2022-12

CLOSING THE TECHNOLOGY GAP: PARTNER FORCE DIGITAL TOOLS FOR INFORMATION ADVANTAGE, PROJECT I-SHAREINFORMATION SHARING, AND HOSTING ADVANCED REMOTE ECOSYSTEM ASSESSMENTS

Foley, Patrick M.; Harris, Peter L.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/71569

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DEFENSE ANALYSIS CAPSTONE REPORT

CLOSING THE TECHNOLOGY GAP: PARTNER FORCE DIGITAL TOOLS FOR INFORMATION ADVANTAGE, PROJECT I-SHARE–INFORMATION SHARING, AND HOSTING ADVANCED REMOTE ECOSYSTEM ASSESSMENTS

by

Patrick M. Foley and Peter L. Harris

December 2022

Thesis Advisor:	Shannon C. Houck
Co-Advisor:	Leo J. Blanken
Second Readers:	Michael R. Stevens Jr.
	Eric Roles, 1st Special Forces Command

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY
(Leave blank)

2. REPORT DATE
December 2022

3. REPORT TYPE AND DATES COVERED
Defense Analysis Capstone Report

4. TITLE AND SUBTITLE
CLOSING THE TECHNOLOGY GAP: PARTNER FORCE DIGITAL TOOLS FOR INFORMATION ADVANTAGE, PROJECT I-SHARE–INFORMATION SHARING, AND HOSTING ADVANCED REMOTE ECOSYSTEM ASSESSMENTS

5. FUNDING NUMBERS

6. AUTHOR(S) Patrick M. Foley and Peter L. Harris

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)

Project ISHARE validated the theory that partner force data-sharing platforms require early iteration with foreign partners to ensure suitable design and create long-term adoption. Strategic competition requires reassessing how U.S. SOF cultivates operational relationships and shares critical data and information between partners. The operational relationships developed by SOF teams must modernize through secure digital tools to merge physical and digital personas for persistent engagement and information sharing. The project assessed two emerging platforms with partners in the Philippines. Survey results indicate that both platforms could be effective for operational use but lack sustainable connectivity for remote areas. The results highlighted that 55% of partner force respondents use unsecured apps to share data with U.S. SOF. Additionally, 66% of respondents agreed that the Civil Knowledge Integration-Tactical Assault Kit (CKI-TAK) or Field Information Support Tool (FIST) would reduce their dependence on unsecured platforms. Survey results, including respondents from over 25 nations, confirmed that partner nations do not provide their forces with the necessary digital tools for COP development and secure data sharing. The in-country assessments inform recommendations to develop next-generation secure partner force data-sharing platforms at the edge for both Mil-Mil and Civ-Mil coordination and use such platforms as a deterrence mechanism in Taiwan.

14. SUBJECT TERMS
U.S. Army Special Operations Forces, Partner Force, Partner Forces, Grey Zone, competition, strategic competition, SOF, advise and assist, ARSOF, civil affairs, Special Forces, JIIM, knowledge management, data, data analysis, visual analysis, Common Operating Picture, China, Counter Terrorism, digital tools, digital platforms, Host Nation, over- the- horizon, communication systems, Civ-Mil, Civilian Military cooperation, Taiwan, TAK, CKI, FIST, Partner Force Reporting, Civil Networks, CKI-TAK

15. NUMBER OF PAGES
99

16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

CLOSING THE TECHNOLOGY GAP: PARTNER FORCE DIGITAL TOOLS FOR INFORMATION ADVANTAGE, PROJECT I-SHARE–INFORMATION SHARING, AND HOSTING ADVANCED REMOTE ECOSYSTEM ASSESSMENTS

Patrick M. Foley
Major, United States Army
BA, Hofstra University, 2006

Peter L. Harris
Major, United States Army
BA, Purdue University, 2011

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN APPLIED DESIGN FOR INNOVATION

and

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Shannon C. Houck
Advisor

Leo J. Blanken
Co-Advisor

Michael R. Stevens Jr.
Second Reader

Eric Roles
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Project ISHARE validated the theory that partner force data-sharing platforms require early iteration with foreign partners to ensure suitable design and create long-term adoption. Strategic competition requires reassessing how U.S. SOF cultivates operational relationships and shares critical data and information between partners. The operational relationships developed by SOF teams must modernize through secure digital tools to merge physical and digital personas for persistent engagement and information sharing. The project assessed two emerging platforms with partners in the Philippines. Survey results indicate that both platforms could be effective for operational use but lack sustainable connectivity for remote areas. The results highlighted that 55% of partner force respondents use unsecured apps to share data with U.S. SOF. Additionally, 66% of respondents agreed that the Civil Knowledge Integration-Tactical Assault Kit (CKI-TAK) or Field Information Support Tool (FIST) would reduce their dependence on unsecured platforms. Survey results, including respondents from over 25 nations, confirmed that partner nations do not provide their forces with the necessary digital tools for COP development and secure data sharing. The in-country assessments inform recommendations to develop next-generation secure partner force data-sharing platforms at the edge for both Mil-Mil and Civ-Mil coordination and use such platforms as a deterrence mechanism in Taiwan.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ARSOF	Army Special Operations Forces
CCP	Chinese Communist Party
CF	Conventional Force(s)
Civ-Mil	civilian-military
CKI-TAK	Civil Knowledge Integration Tactical Assault Kit
CMO	Civil Military Operations
COP	common operating picture
FID	Foreign Internal Defense
FIST	Field Information Support Tool
FVEY	Five Eyes
LP-CRADA	limited purpose cooperative research and development agreement
HA/DR	Humanitarian Assistance and Disaster Relief
JIIM	Joint Interagency Intergovernmental Multinational
KMS	Knowledge Management System
NATO	North Atlantic Treaty Organization
PF	Partner Force
PRC	People's Republic of China
RAA	Remote Advise and Assist
RAA-VAK	Remote Advise and Assist – Virtual Accompany Kit
SFAB	Security Force Assistance Brigade
SME	subject-matter expert
SOF	Special Operations Forces
TAK	Tactical Assault Kit
UI	User Interface
USASOC	U.S. Army Special Operations Command
USEUCOM	U.S. European Command
USINDOPACOM	U.S. Indo-Pacific Command
USSOCOM	U.S. Special Operations Command
USSOUTHCOM	U.S. Southern Command
UW	Unconventional Warfare

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Due to technology gaps, partner forces often use unsecured commercial options to share data with U.S. teams. These options are insufficient and increase risk as malign actors infiltrate commercial networks. Proj. ISHARE assessed two emerging digital information-sharing platforms—Civil Knowledge Information-Tactical Assault Kit (CKI-TAK) and Field Information Support Tool (FIST)—to better inform how U.S. SOF can best develop and utilize digital tools for secure information sharing with partners to support information advantage.

Background: This project was undertaken because Strategic Competition, as highlighted in the 2022 NSS, requires reassessing how U.S. SOF cultivates operational relationships and shares critical data and information between partners. Current digital information platforms used with partners are often U.S.-centric in their development and design and remain limited to tactical applications. As highlighted in Figure 1, the array of unsecured platforms used by partner forces demonstrates a range of vulnerability to the information shared. Furthermore, these platforms are unable to provide the global information-sharing network required for strategic competition. SOF teams must use secure digital tools such as CKI-TAK and FIST to enable persistent engagement with partners for information sharing over the horizon.

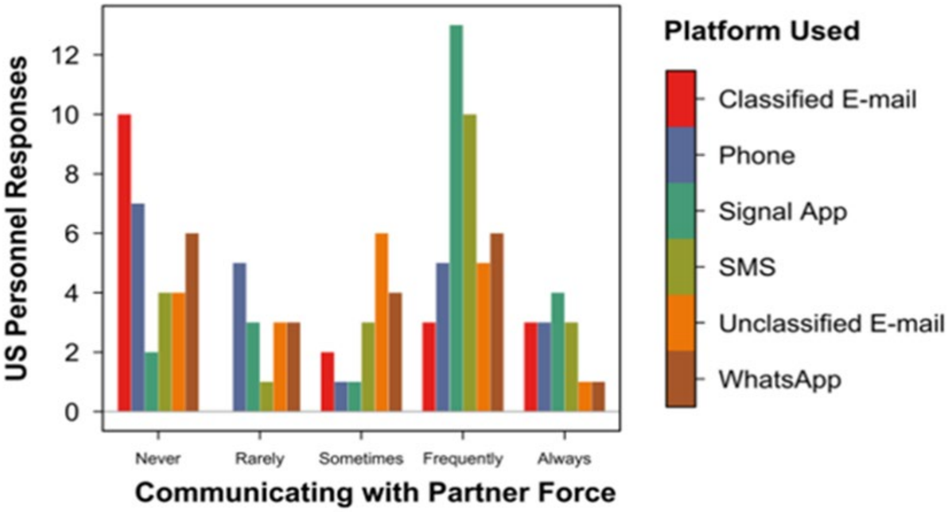


Figure 1. Partner Communication Methods

Research Design: Proj. ISHARE conducted field assessments in the Philippines and survey research with military officers representing over 25 allied and partnered nations in addition to U.S. military personnel over the course of fourteen months. The Proj. ISHARE in-country assessments inform recommendations to develop next-generation secure partner force data-sharing platforms at the edge for both Mil-Mil and Civ-Mil coordination. Additionally, the project built upon the data to conceptualize the use of such platforms to enhance deterrence in places such as Taiwan.

Initial Results: Participant responses indicate that both the CKI-TAK and FIST platforms are assessed as effective for operational use but lack sustainable connectivity for remote operating areas. While 55% of partner force respondents currently use commercial apps to share data and information with U.S. SOF units of action, 66% agreed that access to CKI-TAK or FIST would reduce their dependence on such unsecured platforms. Survey results also confirmed that a majority of partner nations represented in the study do not provide their forces with the necessary digital tools for Common Operating Picture (COP) development and secure data sharing. The initial results confirm that CKI-TAK and FIST have potential. This partner-focused research was conducted at limited additional cost to the DOD, less than $50k.

Way Ahead: The project seeks to continue field testing in additional countries and with new emerging platforms to provide refined region-specific recommendations. The project established a methodology for assessing digital information-sharing tools with partner forces overseas. Proj. ISHARE produced data addressing the theory that partner-force data-sharing platforms require early iteration with foreign partners to ensure suitable design and to promote long-term adoption. Additional coordination and research within Project Convergence, Project Hardwire, and other DOD initiatives is needed to develop secure data lakes and backside architecture to support these types of user interface platforms at the edge.

The partnerships established by over 140 SOF teams across 80 nations are the key access point for information advantage. SOF teams must use digital tools for persistent engagement and information sharing. Assessing emerging secure digital information platforms from a partner force requirements perspective can modernize the relationships U.S. SOF teams foster with partners worldwide to secure the information advantage. As highlighted by the photo below of the NPS research team with the Commanding General of the Philippines Civil-Military Operations Regiment, information-sharing technology development and usage are natural extensions of the vital interpersonal relationships SOF teams build with foreign partners (Figure 2).

THANKSGIVING
FIST & CKI-TAK Demonstration & Assessment
NAVAL POSTGRADUATE SCHOOL
THANKSGIVING
FIST & CKI-TAK Demonstration & Assessment
NAVAL POSTGRADUATE SCHOOL

MAJs Foley and Harris with BGen Lagamon and the Sr. Staff of the PA CMOR. Fort Bonifacio Manila

Figure 2. Research Team Engagement with Civil Military Operations Regiment

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We offer our deepest gratitude to Dr. Shannon Houck, who provided incredible assistance during complex preparation for overseas travel. Her insightful approach and broad background in Psychology and Sociology greatly enhanced our methodology and facets of research. Dr. Leo Blanken has been an immense support in bringing this concept to fruition and connecting us with other like-minded innovators during early development for great advice and inspiration on our journey. We are genuinely indebted to Mr. Michael Stevens for his in-depth technical assistance, institutional knowledge, and support for us and other generations of driven researchers. His help opened doors and created connections for well-balanced work. To LTC Eric Roles, thank you for your support, guidance, and commitment to retaining the SOF comparative advantage. To Dr. Timothy Warren, thank you for your data visualization assistance and mentorship to support our quantitative analysis and data-aggregation. Thank you to each participant who provided invaluable insights, friends at the Graduate Writing Center, and Joseph Lukefahr of the IS Dept. for technical support. Your support was immensely helpful.

Patrick Foley: My deepest and heartfelt thanks to the most incredible woman I have ever met, my wife, Jessica. Thank you for your unwavering support and love during this endeavor to complete two capstone projects and always. Thank you for being the incredible woman, mother, wife, and full-time middle school teacher you are. I greatly appreciate you holding down the fort during my many TDYs during what was supposed to be a “take a knee” tour. Thank you to my wonderful children, Tommy and Kate, for your perseverance and for bringing smiles and joy to the world daily.

Peter Harris: I am profoundly indebted to my bride, Kimberly, for her companionship, listening ear, and persistent parenting during late nights and long days. Because of your support and encouragement, this dream could come true. Oscar, Anders, and Sophie, thank you for your presence when I was home and your patience during time away; it brings me joy to share this time in California with you. I honor John and Beverly Harris, who over 30 years ago inspired me to go to the nations. Thank you, God, for strength, wisdom, and family: including the men from Wednesdays who were there for

me and my family while here, and overseas; and including community in Monterey and Pacific Grove.

I. INTRODUCTION

A. RAPID TECHNOLOGY DEVELOPMENT

The Department of Defense (DOD) has accepted the understanding that competition short of armed conflict with major power adversaries requires rapidly innovating, securing, and integrating our information systems. Yet, despite a significant focus on information operations and data collection in contested areas or the operational edge, not enough has been accomplished. The slow pace of re-posturing our approach to address major power adversaries can be seen clearly in the lack of effective information and data-sharing platforms accessible to U.S. partner forces. This capstone seeks to address the question of how the U.S. Special Operations Command (USSOCOM), specifically Army Special Operations Forces (ARSOF), can close the technology gap with our partners to retain information advantage in the competition space. The research team theorized that including partner force units in the early assessment and iteration of information and data-sharing platforms could increase the long-term viability of such platforms and increase partner force adoption potential to set conditions for securing information advantage. The research team assessed this theory through field assessments of two information-sharing platforms with the partner nation of the Philippines and surveys of the users from that fieldwork. Additional U.S.-based fieldwork was done with U.S. military personnel, and foreign nation military officers represented 25 nations assigned to the Naval Postgraduate School. The two platforms assessed are emerging information and data-sharing platforms in limited use or testing phases with various DOD entities. The field demonstrations and assessments of these platforms tested both the theory of partner forces' inclusion early in the iterative process and also assessed the viability of the actual platforms for long-term adoption. This capstone provides the background that necessitated this research, the methodology of development and implementation of the research approach, and the outcomes of the field demonstrations and assessments of the two platforms. The result of this research offers a potential method for the practical evaluation and long-term integration of data and information-sharing systems that meet the requirements of competition short of armed conflict with major power adversaries and support activities in large-scale combat operations. This paper applies takeaways from the research to a conceptualized application of these information-sharing platforms in Taiwan as a tool to enhance Mil-Mil and Civ-Mil capabilities. The initial output of this capstone project indicates that a U.S. ally or partner forces-centric approach would improve the iterative process of platforms. It shows a greater likelihood of long-term adoption by the U.S. and non-U.S. entities.

