives incident, these teams provide support to domestic authorities.[55]

The mission statement of the National Guard's Civil Support Teams is:

> Identifying CBRN agents/substances, assessing current or projected consequences, advising on response measures, and assisting with appropriate requests for additional follow-on state and federal military forces. Units can also provide immediate response for intentional and unintentional CBRN or hazardous material (HAZMAT) releases and natural or manmade disasters that result in, or could result in, catastrophic loss of life or property.[56]

Because these teams deal specifically with the CBRN/CWMD mission set, they require a C4I system that is tailored to that mission set. For example, the 95th Civil Support Team uses the Adobe connect conferencing tool as an ad hoc cloud-based collaboration system to provide a basic form of C2 and SA. However, it lacks the interoperability and

---

[52] Joint Chiefs of Staff, F-5.

[53] Joint Chiefs of Staff, F-6.

[54] "Weapons of Mass Destruction, Civil Support Team," National Guard, December 2017, http://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/Weapons%20of%20Mass%20Destruction%20Civil%20Support%20Team%20Fact%20Sheet%20(Dec.%202017).pdf.

[55] National Guard.

[56] National Guard.

capability of a true C4I or even a C2 system. Currently, the best solution for these teams is the Mobile Field Kit-CBRN (MFK-CBRN).[57]

MFK-CBRN, or simply MFK is a program developed by the DRTA to meet the needs of Civil Support Teams (CSTs). MFK allows for commanders to monitor specific details about the operators on the ground, such as the amount of air remaining in the operators' tanks and the battery charge level in various connected devices. An additional benefit of MFK is that it communicates with the ATAK, appearing as another ATAK server that can pass data across the ATAK network. This adds expanded functionality for CBRN-specific units that require and understand the additional data provided by MFK, while still allowing them to work in conjunction with Army SOF units that have a tactical-level ATAK network.

(4) ATAK CBRN Capability

With CBRN-specific data aggregation and C2 management systems already in use by U.S. forces, why does the USSOF community need to use the ATAK for a possible CBRN/CWMD response? Because the ATAK is already in use by USSOF, while there are CBRN specific solutions, they would require additional equipment. SOF units responding to this mission set would benefit most by leveraging their current equipment to integrate CBRN sensors into their COP. With the CBRN plug-in, the ATAK allows this. The growing threat of a nuclear crisis in the DPRK means there is an ever-increasing possibility that the action required from USSOCOM and JIIM partners will be proactive in nature. These actions will require the capability to coordinate traditional U.S. and partner SOF units to gain and maintain control over DPRK CBRN assets and infrastructure before a nuclear incident or loss of control can occur. This will require C4ISR capabilities not currently available in the standard C2/C4/C4ISR systems. As USSOCOM attempts to determine what a coordinated action against the North Korean infrastructure and assets will look like, it is readily apparent that this problem set will require a tactical C4ISR system different from traditional, operational-level only systems.

[57] DTRA, email message to authors, July 20, 2018.

The ATAK retains its flexibility no matter the use case because it can be loaded onto any hardware that will run on the Android operating system. It can communicate across any network that allows data transfer as long as the hardware has a connection method. Plug-ins are easy to write because the ATAK uses a common commercially available operating system. This flexibility of network and hardware usage means that it can be used on a network with partner nations over joint coms, or configured to work at a higher classification by using secure comms. While it is likely that SOF units will play a separate part in any operation, they still require the ability to integrate with the larger Army C4I systems to accomplish their mission.

B. IMPLICATIONS OF TECHNOLOGY INTEGRATION AND THE TAK

Sensors in CWMD operations are essential as they allow commanders to make decisions and SMEs to see technical data remotely in near real-time and make technical recommendations to the operator beyond his organic capability. As outlined in JP 3–11, *Operations in Chemical, Biological, Radiological, and Nuclear Environment*, "the necessity for JFCs and staff to have the ability to share information and create a shared understanding allows informed and timely decisions amid massive quantities of operational data."[58] ATP 3–05.11, *Special Operations Chemical, Biological, Radiological, and Nuclear Operations,* discusses offensive CWMD operations and the requirement of SOF chemical reconnaissance detachments conducting WMD interdiction and elimination operations. The chemical reconnaissance detachments must not only have the capability to detect and identify WMD agents and radioactive sources but also the capability to communicate results to a maneuver commander in near real time.[59] The requirements for SME and RAA capability beyond the JOC change in response to time requirements, independent variables of each operation, or even the availability of SMEs to accompany operators or be a part of the joint force HQ.

---

[58] Joint Chiefs of Staff, Operations in Chemical, Biological, Radiological, and Nuclear Environments, III-1.

[59] Department of the Army, *Special Operations Chemical, Biological, Radiological, and Nuclear Operations,* ATP 3–05.11 (Washington, DC: Department of the Army, 2014), 2–2.

There are three levels of identification for possible radiological source in the field: presumptive identification, field confirmation identification, and theater validation identification.[60] Theater validation identification requires the employment of "multiple independent, established protocols and technologies by scientific experts from a fixed or mobile laboratory to characterize a CBRN threat with a high level of confidence and the degree of certainty necessary to support operational level decisions."[61] The advancement of sensor technology and connectivity of the modern SOF operator and the JOC will allow for increased capabilities and validation by scientific experts. This capability will increase the commander's ability to better understand threats, make timely decisions, and share strategic information for follow-on policy.

1. Tools Necessary for JIIM CWMD Operations

As adversaries present new and different dynamic problems and challenges around the world, SOCOM must be prepared to adapt and provide measured responses. Previous research addressed combined operations and advising a partner force to improve its

---

[60] Department of the Army, Multi-Service Tactics Techniques and Procedures for Chemical Biological Radiological and Nuclear Reconnaissance And Surveillance, ATP 3–11.37 (Washington, DC: Department of the Army, 2013), 5–3–5-6.

ATP 3–11.37 defines the three categories as follows and includes a fourth category, definitive identification, which must be performed in a national laboratory:

"**Presumptive identification** is the employment of technologies with limited specificity and sensitivity by general-purpose forces in a field environment to determine the presence of a chemical, biological, radiological, and/or nuclear hazard with a low level of confidence and the degree of certainty necessary to support immediate tactical decisions" 5–3.

"**Field confirmatory identification** is the employment of technologies with increased specificity and sensitivity by technical forces in a field environment to identify chemical, biological, radiological, and/or nuclear hazards with a moderate level of confidence and the degree of certainty necessary to support follow-on tactical decisions" 5–5.

"**Theater validation identification** is the employment of multiple independent, established protocols and technologies by scientific experts in the controlled environment of a fixed or mobile/transportable laboratory to characterize a chemical, biological, radiological, and/or nuclear hazard with a high level of confidence and the degree of certainty necessary to support operational level decisions" 5–6.

"**Definitive identification** is the employment of multiple state-of-the-art, independent, established protocols and technologies by scientific experts in a nationally recognized laboratory to determine the unambiguous identity of a chemical, biological, radiological, and/or nuclear hazard with the highest level of confidence and degree of certainty necessary to support strategic-level decisions" 5–7.

[61] Joint Chiefs of Staff, Operations in Chemical, Biological, Radiological, and Nuclear Environments, B-8.

effectiveness and lethality through the digital presence of U.S. Special Forces advisors using RAA/ADAPT. Situations like a possible instability in nuclear-armed North Korea, or the illegal sale of fissile or radiological material, pose new challenges and require special technical expertise and greater involvement of JIIM partners. Through the proven ATAK and the TAK infrastructures, the possibility exists to integrate emerging technologies at the tactical level, enhance operator effectiveness, and provide relevant technology to the battlefield, and increase operational and JIIM SA. The opportunity has arisen to scale tactical level technology up to the operational level for C2, facilitating technical advising, and providing a common operating picture.

The creation of the JOCTAK and the integration of CBRN sensors reimagines the RAA concept for use during unilateral CWMD operations, where the SFOD-A requires technical expertise beyond the scope of the team or personnel present on the JOC floor. The traditional construct of RAA was a partner force conducting an operation would receive technical advice from a forward-staged Special Forces detachment who had reach back capability to the joint HQ for mission support as required. The unilateral CWMD operations construct facilitated by the JOCTAK provides a similar framework. While the JOC is able to provide much of the warfighting capabilities, any technical requirements—chemical, biological, radiological, or nuclear—could quickly exceed the expertise found within the JOC and require scientific subject matter expertise. For example, from a particular scientist or identification and processing capability at a nuclear research facility located in the continental United States or a North Atlantic Treaty Organization (NATO) partner country.

In the context of unilateral CWMD operations and utilizing the TAK infrastructure as a comprehensive C4I platform, the original tactical level functionality of the ATAK to advise a partner nation will require significant adaptation. JOC requirements include the ability to track and observe multiple elements from different network enclaves, send and receive voice and data communications, receive and view multiple ISR feeds, and access planning documents.

C. CONCLUSION

Comparison of the requirements to achieve the most effective level of JIIM interoperability necessary for a comprehensive CWMD response, and the lack of available systems to implement a response during a CWMD mission set, highlights significant gaps between the current capability and the desired end state. While the strategic and policy guidance for such operations is easy to state, performing such tasks while coordinating with partners is a separate matter and one that currently has no real-world solution. Due to the explicit threat of a CWMD event, it is essential that existing technologies and systems be leveraged to fill this capability gap as quickly and as simply as possible.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TAK APPLIED AS A PROOF OF CONCEPT FOR CWMD C4I

A. MULTI-DOMAIN, MULTILATERAL COLLABORATION OPPORTUNITIES

In order to address the use of the TAK as an operational level C4I mission command system and CBRN tool, we parsed the problem into two areas for further research and development. First is the feasibility of the TAK to function as an operational-level C4I tool, JOCTAK. Second is the ATAK's integration of CBRN sensor technology into tactical operations. Experimentation was conducted through an iterative ground-up approach spanning multiple field experiments. Initial experimentation tested and confirmed the ATAK and TAK networks' ability to aggregate, share, and display tactical-level information across a network. Follow-on experiments tested the integration of CBRN sensors into the network using the ATAK CBRN plug-in and its ability to host multiple nodes of users with various sensors. Similarly, an operations center was established concurrently with all experiments to replicate information requirements, and observe and record end-user implications. Using this approach, we identified specific areas of strength and concern regarding the expansion of the TAK to an operational-level C4I system for CWMD operations.

The development of a JOCTAK as a comprehensive CWMD C4I solution should include the re-development of current software and plug-ins to ensure inter-platform compatibility across the entire TAK network. Although a significant undertaking, this will allow for the most comprehensive aggregation of mission data and a viable starting point for the development of a JOCTAK. Because of the variety of CBRN sensors fielded within the U.S. government and partner forces, the ATAK CBRN plug-in must be able to translate and communicate with all existing U.S. and partner CBRN sensor and C2 program file formats. Additionally, access to the JOCTAK from a remote location through a web portal could provide significant advantages to the way critical information is shared with SMEs and stakeholder organizations. This level of tactical and operational visibility would facilitate both commanders and staff to visualize multiple complex operations across the battlefield and make timely decisions. The JOCTAK's significance is that it solves existing

command-level capability gaps with reliable and known systems. Its further development enables tactical level operations while providing increase reachback support. While this research provides a definite way forward for SOJTF CWMD operations, it has far-reaching implications in a multi-domain JIIM environment where requirements for data flow and information necessary for continuous operations continue to increase.

1. CWMD Potential Operations

The scale of a nuclear crisis on the Korean Peninsula would likely exceed the capricious number of U.S. special operations forces (SOF) and conventional CBRN units available to respond. In the event of a CWMD incident/crisis involving the Democratic People's Republic of Korea, a JIIM response will be required.[62] U.S. CBRN units are available to respond on a two-hour recall; however, they are limited in number. Even with South Korean or other allied country partner units, the number required would likely still greatly outweigh the number of units available. Because of this, there is a high likelihood a conventional unit that is untrained in CBRN/CWMD will encounter or be tasked to deal with CBRN material and require the reach back advice and subject matter expertise.

The coordination and monitoring of both U.S. and allied/partner forces involved in a CWMD mission set will require an unprecedented level of collaboration and information sharing at the operational level, both to assist individual units with the required information from SMEs and to coordinate the movement of all of the units in concert. Additionally, the economic and diplomatic connectivity of Eastern Asia highlights the number of non-U.S. stakeholders in the event of a DPRK CWMD crisis, which will further complicate the necessary coordination.

a. Vignettes

While the possibility of an actual CBRN attack is not a pleasant scenario to imagine, it is one that must be trained for. Given the complex environment of CWMD operations, there will certainly be many different elements involved with any CWMD operation. These elements could be solely within the Department of Defense or expand to include other

[62] Lyford et al., "Preparing for a Crisis," 2.

government and civilian agencies. The Army Training Publication (ATP) 3–90.40, *Combined Arms Countering Weapons of Mass Destruction*, which is a collection of Army CWMD operations lessons learned, clearly states that "CWMD is not a CBRN specialty mission set enabled by maneuver forces: rather, it is a military operation conducted by combined arms teams and enabled by CBRN specialists, EOD, and other technical elements."[63] This means that units of all types, regardless of expertise, are likely to be involved.

Given the size and scope of any possible CWMD operation, the number of units/ agencies involved, including the DOD, would be in the dozens if not more. The need for an efficient way to communicate, battle track, and share information among multiple units at both the tactical and operational levels is imperative for a successful operation. This information sharing would need to consist of pictures, videos, troop location data, and CWMD sensor data, all simultaneously shared across a network. Focusing on the sharing of CWMD sensor data, leaders at both the tactical and operational levels could benefit from the ability to view the same sensor readings, track all units on a universal COP, and receive assistance from SMEs located outside the JOC/HQ. A system capable of handling all of the tasks laid out above would have to be integrated and work across various platforms including multiple mobile devices. Additionally, it would need to be compatible with the equipment and CWMD sensors used by a large variety of agencies. The following notional scenario is what a possible operation might look like with the C4I systems currently in use today.

(1) Vignette One, without the TAK

Negotiations with the Democratic People's Republic of Korea have continued to stall, and the United States along with its allied partners have deployed a large number of additional units to the Korean Peninsula. The Special Operations Joint Task Force Korea has been established to search out and render safe all WMD areas, whether they be manufacturing, assembly, or launch sites, in case the regime collapses.

---

[63] Department of the Army, *Combined Arms Countering Weapons of Mass Destruction*, ATP 3–90.40 (Washington, DC: Department of the Army, 2017), iv, https://fas.org/irp/doddir/army/atp3-90-40.pdf.

Special Forces Operation Detachment-Alpha XXXX deploys across the forward line of troops (FLOT) into the DPRK following the collapse of the regime and discovers a previously unconfirmed WMD missile site. The SFOD-A conducts reconnaissance on the area and requests ISR to gather imagery and other information from the air. After conducting reconnaissance, they assemble out of sight and sound of security forces to consolidate information. They sketch maps of each side of the missile site, list how many security forces were seen, what types of weapons and vehicles were observed, and note any additional structures that were in the area, as well as the roads leading into and out of the objective.

Recon Team 1 mentions seeing a large number of metal drums stacked under an open shed-like structure and notes they appear to have hazardous material markings. Recon Team 2 observes a possible disassembled rocket with the accompanying warhead, engine components, and other unknown parts. Only Recon Team 1 observed the structure and drums because none of the other recon elements could see the structure from their vantage point. The SFOD-A compiles their reconnaissance data and then contacts the SOJTF HQ to report their findings along with a request to destroy the entire site. The SOJTF HQ tells the SFOD-A to remain in place while the ISR footage is examined.

An hour later, the SOJTF HQ contacts the SFOD-A via a satellite communications (SATCOM) voice radio, informing them that the ISR platform confirmed the missile type as one that is possibly carrying a nuclear payload. Therefore, it appears to be a warhead, and the drums contain nuclear material. The SOJTF informs the SFOD-A that they will have to wait for an airstrike because the risk of contaminating the surrounding environment must be evaluated. Meanwhile, at the SOJTF HQ, the Chemical staff cannot positively identify the missile system or components and sends a request for advanced SME assistance in the identification process. It takes an additional hour for the HQ to request assistance from a U.S. defense nuclear research and testing facility for positive identification of the weapons system and likely components. It is ultimately determined that the missile components and metal drums pose no threat of contaminating the area as long as they are not directly targeted during the airstrike. The higher HQ passes this

information down to the SOJTF HQ, which in turn relays the information down to the SFOD-A.