B. FRAMING THE PROBLEM, THE GAP

Over the last 20 years, U.S. Army Special Operations Forces' value proposition has become overly reliant on training and equipping our partners based on measures of lethality. The U.S. SOF community has succumbed to the fallacy that lethality equates to dominance. Lethality is not enough in strategic competition and grey zone activities. Information is the true weapon within competition. This change in the nature of the challenges facing the U.S. requires the Army Special Operations community to revise the value proposition on the ability to engage a partner's ability to gather, control, and share information. Building partnerships create the access point to information. With over 140 teams in 80 nations at any given time, the ARSOF enterprise is built on the relationships forged with America's foreign partners. Building partnerships is the access point for information. These relationships provide the foundation to modernize the ARSOF indigenous approach through developing the digital tools needed to compete in the information age and retain the information advantage. This research addressed the need for more information and data sharing technology field testing with partner forces, the lack of performance data of these types of platforms in the desired use locations, and the gap between *de jure* U.S. Government requirements and *de facto* delivery of technology.

The rapid development of information technologies reinforced the necessity to understand how to best share data streams and information with allies and partners. Many current DOD and commercial efforts focus on developing semi-autonomous and autonomous sensors at the operational edge where secure data-sharing capabilities are limited. These efforts seek to address the issues of data collection and information sharing at the edge where digital tools and communication devices are inhibited. The need remains to undertake a dedicated assessment of how USSOCOM can close the information-sharing technology gap with its key allies and partners to retain the information advantage within the competition space. Information and data-sharing platforms enable users to transmit near real-time information between multiple users, organizations, or devices. While common unsecured commercial forms of such technology, such as simple message service (SMS) and applications such as WhatsApp, Telegram, and Signal, are in everyday use around the globe, secure means of digital communication with built-in graphical overlays or a common operation picture (COP), translation capabilities, and interoperability with existing DOD platforms have not been widely adopted. Limited cases of secure messaging, such as Wikr or closed network information-sharing platforms, cannot fully meet the operational needs of the SOF community when seeking to work digitally with partners.

The relationships U.S. SOF teams forge with their partners are increasingly challenging to maintain and are even jeopardized due to limited options for secure information and data-sharing platforms. The current Remote Advise and Assist Suite is limited to tactical applications and cannot provide a global information-sharing network. Platforms such as secure TAK often require specialized devices that are cost-prohibitive to Partner Forces and are often easily identifiable by their digital signatures. Moreover, because of the technology gap between ARSOF and their partner forces, host nation militaries commonly use commercial options to communicate with ARSOF teams. These unofficial workaround systems are insufficient in that they limit the ability to share information critical to operations in terms of security and capability. Additionally, these systems place both the teams and the partners at risk. Malign actors have infiltrated and operationalized networks and systems where these ostensibly secure workarounds exist.

Early analysis of previous security force development initiatives has indicated that the often-used U.S. military-centric approaches to technology and equipment development undermine long-term adoption by non-U.S. users. The project covered in this paper provides an in-country assessment of two information-sharing platforms, a review of previous case studies, and a conceptualization vignette of U.S.-provided equipment and tools to foreign allies and partners to enhance deterrence postures. The assessment of two digital information-sharing platforms in the Philippines with the Philippine Army will be compared with previous research of cases from Iraq and Afghanistan in which the U.S. military sought to enhance the capabilities of partners by providing platforms and equipment. These evaluations will demonstrate that the assessment of any equipment, particularly digital information-sharing platforms, must be grounded in the partners' long-term operational and strategic needs to differentiate it from previous information-sharing platform assessments such as Palantir Lapis and the Remote Advise and Assist initiative. On the other end of the spectrum, this paper will highlight the Remote Advise and Assist program as an example of a partner forces-centric technology development that was successfully adopted due to the inclusion of a U.S. partner early in the iterative process.

C. SOLUTION DEVELOPMENT

This capstone project, which the research team titled "Project ISHARE," developed a methodology to assess and evaluate emerging information-sharing platforms and assess and incorporate the requirements and needs of allies and partners into this process. In the process of evaluating the viability of using allies' and partners' input on the development of information-sharing platforms, Project ISHARE simultaneously collected data on the viability of two emerging platforms: the Field Information Support Tool (FIST), developed by Kestrel Technologies and the Civil Knowledge Integration-Tactical Assault Kit (CKI-TAK) plugin by Raytheon BBN. Through the development and implementation of a methodology to assess information-sharing platforms in the Philippines with allies and partners, these two platforms were assessed for long-term adoption viability and to inform further iterations of secure data and information sharing between U.S. DOD entities and foreign partners. This methodology was tested in the Philippines when the two platforms, CKI-TAK and FIST, were provided to a limited number of Philippine Army Personnel for assessment. These personnel were surveyed both before and after their five-day usage of the platforms to gain allied forces' perspective on the long-term viability of each platform and to assess if these platforms meet the needs of the Philippine Army.

The 2022 United States National Security Strategy states the U.S. is “in the midst of a strategic competition to shape the future of the international order.”[1] Traditional military activities in the form of large movements of armored columns or the employment of carrier-based strike aircraft will not dominate this competition. Instead, the nature of this competition will be, and currently is, one of social, political, and economic influence. As noted by Daniels and Honn in their 2021 article entitled “To Keep Pace with Rivals, Analyze the Competition Space,” “hybrid threats and grey-zone tactics by malign actors are an increasingly serious threat to U.S. efforts to establish influence in strategic countries.”[2] In this new era of competition, the rapid fielding and adoption of technologies will dominate the character of war.[3] Recent literature such as *Kill Chain*, *Like War*, and *War Made New*, highlights this shift.[4] The competition space, or grey zone, predominantly influences spaces where kinetic military tactics are not applicable. These are the areas the U.S. military will need to revert back to working in. Much like the days of the Cold War, the relationships and the information garnered from those relationships will be the main objectives of military personnel, particularly within the U.S. Army Special Operations community.

[1] Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: White House, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[2] Tommy Daniels and Aaron Honn, “To Keep Pace with Rivals, Analyze the Competition Space,” *War Room* (blog), October 20, 2022, https://warroom.armywarcollege.edu/articles/competition-space/.

[3] Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hachette Books, 2020); Justin Lynch, “Yet Another Article about Information Technology and the Character of War,” War on the Rocks, September 2, 2020, https://warontherocks.com/2020/09/yet-another-article-about-information-technology-and-the-character-of-war/; Christopher Zember and Peter Khooshabeh, “Defense Innovation Is Falling Short,” War on the Rocks, December 15, 2021, https://warontherocks.com/2020/09/defense-innovation-is-falling-short/; Brad D. Williams, “To Transform Tech, DOD Must Stop Being An ‘Innovation Tourist:’ Report,” *Breaking Defense* (blog), July 29, 2021, https://breakingdefense.sites.breakingmedia.com/2021/07/to-transform-tech-dod-should-stop-being-an-innovation-tourist-report/.

[4] Brose, *The Kill Chain*; Max Boot, *War Made New: Weapons, Warriors, and the Making of the Modern World* (New York: Gotham Books, 2007); P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018).

D. RESEARCH INTENT—PRIORITIZING NEEDS OF ALLIES AND PARTNERS

It is critical to aggressively evaluate and assess emerging and evolving digital and information-sharing to close the technology gap between U.S. SOF and their partners. Project ISHARE undertook the assessment of current and emerging digital tools that seek to create and enhance U.S. allies and partners' capabilities to visualize and understand their physical and cyber environments. The project's outputs captured in this paper will inform future requirements by assessing two current platforms' abilities to provide visual COPs with data aggregation capabilities and live text and reporting functions. The assessments evaluated each platform's ability to enable partner forces and U.S. teams to collaborate worldwide. In theory, a suite of digital tools, compiled from existing technologies and tethered to U.S. SOF, could provide 24/7 connectivity on a secured network for communication between ARSOF teams and partner forces from around the corner or over the horizon. The initiative sought to determine how best to leverage digital tools to maintain the personal relationships ARSOF teams build while deployed and address the technology needs of our foreign partners. Additionally, the project sought to assess the value of including the partner forces early on in the iterative process of development to ensure long-term adoption by the allied or partner force or entity.

II. LITERATURE REVIEW

A. INFORMATION SHARING AS A CORNERSTONE OF NATIONAL SECURITY

From autonomous systems to rapidly updatable software, today's armies will see their success or failure determined by the rate of updates to their technology.[5] The U.S. Interim National Security Strategic (NSS) Guidance released in March 2021 speaks to the shift away from a purely kinetic environment predicated on the ability to impose a nation's will through the use of military hardware. The 2021 Interim NSS declares the United States must "better compete and deter gray zone actions."[6] The 2022 NSS goes further, stating, "by modernizing our military, pursuing advanced technologies…, we will have strengthened deterrence in an era of increasing geopolitical confrontation, and positioned America to defend our homeland, our allies, partners, and interests overseas, and our values across the globe."[7] Activities in the grey zone fall short of violence and often employ dual-use technology to advance strategic interests and military objectives. Many defense analysts and scholars have noted the rapid cyber and data ingestion technology research and development progress that near-peer adversaries such as the Peoples' Republic of China (PRC) and the Russian Federation (RF) have made over the last decade by focusing their military modernizations on adopting and merging cyber and communications technologies.[8] These adversaries have rapidly caught up and even surpassed the U.S. in part by developing technologies that have both military and commercial applications.[9]

[5] Lynch, "Yet Another Article about Information Technology."

[6] Joseph R. Biden Jr., *Interim National Security Strategic Guidance* (Washington, DC: White House, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[7] Biden Jr., *National Security Strategy*.

[8] Brose, *The Kill Chain*; David Sacks, "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do to Respond," *Net Politics* (blog), August 8, 2021, https://www.cfr.org/blog/china-huawei-5g; Zember and Khooshabeh, "Defense Innovation Is Falling Short"; Jared Serbu, "DOD's New R&D Chief Prioritizes Moving Prototypes to Real-World Applications," Federal News Network, October 25, 2021, https://federalnewsnetwork.com/on-dod/2021/10/dods-new-rd-chief-prioritizes-moving-prototypes-to-real-world-applications/; James Andrew Lewis, *National Security and the Innovation Ecosystem* (Washington, DC: Center for Strategic & International Studies, 2021), https://www.csis.org/analysis/national-security-and-innovation-ecosystem.

[9] Brose, *The Kill Chain*.

Thus, the U.S. defense community is in agreement that we are in a new era of strategic competition.[10]

As noted previously in this paper, the DOD has accepted the understanding that competition short of armed conflict requires rapidly innovating, securing, and integrating our information and data-sharing platforms. Yet, with all the focus on information operations and data collection at the edge, much remains to be accomplished in certain aspects. While examples such as the establishment of Cyber Command and the funding the Information Warfare Center within the 1st Special Warfare Command are examples of the shifting focus to information-driven operations, these commands require additional tools and resources necessary to achieve their stated missions. Furthermore, while information and data increasingly become a focus of the DOD beyond the intelligence community, the fact remains that little is being done to implement a coherent method to empower our key allies and partners with information and data sharing. While the problem has been identified, service components and congressional leaders continue to debate the proper means to undertake these efforts, exacerbating already unresponsive, bureaucratic acquisition processes.

As the U.S. reallocates forces and reassesses strategic objectives based on strategic competition with major powers, its ability to share and work within common information-sharing platforms with allies and partners is increasingly essential. This need is highlighted by the Federated Mission Networking within NATO's Connected Forces Initiative as

[10] Biden Jr., *Interim National Security Strategic Guidance*; National Intelligence Counsel, *Global Trends 2040: A More Contested World* (Washington, DC: Office of the Director of National Intelligence, 2021), https://www.dni.gov/index.php/gt2040-home; Alan Tidwell, "Being a Better Partner in the Pacific," War on the Rocks, January 28, 2022, https://warontherocks.com/2022/01/being-a-better-partner-in-the-pacific/; Katie Crombe, Steve Ferenzi, and Robert Jones, "Integrating Deterrence across the Gray—Making It More than Words," *Military Times*, December 9, 2021, sec. Commentary, https://www.militarytimes.com/opinion/commentary/2021/12/08/integrating-deterrence-across-the-gray-making-it-more-than-words/; Joe Cheravitch, "Cyber Threats from the U.S. and Russia Are Now Focusing on Civilian Infrastructure," *The RAND Blog* (blog), July 23, 2019, https://www.rand.org/blog/2019/07/cyber-threats-from-the-us-and-russia-are-now-focusing.html; Blake Moore and Jan E. Tighe, "Insecure Communications Like WhatsApp Are Putting U.S. National Security at Risk," Nextgov, December 8, 2020, https://www.nextgov.com/ideas/2020/12/insecure-communications-whatsapp-are-putting-us-national-security-risk/170577/.

described by Kyle Sullivan in the December 2021 volume of Cyber Defense Review.[11] As Sullivan lays out, the integrated communication and information platforms required for NATO to achieve its mission of collective defense have driven development of platforms unlike those the U.S. uses with other allies and partners. Unlike our Five Eyes Alliance (FVEY) allies and NATO allies, many key U.S. partners have not adopted and implemented robust secure communications platforms. Currently, many U.S. partner-force militaries use unsecured workarounds to communicate with American units or rely on in-person communication with little ability to maintain continuity. This is true of the authors' and their peers' experiences from the jungles of the Philippines to the mountains of Guatemala or the deserts of Iraq and valleys of Afghanistan. U.S. Special Operations forces are regularly forced to use platforms such as WhatsApp, Facebook, or others due to the limitations of their partner forces.[12]

As highlighted by the DOD, updates to information platform usage policy outlined in DODI 8170.01, these activities pose clear and present risks to force.[13] Across the DOD, efforts to develop information-sharing platforms have been ongoing for years. However, these platforms have failed to gain widespread adoption for use with allies and partner forces. Thus, this gap remains a critical weakness in U.S. SOF's efforts to extend trust, strengthen partnerships, and improve technical interoperability.

B. TECHNOLOGY USES

The technology required to enable secured communication and common operating picture (COP) sharing with partners exists. Examples include the provision of the Lapis-Palantir System by the U.S. Indo-Pacific Command (USINDOPACOM) to the Armed

[11] Kyle Sullivan, "Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure," *Cyber Defense Review* 6, no. 3 (Summer 2021): 109–18, https://www.jstor.org/stable/48631158.

[12] Blake Moore and Jan E. Tighe, "Insecure Communications Like WhatsApp Are Putting U.S. National Security at Risk," Nextgov.com, accessed January 31, 2022, https://www.nextgov.com/ideas/2020/12/insecure-communications-whatsapp-are-putting-us-national-security-risk/170577/; Sullivan, "Risks to the Mission Partner Environment."

[13] Department of Defense, *Online Information Management and Electronic Messaging*, DoDI 8170.01 (Washington, DC: Department of Defense, 2021), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf.

Forces of the Philippines (AFP), common operation picture platforms provided by U.S. SOF to Afghan partners, and MAGE in Latin America or the integrated systems used by NATO or ROK allies.[14] Yet none of these examples has been adopted or implemented for widespread use. Nevertheless, these efforts do provide a wide range of lessons learned and technological insight into the type of platform needed and the drivers that influence its adoption by both U.S. and Allied or Partner forces.

The time-sensitive nature of Direct-Action missions that dominated the Global War on Terror era placed a premium on quick information sharing that at times came at the expense of not using secure platforms to transmit that data. As a result, the use of non-DOD messaging platforms proliferated across U.S. military units, particularly between U.S. military units and their host nation counterparts. The use of WhatsApp in Afghanistan is a critical example of this. The vulnerability brought about as a result of these platforms use led to the publication of DOD Instruction (DODI) 8170.01—Online Information Management and Electronic Messaging, Section 3.24 of which states: "Do not use non-DOD-controlled electronic messaging services to process nonpublic DOD information, regardless of the service's perceived appearance of security (e.g., "private" Instagram accounts, "protected" tweets, "private" Facebook groups, "encrypted" WhatsApp messages)."[15] The DOD's policy placed clear restrictions on the use of non-DOD platforms and clearly addressed the issues' impact, but did not provide or set in motion the establishment of solutions needed to curtail such usage. The DODI fails to mandate the analysis required for the broad and long-term establishment of a network and tool to

[14] Lead Inspector General, *Operation PACIFIC EAGLE-PHILIPPINES: Lead Inspector General Report to the U.S. Congress* (Washington, DC: Lead Inspector General, 2022), https://oig.usaid.gov/sites/default/files/2020-11/OPE-P_Philippines%20Lead%20Inspector%20General%20Report%20to%20the%20Congress%20of%20the%20United%20States%2C%20July%201%2C%202020%20-%20September%2030%2C%202020_Q4_Sep2020.pdf; Business Wire, "Palantir Awarded $111m Contract to Provide Mission Command Platform for the United States Special Operations Command," Business Wire, May 28, 2021, https://www.businesswire.com/news/home/20210528005069/en/Palantir-Awarded-111m-Contract-to-Provide-Mission-Command-Platform-for-the-United-States-Special-Operations-Command; Brian Hamel, "Using MAGE to Facilitate Mission Command in USSOUTHCOM's Response to Hurricane Eta," *Eumonia Journal*, September 23, 2021, https://www.civilaffairsassoc.org/post/using-mage-to-facilitate-mission-command-in-ussouthcom-s-response-to-hurricane-eta; Sullivan, "Risks to the Mission Partner Environment."

[15] Department of Defense, *Online Information Management and Electronic Messaging*.

connect the partner forces' digital and physical personas. The United States has the most extensive network of uniformed military personnel supporting Allies and Partners yet lacks a unified digital information-sharing platform for partner's use and integration. This official move away from non-DOD platforms creates an urgent need to fill that capability with the secure communication platform that is needed for the new era of competition. The official stance against the use of non-DOD platforms to share data and information highlights the extent to which U.S. personnel and their partners have become reliant on commercial, non-secure platforms.

Various past approaches have led to localized implementation of communication tools between partner forces and U.S. forces. In South Korea, the United States enjoys a rather robust information sharing platform that has enjoyed continuous upgrades and refinement as the nature of information and data collection has evolved. The platform and systems used across NATO and with FVEY Nations again demonstrates capability to achieve the necessary levels of data sharing and aggregation. These iterations have made significant progress toward solutions but have been stopped short of their full capability or wider, long-term adoption.[16] Extensive government programs and private research have produced some of these concepts and outline the challenges of partner nation adoption, choosing the right applications, and short-term contracts that limit continuity.

Research on specific geographic-centric applications demonstrates the complex nature of this understanding and evaluates the drivers of information platform adoption. There is a lack of scholarly research on these tools due to the sensitive nature of discussing military capability gaps, government capabilities, and the competitive nature of government technology development. These realities stifle the free flow of information and platform development. Startups, think-tanks, and long-term government affiliates often hold out information on what technology is available and rarely disclose their methods, making empirical investigation exceedingly challenging. During the research teams'

[16] Hamel, Brian. Eunomia Journal, "Using MAGE to Facilitate Mission Command in USSOUTHCOM's Response to Hurricane Eta"; Lead Inspector General Report to The United States Congress, "Operation Pacific Eagle–Philippines Lead Inspector General Report to The United States Congress"; Kevin Call and Kevin Moody, personal communication-phone call, January 31, 2022.

previous experiences in USINDOPACOM, U.S. Southern Command (USSOUTHCOM), and U.S. European Command (USEUCOM) areas of responsibility, the lack of means to collaborate long-term with partners on this type of digital platform fueled a desire to understand the proximate cause of technology adoption and to design alternative pathways to build trust with foreign partners and prepare them to operate with the United States in strategic and competitive environments.

The need to provide and assist with technology development in Allied and Partner nations is not new. Studies have developed a framework for determining what technology is needed for working within austere environments. Baney et al. studied the limitations of communicating with partners in a scenario to counter weapons of mass-destruction (CWMD) and developed a joint communications platform to allow special operations teams to quickly depict data and information visually to transmit it to higher headquarters for timely decision-making.[17] Their study advanced previous research on the Tactical Assault Kit (TAK) by Schupp, Wetteland, and Ferriter in 2017, which developed a digital tool to facilitate communications between the SOF teams and their higher headquarters.[18] Both of these technologies advanced the ability of teams to communicate with the headquarters and enhance combined understanding of the environment but for various reasons, these lacked international military adoption.

Most recently, Thielenhouse and Roles developed the Remote Advise and Assist (RAA) system to address an operational limitation in Iraq.[19] The system enabled decentralized execution of missions. The digital tool kit they developed allowed SOF to communicate with and affect partner nation forces within austere environments. The RAA system provided imagery and spatial depiction software to enable targeting. While RAA provided a significant step forward technologically to connect the digital and physical

[17] Daniel W. Bandy et al., "Joint Operations Center Tactical Assault Kit (JOCTAK): Evolution Toward Scalable Multilateral SOF C4I" (master's thesis, Naval Postgraduate School, n.d.), http://hdl.handle.net/10945/61230.

[18] Phil Schupp, Sverre Wetteland, and Paddy Ferriter, "ADAPT: Tactical Assault Kit: Collaborative Mission Planner" (Monterey, CA: Naval Postgraduate School, November 2017), http://hdl.handle.net/10945/56573.

[19] Christopher Thielenhaus and Eric Roles, "Virtual Accompany Kits Return to Baghdad: A View from the Front Lines," *Special Warfare* 30, no. 2 (June 2017): 26–29, http://hdl.handle.net/10945/55178.

persona securely in contested environments, it remained limited in capabilities compared to what its technology developers envisioned. The applicability of this research is limited, however, since it focused on one geographic area and did not facilitate acceptance across multiple continents and geographic combatant commands (GCC). In addition, this research did not expand on the use of messaging and digital common operating pictures that facilitates non-lethal targeting with depiction and analysis of the cyber environment, like that used by the Islamic State during the launch of RAA. However, RAA was adopted across U.S. SOF broadly accepted as a "program of record" and fielded across multiple SOF and Security Force Assistance Brigade (SFAB) units.[20] Initial conversations with current units employing the system highlighted that the system, while advanced, is limited in its ability to provide communications beyond the tactical level and to facilitate the sharing or large amounts of data and information.[21]

Kim et al. thoroughly reviewed the Wickr App, which was originally designed by the CIA to address communications vulnerabilities and enhance encryption. While the app provides increased levels of security for textual information and image sharing, it does not have the ability to provide a "live" interactive vocalization tool for situational awareness and operational coordination.[22] Will Loschiavo discusses the All-Partner Access Network (APAN) with Telligent, which allows collaboration and communication across multiple continents and with U.S. international partners.[23] APAN also contains features for instant messaging, data aggregation, and different forums for posting information within a secured data framework. As part of controls, APAN has a controlled access list, a feature that would enable greater sharing with partner nations without the risk that comes with equal access

[20] Irregular Warfare Technical Support Directorate, "Full Spectrum—Remote Advise and Assist—Virtual Accompany Kit," Irregular Warfare Technical Support Directorate, February 1, 2022, https://www.tswg.gov/Projects/I2C/Remote_Advise_Assist.html.

[21] Kevin Call and Kevin Moody, personal communication-phone call, January 31, 2022.

[22] Giyoon Kim et al., "Forensic Analysis of Instant Messaging Apps: Decrypting Wickr and Private Text Messaging Data," *Forensic Science International: Digital Investigation* 37 (June 2021): 1–11, https://doi.org/10.1016/j.fsidi.2021.301138.

[23] iNewswire, "Trace Systems Awarded All Partners Access Network Support Task Order by the Defense Information Systems Agency in Support of the United States Air Force," Digital Journal, January 24, 2022, https://www.digitaljournal.com/pr/trace-systems-awarded-all-partners-access-network-support-task-order-by-the-defense-information-systems-agency-in-support-of-the-united-states-air-force.

for all users.[24] While these features are designed to address partner needs, APAN lacks necessary features for human terrain analysis, complex mapping algorithms, geolocation, and other features essential for partner nation use and adoption.

Recent innovation approaches have demonstrated the value of incorporating partner forces early on in the development phase of defense technologies. The success of the Remote Advise and Assist systems is due to its development in the country with the partner forces designated to be the initial user. As noted by the project co-lead, Eric Roles, the ability to iterate and modify early on based on partner force end-users' inputs enabled rapid and responsive development of the RAA platform.[25] However, while RAVVAC has become a program of record, the methodology to tailor it to a partner force was not replicated. Such international force inclusion in development phases has also been showcased in recent projects at the Naval Postgraduate School. Dr. Leo Blanken and Ms. Kristen Tsolis emphasized the possibilities of enabling U.S. partners to shape the technology solutions needed for their specific challenges.[26] Foreign military students have leveraged their access to U.S. research facilities and military partners to address unique technical problem sets within their home units. The development of low-cost drones free of potentially malign third-party malware is just one example.[27] The incorporation of partner forces early on in the next evolution of secure information-sharing digital tools is perhaps the surest route to enable sustainable, long-term, multi-component adoption.

C. PARTNER NATION TECHNOLOGY ADOPTION

The Unites States' long history of supplying Allies and Partners with military hardware and capabilities provides a blueprint for digital system adoption as well as identified drawbacks from the shortsightedness of foreign-military funded hardware. In the

[24] iNewswire.

[25] Thielenhaus and Roles, "Virtual Accompany Kits Return to Baghdad."

[26] Leo Blanken, Romulo G. Dimayuga II, and Kristen Tsolis, "Making Friends in Maker-Spaces: From Grassroots Innovation to Great-Power Competition," War on the Rocks, January 12, 2021, https://warontherocks.com/2021/01/making-friends-in-maker-spaces-from-grassroots-innovation-to-great-power-competition/.

[27] Blanken, Dimayuga II, and Tsolis.

last 20 years alone, the United States has spent billions to equip the Iraqi and Afghan Armies with weapons, vehicles, aircraft, and physical hardware of all sorts. These efforts and the funding behind them have been largely unsuccessful due to the fundamental differences in the military cultures of the United States and these partial partners. Additionally, the long-term maintenance and servicing of much of this hardware was reliant on an unsustainable U.S. defense contractor-driven solution. These examples demonstrate that first, physical hardware is rarely a cost-effective method to enhancing a partner force's capabilities, and secondly, costly weapons and vehicle platforms do not provide a return on investment due to the partner nation units often being limited in the ability to fund maintenance and upkeep. These facts provided support for the focus on Foreign Military Funding (FMF) to shift to digital platforms and systems for data collection, aggregation, and sharing. These platforms are comparatively inexpensive in comparison to physical weapons systems, vehicle platforms, and aircraft. Moreover, the ability to remotely update, manage, and augment digital platforms can make it more feasible for the U.S. to foster relationships with Partners and Allies.

Matt Cancian observed and documented many pitfalls of transferring and equipping partner nation forces without analysis and sans sustainability determinations.[28] Cancian emphasized the economic factors of supplying foreign partners, such as the benefits to American defense contractors and the defense industry. He also noted the challenge of maintaining systems and the requirement to train and enable partners to take ownership. While these are important factors, Cancian failed to document the partner nation's decision-making regarding the impacts and long-term requirements they would need to shoulder before accepting foreign aid. Some of the strengths in his analysis outline the short-sighted approaches that are often at the foundation of operations involving working with partner nations. These operations, by their nature, inhibit long-term collaboration without sharing cooperative platforms. However, Cancian's focus on hardware and weapons systems demonstrates, perhaps unintentionally, the very need to provide tailorable

[28] Matthew Cancian, "Stop Undermining Partners with 'Gifts,'" War on the Rocks, December 13, 2021, https://warontherocks.com/2021/12/stop-undermining-partners-with-gifts/.

and updatable information systems to partners.[29] Documentation from Cancian's literature lacked a complete assessment from the Iraqi military regarding the systematic use of the equipment provided, the tactics and procedures of use, and cultural aspects of adopting new equipment. Thus, scholars have offered little to no input regarding U.S. equipment specifically designed for use by Allied and Partner forces in support of foreign internal defense (FID), unconventional warfare (UW), and similar defense mission sets. The lesson learned from the provision of billions of dollars of weapons platforms, vehicles, and aircraft must be applied in the digital platform space. Moreover, the failed adoption of these defense hardware platforms further supports the needed investment and implementation of digital tools as a cornerstone of how the United States can best improve its Allies and Partners' capabilities as well as foster its international relationships.

D. THE RESEARCH PROJECT ISHARE

The challenge for the design and adoption of technologies that bridge the technology gap between partner forces and the United States remains complex. No current technology fully integrates partner force practices, the use of digital common operating pictures (COP), and integrated translation of messaging with other needed tools. Such a suite of digital tools is needed to bridge the technological divide between foreign militaries and U.S. SOF. Past studies, literature, and technology initiatives addressed other aspects of employment but lacked long-term adoption by host nations based on assessments of those nations' strategic and operational needs. The need remains to undertake a dedicated assessment on how USSOCOM can close the information-sharing technology gap with its key Allies and Partners to retain the information advantage within the competition space. Moreover, this assessment must be grounded in the operational and strategic needs of the partners to differentiate it from previous information-sharing platform assessments.

Our research assessed limitations to communications platforms with partners and factors of adoption to enable information sharing between foreign and U.S. forces. The capstone project results determine the current technologies and methods of both U.S. SOF

[29] Cancian.

and partner-force communications internally and with each other. The research also identified alternative technologies and methods that are available for the two platforms of interest. Furthermore, this approach will draw out the factors that motivate partner-force adoption of these technologies, rather than a myopic focus on benefits to U.S. acquisitions.

To achieve greater understanding, our study has mapped the current ecosystem of collaborative platforms and digital common operating picture (COP) tools available to U.S. and partner forces. The research identified previous attempts to develop these capabilities–the successes and failures. Furthermore, the research analyzed historical cases across INDOPACOM, SOUTHCOM, EUCOM, and AFRICOM. Surveys and interviews with foreign forces and U.S. SOF teams helped the researchers determine the extent of partner-force communication gaps. The effort coordinated with 1st Special Forces Command (1SFC) and Theater Special Operations Commands (TSOCs) to address battlefield requirements. The research will identify demo-based capabilities, then determine options for necessary plugins. The research coordinated with Security Force Assistance Brigades (SFABs) for future integration. The final piece of research scoped acquisition processes for battlefield use. It did so by identifying costs, determining pathways to long-term adoption, and integrating with ongoing SOF Cloud Architecture Projects. This research answered thesis question using three methods. The research included a field test in the Philippines with the Philippine Army. This field test analyzed the use of features on different platforms and compared the frequencies of usage to identify the trends in order to determine the proper tools most suitable for adoption by a partner forces. The research highlighted additional surveys from partner nation representatives representing over 25 nations and 28 U.S. military users.