The SFOD-A then provides all the necessary targeting information for the airstrike to the SOJTF HQ and sets up in an ambush position to eliminate any enemy combatants that attempt to evade once the airstrike begins. Fifteen minutes later, the airstrike destroys most of the compound except for the shed-like structure, and the SFOD-A subsequently eliminates all other enemies on the target. The SOJTF HQ tasks the SFOD-A to conduct a post-strike battle damage assessment and analyze the remaining missile and drum using specialized CBRN sensors. As part of the CWMD task force, each detachment operating in the area was issued CBRN sensors in the event that they encountered any WMD material. After completing this task, the SFOD-A moves back to the SOJTF HQ for debriefing and passes the CBRN sensor readings off to the SOJTF HQ CBRN detachment for analysis. It is determined that discovered parts and components do contain a low-grade nuclear material and could have been reassembled to create a short-range surface-to-surface-missile. The total time from initial discovery of the weapons site to mission completion was nine hours.

This notional story depicts a situation any SOF unit could experience on the Korean Peninsula. During the course of this hypothetical situation, there were several instances where the capability to aggregate and share various forms of data and information among tactical units, the JOC, and SMEs would have been extremely beneficial to the tactical unit on the ground. The capability to meet these requirements already exists in some form within the TAK network; however, it requires an expansion of existing software capabilities.

(2) Vignette Two, with the TAK

In the previous vignette, we discussed what a possible scenario might look like with today's C4I systems. This is what it may look like with the addition of the TAK infrastructure.

SFOD-A XXXX deploys to the DPRK following the collapse of the regime on the Korean Peninsula as part of SOJTF Korea. While on patrol, the SFOD-A discovers a

previously unknown WMD missile site. The SFOD-A begins conducting reconnaissance on the area as well as request ISR to gather imagery and other information from the air. While conducting reconnaissance, each member of the SFOD-A is equipped with an ATAK device and can see each team member's position on the ground in real time. Because both recon teams were updating their observations in real time with map markers, military symbology, and the chat function, each recon team and remaining members of the detachment were aware of one another's observations. The JOCTAK allowed the SOJTF HQ to monitor the same live and still images of the facility and observed equipment from the detachment. After the detachment finished conducting reconnaissance, they reconsolidate out of sight and sound of the missile site to review the ISR footage and add observer-specific information and details to the final report before sending it forward along with a request to strike the entire stronghold.

The consolidated information sent over the TAK network to the SOJTF HQ provides the amplifying details necessary for personnel at the SOJTF HQ to begin analyzing the site and components remotely. The Chemical Corp staff cannot positively identify the drums, materials, or components and requests advanced SME assistance in the identification process. The SOJTF staff contacts a U.S.-based defense nuclear research and testing facility that is granted access to the network over the internet to positively identify the weapons system and components. After analyzing the photos of the missile site sent by the SFOD-A, the SME positively identifies the missile system and components and can quickly determine that the materials pose no threat of contaminating the area as long as they are not directly targeted during the airstrike. Utilizing the JOCTAK, in a matter of seconds, the higher headquarters passes this information to the SFOD-A.

Unlike the previous scenario, the SOJTF HQ is much more responsive in authorizing the airstrike request because of enhanced SA of the objective from input from the SFOD-A and ISR. The SFOD-A provides all the necessary targeting information for the airstrike via the ATAK and establishes an ambush to eliminate any enemy forces that attempt to escape once the airstrike begins. Fifteen minutes later, when the detachment is able to get into position, the airstrike destroys most of the compound, minus the covered area, and the SFOD-A eliminates all other enemies on the target. The SOJTF HQ tasks the

SFOD-A with analyzing the metal drums and missile components using specialized CBRN sensors. As part of the CWMD Task Force, each detachment operating in the area was issued CBRN sensors in the event that they encountered any WMD material. These specialized sensors are connected to the ATAK and allow both the SOJTF and higher HQ to monitor the sensor data remotely through the JOCTAK. This allows the CBRN SMEs to quickly analyze the drums and components to determine if they are a threat and the HQ element to quickly warn the SFOD-A of any contamination issues and advise them to leave the objective area if necessary. After completion of this task, the SFOD-A moves back to the SOJTF HQ for debriefing.

Because the ATAK facilitates real-time monitoring of CBRN sensor data, the time necessary for analysis is significantly expedited. It is determined that the metal drums do contain a low-grade nuclear material sufficient enough to pose a threat if assembled with the other missile components found on the objective to create short-range surface-to-surface projectiles. The total time from initial discovery of the weapons site to mission completion was two hours. TAK's ability to aggregate and share information to the relevant parties at both the SFOD-A and HQ levels reduced the elapsed time of the operation by more than 75%.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENTS

A. TEST I: NELLIS AFB, SEPTEMBER 2017

1. Experiment Design Considerations

In September 2017, we conducted experimentation at Nellis Air Force Base (AFB) as the first phase of an iterative approach toward validating the use of the ATAK as an operational- and tactical-level SA tool. The purpose of this experiment was to evaluate the effectiveness of the ATAK as a tactical-level SA and C2 tool by testing its ability to aggregate, display, and share critical information across a network that is similar to the data flow and necessary to share critical information in a CWMD/CBRN environment. This experiment provided us with familiarization and a baseline for ATAK at the tactical level before attempting to expand its role as an operational-level C4I system.

2. Introduction

To test the tactical utility of the ATAK and wireless mesh networks (WMN), we traveled to the U.S. Air Force's Weapons School at Nellis AFB.[64] To validate the use of ATAK as a tactical-level SA tool as well as enhance the realism and training value of the Weapons School Weapons Instructor Course (WIC), we established a WMN including internet gateways (IGW) and several ATAK mesh client nodes. We were able to observe the application of the ATAK in a, live-fire, fire support coordination exercise. This test supported the following research questions:

- How can the expansion of the TAK concept to the joint operational level in the form of a JOCTAK improve the collective planning, mission command, and digital collaboration between JIIM partners?

64 "United States Air Force Weapons School," Nellis Air Force Base, accessed April 4, 2018, http://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284156/united-states-air-force-weapons-school/. "The U.S. Air Force Weapons School trains tactical experts and leaders to control and exploit air, space, and cyber on behalf of the Joint Force. It also provides academic and advisory support to numerous units, enhancing air combat training for thousands of service members from the U.S. Department of Defense and allied services each year. Additionally, it provides a controlled learning environment and knowledge trust for best practices in air, space, and cyber combat techniques."

- What are the necessary components and designs for the JOCTAK SA templates and planning knowledge management in a MDB environment?

3. Context/Background

Currently, Joint Terminal Attack Controller (JTAC) students and instructors at the USAF WIC use the ATAK as a digital map on a mobile ad hoc network (MANET). JTAC students and cadre communicate using voice over line of sight (LOS) and SATCOM radios to fellow teams, aircraft, and the JOC at Nellis AFB. During the experiment, there was no capability for communication via the ATAK with the aircraft that were dropping live ordnance. Their standard practice with the ATAK is to load imagery and grid reference graphics (GRG), plot the locations and range rings of known or suspected enemy air defense artillery (ADA) and defensive weapons systems, as well as friendly positions and graphics by hand prior to mission execution.[65]

If operating with a ground force, JTACs are able to use the ATAK through a local WMN using Harris PRC 152 radios and the Harris ANW2 protocol but do not routinely train to do this. Similarly, JTACs do not train to use their radios in a WMN configuration connected to an IGW to access the internet or connect to a remote server. JTAC teams also do not have the ability to share their personal location indicator (PLI) data with the JOC at Nellis AFB through an IGW.[66]

4. Method

We tracked the operations from a JOC established at the Nellis AFB garrison (see Figure 3). The team also collected diagnostics and data transmission information during four day and night missions. Additionally, each member of our team served as a ground force commander (GFC), adding realism to the training scenario for the participating Weapons School students. In real time, students were required to coordinate with a research team member acting as the GFC to call in air support and fire missions during each interval. Research team members serving as GFCs used the ATAK and the WMN to battle track

65 Weapons School Operations Officer, email message to authors, September 10, 2017.

66 Weapons School Operations Officer.

both friendly and enemy positions as well as coordinate through the students for appropriate utilization of air support and ground-based fires.

Figure 3. Naval Postgraduate School (NPS) and WIC students at Nellis AFB live fire range.

The Primary, Alternate, Contingency, and Emergency (PACE) communications architectures established was:

- Primary communications structure (P): ATAK—4G/LTE; Antenna: international maritime satellite (INMARSAT)
- Alternate communications structure (A): ATAK—MPU-4; Antenna: INMARSAT
- Contingency communications structure (C): ATAK—Harris PRC 152 connected to a BGAN (using current SOF inventory)
- Emergency communications structure (E): "Extend the mesh network" ATAK—MPU-4 WMN/ GoTenna/Beartooth—117G radio at JOC

In a real-world operation, a similar PACE plan would enhance the digital collaboration of all elements involved as well as the operator's effectiveness by giving them the capability to use the ATAK through a local WMN using (P) 4G/LTE Antenna, or MPU-4/ MPU-5 through INMARSAT (A), Harris PRC 152 radios and the Harris ANW2

protocol through BGAN (C), and emergency communications structure “extend the mesh” with a combination of MPU-4/ GoTenna/ Beartooth through the 117G at JOC (E).

5. Observations

By incorporating the ATAK into the JTAC training scenarios, we were able to battle track both friendly and enemy positions with great accuracy. The improved SA derived from the ability to visualize enemy and friendly positions in the ATAK as opposed to relying on LOS communications from the tactical elements greatly improved the common operating picture of the JOC. JTAC’s also gained increased efficiency in the development of their CAS 9-line request sequence by being able to instantaneously identify all friendly positions in the ATAK. Depending on the location, the mobile broadband 4G LTE connection was able to facilitate the data throughput required for the operation of the ATAK. We also tested the use of the WMN. On the second day of testing at a more austere location, we were unable to get adequate cellular connectivity and utilized the alternate communications structure. The INMARSAT used in conjunction with the MPU-4 WMN was able to handle the bandwidth requirements of the ATAK network. We team capitalized on the austere location to use the contingency communications structure and observed no issues with the BGAN device.

6. Analysis

Based on the results, we assess that:

1. The architecture of this testbed can serve as a model for increasing the connectivity of SOF teams currently using ATAKs across the various combatant command areas of responsibility. Additional research will need to be conducted to identify effective means of communicating new TAK applications, capabilities, limitations, and usage scenarios for each mission set.

2. The WMN architecture and internet access, when introduced to this environment, provides new capabilities to the operators on the ground and

their higher HQ. Through the incorporation of wireless mesh connectivity, the ATAK becomes more than a digital map.

3. The ATAK system, when used in an MDB environment can improve the effectiveness of operations at both the tactical and operational levels. By aggregating and sharing movements and locations of both friendly and enemy positions, operators on the ground can utilize the ATAK to improve SA not only for tactical commanders but also for command teams and JOCs at higher levels.

4. The existing ATAK infrastructure, when enhanced with the WMN provided by the MPU 4/5 radios and the connectivity of an IGW, would allow operators on the ground to digitally collaborate with aircraft dropping live ordnance in a safer manner. This could give the aircraft crews an extra safety check to de-conflict friendly and enemy positions and lessen the chance that operators on the ground or pilots in the air would either pass or receive incorrect grid coordinates for lethal munitions.

B. TEST II: JIFX I, FEBRUARY 2018

1. Experiment Design Considerations

The February 2018 Joint Interagency Field Experimentation Program (JIFX) effort with the ATAK built on the progress made at Nellis AFB and continued collaboration between different joint partners and the ATAK software developers as needed, to implement necessary changes. Continued collaboration with software developers is extremely important as the development of ATAK plug-ins is a continuing process that presents its own challenges. Because plug-ins are not always co-developed for use on both ATAK and WinTAK, there are often gaps in intercompatibility and the ability to display plug-in specific data. Additionally, because the ATAK core program is updated every 120

days, plug-ins do not always maintain functionality across all versions of the ATAK itself.[67]

Having validated the efficacy of the basic ATAK functionality, The NPS team determined that additional experimentation should expand the proven capability by testing sensor integration and the use of sensors in the CWMD environment. It is necessary to determine how effectively current CBRN plug-ins and sensors currently function with the ATAK at the tactical level, before expanding to an operational level C4I infrastructure.

2. Introduction

In February 2018, the team traveled to the California National Guard's Camp Roberts to conduct the next phase of field experimentation with the ATAK during the quarterly Joint Interagency Field Experimentation Program (JIFX).[68] The facilities at Camp Roberts were able to enhance the realism of the experiment by offering several different military training areas, specifically the Combined Arms Combat Training Facility (CACTF). This allowed the simulation of operations in an urban environment. The team tested several radiological sensors, including one prototype and one proprietary ATAK CBRN plug-in, developed by the Defense Threat Reduction Agency (DTRA).[69] The plug-

[67] Sterling, "TAK LSE Brief"; Operators often are not aware of newly developed sensor applications within the TAK suite. Further, applications often are not cross-platform compatible. For example, applications are not developed for both ATAK and WinTAK platforms concurrently; most applications are developed for ATAK before being developed for WinTAK.

[68] According to the sponsor's webpage, the JIFX program "is an NPS effort that began in 2012 under the sponsorship of the Office of the Secretary of Defense and the Department of Homeland Security." NPS participates in quarterly JIFX events at NPS-owned facilities on McMillan Airfield at Camp Roberts. Similarly, JIFX also "provides an experimentation resource for the Unified Combatant Commands (COCOMs) and other federal agencies. Additionally, local, state, international emergency management, disaster response, and humanitarian assistance organizations participate in JIFX on a regular basis." This experimentation environment is organized in a manner that is austere by nature so that it mimics deployed conditions as close as possible. Additionally, JIFX brings together NPS student researchers, as well as many different elements from the DoD, representatives from the different COCOMs, and private industry companies in a collaborative testing environment that is beneficial to all parties involved. In this unique environment, NPS students can meet and discuss their research with different entities as well as receive recommendations from other participating experimenters/testers that can enhance the student's research or assist it by providing additional network infrastructure. "What Is JIFX?," Naval Postgraduate School," accessed August 6, 2018, https://my.nps.edu/web/fx/what-is-jifx-.

[69] At the time of testing, both ATAK and the plug-in were version 3.6. Both have since received additional updates and continue to be developed and improved.

in and a prototype sensor developed by Draper Labs, the HRM replacement sensor, were both provided for testing.

Because we paired with the NPS Center for Network Innovation and Experimentation (CENETIX) Laboratory, the experiment had multiple goals. The CENETIX team was attempting to determine the most efficient way to utilize various sensors and drones to shorten the detection, location, and identification (DLI) sequence of a radiological source during a wide area search (WAS).[70] We were interested in evaluating the capability of the ATAK paired with the provided plug-in to integrate and transmit data from connected sensors at the tactical level to the operational level JOC. This experiment supported the following research questions:

- How can the expansion of the TAK concept to the joint operational level in the form of a JOCTAK improve the collective planning, mission command, and digital collaboration between JIIM partners?
- How can CWMD sensors and the TAK plug-ins improve the RAA capability among operators, technical specialists, and mission command during a WMD scenario?
- What are the necessary CWMD sensor components and TAK plug-in software designs for meeting future JIIM mission sets?

3. Method

We devised a three-part approach. First, to perform an initial detection of the presence of radiological material; second, to locate the detected source; and finally, to identify the radioactive isotope present and determine if it required follow-on action or not. For the first step, we used RAA techniques with a TOC directing tactical units, and an advise cell was available for subject matter expertise via RAA directly to the tactical-level

[70] For the purposes of this experiment, WAS is defined as an urban area approximately the size and density of a mall, stadium, city block, or other urban structure that is approximately 200 meters squared, where multiple simultaneous detections from multiple sensors and operators are possible.

operators. The TOC coordinated the detection, location, and identification efforts, and the advise cell assisted in adjudication once a source was detected.

During this experiment, NPS students were augmented by multiple DOD entities as well as several private industry participants. Government agency participation included DTRA, Naval Special Warfare (NSW), California Army National Guard (CAARNG) 95th Civil Support Team (CST), CAARNG 9th CST, Lawrence Livermore National Laboratory (LLNL) Radiological Assistance Program (RAP) Team 7, Lawrence Berkeley National Laboratory (LBNL) Research Team, the Camp Roberts base and flight operations support (NPS). Additionally, private industry participation included assistance from Terratracker and Radmet.

With such a large group of different DOD and industry participants collaborating, we had a plethora of sensors at their disposal (see Figure 4). This allowed the team to test plug-in capabilities on multiple sensors and see how those sensors delivered information through the ATAK to the operators on the ground and the TOC where the collection of data could be managed and interpreted.

Figure 4. JIFX I platforms

The following unmanned aerial vehicles (UAV) and unmanned ground vehicles (UGV) were used during the experiment.