E. IDENTIFICATION OF PLATFORMS

First, the study identified available platforms, requested endorsement and requirements from supported commands, identified Naval Postgraduate School students and subject-matter experts (SMEs) to gain insight on uses for communication technologies, established Limited Purpose Cooperative Research and Development Agreements (LP-CRADA), and identified funding to support the effort. The first part of the research identified two different available platforms to compare the characteristics of each other. The CKI-TAK and FIST applications were examined for various qualities based on interface language, mapping, use on and offline, and objective criteria (see Annex 5).

F. COMMAND SUPPORT

The study centered on the operational information sharing platform needs of USSOCOM units. The researchers documented organizational and financial support to the project by both operational and tactical units. Accordingly, researcher team solicited these units for current standing requirements to be wholly or partially fulfilled through the capstone research. The units, including the 8th Psychological Operations Group (POG) Information Warfare Center, the 95th Civil Affairs Brigade, the 1st Special Forces Command (SFC), the U.S. Army Special Operations Command, and the Security Force Assistance Command (SFAC), provided various levels of documentation to demonstrate urgency, interest, and operational need for this research. Due to the public nature of academic research, some of the memorandums that reflect current and future requirements remain protected within classified platforms to meet DOD information security requirements and protect national security. These documents and communications will not be highlighted or referenced in this report.

G. SUBJECT-MATTER EXPERT INTERVIEWS

The research team conducted interviews and surveys one-on-one with international military members to address the perspective of allies and partner nation forces. The questions addressed procedural and organizational use of technology among partner nation units. Interviews and surveys provided information about partner forces' communication platform use, facts about technology access, procedures, usability, and gaps in current tools from an organizational viewpoint. The data from the interviews and surveys provide insight into the current practices of U.S. partners, their procedures, and gaps in current technology from an organizational perspective. The data sets from surveys were aggregated to assess the current requirements of partners, their organizational practices, and identified what features could make long-term adoption of these technologies more feasible, suitable, and acceptable.

H. NPS DEFENSE ANALYSIS STUDENT SURVEYS

The research required a series of survey questions to clarify the facts surrounding communications systems and procedures of partner nation forces with each other and with U.S. forces. The questions revealed clear information regarding the various procedures of U.S. SOF and conventional forces who have deployed with or worked with partner nation forces. See Annex 1 for survey questions by the group.

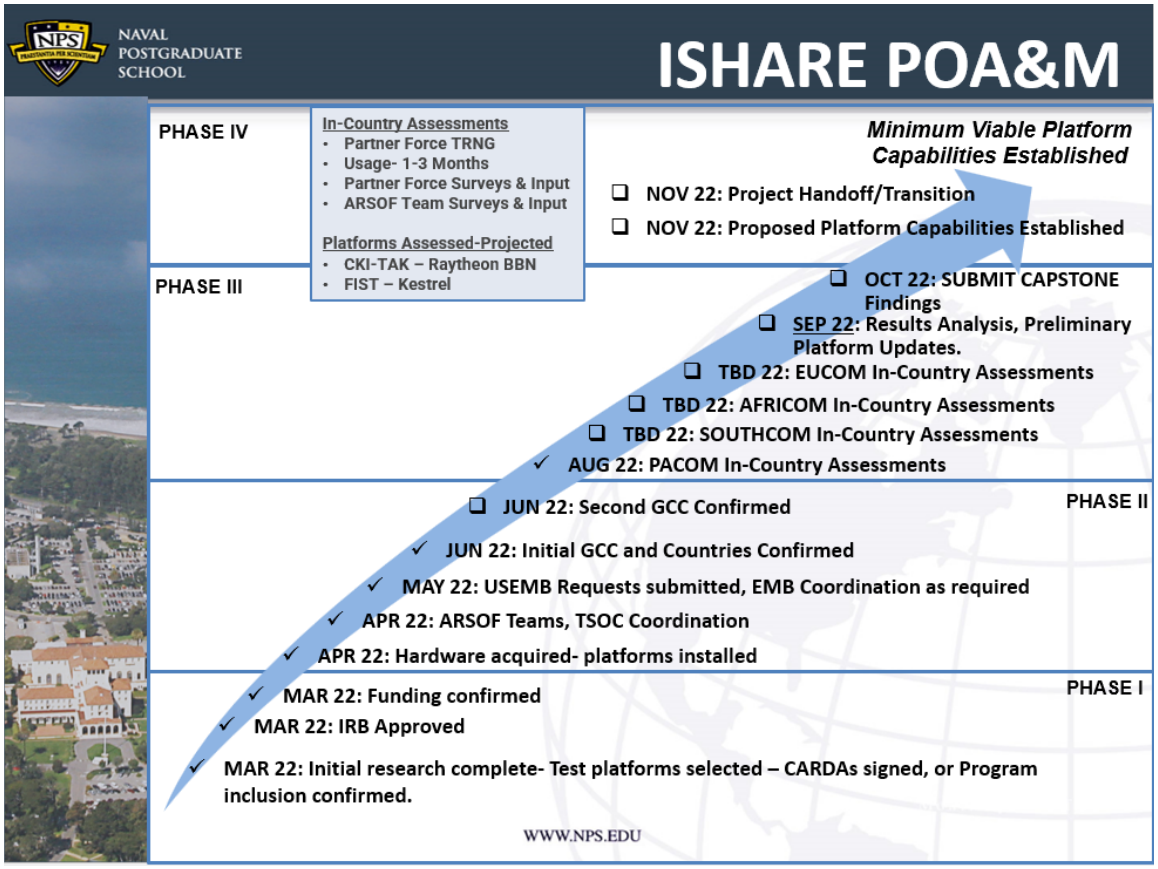
Thus, with requirements identified, hardware and software obtained through industry partners, and subject-matter experts (SMEs) selected, the research transitioned to testing within a specific geographic combatant command, USINDOPACOM. The procedures for using technologies and discussions have uniformity to decrease bias between applications. Criteria for the systems' features and use were documented to measure platform performance against similar platforms. Findings were shared with the industry partners as described in each LP-CRADA.

I. TRAVEL FOR RESEARCH

The research team acquired funding support from the 1st SFC and the NPS Defense Analysis Department. For the field research portion, researchers coordinated with the U.S. military staff of the U.S. Embassy Philippines for entry to theater for demonstration and assessment. Initial field research included US-based demonstrations, assessments, and surveys by Allied and Partner national military officers and U.S. military personnel currently enrolled at the U.S. Naval Postgraduate School and travel to the Philippines. SME interviews and demonstration training were completed in person with partner forces. Most of the application demonstration was completed in-person, with researchers in proximity to partner forces.

J. PROJECT PLAN OF ACTION AND MILESTONES APPROACH

The NPS research team developed an ambition Plan of Action and Milestones (POA&M) to take Proj. ISHARE's theoretical examination of secure information- sharing platforms of into field environments relevant to SOF operational units. Working with staff sections within multiple Theater Special Operations Commands (TSOCs) and U.S. Embassy staff proved to be a critical limiting factor in execution field research in a timeline advantageous the research project's scope. However, to ensure the successful execution of at least one overseas assessment, priority was given to INDOPACOM. This prioritization was due to the parallel conceptualized study of secure information-sharing platforms potential as a deterrence-enhancing mechanism against a potential People's Republic of China Invasion of Taiwan. This will be highlighted in chapter 4 of this paper. The below figure contains an early POA&M for the project proposal for field research timelines. While only one INDOPACOM field assessment was executed by the time of publication of this paper, coordination continues under Proj. ISAHRE for the remaining field assessments.



NAVAL POSTGRADUATE SCHOOL

ISHARE POA&M

PHASE IV

In-Country Assessments
- Partner Force TRNG
- Usage- 1-3 Months
- Partner Force Surveys & Input
- ARSOF Team Surveys & Input

Platforms Assessed-Projected
- CKI-TAK – Raytheon BBN
- FIST – Kestrel

Minimum Viable Platform Capabilities Established

□ NOV 22: Project Handoff/Transition

□ NOV 22: Proposed Platform Capabilities Established

PHASE III

□ OCT 22: SUBMIT CAPSTONE Findings

□ SEP 22: Results Analysis, Preliminary Platform Updates.

□ TBD 22: EUCOM In-Country Assessments

□ TBD 22: AFRICOM In-Country Assessments

□ TBD 22: SOUTHCOM In-Country Assessments

✓ AUG 22: PACOM In-Country Assessments

PHASE II

□ JUN 22: Second GCC Confirmed

✓ JUN 22: Initial GCC and Countries Confirmed

✓ MAY 22: USEMB Requests submitted, EMB Coordination as required

✓ APR 22: ARSOF Teams, TSOC Coordination

✓ APR 22: Hardware acquired- platforms installed

PHASE I

✓ MAR 22: Funding confirmed

✓ MAR 22: IRB Approved

✓ MAR 22: Initial research complete- Test platforms selected – CARDAs signed, or Program inclusion confirmed.

WWW.NPS.EDU

Figure 1. Plan of Action and Milestones as of October 1, 2022

K. DEMONSTRATION TRAINING AND APPLICATION USE PROCEDURES

Researchers conducted a 5-day demonstration and assessment engagement with Philippine partner force participants during the application comparison process. The demonstration and assessment consisted of a video teleconference with the platform developers providing a guided hands-on walkthrough of the platform and live demonstration practice. The demonstration and assessment of each platform was uniform, with the same number of users per group to ensure equality in demonstration and utilization. The metrics of use were aggregated to understand the types of information that partner forces gather, how they use the application, and how often they use it. Further procedures and criteria were developed to give uniformity to the demonstration tools when partner forces are using them.

L. IDENTIFY POTENTIAL EXPANDED APPLICATIONS FOR INFORMATION-SHARING PLATFORMS

Finally, this research highlights the expanded potential value of information-sharing platforms and their utilization with Allies and Partners. The theoretical introduction of CKI-TAK or FIST into the U.S.-Taiwanese dynamic as a practical means for Civ-Mil cooperation during natural or man-made disasters will highlight potential secondary positive implications of such use. The Research reassessed the options for expanding US-Taiwan cooperation in both a mil-mil setting and in a Civ-Mil environment.

III. METHODS

A. DESIGN OVERVIEW

This study was comprised of two phases. In Phase I, the students at the Naval Postgraduate School (n= 29 U.S.; n = 31 foreign) completed pre-use surveys, attended a technology demonstration, used digital platforms to submit reports, and filled out post-use surveys. Phase I served as a pilot test for the field research conducted in the Philippines. Phase II involved the main focus group, and gave researchers a greater understanding of the partner force, Philippine Army soldiers (n = 30). Unique to Phase II, after participants gave consent, they completed an in-person anonymous pre-use questionnaire that assessed familiarity and experience with platforms for information sharing, cyber, civil, and operational analysis practices (refer to Annex 1). Participants then attended a comprehensive technology demonstration in a classroom environment showcased one of two cellphone applications: the Field Information Support Tool (FIST) platform or the Civil Knowledge Integration-Tactical Assault Kit (CKI-TAK) platform. After the demonstration, participants received a practical-use packet with nine scenarios consisting of an explanation and photos of military or Civ-Mil cooperation replicating the situations they may be asked to respond to or report on in an official capacity. The scenarios included natural disasters, civil unrest, maritime incursions, unauthorized activities by a foreign state-owned entity, and infrastructure problems (refer to Annex 4). The scenario packets were designed to prompt participants to submit one report per scenario on either CKI-TAK or FIST. The participants were allotted three hours and instructed to submit reports based on information from the scenario to detail the situation to a command center. Each platform had icons and forms that asked the who, what, when, where, and why for reporting. Additional data fields were available based on the platform and type of report from the user selected. Afterwards, participants completed an in-person anonymous post-use questionnaire that asked whether the platform met established requirements, had an intuitive design, and had the potential for use in the areas or environments their unit commonly operates. Refer to Annex 1, Sections A, B, and C, and D for a complete list of questions.

B. PHASE I: U.S. DEMONSTRATION AND ASSESSMENT

Participants. Phase I included both U.S. and international students at the Naval Postgraduate School (NPS) from the Defense Analysis Department. Two of the 29 U.S. student participants were excluded from the analysis because they did not complete the study. Thirty-one international students also participated, but three were excluded from the analysis because they did not complete the study. All NPS participants were recruited through an e-mail solicitation for voluntary participants. In Phase II, 34 Philippine Army soldiers from six units ranging in experience from private (E-1) to major (O-4) rank voluntarily participated. Four were excluded because they did not complete the study. Philippine participants were selected based on the partnership between a U.S. Civil Affairs Team and the Philippines Army Civil Military Operations Regiment (CMOR).

Phase I Procedure. At the onset of the study, all participants completed questionnaires remotely. Students were given the option of attending one of two technology demonstrations that showcased either the CKI-TAK or FIST application. Participants who chose to complete the study attended a demonstration and received a link for the post-use questionnaire.

During the CKI-TAK application demonstration, eight U.S. students observed a 20-minute overview from the CKI-TAK developers at Raytheon BBN that explained the background for application development, how to navigate the application, and submit reports. Participants then received an Android cellular device for use with the CKI-TAK loaded. Next, participants received a practical use scenario packet, and the research team instructed them to use the prompts from the scenario packet to submit reports into the CKI-TAK application. See Annex 4 for scenarios. Participants then used a QR code to access and submit an online post-use questionnaire.

Participants followed the same procedure for the CKI-TAK application as followed for the FIST application demonstration. Three U.S. participants and three international participants were given a device with the FIST application.[30] After the pre-use survey, demonstration, and report submission segment, participants received a QR code to access and submit an online post-use questionnaire.

C. PHASE II: DEMONSTRATION AND ASSESSMENT IN THE PHILIPPINES

Thirty-four Filipino participants were randomly assigned to two equal groups. They completed one iteration of a two-hour technology demonstration on CKI-TAK and FIST, a report submission segment, and a post-use survey (see Table 1). For quality control, each group was located in a different classroom and unit leadership was not present during the sessions. Demonstrations in the Philippines were designed differently, lasting longer to increase exposure of the application and to permit a clearer demonstration for participants who had less frequent use of English.

Table 1. The Philippines Study Group Phasing

Timeline	CKI-TAK Demonstration Report Submission Post-Use questionnaire	FIST Demonstration Report Submission Post-Use questionnaire
Days 1–2	First Group	Second Group
Days 3–4	Second Group	First Group

During the first iteration, half of the Filipino participants saw the demonstration for CKI-TAK, submitted reports on CKI-TAK, and completed the CKI-TAK post-use questionnaire, then subsequently viewed the demonstration for FIST, submitted reports on FIST, and completed the FIST post-use questionnaire. The second half of Filipino participants completed the same demonstration and assessment as the first, but on alternate days. One group first saw the demonstration for FIST, submitted reports on FIST, and completed the FIST post-use questionnaire. This group then saw the demonstration for

[30] Researchers worked with Raytheon BBN and Kestrel Technology Group, LLC, to ensure that international participants were legally permitted to participate in the exhibition and meet export-control requirements mandated by the U.S. Department of Defense and the U.S. Department of Commerce.

CKI-TAK, submitted reports on CKI-TAK, and completed the CKI-TAK post-use questionnaire. See Table 1 for details. This design allowed participants from the two groups to give stronger feedback concerning the viability of each digital platform, since each control group iterated on each platform. After two days of use, both groups of participants exchanged locations and devices to familiarize, use, and complete a survey to assess the other digital platform. Finally, subject-matter experts were interviewed about the institutional use of digital COPs and nature of platform use in the Philippines. Interview questions are found in Annex 1. Interviews were completed in person in a classroom environment on days one and four, and they lasted 30 minutes each.