- Two mid-size Matrice-600 Pro UAVs (Figure 5)

Figure 5. Matrice 600 Pro[71]

- Two miniature UAVs, Shield AI and "Inspire" Quadrotor systems (Figure 6)

Figure 6. Shield AI UAV[72]

[71] Source: "Matrice 600 Pro," DJI, accessed August 24, 2018, https://store.dji.com/product/matrice-600-pro.

[72] Source: "Products: Artificially Intelligent ISR Asset for Ground Forces," Shield AI, accessed August 24, 2018, https://www.shield.ai/products/.

- NPS robotic mobility platform (RMP) 400 unmanned ground vehicles (UGV) (Figure 7)

Figure 7. Segway RMP 400[73]

- Two TALON systems (Figure 8)

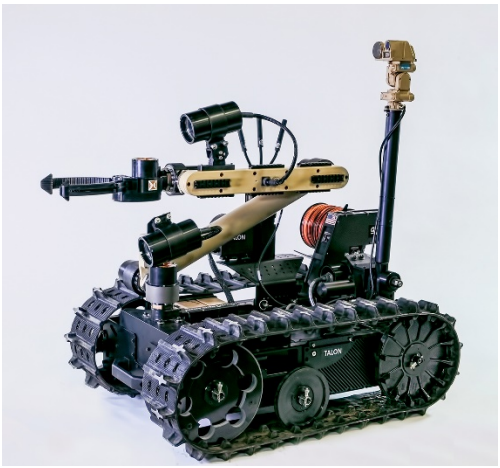

Figure 8. TALON tracked military robot[74]

[73] Source: "Segway RMP 400," Segway, accessed August 24, 2018, https://msu.edu/~luckie/segway/rmp/rmp.html.

[74] Source: "TALON Tracked Military Robot," *Army Technology* (blog), accessed August 24, 2018, https://www.army-technology.com/projects/talon-tracked-military-robot/.

- The following detectors and sensors were used during this experiment: sub-micron multi-beam/LIDAR/ localization and mapping platform (LAMP) sensor (LBNL) (Figure 9)

  The LAMP sensor has the ability to identify sources and create 3-D models of radiological environments in real time. Additionally, LAMP overlays the 3-D model with a heat map showing the specific section of the building or structure of interest.[75]

Figure 9. Localization and mapping platform[76]

- Two HRM replacement miniature sensors (DTRA)

[75] "Localization and Mapping Platform 2.0 2017–114," Intellectual Property Office, June 15, 2018, https://ipo.lbl.gov/lbnl2017-114/.

[76] Adapted from Intellectual Property Office.

- One adaptable radiation aerial monitor (ARAM) sensor (UAV-UGV based LLNL-Terratracker) (Figure 10)

Figure 10. Scintillation sensors for ARAM software.[77]

- Large 4x4x16" NAI gamma detector (DTRA/NPS) (Figure 11)

Figure 11. NAI gamma detector[78]

[77] "Large Volume Scintillation Counter| Berkeley Nucleonics," Berkeley Nucleonics, accessed August 24, 2018, https://www.berkeleynucleonics.com/large-volume-scintillation-counter.

[78] Source: "4 Inch x 4 Inch x 16 Inch NaI(Tl) Scintillation Detector, Energy Resolution: ≤8.5%@662keV(Cs-137)," OST Photonics, accessed August 24, 2018, https://www.ost-photonics.com/product/4%e2%80%b3x4%e2%80%b3x16%e2%80%b3-naitl-scintillation-detector/.

- identiFINDER R-400 (NPS) (Figure 12)

Figure 12. identiFINDER R400[79]

Each platform was fitted with a specific radiological/nuclear (R/N) sensor (based on payload capability) and was tested to determine the time required to DLI a radiological source. For each test iteration, a small radiological source was hidden, and various sensors (attached to a specific unmanned platform) were employed to complete the three separate portions of the experiment. Using the ATAK architecture, our goal was to first perform an initial detection of the presence of radiological material, without a locational component; second, to locate the detected source; and finally, to identify the radioactive isotope present and determine if it required follow-on action or not. We conducted multiple iterations using the DLI model with the various sensors equipped on the different unmanned platforms available. After several iterations, the most efficient WAS sequence was established:

Step 1: Detect (D), by searching the outermost perimeter by driving large adaptable radiation aerial monitor (ARAM) sensors and a UGV-based small (ARAM) sensor.

Step 2: Locate (L) by flying a mid-size Matrice-600 UAV with the LIDAR-LAMP sensor (Figure 13).

79 Source: "IdentiFINDER R400 All-Purpose Radionuclide Identification Device," FLIR Systems, accessed August 26, 2018, https://www.flir.com/products/identifinder-r400/.

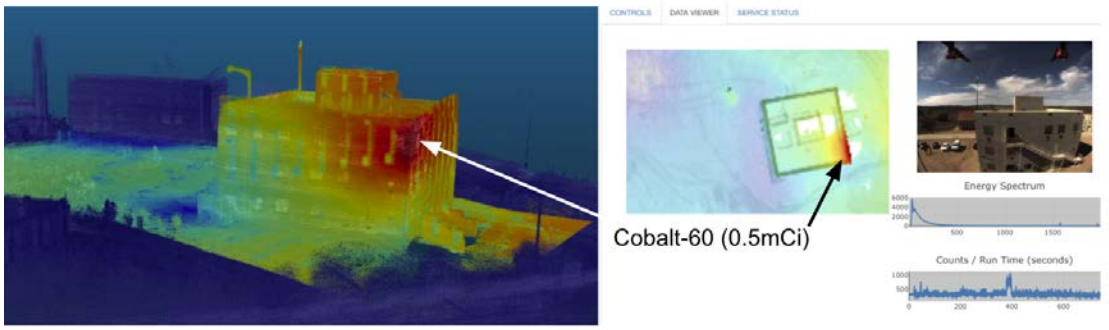

Figure 13. LAMP LIDAR 3D heatmap

Step 3: Build an internal mapping of the structure utilizing Shield AI (Figure 14).

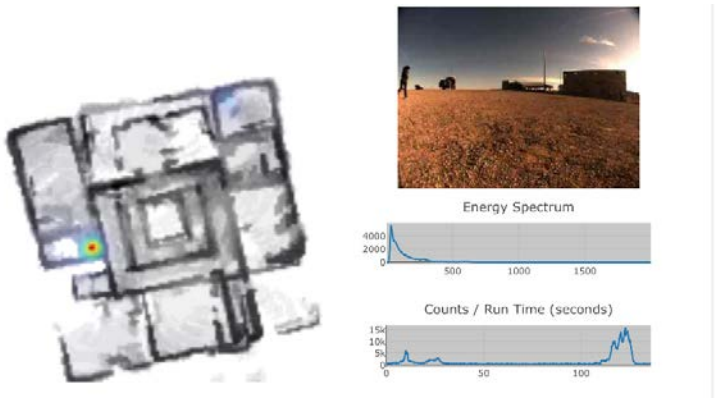

Figure 14. Shield AI 2D LIDAR mapping

Step 4: Identify (I) via flights by "Inspire" UAV, equipped with the miniature HRM sensor.

Step 5: Secondary identification and the establishment of a visual feed on the source by two simultaneously searching Talon stair-climbing UGVs equipped with identiFINDER 2 sensors

Note: This detect, locate, and identify sequence took approximately 1 hour and 25 minutes from the time we initiated the scenario until the radiological source was identified as a specific isotope.[80]

[80] Alex Bordetsky, "NMOC Wide Area Search (WAS) Experiment Revised," May 2018, https://nps.app.box.com/file/283014025256.

4. Observations

Using the TAK network and CBRN plug-in we were able to perform all of these functions using a single application. The plug-in integrated multiple sensors and broadcast the data across the network. The sensor data is shown as a breadcrumb trail or heat map of sensor activity above a specified detection threshold. This allowed an operator or UAV to walk or fly a set route and see where readings increased or decreased along that route, what isotopes were detected, and the percentage of accuracy for assessed isotope identification.

Furthermore, the ATAK CBRN combination allowed that information to be shared across the ATAK network to anyone else who has the application, allowing for coordination of multiple sensors and agents from the JOC. The CBRN plug-in also has the capability for another user to control the settings of the sensor remotely. This allowed a remote operator to change sensor settings, thresholds, etc. This capability could be used not only on a UAV bearing a remote sensor but also potentially on undercover agent or untrained units that are not in a position to manually monitor and change sensor or application settings.

In the course of the experiment, we noted that the ATAK CBRN plug-in was useful when the ATAK network was functioning as designed. It worked well with the sensor provided by DTRA (HRM replacement) and allowed detection of radiological sources as well as isotope identification directly from the ATAK phone. Additionally, the plug-in supported multiple sensors and allowed remote access to the sensor data from another ATAK device as designed. This information could also be viewed from the TOC on an ATAK-CBRN-equipped phone as well as by the advise cell SME to confirm the need for further action or dismiss a false reading (in the event of the sensor detecting a false source such as thoriated tungsten welding rods).

The primary problem noted during testing was a slow refresh rate on the data sent to the ATAKs from the HRM replacement sensor. When the sensor was either mounted to an unmanned system or handheld, the spike in detection would appear on the ATAK phone after the sensor had already passed the area where the source was located if moving at a moderate pace. This made using the sensor for the location of the source difficult on the

heat map display, as the lag between detection and the reported location on the phone's GPS did not always synchronize correctly. The authors' conversation with Tom McKnight indicated that newer versions of the sensor were in development at the time of testing and that they would have a faster refresh rate as well as the possibility to connect to a phone via a hardwired USB cable instead of relying only on Bluetooth connectivity.[81]

From a C2 standpoint, the primary deficiency was the lack of the WinTAK integration for the plug-in. As mentioned earlier, plug-ins developed for the ATAK do not always function correctly with the WinTAK, and it is impractical to display an ATAK screen on a monitor and use it in the TOC. This made coordination of units by the TOC and advice from the SME more difficult, as they were limited to using a phone-sized screen.

The communications infrastructure between the experiments at Nellis WIC and JIFX I differed due to the nature and objectives of each experiment. During the First experiment, the alternate architecture was used (WMN utilizing MPU 4/5). This was not copied during the second experiment. Because of this, network connectivity became a limiting factor as the team's physical location at Camp Roberts in the CACTF provided challenges to network connectivity using the local wireless node provided onsite and cellular data connectivity. This oversight was remedied by collocating the TOC and advise cell at the CACTF with the tactical search element, allowing for a local area network to be used.

5. Analysis

From an integration perspective, the HRM replacement/ATAK combination is better suited for a person to carry as opposed to having it positioned on a UAV. The Bluetooth connection required for the sensor is easily disrupted by the radio-frequency interference caused by flying the UAV. Because of the disruption, the operator must maintain close proximity to stay connected while flying. In a test with no UAV, where the ATAK phone and sensor were carried by a student researcher, the connection was maintained out to approximately 100 ft. However, when tested with the UAV, the ATAK

[81] Personal communication with Tom McKnight, DRAPER Labs, March 1 2018.

phone needed to stay within about 1 ft of the sensor or it lost connectivity as soon as the UAV launched. While it is possible to remotely monitor the sensor via the ATAK network, the sensor requires an embedded communications capability. The phone was used as a field expedient connectivity solution, something that is impractical in a hostile environment. Additionally, it would be impractical to fly the phone, sensor, and radio for maintaining network connectivity on most small platforms due to weight restrictions. Additional development of the UAV payload-carrying capability (appropriate attachments for the sensors) needs to be developed before follow-on testing and eventual fielding to SOF units.

The lack of WinTAK integration is a significant issue for further development of the JOCTAK. While the Android platform provides a good solution for the field, it is impractical to run everything in the JOC from an Android phone or through an emulator. The NPS team identified the short flight times (less than 30 minutes) of small UAVs used as a major impediment to adoption of a similar drone detection capability by forward-operating units. Additionally, the inability to use radiation sensors from a large standoff distance for initial detector further complicates the use of UAVs by prohibiting the adoption of larger, high-altitude platforms with increased loiter times.

C. TEST III: JIFX II, AUGUST 2018

1. Experiment Design Considerations

For the August 2018 experiment, we determined that further testing of sensor integration into the CBRN plug-in and remote monitoring of sensors from the TOC or JOC needed to be performed. Further evaluation of the current capabilities of the TAK as a CWMD C4I system would determine what changes and improvements the JOCTAK would require over the current TAK system. This testing included the pairing of multiple sensors to a single ATAK device as well as monitoring multiple phones with paired sensors from the JOC. Additionally, it was determined that testing a larger variety of sensors would be desirable as many of the sensors available were not capable of direct connection to the CBRN plug-in, either because they had no external connectivity or they did not communicate using the DTRA N42 file format required by the plug-in.

2. Introduction

In August 2018, we returned to the California National Guard's Camp Roberts to conduct the final phase of field experimentation with the ATAK and CWMD sensor integration. The team once again paired up with NPS's CENETIX Research Center for continued use of both their equipment and expertise with wireless mesh networks. The purpose of JIFX II was to build on the testing conducted at JIFX I in February 2018, which focused on a single sensor integrated with a single device at the tactical level. During JIFX II we expanded on the previous testing by attempting to determine the limits of sensor integration into the ATAK architecture. First, for this experiment, we tested the CBRN plug-in's ability to integrate multiple sensors per device (ATAK phone) as well as the overall integration of each specific sensor. Second, the team attempted to determine the sensors that worked well with the ATAK and the ones that did not.

The experiment attempted to replicate multiple ground elements working in concert at different locations using multiple radiological detection devices and to test whether the TAK infrastructure along with the CBRN plug-in would support numerous devices simultaneously. Testing further advanced our goal of utilizing the TAK network to address the lack of an operational level JTF mission command system that can work as an aggregation tool to combine data feeds from multiple tactical elements and sensors in a single system. As U.S. and partner nation forces conduct CWMD operations, they must have the capability to share information and alerts between tactical unit members and a higher headquarters. Additionally, they need to maintain command, control, and shared SA during operations. This experiment supported the following research questions:

- How can the expansion of the TAK concept to the joint operational level in the form of a JOCTAK improve the collective planning, mission command, and digital collaboration between JIIM partners?
- What are the necessary components and designs for a JOCTAK SA templates and planning knowledge management in an MDB environment?
- What are the necessary CWMD sensor components and TAK plug-in software designs for meeting future JIIM mission sets?

3. Method

Using the JIFX training environment and a collaborative approach, we received technical assistance from two different elements: the California Army National Guard's 95th CST and LLNL. The 95th CST sent CBRN SMEs to assist in the use of the various sensors tested.[82]

In addition to the SMEs, the 95th CST also provided technical advice and multiple sensors to conduct CBRN plug-in integration training. LLNL provided a representative that aided by supplying a recently developed Radiation Field Training Simulator (RaFTS) that "provides realistic radiation detection training by directly transmitting simulate radiation readings into the analog amplifier of real detectors."[83] The system in Figure 15 is shown using the ARAM.

Figure 15. LLNL RaFTS system[84]

Because the RaFTS replicates live radioactive sources directly to the sensor, it allowed the NPS team a secondary means of testing the CBRN plug-in's capability and

82 "California Civil Support Team Enhances Civilian Partnerships," National Guard, accessed August 16, 2018, http://www.nationalguard.mil/News/Article/576048/california-civil-support-team-enhances-civilian-partnerships-through-training/. The 95th CST is an active duty guard unit with the primary mission of supporting civil authorities at the direction of the governor.

83 "Ultra-Realistic Radiation Detection Training without Using Radioactive Materials," Lawrence Livermore National Laboratory, January 14, 2015, https://www.llnl.gov/news/ultra-realistic-radiation-detection-training-without-using-radioactive-materials.

84 Source: Lawrence Livermore National Laboratory.

integration into the ATAK.[85] Additionally, we tested both the military and civilian (MIL/CIV) variants of the CBRN plug-in across all phases of experimentation to determine cross-compatibility for CIV-MIL use.

We devised a three-step approach to test sensor integration and the overall ATAK compatibility.

Step I consisted of testing the CBRN plug-in capability by pairing a single sensor to a single ATAK device. Utilizing the WMN functionality of the MPU-4 radios and a repeater, the team tested various sensor integration with the ATAK using the CBRN plug-in provided by DTRA.