D. STRATEGY FOR DIGITAL PLATFORM COMPARISON

The responses from the Philippine participants on the characteristics of FIST and CKI-TAK provide a point of comparison for the study. After using either the FIST or CKI-TAK, study participants were asked how the digital platforms meet the established operational requirements or needs of units in their organization. Survey questions addressed the following subjects: unit operational, intelligence, and targeting requirements; platform connectivity; suitability of platform layout; alternate communication requirements; and platform potential for future use in bilateral training and exercises. With the exception of multiple-choice questions to understand unit practices, each question in the FIST and CKI-TAK post-use questionnaires used a Likert scale to assess response values from 1–5, indicating (1) Never, (2) Rarely, (3) Sometimes, (4) Frequently, or (5) Always. Other responses ranged from (1) Strongly Disagree to (5) Strongly Agree. Survey questions were based on an assessment criteria framework with fifteen categories for technology adoption. More information on these criteria is to be found in Annex 5.

E. DEMONSTRATION AND ASSESSMENT RESULTS

Overall results. The questions were separated into scaled responses and multiple-choice responses from U.S. and international NPS students and Philippine Army participants' responses to understand the facets of technology adoption by partner forces from each perspective. U.S. study participants' responses helped gauge the extent of unsecure information technology use with and by partner force units and validated that partner forces' operational communication relies on open-source platforms. International NPS student responses suggest that U.S. partner nation forces tend to rely on unsecured technologies for sharing information with U.S. partners. Philippine Army responses indicated that current information-sharing platforms require additional testing and development in the geographic areas where partner forces train and deploy, CKI-TAK and FIST still have potential to meet Philippine operational requirements, and could supplant the use of non-secure commercial platforms. The Philippine sample identified a heavy reliance on commercial communication platforms and an emphatic willingness to use alternate tools such as CKI-TAK or FIST in their place. The following sections detail the findings from each phase and participant group.

1. U.S. NPS Students' Results

U.S. NPS students' responses indicated that the majority of foreign police and military lack secure technologies to communicate with U.S. SOF. U.S. students also reported that partner forces mainly describe the Civ-Mil and social environment with U.S. counterparts using hand-written, rudimentary sketches on paper that they physically hand someone, or open-source platforms such as WhatsApp, Signal, and Telegram. Responses indicated that 33% and 50%, respectively, of international military and police partners rarely or never had secure means to communicate with U.S. military (see Figure 2).

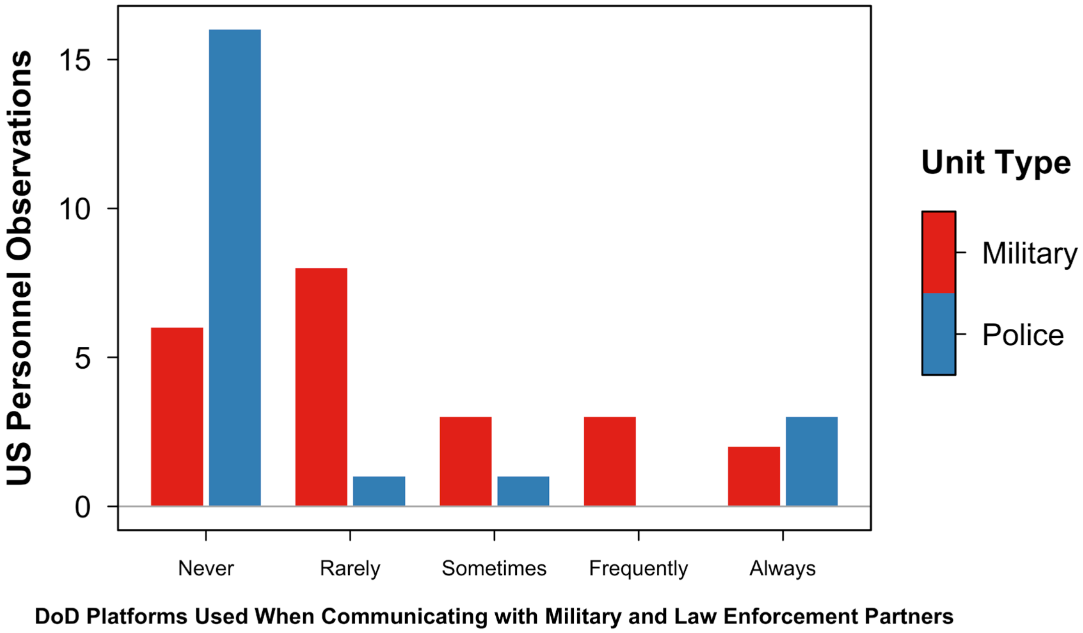


Figure 2. Continuity Methods: Partner Force and U.S. SOF

U.S. study participants gave strong indications that Signal, a commercial messaging platform, rated highest against all other methods that U.S. units used to pass information from a partner force to maintain continuity (see Figure 3). U.S. respondents noted that the second leading means to share information from partners was SMS (see Annex 2 and Annex 3) While Signal, WhatsApp, and other tools have end-to-end encryption, they are also owned by public corporations.[31] SMS is not secure from analysis by foreign governments or telecommunication corporations because of a reliance on cellphone network providers ranging from state-owned to private.[32]

[31] Laurens Cerulus, "EU Commission to Staff: Switch to Signal Messaging App," *POLITICO*, February 20, 2020, https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/.

[32] John Bacon, "Someone in China Could Be Reading Your Texts," *USA Today*, November 16, 2016, https://www.usatoday.com/story/tech/2016/11/16/someone-china-could-reading-your-texts/93951846/.

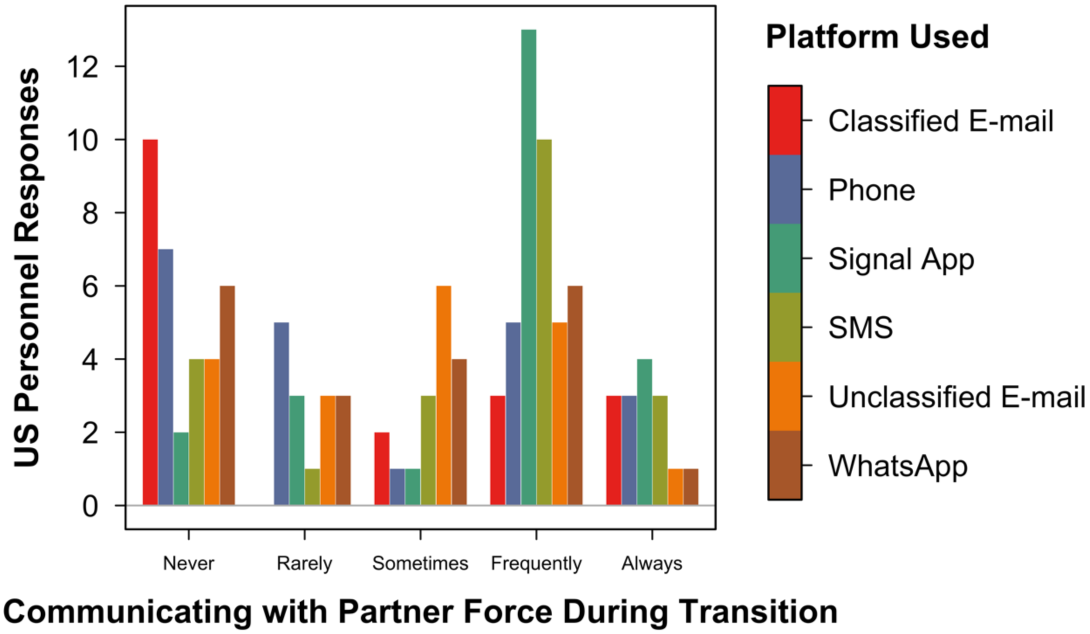


Figure 3. Civ-Mil Tools Used by Foreign Partner with U.S. SOF

When asked what were the key methods for communicating with partner forces to share visual information, U.S. participants noted that partner forces used a hand-written sketch passed from a partner force or an open-source tool to share information with U.S. forces over 70% of the time (see Annex 2). Four in ten U.S. respondents noted that partner forces primarily described the cyber environment to U.S. forces using WhatsApp, Signal, and Telegram (see Figure 3). While none of these figures had statistical significance, these measures of use amplify the need for secure technologies to close the gap between U.S. and partner forces.

2. International NPS Students' Results

International NPS students, many of whom are military officers, similarly indicated that the main tools used to understand the operational environment are Google and other commercial means. While International NPS respondents stated that official email and chat were the main method for sharing data within their unit, few listed a digital COP as an essential component of their information-sharing plan (see Figure 4). Questionnaire figures also found that information is transferred through physical means more habitually than through a digital COP (see Annex 2). Furthermore, foreign entities provide digital tools to cover partner force needs (see Annex 2). With few other alternatives, 50% of international students used Google or another unsecure tool as a common operating picture (see Annex 2).

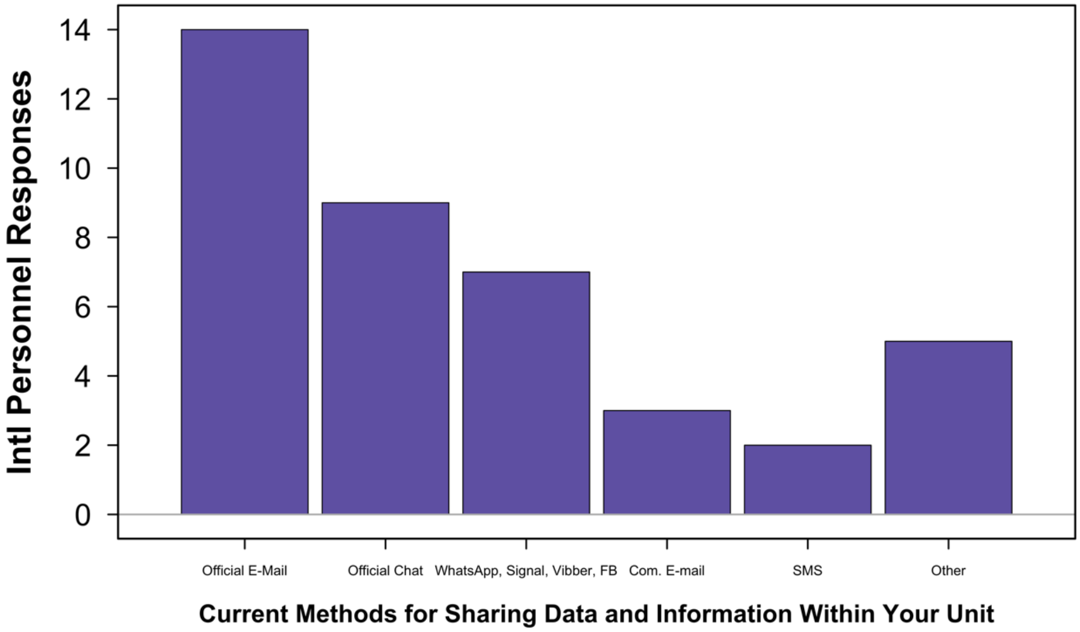


Figure 4. Main Common Operating Picture Platforms

Furthermore, of international NPS participants who use foreign digital platforms, 75% categorically retain current technology from foreign companies and 75% use technologies provided by a foreign government (see Annex 2). These data points on foreign influence may indicate that foreign governments have failed to provide the necessary digital COP, or failed to make an acceptable offer for such a platform that exceeds the standards of sharing information using Google.

Of international officers represented at NPS, 23% of respondents do not have a primary platform to understand the operating environment while 32% use basic transfer software to process this information (see Annex 2). Only 29% of international participants have unit-provided digital tools such as a COP software to share information to understand the operational environment (see Annex 2).

3. Philippine Military Results

Philippine Army responses stressed that platforms used in this study score low in connectivity, but CKI-TAK and FIST nevertheless meet unit operational requirements that could supplant commercial communication platforms. After using CKI-TAK, over 57% of respondents noted that the platform would sometimes or frequently meet long-term use of Philippine units' operational requirements (see Annex 1 and Annex 2). Similarly, 67% of respondents noted that FIST would frequently or always meet long-term use of Philippine units' operational requirements (see Figure 5). Similar to international NPS student responses, the Philippine Army Participants have a heavy reliance on commercial means versus a secured platform to share Civ-Mil information.

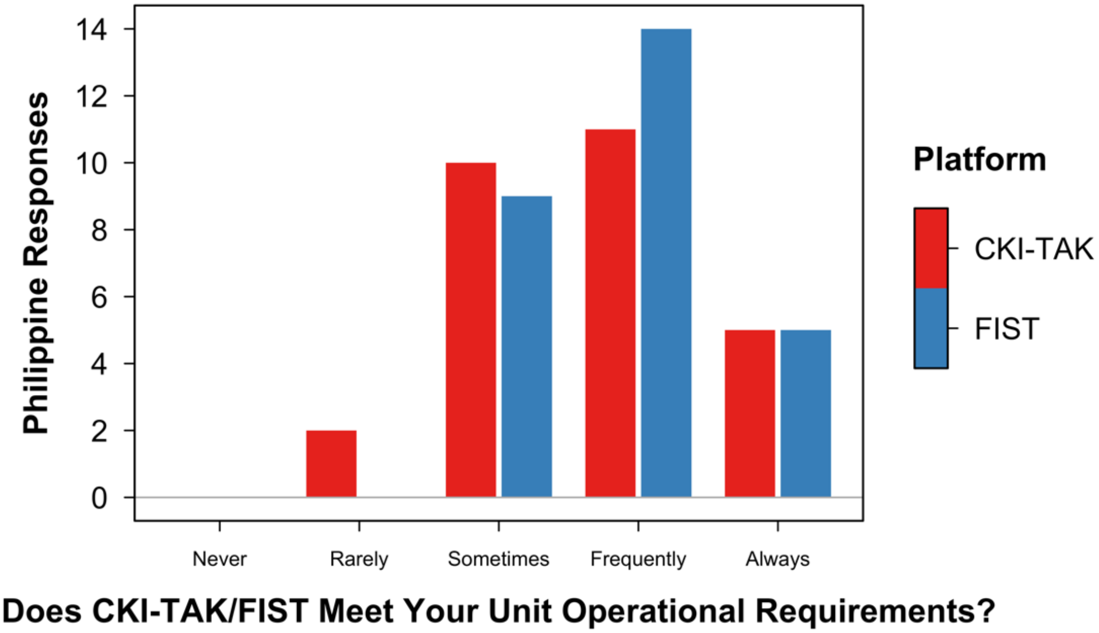


Figure 5. The Philippines Operational Requirements: CKI-TAK vs. FIST

When it comes to the question about the vulnerability of platforms in the Philippines, respondents indicated that terrain *prominently* impacts the use of a digital tool that requires Wi-Fi or cellular connectivity with a mean score of 3.8 and 3.66, respectively, for CKI-TAK and FIST (see Figure 6 and Annex 1, Section D and Annex 2).