Sensors used/tested:

- Three Nucsafe Man-Portable Radiation Detection Systems (MPDS) (Figure 16). The NPS team received two Nucsafe Guardian Defender MPDS backpacks from the 95th CST, and a third Nucsafe Guardian Predator MPDS backpack was provided by DTRA. In both cases, the MPDS consists of multiple components that allow it to be used in a low profile, low visibility format. It is capable of detecting gamma-ray and neutron emissions depending upon configuration. Significant to the use of the MPDS is its ability to also identify the source after location.[86]

85 "Ultra-Realistic Radiation Detection Training without Using Radioactive Materials," Lawrence Livermore National Laboratory, January 14, 2015, https://www.llnl.gov/news/ultra-realistic-radiation-detection-training-without-using-radioactive-materials.

86 "Guardian Predator Portable Radiation Search Tool," EPE, 2018, https://www.epequip.com/catalogue/all-hazards-management/guardian-predator-portable-radiation-search-tool/.

Figure 16. Nucsafe MPDS.[87]

- One handheld identiFINDER R400 and one identiFINDER II detection systems (Figure 17). As before, the models varied slightly, but the functionality and capability of the actual sensors are relatively similar. The identiFINDER series of sensors are radioisotope identification devices (RIID) capable of detecting gamma and neutron sources as well as identify the source with a high degree of certainty once it is located.[88]

[87] Adapted from EPE.

[88] Source: "IdentiFINDER R400 Radiation Detector," All Safe Industries, accessed August 16, 2018, https://www.allsafeindustries.com/flir-identifinder-r400.aspx.

Figure 17. identiFINDER II detection system.[89]

- Two handheld ORTEC Micro Detective devices (Figure 18). An ORTEC Microdetective HX was provided by the 95th CST, and an ORTEC EX100R was provided by DTRA. As with the other two types of sensors, the two ORTEC systems varied slightly, but capability and overall functionality remained the same. The ORTEC devices are capable of accurate nuclide identification based on both gamma and neutron detection. This device, like the others tested, is capable of identifying the source after detection has occurred.[90]

89 All Safe Industries.

90 "Micro-Detective Ultra light, Portable Hand Held Radioisotope Identifier," ORTEC, accessed August 16, 2018, https://www.ortec-online.com/products/nuclear-security-and-safeguards/hand-held-radioisotope-identifiers-riids/micro-detective.

Figure 18. ORTEC Micro Detective HX detection device[91]

Step II testing connected multiple sensors to a single device (ATAK phone). This allowed a remote user at the JOC/operational level to view data from multiple sensors through the ATAK network.

Step III increased the number of sensors and devices on the ATAK network. The purpose was to test the ATAK's ability to aggregate both multiple sensors connected to a single ATAK device via the CBRN plug-in as well as multiple ATAK devices each connected to more than one sensor. This also tested the network's ability to handle a larger amount of data being sent from the tactical level to the JOC for remote viewing and better SA at the operational level.

4. Observations

The Nucsafe MPDS was the only Sensor that would effectively connect to the ATAK using the CBRN plug-in and operate as desired.

Step I: For single sensor-single device testing, the Nucsafe backpacks were used as they performed best with the plug-in. During the testing, the students were able to view data transmitted from the sensor on the local ATAK device; as well as view data remotely at the JOC. Students were also able to pass text communications and pictures across the

91 "Micro-Detective Ultra Light Portable RIID | RUGGED RIID | AMETEK ORTEC," accessed August 16, 2018, https://www.ortec-online.com/products/nuclear-security-and-safeguards/hand-held-radioisotope-identifiers-riids/micro-detective.

network. A split view of the ATAK running the CBRN plug-in and a screenshot of students reading measurements from the Nucsafe backpack wrist monitor is shown in Figure 19.

Figure 19. ATAK R/N plug-in (left) and Nucsafe wrist monitor (right)

Step I was successful. It allowed the personnel at the tactical level to integrate sensor data into the TAK network and remote viewing at the JOC. Additionally, a student located at the JOC was able to remotely initiate a sample collection and perform isotope identification of the source (see Figure 20), using the Nucsafe backpack remotely via the CBRN plug-in.

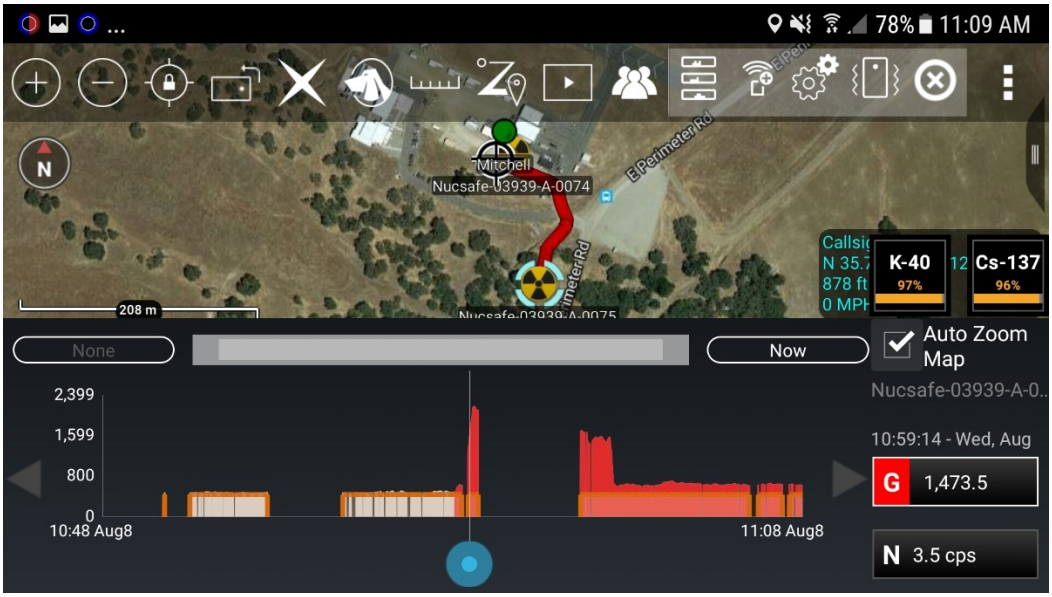

Figure 20. Remote viewing of sensor data (from JOC) connected to the ATAK network via R/N plug-in

Step II: In contrast to the use of the CBRN plug-in paired with the HRM replacement sensor used in the first JIFX experiment we found it difficult to operate with the wider variety of sensors available for JIFX II. While the HRM replacement sensor provided by Draper for the first experiment was specifically designed to work with the CBRN plug-in, the sensors used in JIFX II were not. Of the sensors available, it only functioned adequately on the Nucsafe MPDS. Following is a breakdown of all sensors and their specific configurations with the CBRN plug-in, the ATAK devices, and the MPU-4 radios as well as the issues that the NPS team discovered with the assistance from the 95th CST.

a. Guardian Defender Nucsafe MPDS

As per the CBRN plug-in instructions, the MPDS was connected to the MPU-4 radios via a cat5 ethernet connection and functioned in that configuration. Other possible ways to fix wireless connectivity issues included using the paired Android device with

network connectivity (SIM card) or hard lining/wiring it using a bridging device to connect to the MPU-4s.[92]

Additionally, the MPDS sensors had to be adjusted for a non-standard network configuration prior to use with the wireless mesh network setup by CENETIX. The 95th CST was able to perform the necessary changes. Once the sensors were configured and connected to the MPU-4 radios via Ethernet connections, the ATAK phones were then wirelessly connected to the same MPU-4 as MPDS. Within the ATAK application plug-in, the Internet Protocol (IP) address of the MPDS sensor was entered, and the phone was then capable of connecting to the sensor and had full control of the backpack. Once configured correctly the MPDS worked as intended with the CBRN plug-in.

b. Nucsafe Guardian Predator MPDS

This sensor, loaned to the NPS team from DTRA, was an older model than the sensors provided by the 95th CST. It came with the required software but was incompatible with the software provided by the 95th CST MPDSs. Because of the differences in model types and resulting software issues, we were unable to change the IP address or configure the domain/range in order to connect this sensor to the MPU-4 radios or the ATAK phones.

c. identiFINDER R400 and identiFINDER 2

The identiFINDER series of sensors were some of the more challenging to use with the CBRN plug-in. The sensors themselves are very capable and lightweight, easy to read, and user-friendly. However, they were the only two sensors that had no preconfigured profile for connection to the CBRN plug-in. The NPS team attempted to connect to the sensors as a generic DTRA N42 and DTRA N42 commandable device using the identiFINDER and Samsung phones Bluetooth connection. Despite being able to pair the sensor and phones via Bluetooth, the connection was not successful with the ATAK application. The connection was also attempted using the SRD sensor option in the plug-in to the mac address of the identiFINDER, but no connection was established. Also noted was the identiFINDER's incompatibility with Windows 10. Using the devices internal

[92] Draper Labs, email message to authors, May 31, 2018.

USB port connected to a Windows 10 computer multiple attempts were made to program the devices network settings to no avail. The devices software settings were finally accessed from a Windows 7 PC but still unable to be connected to the ATAK application.

d. ORTEC Microdetective HX and ORTEC EX100R

There was a preconfigured connection profile within the CBRN plug-in for the ORTEC sensors. Both sensors were able to utilize their respective built-in PDA devices, with a Windows CE operating system, to connect to the Wi-Fi hotspot generated by an MPU-4 radio. Once established the connection was unstable and would drop periodically. We attempted troubleshooting by verifying that the IP address of the ORTEC sensors was changed according to the instructions within the ATAK CBRN application as well as the Detective EX-application within the Windows CE device, which is part of the ORTEC sensor itself. This was eventually determined to be a hardware fault in the MPU-4 radio used as a Wi-Fi connection point for the sensors. Once corrected, both devices were eventually connected to the MPU-4 radios and able to maintain stable connections.

After a connection to the MPU-4 was established with the ORTEC, an ATAK device was connected to the same MPU-4, and a pairing was established with the sensor using the preconfigured option in the CBRN plug-in. Once connected, the functionality of the sensors was minimal. They could be viewed in the ATAK but were not commandable. Any attempt to initiate a remote collection or view past readings caused the CBRN plug-in to crash or present an error message. Also, after initiating a collection locally on the device, it was not viewable on the connected ATAK phone even though the data was present and visible from the sensor.

Step III: Step III was initially planned as the final progression in the sequence of increasing the number of sensors and devices on the TAK network. It was intended to test the TAK networks ability to aggregate data from multiple ATAK phones and associated sensors with the CBRN plug-in. However, due to the aforementioned sensor integration issues, it was not possible to complete Phase III as designed because the only sensors that would properly connect to the CBRN plug-in were the Nucsafe Guardian Defender MPDS backpacks. Therefore, the research team decided to capitalize on time available and

integrate a newly developed ATAK compatible application named Virtual Radiation Training through Ubiety System (VIRTUS) (see Figure 21) provided by DTRA. This allowed the us to continue testing the ATAK sensor integration and communication between devices across the TAK network.

Figure 21. VIRTUS ATAK plug-in[93]

VIRTUS was created by DTRA to provide realistic training in the absence of actual radiological sources and detectors. VIRTUS is a suite of Android apps that run on Android phones and tablets.[94] While it is similar to the simulated sources created by the RaFTS system, the VIRTUS software simulates both the source and sensor, whereas RaFTS provides a simulated input to an existing sensor. A simulated source being placed on the map by a student using VIRTUS at the CACTF training site is shown in Figure 22.

[93] Source: "VIRTUS," Defense Threat Reduction Agency, accessed August 13, 2018, http://www.dtra.mil/Mission/WMD-Training-and-Education/VIRTUS/.

[94] Defense Threat Reduction Agency.

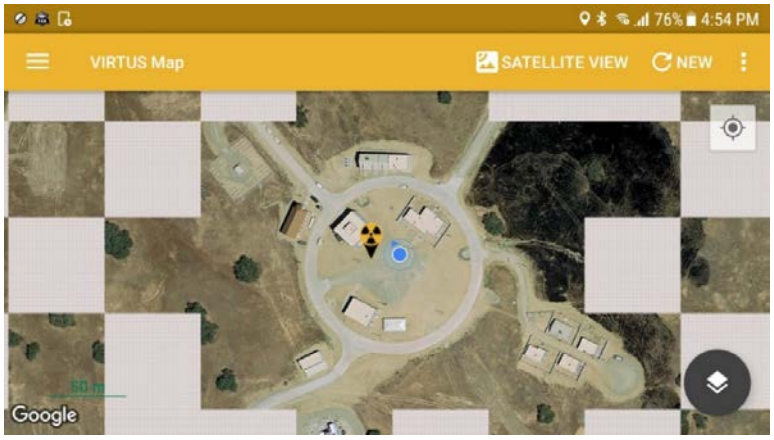

Figure 22. VIRTUS application placing simulated source next to students at CACTF training site.

We configured the VIRTUS application in the ATAK devices while utilizing the existing WMN provided by the MPU-4 radios and was able to execute a scenario using simulated sources with simulated sensors successfully. The JOC was able to successfully track the location on the source by remotely monitoring the ATAK devices and their associated simulated sensor. The location of the ATAK devices and the simulated sensors is shown in Figure 23. Additionally, the team used a second ATAK device to simulate a second sensor, demonstrating the capability to share two virtual sensor feeds across the ATAK network.

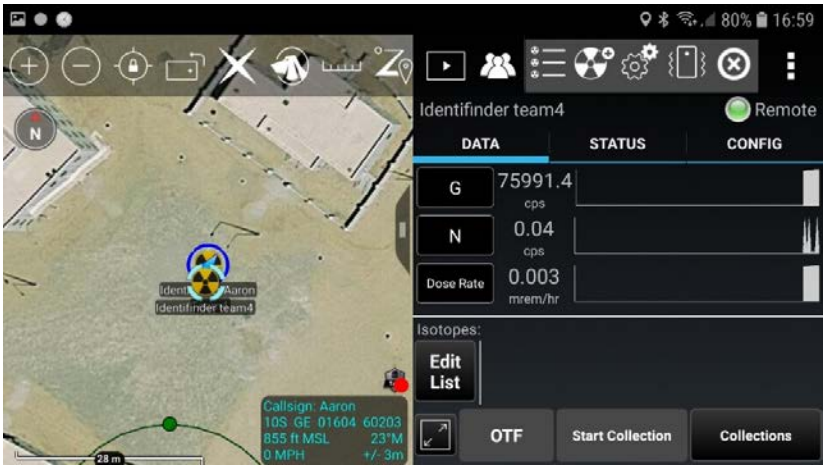

Figure 23. VIRTUS simulated sensor tracking.

5. Analysis

Despite the issues experienced during this round of experimentation, there were valuable findings.

1. The inter-compatibility between the military and civilian variants of the ATAK and their respective CBRN plug-ins works very well, with sensors that are not supported in the ATAK civilian variant still visible if connected to the military variant and shared on the network. This would allow easy integration between U.S. military forces and civilian or partner nation services that do not have access to the ATAK military variant due to international trade and arms regulations.

2. Despite the fact that there are options for integration of multiple sensors into the plug-in, actual compatibility and function are very limited in certain cases.

3. When paired with a sensor that functions as expected, the ATAK in combination with the CBRN plug-in provides the necessary information and sensor data for JOC-level decision making and SME advising of CBRN/CWMD operations.

4. The ATAK RAA framework is capable of being repurposed for unilateral advising by a SME providing analysis to a tactical level unit remotely in near real time.

D. CONCLUSION OF EXPERIMENTATION

There is also an immediate need to revamp the existing sensor integration into the ATAK via the CBRN plug-in application. This is mainly a coding and software development issue that must to be addressed for proper functionality. Additionally, the lack of backwards compatibility of ATAK versions and plug-ins continues to hamper effective use. Operators are unable to use the most recent build for fear of plug-in incompatibility. This could limit the use of other mission essential plug-ins that may have become available with new ATAK builds.

Currently, the envisioned version of the JOCTAK is still in the beginning stages of development. One of the primary issues in our testing was the lack of WinTAK or WebTAK integration, which required the use of Android devices instead of Windows-based PCs in the JOC. Additionally, at the tactical level, the difficulty pairing the ATAK devices with the sensors as designed limited the usefulness of the CBRN plug-in. Despite the number of sensors listed as compatible within the CBRN plug-in, only one prototype and two production sensors proved to be fully functional during our experimentation. Finally, unrelated to the TAK program itself, the most significant overall problem resulted from network connectivity issues due to communication disruption.

1. Future Research Areas

Key items for future research and the incorporation of JIIM Partners:

- Identifying systems and sensors used by JIIM partners
- Integrating ATAK in an RAA/CWMD with JIIM partner's equipment
- Identifying their data format standards and compatibilities issues with the ATAK
- Moving forward with U.S. systems' integration, researching and identifying how to develop our own systems and sensors to enhance JIIM compatibility

We have multiple mission command systems and CBRN sensors, but none of them are unified into a reliable system that truly fits the mission requirements and needs.

There needs to be an overhaul or a more concerted effort to ensure cross-platform integration: SYSTEMATIC to TAK, MFK to ATAK/JOCTAK. Based on the field experiments, the following are proposed future research focus areas:

- Determine the feasibility of using ATAK plug-ins with WinTAK, potentially using a software redesign or emulator.

- CBRN application, programmers need to perform a more robust verification of compatibility with desired sensor types to include different software and hardware versions.

- Determine the feasibility of using a Cursor on Target formatted output for the CBRN plug-in for the purposes of allowing non-Android-based TAK devices to view the sensor data generated and collected by the plug-in.

- Finally, test the intercompatibility of SITAWARE and ATAK in order to determine if the SITAWARE system provides more stable network connectivity as claimed by Systematic Inc.

We recommend that these research focus areas be explored in coordination with the Special Operations Program Executive Offices in the future.

Additionally, the research team conducted experimentation with the ATAK and the Polish Special Forces in September 2018. Although not be captured in this capstone project, this experiment marks the beginning of testing with a SOF partner and broadens the problem set to include the European theater of operations. Recognizing nuclear and existential threats exist outside of the Korean theater of operations the opportunity and need to work more closely with SOCEUR, and our NATO SOF partners will continue to grow.

V. CONCLUSION AND RECOMMENDATIONS

Our research and experimentation identified the necessary CWMD sensor compatibility requirements and TAK plug-in software designs for meeting future JIIM mission sets. Additionally, we demonstrated that the JOCTAK, when properly implemented, will solve the identified gaps in CWMD C4I Operations.

1. A near real-time common operational picture and improved situational awareness across all pertinent partners will facilitate JIIM operations.

2. The capability to have an integrated C4I system with collective planning, mission command, and digital collaboration in near real-time between JIIM partners during all phases of CWMD operations.

3. The capability to integrate sensors into the TAK network and allow an advanced RAA capability among operators, technical specialists, and mission command during a CWMD scenario.

Although the U.S. Army is taking steps to fix its current C4I, a gap remains. The C4I capabilities provided by the Army's adoption of Systematics' SITAWARE as its primary mission command system and common operating picture tool will go a long way toward modernizing it. However, a need still exists regarding the support provided to the SOF warfighter from the operational level commands. JOC integration of the TAK system will fill that gap with a system that has proven itself at a tactical level.

This adoption is not a panacea, however, even if the Army improves its C4I systems the gaps between U.S. SOF and JIIM partners will still exist with little or no improvement, leaving the same issues for JIIM collaboration unsolved. The adoption and integration of a TAK component to U.S. SOF and JIIM partners C4I systems will provide a commonality capable of bridging the gap that currently exists.

JOCTAK's significance is not simply that it is something new or innovative, although it is that, but also that it solves existing command-level capability gaps with reliable and known systems, whose further development enables tactical-level operations.

While this research provides a definite way forward for SOJTF CWMD operations, it has far-reaching implications in a multi-domain environment where data flow and information necessary for continuous operations continues to increase.

As the development of the JOCTAK moves forward, we propose the following recommendations. First and foremost, it must maintain the flexibility that has made the ATAK system so successful and focus on enabling operations at the tactical level. It should not be tied to a specific hardware platform. Because of the Android platform's inability to provide a robust JOC capability with the larger displays and greater processing power required, we suggest that it be based on WinTAK, WebTAK, or a combination of the two. Due to the developmental state of both of those programs, we suggest WinTAK, as it is more mature and already in use. Whichever option is chosen, it must have the capability to run in an austere location on a local machine while maintaining the capacity for outside SMEs to connect remotely and view relevant data or other information sent from the tactical units or the JOC. Also, it must maintain the ability to allow commanders to discriminate the data that individuals connected remotely have access to through network federation.

Second, WinTAK lacks the capability for inter-compatibility with ATAK plug-ins across the entire TAK network. JOCTAK must have the ability to effectively see the data from ATAK plug-ins and interact with them. Possible methods to accomplish this include creating equivalent Windows-based plug-ins for WinTAK, using Cursor on Target message and file format to display the relevant information, using an emulator to allow the Android plug-in to function with WinTAK, or using a web browser-based solution. Pending the successful implementation of cross-platform compatibility for plug-ins and associated data, we believe the baseline capabilities of WinTAK with the current inventory of plug-ins already in operation will suffice for an initial or beta version of the JOCTAK. ATAK's previously demonstrated rapid development cycle will prevent any operational shortages following the identification of a needed capability. The ever-growing ATAK plug-in library as a result of operational and training use in conjunction with regularly trained staff exercises will allow the development of JOC/AO specific capabilities.

Third, it has to be easy for developers to build plug-ins that are compatible across the spectrum of CBRN sensors. The JOCTAK not only has to be able to integrate with ATAK devices but also with the plethora of sensors and their accompanied software.

Finally, but perhaps most importantly for a JIIM CWMD response, this system should be tested as robustly as possible with trusted JIIM partners for susceptibility to enemy counter-measures. This will determine the level and effectiveness of interoperability it provides in a JIIM environment and adapt the development of the JOCTAK as necessary.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. EXPERIMENT WORKSHEETS

JIFX I Camp Roberts, CA. FEB-MAR 2018

Appendix I (Part A, Phase I) to Annex C

Short Title	Multi-Threaded Experiment (MTX) WAS Sensor/Fusion Testing - Camp Roberts, CA
Phase	**Part A, Phase I (27 Feb 2018)**
Experiment Objectives	Facilitate C-WMD SA across operational spectrum by exploring ways to optimize operational and technological aspects of C-WMD WAS operations.
Operational Level Problem	Military forces do not have an aggregation tool to fuse data feeds from multiple rad/nuc operators and sensors and maintain shared SA during searches for nuclear materials of concern (NMOC). We define WAS for the purposes of this experiment as an urban area approximately the size and density of a mall, stadium, or city block, where multiple simultaneous detections from multiple sensors and operators are possible and where each may require real-time adjudication by reachback SMEs.
Tactical Level Problem	U.S. forces need to minimize the time required to DLI NMOC during WAS operations while maximizing force protection. Remote sensors mounted on UxVs can expedite search operations and reduce risks to friendly forces. Multiple feeds enhance RAA operator SA but challenge their coordination abilities. We need to improve ATAK R/N sensor integration to support SA, mission command and collaborative planning between operational elements during WAS operations.
Research Questions	What factors affect ATAK-WinTAK ingestion and display of multiple R/N sensor feeds during WAS? What factors affect HRM sensor data feed from and integration onto a mini UAV? What factors affect ARAM sensor data feed from and integration onto a UAV? What factors affect LIDAR sensor data feed from aboard Matrice UAV? What factors affect 2x4x16” NAI detector data feed from aboard Segway UGV?
Technical Tasks	Evaluate whether sensors operate and transmit properly when mounted on UxVs Evaluate ATAK R/N plug-in capability. Evaluate capability of mesh network to support UxV/sensor formation (using ATAK mesh network supported by TAK server). Evaluate feasibility of using a UxV formation assets to support D-L phases. Evaluate effects of predictive mapping of alert tracks.

Independent Variables	Source material A vs B (Type/strength) Location of source material (in/around buildings)
Reachback Model	Reachback between forward-deployed R/N search team and RAA cell at HQ
Constraints	Weather conditions Intervening terrain UAV battery life Stand-off range requirements
Criteria	Ability of operator to use GUI Ability of RAA cell to coordinate various sensors
Location	**MOUT Site, Camp Roberts, CA**
Date	**Tue, 27 Feb**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS) 95th Civil Support Team (CST) (CAARNG) RAP Team 7 (LLNL) Research Team (LBNL) Camp Roberts base and flight operations support (NPS) Terratracker RadMet
MIO-CWMD Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).
Local Test Bed Components in Use	UxVs Segway UGV Shield AI Quadrotor UAV Matrice 600 Hexarotor UAV Detectors and Sensors Sub-micron multi-beam / LIDAR sensor (LBNL) ARAM sensor (Terratracker) 2x4x16” NAI gamma detector (DTRA/NPS) identiFINDER R-400 (NPS) HRM replacement mini sensors (DTRA) Software

	ATAK R/N plug-in (NPS) Wireless mesh network Sources/NORM	
Scenario	U.S. military search teams are conducting WAS operations in urban terrain in a Pacific region partner nation to detect, locate, and identfy stolen NMOC. Their mission was initiated after intelligence tips led to the surveillance of some suspected Daesh terrorist sympathizers in the Santo Francese area. The suspects appear to have obtained and are attempting to sell some materials stolen from a nearby university medical hospital in October 2017. The sympathizers are still suspected to be in central Calitopia. In January 2018, the sympathizers were believed to be aboard a small craft during a routine safety stop by a Santo Francese maritime police boat outside of Santo Francese Bay when the SFPD ARAM sensor unexpectedly alerted. During secondary screening by the SFPD boat, the small craft in question exchanged gunfire, sped off, and was eventually lost in fog and local maritime large ship traffic. Despite continued vigilance by the SFPD maritime police, intelligence now indicates that the smugglers have moved inland and southward toward the Santa Josefine urban area. It remains unknown whether the NMOC have been sold or transferred to terrorists, but it is assessed that the material is still in the area as of early February 2018. With the help of remote U.S. DoE/LLNL Triage SMEs, the spectra readings from the SFPD boat were later analyzed and estimated to possibly match the signature of the missing university material. Authorities have requested all capable agencies to search for the NMOC, which is believed to be Cesium 137, but the readings were insufficiently long for an accurate estimate, and the sensor may have been too close to the suspect boat's engine compartment, distorting the sensor readings. There is speculation that the suspects may be trying to mask (erroneously) using Thorium-treated welding rods and a thick casing material to hide the signature. Sketchy intelligence available from monitoring traffic on the dark web contains indirect chatter about attacking concentrations of civilians to cause "shocking" casualties, prompting a focus on large sporting events, concerts, and malls. This intelligence is being tentatively correlated to a lead from a local, previously reliable informant who is a recent Syrian refugee of Kurdish descent. The informant reports that in local tea shop circles, influential locals are increasingly critical of decadent Western women and frustrated over the social liberalization changes going on in Saudi Arabia. There are some female-oriented music concerts occurring in the near future	

	in the Santa Josefine area, which are of increased concern, and available teams are expected to be dispatched to several of them. Currently, a joint SOF team has been assigned the mission to search for the NMOC in a portion of a particular Santa Josefine warehouse area where a vigilant local business security guard has reported suspicious after-hours activities by individuals who are not known to belong to the neighboring companies. The SOF team has begun conducting radiological search employing low-visibility techniques to avoid drawing attention, but is now prepared to augment with small UxV systems due to the urgency of the situation based on the intelligence assessment.
Scheme	Phase I consists of the baseline scenario wherein multiple manned and unmanned sensors feed data individually to the TOC (at McMillan EOC) for fusion in the RAA portal. This precedes the later integration scenarios (Ph II, III). Steps: 1. Crew assembles UxVs with sensors at MOUT site. 2. Conduct safety checks and verify co-use and deconfliction. 3. Conduct AM sequential individual sensor/UAV trials to detect and locate sources (based on battery duration of UAVs). 4. Perform platform adjustments as required. 5. Conduct PM sequential individual sensor/UAV trials to detect and locate sources (based on battery duration of UAVs).

Phase Sequence

Activity	NPS (PST)	DC (+3)
JIFX AM Brief (key personnel)	0800-0830	1100-1130
Assemble kits for transport to MOUT site	0800-1000	1100-1300
Move to MOUT site	1000-1030	1300-1330
Set-up/Assembly at MOUT site	1030-1330	1330-1630
Multi-sensor Trials	1330-1600	1630-1900
Recover	1600-1615	1900-1915
RTB	1615-1640	1915-1940
CENETIX Hotwash at TOC	1600-1700	1900-2000
JIFX PM Debrief at TOC (all personnel)	1700-1730	2000-2030

RQ I-1	What factors affect ATAK-WinTAK ingestion and display of multiple R/N sensor feeds during WAS?	
	MoPs	**Data Collector**
	Multiple sensor data are monitorable for DLI of NMOC	Search TM and Advise Cell
	Realtime / NRT upload / stream of multiple DLI data	"
	Identification of high and low ends of data transmission and receive rate	"
	Monitorability of data	"
RQ I-2	What factors affect HRM sensor data feed from, and integration onto, a mini UAV?	
	MoPs	**Data Collector**
	Breaks in N42 message flow	Bourakov/Mejia
	Delays with N42 ingestion	"
	Problems with N42 posting	"
RQ I-3	What factors affect ARAM sensor data feed from, and integration onto a UAV?	
	MoPs	**Data Collector**
	Breaks in N42 message flow	Bourakov/Mejia
	Delays with N42 ingestion	"
	Problems with N42 posting	"
RQ I-4	What factors affect LIDAR sensor data feed from aboard Matrice UAV?	
	MoPs	**Data Collector**
	Separate Document	Bourakov/Mejia
	"	"
	"	"
RQ I-5	What factors affect 2x4x16" NAI detector data feed from aboard Segway UGV?	
	MoPs	**Data Collector**
	Breaks in N42 message flow	Bourakov/Mejia
	Delays with N42 ingestion	"
	Problems with N42 posting	"
Other	**Network Logs**	System Latency	Bourakov

Data Collection	**Tech Obsns**	Network S/W issues Network H/W issues Sensor Equipment issues	Bourakov Bourakov/Mejia Bourakov
	Obsr Notepad	Text chat thread	Wendt
	SA View	Screen captures of SA View COP	Wendt
Observer Notepad/ Radio Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Sverre (at NPS) "TOC"—Mullins "Engineer"—Bourakov "RB Cell"—Mitchell	"Matrice 1"—Bandy "Matrice 2"—Goldan "Shield"—Masters "95 CST"—Efros/Shilk "9 CST"—Foss/TBD "RiiD"—Wendt

Appendix II (Part A, Phase II) to Annex C

Short Title	**Multi-Threaded Experimentation (MTX) WAS Sensor/Fusion Testing - Camp Roberts, CA**
Phase	**Part A, Phase II (28 Feb 2018)**
Experiment Objectives	Facilitate CWMD SA across operational spectrum by exploring ways to optimize operational and technological aspects of CWMD WAS operations.
Operational Level Problem	Military forces do not have an aggregation tool to fuse data feeds from multiple rad/nuc operators and sensors and maintain shared SA during searches for NMOC. We define WAS for the purposes of this experiment as an urban area approximately the size and density of a mall, stadium, or city block, where multiple simultaneous detections from multiple sensors and operators are possible and where each may require real-time adjudication by reachback SMEs.
Tactical Level Problem	U.S. forces need and minimize the time required to DLI NMOC during WAS operations while maximizing force protection. Remote sensors mounted on UxVs can expedite search operations and reduce risks to friendly forces. Multiple feeds enhance RAA operator SA, but challenge their coordination abilities. In order to improve ATAK, R/N sensor integration to support SA, mission command and collaborative planning between operational elements. During WAS operations the specific constraints regarding the UxV-based R/N sensor maneuvering as well as sensor/UxV data feed sequencing need to be identified. The major problem addressed by the Phase II experiment is to evaluate those constraints and to assess their effects on the DLI timeline. The second problem addressed by the Phase II experiment is how to improve ingestion, display, and feedback to multiple sensor operators by the Advise Cell and maximize efficiency in terms of the DLI timeline

Research Questions	1. How does ATAK app R/N sensor data affect SA, mission command, and collective planning between elements during WAS operations? 2. What factors affect ATAK-WinTAK ingestion and display of multiple R/N sensor feeds during WAS? 3. What factors affect display of multiple R/N sensor feeds at Advise Cell/HQs? 4. What are the maneuvering constraints and effects on the DLI timeline for HRM sensor onboard Shield AI? 5. What are the maneuvering constraints and effects on the DLI timeline for ARAM sensors onboard UxVs? 6. What are the maneuvering constraints and effects on the DLI timeline for a LIDAR sensor onboard a UxV? 7. What are the maneuvering constraints and effects on the DLI timeline for ARAM sensors onboard UGVs? 8. What are the maneuvering effects of identiFINDER sensor on the DLI timeline onboard UGVs? 9. What are priority data feeds to display to support Advise Cell/HQs DM process)?
Technical Tasks	Evaluate ATAK R/N plug-in capability. Evaluate capability of mesh network to support UxV/sensor formation (using ATAK mesh network supported by TAK server). Evaluate feasibility of using a UxV formation assets to support DL phases: Evaluate effects of predictive mapping of alert tracks.
Independent Variables	Maneuvering (pattern/distance/ToT) ARAM Sensor onboard Matrice UAV Maneuvering HRM sensor onboard Shield AI UAV Maneuvering LIDAR sensor onboard Matrice UAV Maneuvering ARAM sensor onboard RMP 400 UGV Maneuvering LIDAR sensor onboard RMP 400 UGV Maneuvering LIDAR sensor onboard Talon UGV Maneuvering identiFINDERs operated by dismounted team Frequency of data feeds from ARAM, HRM, LIDAR, and IdentIFINDER sensors Enabling Sensor-ATAK-WinTAK data fusion display in the Advise Cell screen Enabling NPS Testbed and WinTAK fusion views integration Type/strength of source material (2 ea different sources) Location of source material (in/around buildings)
Reachback Model	1. Reachback between forward-deployed R/N search team and RAA cell at HQs 2. Reachback between RAA Cell at HQs and LLNL Triage SMEs