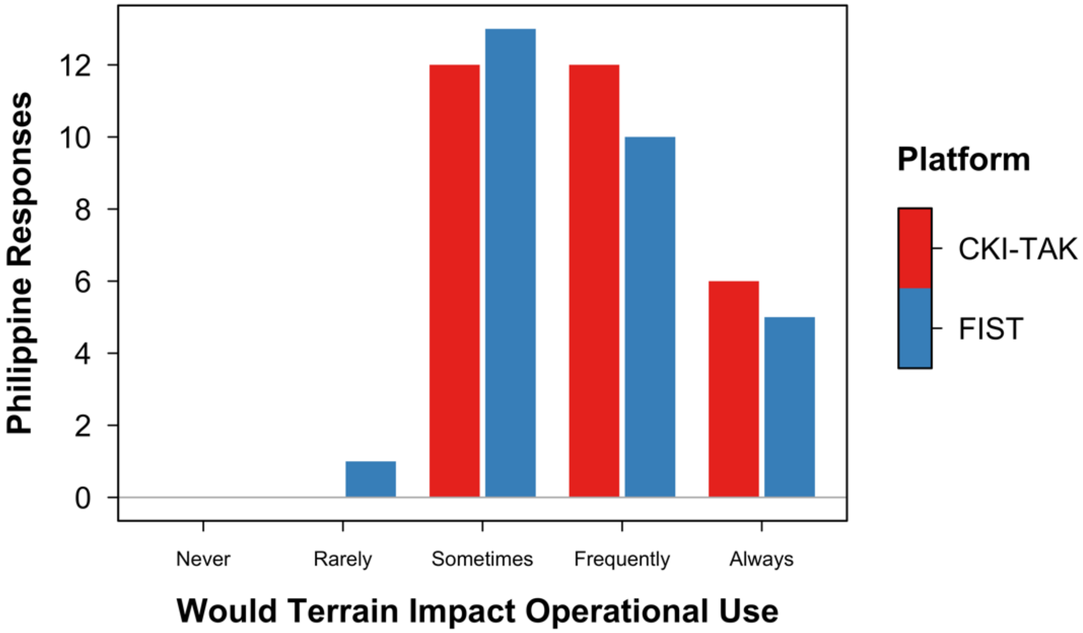


Figure 6. CKI-TAK and FIST Use Impacted by Terrain Conditions

Philippine Army respondents shared responses about organizational use of platforms for information sharing as seen in Figure 7. Over 64% of respondents indicated that their unit shares images, digital maps, and other digital graphics across units and echelons using commercial e-mail and commercial platforms including WhatsApp, Signal, Viber, and Facebook more frequently than a COP (see Annex 2).

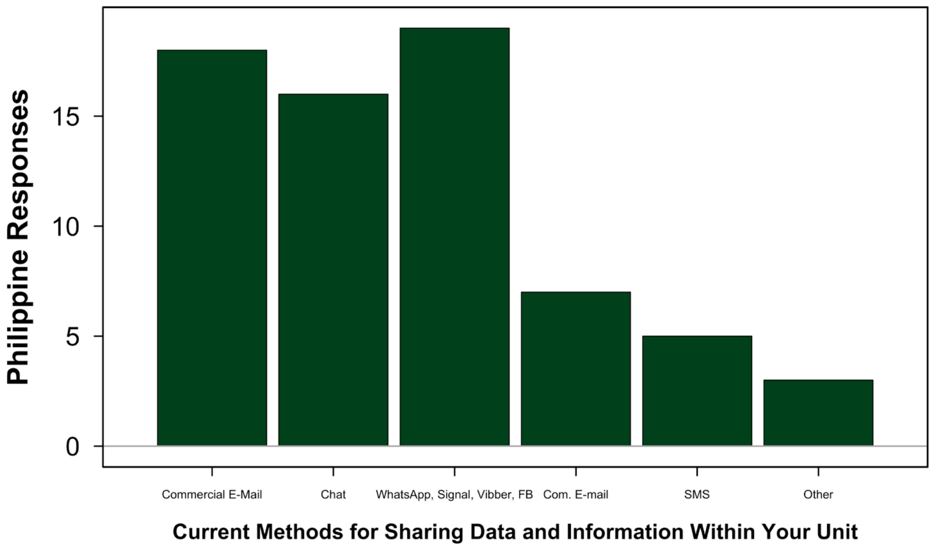


Figure 7. Unit Information Sharing Methods

Based on the demonstration and assessment methodology, the Philippine Army participants were divided whether the unit would decrease use of alternate tools based on FIST or CKI-TAK. Notwithstanding, a majority of participants posited that reliance on commercial tools would decrease proportionally to an increase in platform use. A mere 33% of those who used CKI-TAK disagreed that the platform would supplant the use of alternate tools such as email, social media, and WhatsApp (see Figure 5 and Annex 2). Specifically, 46% of participants strongly agreed that CKI-TAK internal unit use would decrease the use of unsecured communication means, similar to the 45.4% who reported the same about FIST. (see Figure 5 and Annex 1, Section D). When given the option, fewer than 5% disagreed that the use of CKI-TAK would lead to a decrease in reliance on unsecured communication platforms.

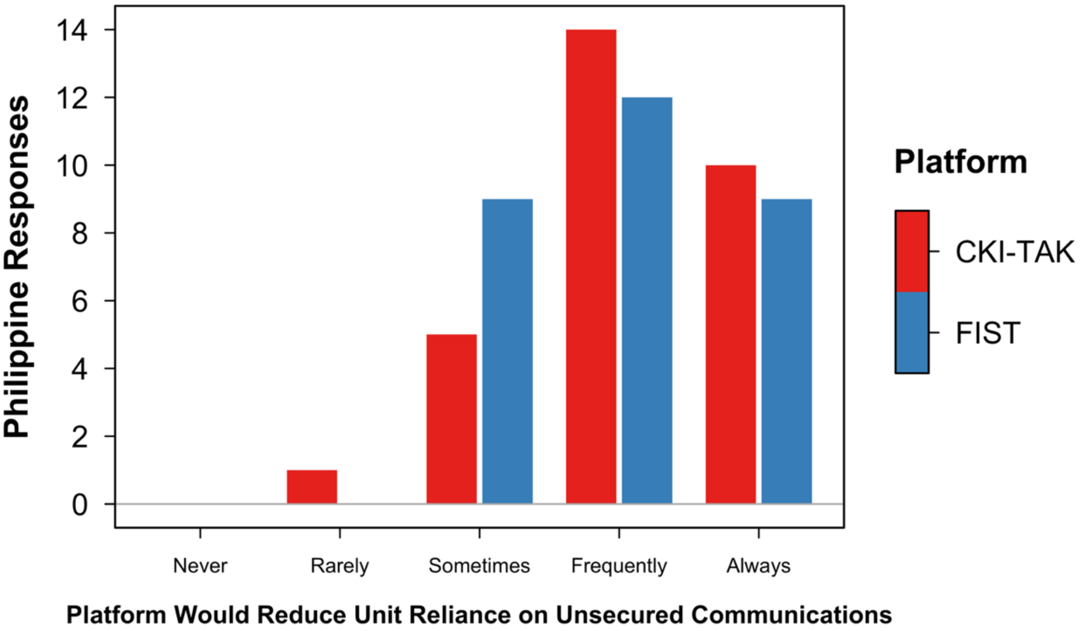


Figure 8. FIST or CKI TAK would Offset Unsecure Platform Use

F. ANALYSIS

Primary Dataset Discussion. The results from the Philippines in-country assessment indicated that while the platforms had a low rating to meet connectivity requirements, the platforms still feasibly support operational, time, reporting, and medical evacuation requirements. Overall, the findings confirmed that current technologies must be placed into use abroad with a partner force to acquire the necessary input to enable long-term information sharing.

1. U.S. Study Analysis

Many findings and implications from the U.S. portion of the study confirmed the hypothesis from U.S. and international military students that gaps exist between U.S. and foreign partners that may lead to vulnerabilities due to a lack of secure digital COP and reliance on commercial platforms. A majority of Partners and Allies reported that they rely on Google to understand the operating environment. Foreign forces working with U.S. units frequently rely on Signal and other applications to communicate. Over 50% of the time, sketches and commercial tools are used to depict the information environment. While many partners are working in the modern environment, most governments have not invested in the proper digital infrastructure to capture data and undermine adversaries. This creates an opportunity for the U.S. to enhance its preferred-partner status through developing access and applications for these partners to share with U.S. forces- and with their own units and NGOs on secure platforms.

2. Philippine Study Analysis

When comparing CKI-TAK and FIST, both platforms require additional user interface development to a meet the needs of partner forces. Generally, both platforms would greatly enhance partner force understanding of their area of operations and meet operational requirements.

Geographic Constraints. When merging observations from all surveys and interviews from Phase II, this body of work indicates that CKI-TAK and FIST need additional development to overcome connectivity challenges that stem from the geographic reality of the Philippine Army's operating environment. Results from the survey and interviews indicated a critical shortcoming in both CKI-TAK and FIST. The platforms rated 3.66/5 and 3.80/5, respectively, for internet connectivity limitations based on terrain (see Annex 2). The platform's constrained ability to connect digitally in certain environments could indicate that platform development lacked on-the-ground testing and assessment. Similarly, CKI-TAK and FIST scored low in the ability to share operational information with non-governmental organizations (NGOs) at 3.16/5 and 3.54/5, respectively. A subject-matter expert in the Philippines noted that digital platforms designed without input from the Armed Forces of the Philippines created a gap in information.[33] Since many NGOs work in remote areas of the Philippines in cooperation with the military, one could infer that the two results are related, but not with statistical certainty. The impact of geography on these digital platforms implies a lack of partner-force input early in the process of creating the applications for use in remote combat zones.

[33] Arvin R. Lagamon, Brigadir General, Philippine Army, Personnal Communication- Discussion and Breifing, September 5, 2022.

Operational requirements. Results indicated that both FIST and CKI-TAK would meet operational requirements, but FIST had a greater aptitude, 3.86/5, to do this versus CKI-TAK, 3.68/5 (see Annex 2). Regardless, both platforms scored the same, 3.90/5, when users were asked whether the platform would meet operational requirements to gain situational understanding of the area of operations (see Annex 2). The very comparable scores placed both platforms in a similar category.

Time. While participants stated that training to use CKI-TAK, 3.93/5, was more feasible within unit time constraints than FIST, 3.77/5, individuals indicated that once trained, FIST would meet reporting requirements more expeditiously, 3.93/5, versus 3.79/5 (see Annex 2). Thus, platforms developed to create a nexus between U.S. partners and U.S. SOF must employ an intuitive user interface with simple steps to troubleshoot challenges and maximize operating time. An ideal platform should require the right balance of time to learn the features and ease of use that will increase submission and decrease relay times between users and their command centers.

Reporting Requirements. Statistics indicate that CKI-TAK has formatting more likely (m=4.00/5) to meet unit reporting requirements than FIST (m=3.89/5) (see Annex 2). Due to varying reporting requirements, the Philippine units' reliance on Gmail to share and catalog information could be effectively succeeded, should an alternate platform be assessed in the Philippines and leveraged to secure both internal Philippine Army and external, bilateral communication with U.S. units. Surprisingly, FIST scored slightly higher at 3.79/5, versus 3.72/5, for the ability to meet requirements in the appropriate language than CKI-TAK which has more submission capabilities in multiple languages (see Annex 2). More exposure through additional use and practice in real-world scenarios or future study iterations would give participants additional practice to fully evaluate language and translation requirements.

Medical Evacuation and Exercises. Pointedly, both platforms were rated favorably on a 1–5 scale with regard to use for medical evacuations (m=4) and for bilateral training and exercises with the U.S. (m=3.93) (see Annex 2). While the questionnaire asked if Filipinos were willing to receive information from the U.S. during exercises, these elevated ratings could indicate that the Philippines Army is inclined to work more closely with the

United States via these platforms during routine exercises, and that it may have interest in expanding collaboration.

Alternate Methods. Participants generally agreed that the Philippines Army is currently more inclined to share information, graphics, maps, and images for the unit on social media than with any other digital platform; Filipinos somewhat agreed that use of either FIST or CKI-TAK would reduce reliance on unofficial communication platforms (m=4.05/5) (see Annex 2). This link between the current practices and alternate technologies could indicate an opportunity to guide Philippine partners away from commercial platforms toward encrypted alternatives.

Partner forces found digital platforms effective for meeting operational needs particularly based on timeline, operational information, and capacity for medical evacuation. In summary, the scope of Proj. ISHARE methodology provides a framework for future iterations of demonstration and analysis with partner forces. The results found strong indications that additional iterations including demonstration and assessment must be completed with partner forces to diminish the trend of short-term technology contracts that end abruptly and break trust between the U.S. and partner forces. To ensure long-term integration and to increase enduring trust through collaboration, U.S. partners and allies must share their voice in the digital COP assessment process. Findings may indicate that CKI-TAK and FIST capabilities fit Philippine partner force requirements for operations, cyber, and civil information sharing.

While this study sought to identify and address the technology gap that exists between USSOCOM and its international partners and allies, the datasets, demonstrations, and assessments have a limited scope. The findings are broadly applicable, but responses to surveys during both parts of the study were under statistically significant (*P*= .005) values due to a small sampling size. Study participants in the U.S. came from a narrow segment of the population, most participants were from the U.S. Army. Further studies should include larger sampling from other services to account for error, and should include greater representation across ranks and echelons from recently-redeployed U.S. SOF teams. Of the international student population, future studies should consider expanding the sample to include international participants from other staff colleges to broaden the study's applicability with a larger sample size to achieve additional, generalizable findings. Since participation in the U.S. study was limited mainly due to the completion of pre-use questionnaires, consideration is required to determine proper incentives for additional student involvement to increase successive platform demonstration and assessment participation.

The study in the Philippines also contained a set of limitations that should be expanded upon to increase result validity. The study was constrained to Philippine Army respondents which should be expanded to other Philippine armed forces branches and incorporate feedback from the NGOs that work with these units and U.S. SOF. Furthermore, the study was limited to Manila rather than involving units and individuals actively communicating in combat zones. Survey methodology was constrained to use the same facilitators as part of the demonstration and assessment, but additional studies should also include non-affiliated survey proctors to control for variance. While the study sought to complete a demonstration and assessment in six countries, the time and funding constraints inhibited U.S. external research to the Philippines alone. Ultimately, this study lacked input from multiple GCCs and requires additional studies across other GCCs to ensure broad applicability and necessary input for future technological research and design with an indigenous approach. Alternately, serious consideration should be granted for use across other USINDOPACOM countries to increase use in environments where U.S. forces may have less presence on the ground.

IV. CONCEPTUALIZED CASE STUDY—TAIWAN

A. INFORMATION SHARING AS PART OF INTEGRATED DETERRENCE

Enhancing a partner nation's military ability to coordinate with its civilian counterparts in peacetime can provide a robust platform for supporting a resistance force during an invasion. The assessments of the CKI-TAK and FIST platforms can be applied to a conceptualized employment of these types of platforms in areas where the U.S. and its partners seek to enhance deterrence against a potential third-party aggressor nation such as in Taiwan or Ukraine. While ongoing efforts in Ukraine limit the ability to discuss the full potential of these types of platforms in that AOR, the following conceptualization of use in Taiwan will provide further value for the scope of Proj. ISHARE's efforts.

Foreign militaries need information and data-sharing platforms for use internally, with U.S. partners, and with their civilian counterparts. This has been demonstrated through the outputs of this fieldwork in the Philippines using the CKI-TAK and FIST. While interviews, discussions, and surveys with the Philippines Civil Military Operations Regiment leadership and personnel highlighted this need for lessons learned from responding to natural disasters, the correlation can be made to other types of crisis responses in the region. Using the CKI-TAK and FIST assessments in the Philippines as a starting point, the conceptual introduction of these platforms to a partner such as Taiwan can be assessed to determine its ability to enhance deterrence messaging to a potential aggressor.