Environmental Constraints	Weather conditions Intervening terrain UAV battery life Stand-off range requirements Network bandwidth Sensor-advise Cell networking interrupts Advise cell-SME reachback interrupts Autonomous mode of Shield AI quadrotor
Criteria	Ability of operator to use GUI Ability of RAA cell to coordinate various sensors
Location	**MOUT Site, Camp Roberts, CA**
Date	**Wed, 28 Feb**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS) 95th Civil Support Team (CST) (CAARNG) 9th CST (CAARNG) RAP Team 7 (LLNL) Research Team (LBNL) Camp Roberts base and flight operations support (NPS) Terratracker RadMet
MIO-CWMD Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).
Local Test Bed Components in Use	UxVs Segway UGV Talon UGV Shield AI Quadrotor UAV Matrice 600 Hexarotor UAV Detectors and Sensors Sub-micron multi-beam/LIDAR sensor (LBNL) ARAM sensor (Terratracker) 2x4x16” NaI detector (DTRA/NPS) 2x4x16” NaI detector (NPS)

	identiFINDER R-400 (NPS) HRM replacement mini sensors (DTRA) Software ATAK R/N plug-in (NPS) Wireless mesh network Sources/NORM (LLNL)	
Scenario	U.S. military search teams are conducting WAS operations in urban terrain in a Pacific region partner nation to detect, locate, and identify stolen NMOC. Their mission was initiated after intelligence tips led to the surveillance of some suspected Daesh terrorist sympathizers in the Santo Francese area. The suspects appear to have obtained and are attempting to sell some materials stolen from a nearby university medical hospital in October 2017. The sympathizers are still suspected to be in central Calitopia. In January 2018, the sympathizers were believed to be aboard a small craft during a routine safety stop by a Santo Francese PD maritime police boat outside of Santo Francese bay when the SFPD ARAM sensor unexpectedly alerted. During secondary screening by the SFPD boat, the small craft in question exchanged gunfire, sped off, and was eventually lost in fog and local maritime large ship traffic. Despite continued vigilance by the SFPD maritime police, intelligence now points that the smugglers have moved inland and southward toward the Santa Josefine urban area. It remains unknown whether the NMOC have been sold or transferred to terrorists, but it is assessed that the material is still in the area as of early February 2018. With the help of remote U.S. DoE/LLNL Triage SMEs, the spectra readings from the SFPD boat were later analyzed and estimated to possibly match the signature of the missing university material. Authorities have requested all capable agencies to search for the NMOC, which is believed to be Cesium 137, but the readings were insufficiently long for an accurate estimate, and the sensor may have been too close to the suspect boat's engine compartment, distorting the sensor readings. There is speculation that the suspects may be trying to mask (erroneously) using Thorium-treated welding rods and a thick casing material to hide the signature. Sketchy intelligence available from monitoring traffic on the dark web is indirect chatter about attacking concentrations of civilians to cause "shocking" casualties, prompting a focus on large sporting events, concerts, and malls. This intelligence is being tentatively correlated to a lead from a local, previously reliable informant who is a recent Syrian	

	refugee of Kurdish descent. The informant reports that in local tea shop circles, influential locals are increasingly critical of decadent Western women and frustrated over the social liberalization changes going on in Saudi Arabia. There are some female-oriented music concerts occurring in the near future in the Santa Josefine area, which are of increased concern, and available teams are expected to be dispatched to several of them. Currently, a joint SOF team has been assigned the mission to search for the NMOC in a portion of a particular Santa Josefine warehouse area where a vigilant local business security guard has reported suspicious after-hours activities by individuals who are not known to belong to the neighboring companies. The SOF team has begun conducting radiological search employing low visibility techniques to avoid drawing attention, but is now prepared to augment with small UxV systems due to the urgency of the situation based on the intelligence assessment. Triage Cell at LLNL has been alerted and is prepared to provide reachback support to the teams to identify any NMOC if/when required.

Scheme	Phase II consists of the more integrated scenario wherein multiple manned and unmanned sensors feed data **simultaneously** via MANET to the TOC (at McMillan EOC) for fusion in the RAA portal. Search team and RAA cell will rehearse procedures to conduct reachback with LLNL Triage SMEs for integrated scenario in Phase III. Steps: 1. Crew assembles UxVs with sensors at MOUT site. 2. Conduct safety checks and verify co-use and deconfliction. 3. Conduct AM **combined/simultaneous** sensor/UAV trials to detect and locate sources (based on battery duration of UAVs). 4. Perform platform adjustments as required. 5. Conduct PM **combined/simultaneous** sensor/UAV trials to detect and locate sources (based on battery duration of UAVs).

Phase Sequence	**Activity**	**NPS (PST)**	**DC (+3)**
	JIFX AM Brief (selected personnel)	0800-0830	1100-1130
	CENETIX AM huddle (all)	0830-0915	1130-1215
	Assemble kits for transport to MOUT site	0915-0945	1215-1245
	Move to MOUT site	0945-1015	1245-1315
	Set-up/Assembly at MOUT site	1015-1100	1315-1400
	Multi-sensor Trial #1	1100-1230	1400-1530
	Food and Water Break Reset/Adjust as Required	1230-1300	1530-1600
	Multi-sensor Trial #2	1300-1600	1600-1900
	Recover	1600-1630	1900-1930
	RTB	1600-1630	1900-1930
	CENETIX Hotwash at Airfield	1630-1700	1930-2000
	JIFX PM Debrief (all personnel)	1700-1730	2000-2030

RQ II-1	How does ATAK R/N sensor integration affect SA, mission command, and collective planning between elements during WAS operations?	
	MoPs	**Data Collector**
	Persistent COP and S/A shared across individual elements and Advise Cell	Search TM and Advise Cell
	Continuous communication link between search elements/ Advise Cell	"
	Improved C2 visibility of search team actions for Advise Cell	"
RQ II-2	What factors affect ATAK / WinTAK ingestion and display of multiple R/N sensor feeds?	

	MoPs	Data Collector
	Fraction of multiple sensor data feeds delivered at each DLI phase	Search TM and Advise Cell
	Real-time / NRT upload / stream of multiple DLI data	“
	Identification of high and low ends of data transmission and receive rate capability	“
	Identification of high priority data feeds	“
RQ II-3	What factors affect display of multiple R/N sensor feeds at Advise Cell/ HQs?	
	MoPs	**Data Collector**
	Successful utilization of multiple sensors data for DLI of NMOC	Search TM and Advise Cell
	Real-time / NRT upload / stream of multiple DLI data	“
	Identification of high and low ends of data transmission and receive rate capability	“
	Monitorability of respective elements	“
RQ II-4	What are the maneuvering constraints and effects on the DLI timeline for HRM sensor onboard Shield AI?	
	MoPs	**Data Collector**
	Most informative maneuver pattern for DLI	Sensor Operator
	Most informative stand-off distance threshold to source for DLI	“
	Preferred Ground Station (operator)-Sensor distance	“
	Sensor acquisition time threshold	“
RQ II-5	What are the maneuvering constraints and effects on the DLI timeline for ARAM sensors onboard Matrice UxVs?	
	MoPs	**Data Collector**
	Most informative maneuver pattern for DLI	Sensor Operator
	Most informative stand-off distance threshold to source for DLI	“
	Preferred Ground Station (operator)-Sensor distance	“
	Sensor acquisition time threshold	“
RQ II-6	What are the maneuvering constraints and effects on the DLI timeline for a LIDAR sensor onboard a Matrice UxV?	
	MoPs	**Data Collector**

	Most informative maneuver pattern for DLI	Sensor Operator
	Most informative stand-off distance threshold to source for DLI	“
	Preferred Ground Station (operator)-Sensor distance	“
	Sensor acquisition time threshold	“
RQ II-7	What are the maneuvering constraints and effects on the DLI timeline for ARAM sensors onboard UGVs?	
	MoPs	**Data Collector**
	Most informative maneuver pattern for DLI	Sensor Operator
	Most informative stand-off distance threshold to source for DLI	“
	Preferred Ground Station (operator)-Sensor distance	“
	Sensor acquisition time threshold	“

RQ II-8	What are the maneuvering effects of an identiFINDER sensor operated by a dismounted unit on the DLI timeline?		
	MoPs		**Data Collector**
	Most informative maneuver pattern for DLI		Sensor Operator
	Most informative stand-off distance threshold to source for DLI		"
	Preferred Ground Station (operator)-Sensor distance.		"
	Sensor acquisition time threshold		"
RQ II-8	What are priority data feeds to display to support Advise Cell/HQs DM process)?		
	MoPs		**Data Collector**
	Most informative maneuver pattern for DLI		Sensor Operator
	Most informative stand-off distance threshold to source for DLI		"
	Preferred Ground Station (operator)-Sensor distance		"
	Sensor acquisition time threshold		"
Other Data Collection	**Network Logs**	System Latency	Bourakov
	Tech Obsns	Network S/W issues Network H/W issues Sensor Equipment issues	Bourakov Bourakov Bourakov
	Obsr Notepad	Text chat thread	Wendt
	SA View	Screen captures of SA View COP	Wendt
Observer Notepad/ Radio Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Sverre (at NPS) "NOC"—Mullins "Engineer"—Bourakov "RAA Cell"—Goldan	"Matrice 1"—Bandy CACTF IS—Stukova/ Crawford "Shield"—Masters "95 CST"—Efros/Shilk "9 CST"—Foss/TBD

Appendix III (Part A, Phase III) to Annex C

Short Title	**Multi-Threaded Experimentation (MTX)** **WAS Sensor/Fusion Testing - Camp Roberts, CA**
Phase	**Part A, Phase III (1 March 2018)**
Experiment Objectives	Facilitate CWMD SA across operational spectrum by exploring ways to optimize operational and technological aspects of CWMD WAS operations.

Operational Level Problem	Military forces do not have an aggregation tool to fuse data feeds from multiple rad/nuc operators and sensors and maintain shared SA during searches for nuclear materials of concern (NMOC). We define WAS for the purposes of this experiment as an urban area approximately the size and density of a mall, stadium, or city block, where multiple simultaneous detections from multiple sensors and operators are possible and where each may require real-time adjudication by reachback SMEs.
Tactical Level Problem	U.S. forces need and minimize the time required to Detect, Locate, and Identify NMOC during WAS operations while maximizing force protection. Remote sensors mounted on UxVs can expedite search operations and reduce risks to friendly forces. Multiple feeds enhance RAA operator SA but challenge their coordination abilities. Correspondingly, the main tactical problem that Phase III addresses is to identify the best combinations of R/N sensor-UxV platform maneuvering and sequencing during the DLI cycle coordinated Advise Cell (RAA operator) for minimizing time and maximizing adjudication speed required for WAS completion.
Research Questions	1. How can ATAK R/N sensor improve SA, mission command, and collective planning between elements during WAS operations? 2. What factors affect ATAK / WinTAK ingestion and display of multiple R/N sensor feeds? 3. What factors affect ability of operators to conduct synchronous reachback between sensor operators and Triage SMEs during the Identify phase? 4. What is optimal sequencing effect to minimize the DLI timeline for an HRM sensor onboard a Shield AI, subject to ARAM-Matrice, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, dismounted identiFINDER feed augmentation? 5. What is optimal sequencing to minimize DLI timeline for ARAM-Matrice sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, dismounted identiFINDER feed augmentation ? 6. What is optimal sequencing to minimize DLI timeline for LIDAR-Matrice sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation? 7. What is optimal sequencing on minimize DLI timeline for ARAM-UGV sensor usage, subject to HRM-Shield AI, ARAM-Matrice, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation? 8. What is optimal sequencing to minimize DLI timeline for LIDAR-UGV sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, RadMet unattended, identiFINDERs dismounted feeds augmentation?

	9. What is optimal sequencing to minimize DLI timeline for RadMet-Unattended sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation? 10. What is optimal sequencing to minimize DLI timeline for identiFINDERs dismounted feeds sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RedMet unattended, RadMet-Unattended?
Technical Tasks	Evaluate ATAK R/N plug-in capability. Evaluate capability of mesh network to support UxV/sensor formation (using ATAK mesh network supported by TAK server). Evaluate effects of predictive mapping of alert tracks.
Independent Variables	Sequencing ARAM sensor onboard Matrice UAV Sequencing HRM sensor onboard Shield AI UAV Sequencing LIDAR sensor onboard Matrice UAV Sequencing ARAM sensor onboard RMP 400 UGV Sequencing LIDAR sensor onboard RMP 400 UGV Sequencing LIDAR sensor onboard Talon UGV Sequencing identiFINDERs operated by dismounted Sequencing RedMet Unattended sensors Frequency of data feeds from ARAM, HRM, LIDAR, and identiFINDER sensors Enabling sensor-ATAK-WinTAK data fusion display in the Advise Cell screen Enabling NPS Testbed and WinTAK fusion views integration Type/strength of source material (2 ea different sources) Location of source material (in/around buildings)
Reachback Model	1. Reachback between forward deployed R/N search team and RAA Cell at HQs 2. Reachback between RAA Cell at HQs and Triage SMEs
Environmental Constraints	Weather conditions Intervening terrain UAV battery life Stand-off range requirements Network bandwidth Sensor-Advise Cell networking interrupts Advise Cell-SME reachback interrupts
Criteria	Ability of operator to use GUI Ability of RAA cell to coordinate various sensors

Location	MOUT Site, Camp Roberts, CA
Date	**Thu, 1 Mar**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS) 95th Civil Support Team (CST) (CAARNG) 9th CST, CAARNG RAP Team 7 (LLNL) Research Team (LBNL) Camp Roberts base and flight operations support (NPS) Terratracker RadMet
MIO-CWMD Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).
Local Test Bed Components in Use	UxVs Segway UGV (NPS) Talon UGV (95th CST) Shield AI Quadrotor UAV (NSW) Matrice 600 Hexarotor UAV (NPS) Detectors and Sensors Sub-micron multi-beam / LIDAR sensor (LBNL) ARAM sensor (Terratracker) 2x4x16” NaI gamma detector (DTRA/NPS) 2x4x16” NaI detector (NPS) identiFINDER R-400 (NPS) HRM replacement mini sensors (DTRA) Software ATAK R/N plug-in (NPS) Wireless mesh network Sources/NORM (LLNL)
Scenario	U.S. military search teams are conducting WAS operations in urban terrain in a Pacific region partner nation to detect, locate, and identify NMOC. Their mission was initiated after intelligence tips led to the surveillance of some suspected Daesh terrorist sympathizers in the Santo Francese area. The suspects appear to have obtained and are attempting to sell some materials stolen from a nearby university medical hospital in

	October 2017. The sympathizers are still suspected to be in central Calitopia. In January 2018, the sympathizers were believed to be aboard a small craft during a routine safety stop by a Santo Francese PD maritime police boat outside of Santo Francese bay when the SFPD ARAM sensor unexpectedly alerted. During secondary screening by the SFPD boat, the small craft in question exchanged gunfire, sped off, and was eventually lost in fog and local maritime large ship traffic. Despite continued vigilance by the SFPD maritime police, intelligence now points that the smugglers have moved inland and southward toward the Santa Josefine urban area. It remains unknown whether the NMOC have been sold or transferred to terrorists, but it is assessed that the material is still in the area as of early February 2018. With the help of remote U.S. DoE/LLNL Triage SMEs, the spectra readings from the SFPD boat were later analyzed and estimated to possibly match the signature of the missing university material. Authorities have requested all capable agencies to search for the NMOC, which is believed to be Cesium 137, but the readings were insufficiently long for an accurate estimate, and the sensor may have been too close to the suspect boat's engine compartment, distorting the sensor readings. There is speculation that the suspects may be trying to mask (erroneously) using Thorium-treated welding rods and a thick casing material to hide the signature. Sketchy intelligence available from monitoring traffic on the dark web is indirect chatter about attacking concentrations of civilians to cause "shocking" casualties, prompting a focus on large sporting events, concerts, and malls. This intelligence is being tentatively correlated to a lead from a local, previously reliable informant who is a recent Syrian refugee of Kurdish descent. The informant reports that in local tea shop circles, influential locals are increasingly critical of decadent Western women and frustrated over the social liberalization changes going on in Saudi Arabia. There are some female-oriented music concerts occurring in the near future in the Santa Josefine area, which are of increased concern, and available teams are expected to be dispatched to several of them. Currently, a joint SOF team has been assigned the mission to search for the NMOC in a portion of a particular Santa Josefine warehouse area where a vigilant local business security guard has reported suspicious after-hours activities by individuals who are not known to belong to the neighboring companies. The SOF team has begun conducting radiological search employing low-visibility techniques to avoid drawing

	attention, but is now prepared to augment with small UxV systems due to the urgency of the situation based on the intelligence assessment. Upon detection and location of suspected NMOC, the search team coordinates via the RAA Cell at HQs directly with the LLNL Triage SMEs to identify the materials.
Scheme	Phase III consists of the **fully integrated** scenario wherein multiple manned and unmanned sensors feed data simultaneously via MANET to the TOC (at McMillan EOC) for fusion in the RAA portal. This phase incorporates all aspects of Detect-Locate-Identify, including **reachback to Triage SMEs** for adjudication. Steps: 1. Crew assembles UxVs with sensors at MOUT site. 2. Conduct safety checks and verify co-use and deconfliction. 3. Conduct AM **combined/simultaneous** sensor/UAV trials to detect and locate sources (based on battery duration of UAVs). 4. Perform platform adjustments as required. 5. Conduct PM **combined/simultaneous** sensor/UAV trials to detect and locate sources (based on battery duration of UAVs).

Phase Sequence

Activity	NPS (PST)	DC (+3)
AM JIFX Brief (selected personnel)	0800-0830	1100-1130
Assemble kits for transport to MOUT site	0800-0830	1100-1130
Move to MOUT site	0830-0900	1130-1200
Set-up/Assembly at MOUT site	0900-0930	1200-1230
Multi-sensor Trial #1	0930-1030	1230-1330
Multi-sensor Trial #2	1030-1130	1330–1430
Battery Recharge/Break	1130-1230	1430-1530
Reset/Adjust as Required	1230-1330	1530-1630
Multi-sensor Trial #3	1330-1430	1630-1730
Multi-sensor Trial #4	1430-1530	1730-1830
Recover	1530-1600	1830-1900
RTB	1600-1630	1900-1930
CENETIX Hotwash at Airfield TOC	1600-1630	1900-1930
JIFX PM Debrief (all personnel)	1630-1700	1930-2000

RQ III-1	How can ATAK R/N sensor improve SA, mission command and collective planning between elements during WAS operations?	
	MoPs	**Data Collector**
	Persistent common operational picture and S/A shared across individual elements, Advise Cell, and HQ	Search TM and Advise Cell
	Continuous communication link between search elements, Advise Cell, and HQ	“
	Improved C2 capability of search team leader, Advise Cell, and HQ	“

RQ III-2	What factors affect ATAK / WinTAK ingestion and display of multiple R/N sensor feeds?	
	MoPs	**Data Collector**
	Successful utilization of multiple sensors data for DLI of NMOC	Search TM and Advise Cell
	Realtime / NRT upload / stream of multiple DLI data	"
	Identification of high and low ends of data transmission and receive rate capability	"
	Monitorability of respective elements	"
RQ III-3	What factors affect ability of operators to conduct synchronous reachback between sensor operators and Triage SMEs during the Identify phase?	
	MoPs	**Data Collector**
	Number of additional screening requests from SMEs	Advise Cell
	Delays of SME responses to sensor feeds and Advise Cell requests	"
	Delays in actionable responses by sensor operators to SME requests	"
RQ III-4	What is optimal sequencing effect to minimize the DLI timeline for an HRM sensor onboard a Shield AI, subject to ARAM-Matrice, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, dismounted identiFINDER feed augmentation?	
	MoPs	**Data Collector**
	Simultaneous or sequential order during Detect Phase	Advise Cell
	Duration of acquisition time during Detect Phase	"
	Simultaneous or sequential order during Locate Phase	"
	Duration of acquisition time during Locate Phase	"
	Simultaneous or sequential order during Locate Phase	"
	Duration of acquisition time during Identify Phase	"
RQ III-5	What is optimal sequencing to minimize DLI timeline for ARAM-Matrice sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation?	
	MoPs	**Data Collector**
	Simultaneous or sequential order during Detect Phase	Advise Cell
	Duration of acquisition time during Detect Phase	"

	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Locate Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Identify Phase	“
RQ III-6	What is optimal sequencing to minimize DLI timeline for LIDAR-Matrice sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-UGV, RadMet unattended, IdentiFinders dismounted feeds augmentation?	
	MoPs	**Data Collector**
	Simultaneous or sequential order during Detect Phase	Advise Cell
	Duration of acquisition time during Detect Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Locate Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Identify Phase	“
RQ III-7	What is optimal sequencing on minimize DLI timeline for ARAM-UGV sensor usage, subject to HRM-Shield AI, ARAM-Matrice, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation?	
	MoPs	**Data Collector**
	Simultaneous or sequential order during Detect Phase	Advise Cell
	Duration of acquisition time during Detect Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Locate Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Identify Phase	“
RQ III-8	What is optimal sequencing to minimize DLI timeline for LIDAR-UGV sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, RadMet unattended, identiFINDERs dismounted feeds augmentation?	
	MoPs	**Data Collector**
	Simultaneous or sequential order during Detect Phase	Advise Cell
	Duration of acquisition time during Detect Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Locate Phase	“
	Simultaneous or sequential order during Locate Phase	“
	Duration of acquisition time during Identify Phase	“

RQ III-9	What is optimal sequencing to minimize DLI timeline for RadMet-Unattended sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RadMet unattended, identiFINDERs dismounted feeds augmentation?		
	MoPs		**Data Collector**
	Simultaneous or sequential order during Detect Phase		Advise Cell
	Duration of acquisition time during Detect Phase		"
	Simultaneous or sequential order during Locate Phase		"
	Duration of acquisition time during Locate Phase		"
	Simultaneous or sequential order during Locate Phase		"
	Duration of acquisition time during Identify Phase		"
RQ III-10	What is optimal sequencing to minimize DLI timeline for identiFINDERs dismounted feeds sensor usage, subject to HRM-Shield AI, ARAM-UGV, LIDAR-Matrice, LIDAR-UGV, RedMet unattended, RadMet-Unattended?		
	MoPs		**Data Collector**
	Simultaneous or sequential order during Detect Phase		Advise Cell
	Duration of acquisition time during Detect Phase		"
	Simultaneous or sequential order during Locate Phase		"
	Duration of acquisition time during Locate Phase		"
	Simultaneous or sequential order during Locate Phase		"
	Duration of acquisition time during Identify Phase		"
Other Data Collection	**Network Logs**	System Latency	Bourakov
	Tech Obsns	Network S/W issues Network H/W issues Sensor Equipment issues	Bourakov Bourakov Bourakov
	Obsr Notepad	Text chat thread	Wendt
	SA View	Screen captures of SA View COP	Wendt
Observer Notepad/ Radio Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Sverre (at NPS) "NOC"—TBD "OPS"—Mullins "Engineer"—Bourakov "RB Cell"—Mitchell	"Matrice 1"—Bandy "Matrice 2"—Goldan "Shield"—Masters "95 CST"—Efros/Shilk "9 CST"—Foss/TBD

JIFX II Camp Roberts, CA. AUG 2018

Appendix I (Live-Ex Part A, Test I) to Annex C

Short Title	RAA Implement TAK as an Operational Level C4I Tool
Phase	**Part A, Test I; Single Node / Single Sensor**
Experiment Objective	This experiment will advance previous testing of CBRN sensor integration into the TAK infrastructure. The objective of this experiment is to evaluate the effectiveness of specialized CWMD sensors and TAK plug-ins and how they improve RAA capability between operators, technical specialists, and mission command functions during a CWMD scenario.
Operational Level Problem	Operational level (JTF) mission command systems currently do not have an aggregation tool that combines data feeds from multiple tactical elements and sensors in a single system to maintain C2 and shared SA during operations, specifically in a CWMD scenario. As U.S. and partner nation forces conduct CWMD operations, they must have the capability to rapidly share information and alerts between tactical unit members and a higher headquarters.
Tactical Level Problem	Tactical elements need ATAK R/N and other sensor integration to support SA, mission command, task coordination, and collaborative planning between tactical elements during CWMD operations. Tactical elements need an external handheld information-sharing tool to synchronously collaborate with remote CBRN subject matter experts. Tactical elements need an internal handheld information sharing tool to self-organize and RAA to a changing CWMD situation.
Research Questions	1. Can the JOC RAA Cell and tactical units exchange sensor data in near real time? 2. What factors affect the TAK infrastructure operating as a C4I tool and integrating sensors in a CWMD scenario? 3. What factors affect the JOC-to-sensor remote management capability using the CBRN plug-in and a connected sensor?
Technical Tasks	Pair associated sensor(s) with ATAK phone(s) Establish TAK infrastructure Establish a network (MANET, WIFI, Cellular) Verify sensor operability
Design (Independent Variables)	Distance between sensor and ATAK device Network type/distance—WIFI, MANET, Cellular Size/Content of R/N data exchanged
Reachback Model	Tactical element to RAA Cell at JOC; JOC to remote R/N SME. May include direct comms or RAA Cell may mediate interaction. JOC may need to simulate remote SME distance.

Functional Constraints	Network signal strength Capacity of the network Weather conditions Limited WinTAK compatibility Ability of RAA cell to coordinate various sensors
Criteria (Dependent Variables)	Ability of JOC and operators to exchange data through TAK TAK data throughput
Location	**Camp Roberts, CA**
Date	**Mon-Thu, 6–9 Aug 2018**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS)
Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).
Local Test Bed Components in Use	Software ATAK WinTAK ATAK R/N plug-in Wireless mesh network MPU-4/5s Android Phones R/N Sensors
Scheme	Phase I consists of **single** manned sensors connected to **individual** nodes and the JOC RAA Cell for fusion and C2 functions. Search team and RAA Cell will rehearse procedures to conduct reach-back and provide assistance / updates. Steps: 1. Assemble sensors at MOUT site. 2. Establish ATAK connectivity with single sensor and confirm connectivity with JOC. 3. Conduct safety checks and verify co-use and deconfliction. 4. Conduct AM sensor trials to Detect, Locate, and identify R/N source. 5. Perform platform and network adjustments as required. 6. Conduct PM sensor trials to Detect, Locate, and identify R/N source.
Phase Sequence	**Activity** — **NPS (PST)** **AM Brief** — 0800-0830 **Setup** — 0830-0900 **Field Test 1/ Phase I** — 0900-1200

	Break		1200-1300
	Field Test 2 / Phase II		1300-1600
	Recover		1600-1630
	RTB		1630-1700
	AAR at TOC		1700-1730
RQ I-1	Can the JOC and tactical units send and receive sensor data in near real time?		
	MoPs		**Data Collector**
	JOC / Tactical unit able to transmit and receive CBRN data feed		Tactical Unit / JOC
	Measured latency of data feed and its effect on operations		"
	Quality of data flow		"
RQ I-2	What issues prohibit the current TAK infrastructure from operating as a C4I tool and integrating sensors in a CWMD scenario?		
	MoPs		**Data Collector**
	Functionality of CBRN plug-in on Android ATAK platform		Tactical Unit / JOC
	Functionality of CBRN plug-in on Windows WinTAK platform		"
	Ability of TAK to process single sensor data feeds		"
RQ I-3	What is the JOC to sensor remote management capability with the CBRN plug-in and connected sensor?		
	MoPs		**Data Collector**
	JOCs ability to manipulate individual sensor settings remotely?		Tactical Unit / JOC
	JOCs ability to simultaneously manipulate multiple sensor settings remotely Phase I?		"
	JOCs able to receive multiple sensor data feeds		"
	Measured latency of changes		"
Other Data Collection	**Network Logs**		
	Tech Obsns	Network S/W issues Network H/W issues Sensor Equipment issues	
	Obsr Notepad	Text chat thread	

	SA View	Screen captures of SA View COP	
Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Mullins "CP"—Parsons "Engineer"—Bourakov	"RAA Cell"—Mitchell "IT"—Goldan

Appendix II (Live-Ex Part A, Test II) to Annex C

Short Title	**RAA** **Implement TAK as an Operational Level C4I Tool**
Phase	**Part A, Test II; Single Node / Multi Sensor**
Experiment Objectives	This experiment will advance previous testing of CBRN sensor integration into the TAK infrastructure. The objective of this experiment is to evaluate the effectiveness of specialized CWMD sensors, and TAK plug-ins and how they improve remote advise and assist (RAA) capability between operators, technical specialists, and mission command functions during a CWMD scenario.
Operational Level Problem	Operational level (JTF) Mission Command systems currently do not have an aggregation tool that combines data feeds from multiple tactical elements and sensors in a single system to maintain C2 and shared SA during operations, specifically in a CWMD scenario. As U.S. and partner nation forces conduct CWMD operations, they must have the capability to rapidly share information and alerts between tactical unit members and a higher headquarters.
Tactical Level Problem	Tactical elements need ATAK R/N and other sensor integration to support SA, mission command, task coordination and collaborative planning between tactical elements during CWMD operations. Tactical elements need an external handheld information-sharing tool to synchronously collaborate with remote CBRN subject matter experts. Tactical elements need an internal handheld information sharing tool to self-organize and RAA to a changing CWMD situation.
Research Questions	1. Can the JOC RAA Cell and tactical units exchange sensor data in near real time? 2. What factors affect the TAK infrastructure operating as a C4I tool and integrating sensors in a CWMD scenario? 3. What factors affect the JOC-to-sensor remote management capability using the CBRN plug-in and a connected sensor? 4. What is the JOC to sensor remote management capability with the CBRN plug-in and connected sensor?
Technical Tasks	Pair associated sensor(s) with ATAK phone(s) Establish TAK infrastructure Establish a network (MANET, WIFI, Cellular) Verify sensor operability

Design (Independent Variables)	Distance between sensor and ATAK device Network type/distance (WIFI, MANET, Cellular) Size/Content of R/N data exchanged
Reachback Model	Tactical element to RAA Cell at JOC; JOC to remote R/N SME. May include direct comms or RAA Cell may mediate interaction. JOC may need to simulate remote SME distance.
Functional Constraints	Network signal strength Capacity of the network Weather conditions Limited WinTAK compatibility Ability of RAA cell to coordinate various sensors
Criteria (Dependent Variables)	Ability of JOC and operators to exchange data through TAK TAK data throughput
Location	**Camp Roberts, CA**
Date	**Mon-Thur, 6–9 Aug 2018**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS)
Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).
Local Test Bed Components in Use	Software ATAK WinTAK ATAK R/N plug-in Wireless mesh network MPU-4/5s Android Phones R/N Sensors
Scheme	Phase I consists of **single** manned sensors connected to **individual** nodes and the JOC RAA Cell for fusion and C2 functions. Search team and RAA Cell will rehearse procedures to conduct reach-back and provide assistance / updates. Steps: 1. Assemble sensors at MOUT site. 2. Establish ATAK connectivity with single sensor and confirm connectivity with JOC. 3. Conduct safety checks and verify co-use and deconfliction. 4. Conduct AM sensor trials to Detect, Locate, and identify R/N source. 5. Perform platform and network adjustments as required.