The political sensitivities of supporting Taiwan create ever increasingly complex dilemmas for the U.S. due to the growing military might of the People's Republic of China, global economic inter-reliance, and the persistent Chinese Communist Party's claim to Taiwan as a legitimate territory of the mainland. One possible method to modernize the U.S. deterrence effort against Chinese aggression is expanding the civilian-military information-sharing platforms between the U.S. and Taiwanese entities. Exploring the potential benefits of developing Civ-Mil humanitarian assistance and disaster relief (HADR) coordination systems, which both FIST and CKI-TAK could provide, offers unique opportunities for expanded deterrence options. Such an undertaking would capitalize on grey zone competition opportunities within the framework of HADR. Based on our ongoing research of information and data-sharing platforms, we can evaluate several potential impacts and benefits of creating and synchronizing collaboration platforms that integrate U.S. and Taiwanese HADR response capabilities by both civilian and military entities.

Given the U.S. policy of strategic ambiguity, the Taiwan problem set can be defined as dominated by the grey zone in which the U.S. must use military capabilities cautiously and short of armed conflict but with clear intent. Grey zone activities and deterrence are rooted in the fundamental understanding that the U.S. must secure a competitive advantage within the information environment to be successful in the strategic competition space. The introduction of expanded combined HADR Knowledge Management Systems (KMS) and Command and Control (C2) systems in Taiwan would support partner force knowledge management system development and Joint Interagency, Intergovernmental, and Multinational (JIIM) information management platforms across USASOC and the DOD. Specifically, the use of CKI-TAK or FIST may improve the effectiveness of knowledge management and, thus coordination between Taiwanese military and civilian entities as well as with U.S. forces. The following examination of the Taiwan deterrence problem set will inform the value of developing partner-force KMS-C2, such as CKI-TAK and FIST systems, to incorporate civilian entities in host nations as a means of enhanced deterrence.

B. THE TAIWANESE CASE—BACKGROUND

Due to the fact that the U.S. intelligence officials assess that the Chinese Communist Party (CCP) seeks to take control of Taiwan within this decade, the United States must reexamine the methods available to deter China.[34] As the CCP becomes increasingly belligerent towards Taiwan and other Asian nations, we must reframe our understanding of the tools available to counter the People's Republic of China's (PRC)

[34] Brad Lendon, "Chinese Threat to Taiwan 'closer to Us than Most Think,' Top U.S. Admiral Says," CNN, March 24, 2021, https://www.cnn.com/2021/03/24/asia/indo-pacific-commander-aquilino-hearing-taiwan-intl-hnk-ml/index.html.

activities within the paradigm of strategic competition. The U.S. and its allies have limited options to demonstrate their security commitment to Taiwan's territorial integrity. The Taiwanese problem set is perhaps the most likely flashpoint from which the U.S. and the PRC can fall into the Thucydides' Trap.[35] The trap highlights that rising powers and existing or declining powers have historically come into violent conflict as the declining power seeks to retain its status and the rising power seeks to assert itself as a peer or domain power.[36] While the PRC has evolved its approach to the Taiwan issue as a cornerstone of its larger expansionist strategy, the U.S. has struggled to modernize its methods and strategy for deterrence. Expansive strengthening of Taiwan's military defenses and continued arms sales further emboldens the PRC's military and weapons buildup. Overtly increased diplomatic relations signaling support to Taiwan's independence risks economic and diplomatic retaliation from the PRC. Currently, the PRC's stated goal of reclaiming Taiwan appears to be within reach.

The United States' "Strategic Ambiguity" approach seeks to leave the PRC guessing what the red lines are and how the U.S. would respond.[37] While some detractors would submit that the current application of Strategic Ambiguity has not slowed the PRC's aggressive posturing, we must recognize that there is value in the current ambiguity policy. The fact that the PRC has capitalized on military leap-ahead technology, inconsistent U.S. foreign policy signals, and an increasingly divided international community to further its claim of Taiwan as a rogue province are not entirely the result of the strategic ambiguity approach. While recent public comments by the Biden administration have removed much of this ambiguity in terms of the US's intention to support the defense of Taiwan with

[35] Graham T. Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston: Houghton Mifflin Harcourt, 2017).

[36] Allison.

[37] Nien-chung Chang-Liao and Chi Fang, "The Case for Maintaining Strategic Ambiguity in the Taiwan Strait," *Washington Quarterly* 44, no. 2 (2021): 45–60, https://doi.org/10.1080/0163660X.2021.1932088.

ground troops if necessary, strategic ambiguity is not a complete failure.[38] A retooling of the methods used within the existing framework of Strategic Ambiguity can modernize the strategy and capitalize on the same grey zone activities that the PRC has used to expand its countering of U.S. activities in the INDO-PACIFIC. Updating Strategic Ambiguity to include additional Civ-Mil collaborative exercises and systems would likely further complicate the PRC's existing approach to Taiwan. Such exercise would incorporate Taiwanese military and civilian entities along with U.S. military and civilian entities in national responses to natural and manmade disasters. Given that the island nation is susceptible to earthquakes, large scale flooding, and typhoons, the expansion of such drills would have immediate positive outcomes in fostering preparedness. More importantly, the expansion of these drills would highlight the need for robust information and data-sharing platforms in a field environment with remote access capability and the ability to visually depict geographical overlays with near real-time images and icons for shared situational awareness. Thus, these exercises are a natural testing ground and introduction point for digital tools such as CKI-TAK and FIST. Introducing these dual-purpose platforms would further demonstrate the U.S. commitment to Taiwan without formally increasing military support.

The reinvigoration of a U.S. whole-of-government approach rooted in information and data-sharing integration of Humanitarian Assistance and Disaster Relief response capabilities may provide a firm foundation to reestablish clear deterrence to further aggression from the PRC towards Taiwan. Initial assessments of the CKI-TAK and FIST platforms indicate that expanded collaborative Civilian-Military HADR KMS-C2 platforms could be a salient catalyst to a more robust deterrence strategy against the PRC.

Current HADR capabilities and cooperation between the U.S. and Taiwan are primed for expanded integration. A global leader in HADR, the Taiwanese government

[38] David Brunnstrom and Trevor Hunnicutt, "Biden Says U.S. Forces Would Defend Taiwan in the Event of a Chinese Invasion," Reuters, September 19, 2022, https://www.reuters.com/world/biden-says-us-forces-would-defend-taiwan-event-chinese-invasion-2022-09-18/; CBS News, "Biden Tells 60 Minutes U.S. Troops Would Defend Taiwan, but White House Says This Is Not Official U.S. Policy," CBS News, September 18, 2022, https://www.cbsnews.com/news/president-joe-biden-taiwan-60-minutes-2022-09-18/; Chang-Liao and Fang, "The Case for Maintaining Strategic Ambiguity."

and non-governmental sectors have vast knowledge to share with the U.S. As the primary provider of logistical capabilities to HADR responses within INDO-PACOM, the United States is a natural partner for Taiwan in HADR. The two nations currently hold regular HADR workshops and have jointly responded to natural disasters in the Philippines, Japan, Haiti, and throughout the globe.[39] Objections by PRC officials to expand cooperation and integration in HADR abilities would place China in the position of opposing an internationally recognized need. Numerous nations have benefited from both Taiwanese and U.S. support in times of national disaster and humanitarian crisis. Expanded relations between the U.S. and Taiwan in this area would likely limit the retaliatory options available to the PRC. Thus, the introduction of platforms such as CKI-TAK and FIST fall in line with existing lines of cooperation between U.S. and Taiwanese government entities.

While natural integration of other defense-related capabilities would likely result, rooting them in HADR provides an authentic and marketable primary rationale for increased collaboration. Moreover, using these types of platforms to access both military and civilian government agencies would foster expanded whole of government approach to the deterrence problem set. This approach incorporates entities and agencies not traditionally seen as part of the defense apparatuses of the U.S. or Taiwan. Through the inclusion of these entities, such as a FEMA, USAID on the U.S. side and the Taiwan's Disaster Management Agency, a more robust resistance capability is demonstrated. Leveraging the whole-of-government approach through Civ-Mil initiatives could expand the options available to signal deterrence objectives.

The post-WWII nature of the bi-lateral relationship between the U.S. and China must not be used as a foundation for current engagements. Western governments, led by the U.S., gambled that economic prosperity brought on by liberalized-market economies would win over the communist leaders and people in mainland China. They believed this would lead to democratic reforms within China. They have been proven wrong by the swift

[39] Thesys, *Humanitarian Assistance and Disaster Relief (HADR) Health Support NMD* (Taipei: Medical Affairs Bureau, 2021), http://mab.mnd.gov.tw/; Janice Leister, "Pacific Partnership 2021 Mission Concludes in Palau," U.S. Indo-Pacific Command, August 13, 2021, https://www.pacom.mil/Media/News/News-Article-View/Article/2731776/pacific-partnership-2021-mission-concludes-in-palau/.

consolidation of power by Xi Jinping.[40] The CCP has cracked down on Hong Kong, militarized its manmade islands across the South China Sea, and removed the word "peaceful" from its platform regarding the reunification of Taiwan with the mainland.[41] In 2019 both the incoming and outgoing Indo-Pacific Command commanding officers predicted the PRC taking active military measures within the next six years to reclaim Taiwan.[42] The 2014 annexation of Crimea region and 2021 invasion of eastern Ukraine by Russia has demonstrated that the occupation and forceful capture of sovereign territory is not a thing of the past. The current application of the strategy of ambiguity backed by possible military power projection is no longer practical alone in the current construct of strategic competition.

The U.S. must reassess the means available to deter any attempt to overtake Taiwan forcefully or coercively. While China has dramatically expanded its military power and capabilities, including its nuclear arsenal, there is still no consensus that it can forcibly take Taiwan. Traditionally, the U.S. has relied heavily on military arms sales and show of force demonstrations within the Taiwan Strait to highlight support for Taiwan's autonomy. These approaches have lacked a whole-of-government approach and highlighted a one-dimensional means of deterrence. This one-dimensional approach has resulted in military responses from the PRC. Over the last two years, the number of air and naval incursions into Taiwanese territory by Chinese military craft have regularly increased.[43] Currently, the U.S. Strategic Ambiguity and inconsistent support to Taiwan fail to capitalize on all

[40] Timothy R. Heath, *The Consolidation of Political Power in China under Xi Jinping: Implications for the PLA and Domestic Security Forces.* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/testimonies/CT503z1.html.

[41] Yew Lun Tian and Yimou Lee, "China Drops Word 'peaceful' in Latest Push for Taiwan 'Reunification,'" Reuters, September 12, 2021, https://www.reuters.com/article/us-china-parliament-taiwan/china-drops-word-peaceful-in-latest-push-for-taiwan-reunification-idUSKBN22Y06S.

[42] Lendon, "Chinese Threat to Taiwan."

[43] Lendon; Ned Price, "PRC Military Pressure against Taiwan Threatens Regional Peace and Stability," U.S. Department of State Press Releases, September 12, 2021, https://www.state.gov/prc-military-pressure-against-taiwan-threatens-regional-peace-and-stability/; BBC News, "Taiwan Says 19 Chinese Warplanes Entered Air Defence Zone," BBC News, September 6, 2021, https://www.bbc.com/news/world-asia-58459128.

facets of U.S. whole-of-government capabilities and thus is a weak deterrent to China which demands a modern appraisal.

The U.S. can apply current policy to support expanded Civ-Mil activities with Taiwan with expanded information and data sharing platforms. The United States' historical and economic relations with the Republic of China and the People's Republic of China create a complex security dilemma to seek stability in the cross-strait relationship. The United States-Taiwan security partnership is distinctive due to the lack of U.S. recognition of the Taiwanese Government.[44] The April 1979 Taiwan Relations Act of April (TRA) remains in effect as the framework guiding U.S. policy towards Taiwan.[45] The TRA explicitly calls for the arming of the island nation and the preservation of peace and security in the region.[46] While arms sales and foreign military training have been a cornerstone of the TRA, the other methods of U.S. support have fallen short. The TRA calls for "promot [ing] extensive, close, and friendly commercial, cultural, and other relations between the people of the United States and the people on Taiwan."[47] This language within the TRA provides the legal grounds from which the U.S. can undertake increased disaster response Civ-Mil collaboration efforts focused on information-sharing systems development. Although delicate, the U.S. can use existing and accepted policy and legal grounds to justify shifting its focus within the complex security dilemma of the cross straight relationship. Further assessments of the legal parameters of the TRA as well as the political appetite of U.S. leaders in Congress and the administration, are needed to assess the potential to bring this conceptualization to fruition.

C. THE CONCEPTUAL APPLICATION

Implementing a highly integrated Civ-Mil knowledge management and C2 platform based on the capabilities of systems focused on HADR cooperation can bolster a

[44] Richard C. Bush, *The United States Security Partnership with Taiwan* (Washington, DC: Brookings Institution, 2016), https://www.brookings.edu/research/the-united-states-security-partnership-with-taiwan/.

[45] Taiwan Relations Act, Pub. L. No. 96–8, 93 Stat. 14 (1979) https://www/congress.gov/96/statute/STATUTE-93/STATUTE-93-Pg14.pdf

[46] Taiwan Relations Act

[47] Taiwan Relations Act

larger deterrence strategy by demonstrating effective interoperability of U.S.-Taiwanese systems. Our fieldwork has demonstrated that both CKI-TAK and FIST have shown early viability of being such a tool. The introduction of these platforms in Taiwan will have a secondary deterrent effect of placing U.S. government and military personnel on the ground in Taiwan on a persistent basis creating a tripwire and assurance of imposed costs trigged by any aggression against Taiwan.

Using digital information-sharing platforms under the auspices of HADR activities can be a means to clearly demonstrate the clear conduits of information management interoperability between U.S. and Taiwanese entities. The U.S. Army defines knowledge management as "the process of enabling knowledge flow to enhance shared understanding, learning, and decision-making. It is done through the creation, organization, integration and sharing of knowledge between leaders and subordinates in order to improve adaptability, integration and synchronization enabling effective decision making."[48] In executing HADR responses, KMS-C2 is vital to ensure a common understanding of the events unfolding, the proper methods of response, and the resources needed and available. Humanitarian Assistance programs support stability in conflict regions using aid and relief following natural or manmade disasters, while international disaster relief seeks to deliver life-saving assistance during disasters and crises.[49] Combined, HADR is a powerful soft power tool within the international arena.[50] Traditionally HADR responses are undertaken through multinational cooperation. Such ventures are often rife with coordination conflicts and interoperability obstacles. As noted by Dorasamy et al., "Literature suggests that emergency management efforts benefit from well-integrated knowledge-based emergency

[48] U.S. Army Combined Arms Center, "Army Knowledge Management Proponent (AKM)," U.S. Army Combined Arms Center, September 14, 2021, https://usacac.army.mil/organizations/mccoe/akm.

[49] Defense Security Cooperation Agency, "Humanitarian Assistance and Disaster Relief," DSCA AT 50, September 14, 2021, https://www.dsca.mil/50th-anniversary/humanitarian-assistance-and-disaster-relief.

[50] Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004).

management information systems (EMIS)."[51] EMIS is essentially civilian parlance for KMS-C2. Building on the benefits of KMS-C2 would open opportunities to demonstrate more extensive interoperability and unified formation between the U.S. and Taiwan.