	6. Conduct PM sensor trials to Detect, Locate, and identify R/N source.

Phase Sequence	Activity	NPS (PST)
	AM Brief	0800-0830
	Setup	0830-0900
	Field Test 1/ Phase I	0900-1200
	Break	1200-1300
	Field Test 2 / Phase II	1300-1600
	Recover	1600-1630
	RTB	1630-1700
	AAR at TOC	1700-1730

RQ I-1	Can the JOC and tactical units send and receive sensor data in near real time?	
	MoPs	**Data Collector**
	JOC/Tactical unit able to transmit and receive CBRN data feed	Tactical Unit / JOC
	Measured latency of data feed and its effect on operations	"
	Quality of data flow	"
RQ I-2	Can the TAK infrastructure support multiple sensor feeds?	
	MoPs	**Data Collector**
	Tactical unit able to operate and view multiple sensor feeds	Tactical Unit / JOC
	Realtime / NRT upload / stream of multiple data feeds	"
	Measured latency of data feeds	"
RQ I-3	What issues prohibit the current TAK infrastructure from operating as a C4I tool and integrating sensors in a CWMD scenario?	
	MoPs	**Data Collector**
	Functionality of CBRN plug-in on Android ATAK platform	Tactical Unit / JOC
	Functionality of CBRN plug-in on Windows WinTAK platform	"
	Ability of TAK to process multiple sensor data feeds	"

RQ I-4	What is the JOC to sensor remote management capability with the CBRN plug-in and connected sensor?		
	MoPs		**Data Collector**
	JOCs ability to manipulate individual sensor settings remotely		Tactical Unit / JOC
	JOCs ability to simultaneously manipulate multiple sensor settings remotely		"
	JOCs able to receive multiple sensor data feeds		"
	Measured latency of changes		"
	Tech Obsns	Network S/W issues Network H/W issues Sensor equipment issues	
	Obsr Notepad	Text chat thread	
	SA View	Screen captures of SA view COP	
Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Mullins "CP"—Parsons "Engineer"—Bourakov	"RAA Cell"—Mitchell "IT"—Goldan

Appendix III (Live-Ex Part A, Test III) to Annex C

Short Title	**RAA** **Implement TAK as an Operational Level C4I Tool**
Phase	**Part A, Test III; Multi Node / Multi Sensor**
Experiment Objective	This experiment will advance previous testing of CBRN sensor integration into the TAK infrastructure. The objective of this experiment is to evaluate the effectiveness of specialized CWMD sensors and TAK plug-ins and how they improve RAA capability between operators, technical specialists, and mission command functions during a CWMD scenario.
Operational Level Problem	Operational level (JTF) mission command systems currently do not have an aggregation tool that combines data feeds from multiple tactical elements and sensors in a single system to maintain C2 and shared SA during operations, specifically in a CWMD scenario. As U.S. and partner nation forces conduct CWMD operations, they must have the capability to rapidly share information and alerts between tactical unit members and a higher headquarters.
Tactical Level Problem	Tactical elements need ATAK R/N and other sensor integration to support SA, mission command, task coordination and collaborative planning between tactical elements during CWMD operations.

	Tactical elements need an external handheld information-sharing tool to synchronously collaborate with remote CBRN subject matter experts. Tactical elements need an internal handheld information sharing tool to self-organize and RAA to a changing CWMD situation.
Research Questions	1. Can the JOC RAA Cell and tactical units exchange sensor data in near real time? 2. What factors affect the TAK infrastructure operating as a C4I tool and integrating sensors in a CWMD scenario? 3. What factors affect the JOC-to-sensor remote management capability using the CBRN plug-in and a connected sensor? 4. What is the JOC to sensor remote management capability with the CBRN plug-in and connected sensor?
Technical Tasks	Pair associated sensor(s) with ATAK phone(s) Establish TAK infrastructure Establish a network (MANET, WIFI, Cellular) Verify sensor operability
Design (Independent Variables)	Distance between sensor and ATAK device Network type/distance—WIFI, MANET, Cellular Size/Content of R/N data exchanged
Reachback Model	Tactical element to RAA Cell at JOC; JOC to remote R/N SME. May include direct comms or RAA Cell may mediate interaction. JOC may need to simulate remote SME distance.
Functional Constraints	Network signal strength Capacity of the Network Weather conditions Limited WinTAK compatibility Ability of RAA cell to coordinate various sensors
Criteria (Dependent Variables)	Ability of JOC and operators to exchange data through TAK TAK data throughput
Location	**Camp Roberts, CA**
Date	**Mon-Thur, 6–9 Aug 2018**
Players	CENETIX research students (NPS) CENETIX Monitoring and Control team (NPS)
Testbed Infrastructure	CENETIX Testbed Portal TAK server Deployable MANET components Testbed MANET (NPS ATAK IP space) SA and data capture tools Sensor nodes Data will be collected and disseminated using NPS SA and data

	capture tools, WinTAK (for ATAK view), and Network Management Tools (Solar Winds, Wave Relay app, etc).	
Local Test Bed Components in Use	Software ATAK WinTAK ATAK R/N plug-in Wireless mesh network MPU-4/5s Android Phones R/N Sensors	
Scheme	Phase I consists of **single** manned sensors connected to **individual** nodes and the JOC RAA Cell for fusion and C2 functions. Search team and RAA Cell will rehearse procedures to conduct reach-back and provide assistance / updates. Steps: 1. Assemble sensors at MOUT site. 2. Establish ATAK connectivity with single sensor and confirm connectivity with JOC. 3. Conduct safety checks and verify co-use and deconfliction. 4. Conduct AM sensor trials to detect, locate, and identify R/N source. 5. Perform platform and network adjustments as required. 6. Conduct PM sensor trials to detect, locate, and identify R/N source.	

Phase Sequence	**Activity**	**NPS (PST)**
	AM Brief	0800-0830
	Setup	0830-0900
	Field Test 3/ Phase III	0900-1200
	Break	1200-1300
	Field Test 4 / Phase III	1300-1600
	Recover	1600-1630
	RTB	1630-1700
	AAR at TOC	1700-1730
RQ I-1	Can the JOC and tactical units send and receive sensor data in near real time?	
	MoPs	**Data Collector**
	JOC / Tactical unit able to transmit and receive CBRN data feed	Tactical Unit / JOC
	Measured latency of data feed and its effect on operations	“
	Quality of data flow	“
RQ I-2	Can the TAK infrastructure support multiple sensor feeds?	
	MoPs	**Data Collector**
	Tactical unit able to operate and view multiple sensor feeds	Tactical Unit / JOC
	Realtime / NRT upload / stream of multiple data feeds	“
	Measured latency of data feeds and its effect on operations	“
RQ I-3	What issues prohibit the current TAK infrastructure from operating as a C4I tool and integrating sensors in a CWMD scenario?	
	MoPs	**Data Collector**
	Functionality of CBRN plug-in on Android ATAK platform	Tactical Unit / JOC
	Functionality of CBRN plug-in on Windows WinTak platform	“
	Ability of TAK to process multiple sensor data feeds	“
RQ I-4	What is the JOC to sensor remote management capability with the CBRN plug-in and connected sensor?	
	MoPs	**Data Collector**

	JOC's ability to manipulate individual sensor settings remotely			Tactical Unit / JOC
	JOC's ability to simultaneously manipulate multiple sensor settings remotely.			"
	JOC's ability to receive multiple sensor data feeds			"
	Measured latency of changes			"
	Tech Obsns	Network S/W issues Network H/W issues Sensor equipment issues		
	Obsr Notepad	Text chat thread		
	SA View	Screen captures of SA View COP		
Naming Convention	**Callsign**	"PI"—Bordetsky "NPS NOC"—Mullins "CP" -Parsons "Engineer"—Bourakov	"RAA Cell"—Mitchell "IT"—Goldan	

LIST OF REFERENCES

Arms Control Association. "Nuclear Weapons: Who Has What at a Glance." Accessed August 10, 2018. https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat.

Army Technology. "TALON Tracked Military Robot." *Army Technology* (blog). Accessed August 24, 2018. https://www.army-technology.com/projects/talon-tracked-military-robot/.

Brown, Robert B., and David G. Perkins. "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight." War on the Rocks. August 18, 2018. https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/.

Conroy, Ryan. "Special Tactics Saves Lives in Hurricane Harvey Aftermath." U.S. Air Force. August 31, 2017. https://www.af.mil/News/Article-Display/Article/1297004/special-tactics-saves-lives-in-hurricane-harvey-aftermath/.

CradlePoint. "CradlePoint Mobile Networks." Accessed May 23, 2018. https://cradlepoint.com.

Cunningham, William T. "Too Big to Fail: The U.S. Government Counter Weapons of Mass Destruction Enterprise." Master's thesis. Naval Postgraduate School, 2014.

Defense Threat Reduction Agency. "VIRTUS." Accessed August 13, 2018. http://www.dtra.mil/Mission/WMD-Training-and-Education/VIRTUS/.

Department of the Army. *Combined Arms Countering Weapons of Mass Destruction.* ATP 3–90.40. Washington, DC: Department of the Army, 2017. https://fas.org/irp/DoDdir/army/atp3-90-40.pdf.

Department of the Army. *Mission Command.* ADP 6–0. Washington, DC: Department of the Army, 2014.

Department of the Army. *Multi-Service Tactics Techniques and Procedures for Chemical Biological Radiological and Nuclear Reconnaissance and Surveillance.* ATP 3–11.37. Washington, DC: Department of the Army, 2013.

Department of the Army. *Special Operations Chemical, Biological, Radiological, and Nuclear Operations,* ATP 3–05.11. Washington, DC: Department of the Army, 2014.

DJI. "Matrice 600 Pro." Accessed August 24, 2018. https://store.dji.com/product/matrice-600-pro.

Dries, William. “Some New, Some Old, All Necessary: The Multi-Domain Imperative.” War on the Rocks. March 27, 2017. https://warontherocks.com/2017/03/some-new-some-old-all-necessary-the-multi-domain-imperative/.

Ebbutt, Giles. “Integrated Command and Control from Joint Headquarters to the Tactical Edge.” *IHS Jane’s International Defense Review* 47 (May 2014): 1–6. Accessed July 5, 2018. http://www.janes360.com/images/assets/724/38724/Systematic_reprint.pdf.n

Ebbutt, Giles. “US Army Expands Use of SitaWare.” Jane’s by IHS Markit. February 9, 2018. http://www.janes.com/article/77780/us-army-expands-use-of-sitaware.

EPE. “Guardian Predator Portable Radiation Search Tool.” 2018. https://www.epequip.com/catalogue/all-hazards-management/guardian-predator-portable-radiation-search-tool/.

Ferriter, Michael, and Phil Schupp. “ADAPT Team Inauguration Trip Report.” Herndon, VA: Interagency Joint Operations Center and Monterey, CA: Naval Postgraduate School, January 2017.

Ferriter, Michael, Phil Shupp, and Sverre Wetteland. “Organizing Chaos: The Tactical Assault Kit Collaborative Mission Planner.” Master’s thesis. Naval Postgraduate School, 2017. https://calhoun.nps.edu/handle/10945/56915.

FLIR Systems. “IdentiFINDER R400 All-Purpose Radionuclide Identification Device.” Accessed August 26, 2018. https://www.flir.com/products/identifinder-r400/.

Gramer, Robbie, and Emily Tamkin. “Decades of U.S. Diplomacy with North Korea: A Timeline.” *Foreign Policy,* March 12, 2018. https://foreignpolicy.com/2018/03/12/a-timeline-of-u-s-negotiations-talks-with-north-korea-trump-kim-jong-un-pyongyang-nuclear-weapons-diplomacy-asia-security/.

Guterres, Antonio. “Opening Remarks at Press Encounter, September 5, 2017.” United Nations. https://www.un.org/sg/en/content/sg/speeches/2017-09-05/secretary-generals-press-encounter.

Intellectual Property Office. “Localization and Mapping Platform 2.0 2017–114.” June 15, 2018. https://ipo.lbl.gov/lbnl2017-114/.

Joint Chiefs of Staff. *Countering Weapons of Mass Destruction.* JP 3–40. Washington, DC: Joint Chiefs of Staff, 2014.

Joint Chiefs of Staff. *Multinational Operations.* JP 3–16. Washington, DC: Joint Chiefs of Staff, 2013.

Joint Chiefs of Staff. *Operations in Chemical, Biological, Radiological, and Nuclear Environments.* JP 3–11. Washington, DC: Joint Chiefs of Staff, 2013.

Lawrence Livermore National Laboratory. “Ultra-Realistic Radiation Detection Training without Using Radioactive Materials.” January 14, 2015. https://www.llnl.gov/news/ultra-realistic-radiation-detection-training-without-using-radioactive-materials.

Lyford, John, James M. Rowland, Kristopher B. Valenti, and Ross C. Huddleston. “Preparing for a Crisis: Network Coordination to Deal with North Korea’s WMD.” Master’s thesis. Naval Postgraduate School, 2017.

McKaughan, Jeff. “Q&A with Lieutenant General Tovo.” *Special Operations International*, October 2016. https://issuu.com/jeffmckaughan/docs/specops_14-7_final.

Mehney, Paul D. “U.S. Army Marches Toward Coalition Interoperability.” *Signals*, March 2018.

Michael J. Kristan, Jeffrey T. Hamalainen, Douglas P. Robbins, and Patrick J. Newell. “Cursor-on-Target Message Router User’s Guide.” MITRE Corporation, 2009. https://www.mitre.org/sites/default/files/pdf/09_4937.pdf.

National Guard. “California Civil Support Team Enhances Civilian Partnerships.” Accessed August 16, 2018. http://www.nationalguard.mil/News/Article/576048/california-civil-support-team-enhances-civilian-partnerships-through-training/.

National Guard. “Weapons of Mass Destruction, Civil Support Team.” December 2017. http://www.nationalguard.mil/Portals/31/Resources/Fact%20Sheets/Weapons%20of%20Mass%20Destruction%20Civil%20Support%20Team%20Fact%20Sheet%20(Dec.%202017).pdf.

NATO. “Statement by the NATO Secretary General on the Actions against the Syrian Regime’s Chemical Weapons Facilities and Capabilities.” Accessed August 22, 2018. http://www.nato.int/cps/en/natohq/news_153661.htm.

Naval Postgraduate School. “What Is JIFX?” Accessed August 6, 2018. https://my.nps.edu/web/fx/what-is-jifx-.

Nellis Air Force Base. “United States Air Force Weapons School.” Accessed April 4, 2018. http://www.nellis.af.mil/About/Fact-Sheets/Display/Article/284156/united-states-air-force-weapons-school/.

ORTEC. “Micro-Detective Ultra Light Portable RIID.” Accessed August 16, 2018. https://www.ortec-online.com/products/nuclear-security-and-safeguards/hand-held-radioisotope-identifiers-riids/micro-detective.

OST Photonics. “4 Inch x 4 Inch x 16 Inch NaI(Tl) Scintillation Detector, Energy Resolution: ≤8.5%@662keV(Cs-137).” Accessed August 24, 2018. https://www.ost-photonics.com/product/4%e2%80%b3x4%e2%80%b3x16%e2%80%b3-naitl-scintillation-detector/.

Pomerleau, Mark. “Here’s What the Army’s Tactical Network for the Future Will Look Like.” C4ISRNET, October 3, 2017. https://www.c4isrnet.com/it-networks/2017/10/02/heres-what-the-armys-tactical-network-for-the-future-will-look-like/.

Rumsfeld, Donald H. “Designation of Responsibilities for Combating Weapons of Mass Destruction to Commander, U.S. Strategic Command.” Office of the Secretary of Defense, January 6, 2005.

Segway. “Segway Robotic Mobility Platforms (RMP).” Accessed August 24, 2018. https://msu.edu/~luckie/segway/rmp/rmp.html.

Shield AI. “Products: Artificially Intelligent ISR Asset for Ground Forces.” Accessed August 24, 2018. https://www.shield.ai/products/.

Stanfield, Erik J. “Lost in Translation: Lessons from Counterterrorism for a More Proactive Weapons of Mass Destruction Strategy.” Master’s thesis. Naval Postgraduate School, 2017. https://calhoun.nps.edu/handle/10945/55539.

Sterling, Josh. “TAK LSE Brief.” PowerPoint, USSOCOM 2018 TAK Working Group, Pinehurst, North Carolina, August 13, 2018. https://www.milsuite.mil/books/groups/2018-tak-off-site.

TerraTracker. “ARAM Technology—Adaptable Radiation Area Monitors.” Accessed August 20, 2018. https://terratracker.com/aram-technology/.

Thielenhaus, Christopher, and Eric Roles. “Virtual Accompany Kits Return to Baghdad: A View from the Front Lines.” *Special Warfare* 30, no. 2 (2017): 26–29.

Thielenhaus, Christopher, Pat Traeger, and Eric Roles. “Reaching Forward in the War against the Islamic State.” *Prism: A Journal of the Center for Complex Operations* 6, no. 3 (2016): 96–108.

Under Secretary of Defense for Policy. *DOD Countering Weapons of Mass Destruction*. DOD Policy Directive 2060.02. Washington, DC: Under Secretary of Defense for Policy.

United States Government. “TAK.” Accessed August 23, 2018. https://takmaps.com/.

Usbeck, Kyle, Matthew Gillen, Joseph Loyall, Andrew Gronosky, Joshua Sterling, Ralph Kohler, Kelly Hanlon, et al. “Improving Situation Awareness with the Android Team Awareness Kit (ATAK).” In *Proceedings SPIE Defense and Security* 9456 (2015): 94560R-1-94560R-22. https://doi.org/10.1117/12.2180014.

White House. *United States National Security Strategy 2017*. Washington, DC: U.S. Government Printing Office, December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California