D. VALUE OF SECURE DIGITAL INFORMATION SHARING

The United States must reexamine available deterrence approaches as the PRC becomes increasingly belligerent towards Taiwan. Reframing the understanding of the tools available to counter the PRC's activities and rhetoric within the paradigm of strategic competition is required. The U.S. must assess the effectiveness of various levels of influence and engagement to protect the international norms championed by the U.S. The U.S. must retool its current overreliance on 'hard' military power projection as the primary deterrent capability. Maintaining the territorial integrity of the first island chain within the Western Pacific Ocean is of paramount national security to the United States. Free navigation of vital waterways and the region's stability through preserving the status quo is critical to U.S. and global economic security. The U.S. must support smaller democratic states with liberalized economies to promote the rules-based international norms that have increased global prosperity for the last 75 years. As the nature of war and conflict evolves with the expansion of information technology, formidable A2AD systems, and hypersonic weapons, a review of civil-military cooperative endeavors toward deterrence provides alternative tools to demonstrate security commitments without overt militarization.

Bernard Brody notes that the end of WWII resulted in the primary use of a military shifting from winning wars to deterring them.[52] This truth has grown into the U.S. overreliance on military strength as its dominant deterrence tool. It can be argued that such reliance has become archaic, and this research may demonstrate a method to retool military activities to address competition and non-kinetic military activities.

[51] Magiswary Dorasamy, Murali Raman, and Maniam Kaliannan, "Knowledge Management Systems in Support of Disasters Management: A Two Decade Review," *Technological Forecasting and Social Change*, Planning and Foresight Methodologies in Emergency Preparedness and Management, 80, no. 9 (November 2013): 1834–53, https://doi.org/10.1016/j.techfore.2012.12.008.

[52] Bernard Brodie, *The Anatomy of Deterrence*, RR-RM2218 (Santa Monica, CA: RAND Corporation, 1958), 173, https://www.rand.org/pubs/research_memoranda/RM2218.html.

While significant literature addresses the utility of U.S. personnel on the ground as a means of deterrence and the value of humanitarian assistance and disaster relief cooperation with Taiwan, the melding of these pursuits has been less explored. A growing body of defense and policymakers support the deployment of U.S. military forces to Taiwan on a persistent basis.[53] Multinational exercises and conferences on HADR have highlighted the impressive capabilities of the Taiwanese systems in the disaster response realm.[54] This body of literature does not overtly correlate this capability with a more extensive deterrence capability. Moreover, academic and military reviews of the placement of the U.S. military personnel or systems in Taiwan fail to articulate the rationale for their placement other than to state it would deter the PRC and reassure Taiwan. Such a move would only further antagonize the PRC. Limited academic works highlight the use of the TRA as a conduit for Civ-Mil collaboration on HADR within Taiwan. Subsequently, the deterrence applications of such collaborations have not been fully analyzed.

The data and outputs of Proj. ISHARE's field research in the Philippines demonstrates that information and data-sharing platforms are both needed by partner forces and would fill critical capabilities gaps for both the partner and U.S. Forces. The Philippines geographic location, island nation status, proximity to China, and ongoing territorial disputes with the PRC make it a valuable testbed for assessments of digital information sharing platforms that could be used with Taiwanese Partners. Philippine users of CKI-TAK and FIST noted that the platforms would reduce reliance on non-sure commercial platforms and would increase communications with U.S. Partners and Civilian

[53] Michael Mazza, "Imagining a New U.S. Military Presence in Taiwan," American Enterprise Institute Op-Ed, May 17, 2020, https://www.aei.org/op-eds/imagining-a-new-us-military-presence-in-taiwan/; Michael E. O'Hanlon, "An Asymmetric Defense of Taiwan," *Order from Chaos* (blog), April 28, 2021, https://www.brookings.edu/blog/order-from-chaos/2021/04/28/an-asymmetric-defense-of-taiwan/; Loren Thompson, "Taiwan Tripwire: A New Role for the U.S. Army In Deterring Chinese Aggression," *Forbes*, August 25, 2021, https://www.forbes.com/sites/lorenthompson/2021/03/26/taiwan-tripwire-a-new-role-for-the-us-army-in-deterring-chinese-aggression/; Josh Rogin, "To Avoid Conflict, the United States Must Deter Chinese Aggression: The U.S. Must Adjust Its Strategy as China Races Forward," *Washington Post*, 2019, https://www.washingtonpost.com/opinions/global-opinions/to-avoid-conflict-the-united-states-must-deter-chinese-aggression/2019/06/06/400b8ef0-8899-11e9-98c1-e945ae5db8fb_story.html; Kelvin Chen, "US Special Forces to Train Taiwan Soldiers after Annual War-Games," *Taiwan News*, May 31, 2021, https://www.taiwannews.com.tw/en/news/4213647.

[54] Central News Agency, "U.S., Taiwan Launch Disaster Preparedness Cooperation," Focus Taiwan, March 11, 2021, https://focustaiwan.tw/politics/202103110004; Leister, "Pacific Partnership 2021 Mission Concludes in Palau."

counterparts. This data indicates that the introduction of such platforms in Taiwan would have similar output. Such outputs would support the deterrence efforts as well as bolster Civ-Mil cooperation need for both HADR operations as well as for use in support of resistance activities in the event of an invasion.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

This capstone validated the theory that secure digital data-sharing platforms require early iteration with foreign partners to ensure suitable design to meet the partner forces' needs and to create long-term adoption. Moreover, the field research indicates the initial hypothesis that properly developed digital tools can be used to merge partner forces digital and physical habits for communicating with SOF teams to enable a digital forward presence when such platforms are provided to a partner force. The data from over 70 respondents representing 27 nations indicates that non-secure messaging and information platforms use remains high among U.S. Allies and Partners. This usage is particularly high when information is shared between U.S. SOF and non-FVEY partner forces. While current programs of record such as the Full Spectrum- Remote Advise and Assist – Virtual Accompany Kit (RAA-VAK) provide local tactical secure information and data-sharing capabilities, such systems lack the ability to connect over the horizon in the manner required to support today's strategic competition dynamics. Further refinement of systems such as CKI-TAK and FIST, which enable over-the-horizon near real-time data sharing in a common operating picture and report generation format, is needed. Development and refinement must be completed with a partner force-centric approach to ensure regional-specific user interfaces and connectivity requirements are developed early on to increase the likelihood of long-term adoption of such digital tools.

Strategic competition requires reassessing how U.S. SOF cultivates operational relationships and shares critical data and information between allies and partners. The SOF community must further develop digital tools such as CKI-TAK and FIST to modernize these operational relationships. These platforms can potentially expand the ability to foster persistent engagement and information sharing without placing a premium on the geographic location of the SOF team. Information is the true weapon within competition and the partnerships established by over 140 SOF teams across 80 nations are the key access point for information advantage. Current digital information platforms used with partners are often US-centric in their development and design and remain limited to tactical applications. These platforms cannot provide a global information-sharing network required to compete globally for information advantage. This research confirms that technology gaps often lead to partner forces using un-secure commercial options to share data with U.S. teams. These options are insufficient and increase risk as malign actors infiltrate or maintain control over commercial networks. Proj. ISHARE has produced data supporting the criticality of fostering assess to secure digital information platforms for partner forces. This data can help inform and shape next-generation data and information-sharing platforms. The refinement of digital information platform development would vastly improve the means and methods U.S. SOF teams could employ to cultivate and foster the operational relationships critical to SOF activities and U.S. national objectives.

The results of Proj. ISHARE's field assessment in the Philippines indicates that both CKI-TAK and FIST are deemed effective for operational use but lack sustainable connectivity for remote operating areas. While 55% of partners force respondents used commercial apps to share with U.S. SOF, 66% agreed that the use of the CKI-TAK and FIST would reduce their dependence on non-secured platforms. Survey results that included respondents from over 25 nations confirmed that partner nations do not provide their forces with the necessary digital tools for COP development and secure data sharing. The project-developed data supports the theory that data-sharing platforms require early iteration with foreign partners to ensure suitable design to meet the partner forces' needs.

The Proj. ISHARE assessment of CKI-TAK and FIST information-sharing platforms advanced the theory that partner-centric development could lead to a higher likelihood of long-term adoption, thus creating a means to modernize data and information sharing among our Allies and partners. The project's use of in-country assessments of these two emerging platforms can inform recommendations to develop the next generation of secure digital platforms. Such platforms must be built to enhance both U.S. forces and, more importantly, the partners' ability to visualize and understand their physical and cyber environments. The DOD must tailor information and data-sharing digital tools to the operational requirements of regional partners. The user interfaces of these tools must have robust translation capabilities but cannot rely on AI-driven translation alone.

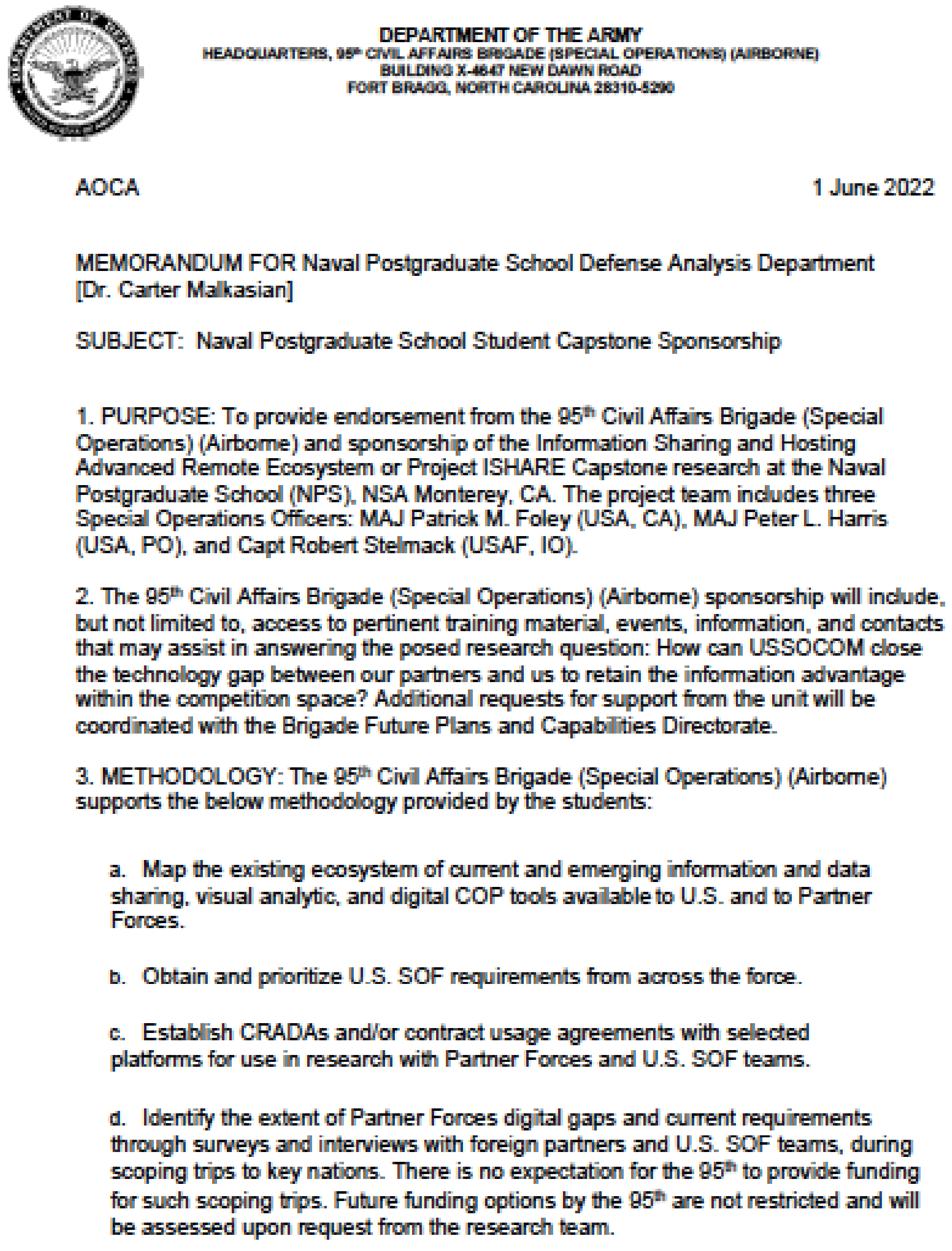
Additionally, U.S. forces must commit to the long-term use of these platforms. Previous implementation of such platforms, such as Palantir Lapis, which have been defunded, undermine the potential for partners to use U.S. promoted platforms in the future. As demonstrated in the data highlighted in Chapter III, partners seek access to secure information-sharing platforms and lack the ability to provide these platforms to their forces. While many partners are working in the modern environment, many governments have not invested in the necessary digital infrastructure to capture data and undermine adversaries. This creates an opportunity for the U.S. to enhance its preferred partner status by developing access to secure platforms. Thus, the U.S. can greatly enhance partner cooperation and integration through information-sharing platform development with partners.

While Proj. ISHARE focused on the user interface and partner requirements at the edge, more research and coordination must be undertaken to develop connectivity and redundancy with DOD managed backside architectures and data lakes. Moving forward, Proj. ISHARE must be put to use within the Project Convergence construct to ensure these platforms are interoperable with other emerging capabilities. Additionally, the development of the data lakes and backside architectures to support data and information sharing from the edge must be more fully integrated into the methodology of future in-country demonstrations and assessments. Further research should enhance cooperation opportunities with USASOC and 1st SFC initiatives such as Proj. Hardwire. Such cooperation would more clearly define the viability of CKI-TAK and FIST platforms and provide a clear understanding of the data volumes expected by these emerging architectures. Finally, additional exploration of using low earth orbit messed satellite networks to provide persistent connectivity to the devices upon which these platforms run is critical to overcoming the connectivity issues identified in remote areas. Ongoing research on the viability of low-earth orbit satellite networks for secure communication would significantly enhance the long-term adoption of information-sharing platforms by partner forces.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SPONSORSHIP MEMORANDUMS

A. 95TH CIVIL AFFAIRS BRIGADE (AIRBORNE)



DEPARTMENT OF THE ARMY
HEADQUARTERS, 95th CIVIL AFFAIRS BRIGADE (SPECIAL OPERATIONS) (AIRBORNE)
BUILDING X-4647 NEW DAWN ROAD
FORT BRAGG, NORTH CAROLINA 28310-5290

AOCA 1 June 2022

MEMORANDUM FOR Naval Postgraduate School Defense Analysis Department
[Dr. Carter Malkasian]

SUBJECT: Naval Postgraduate School Student Capstone Sponsorship

1. PURPOSE: To provide endorsement from the 95th Civil Affairs Brigade (Special Operations) (Airborne) and sponsorship of the Information Sharing and Hosting Advanced Remote Ecosystem or Project ISHARE Capstone research at the Naval Postgraduate School (NPS), NSA Monterey, CA. The project team includes three Special Operations Officers: MAJ Patrick M. Foley (USA, CA), MAJ Peter L. Harris (USA, PO), and Capt Robert Stelmack (USAF, IO).

2. The 95th Civil Affairs Brigade (Special Operations) (Airborne) sponsorship will include, but not limited to, access to pertinent training material, events, information, and contacts that may assist in answering the posed research question: How can USSOCOM close the technology gap between our partners and us to retain the information advantage within the competition space? Additional requests for support from the unit will be coordinated with the Brigade Future Plans and Capabilities Directorate.

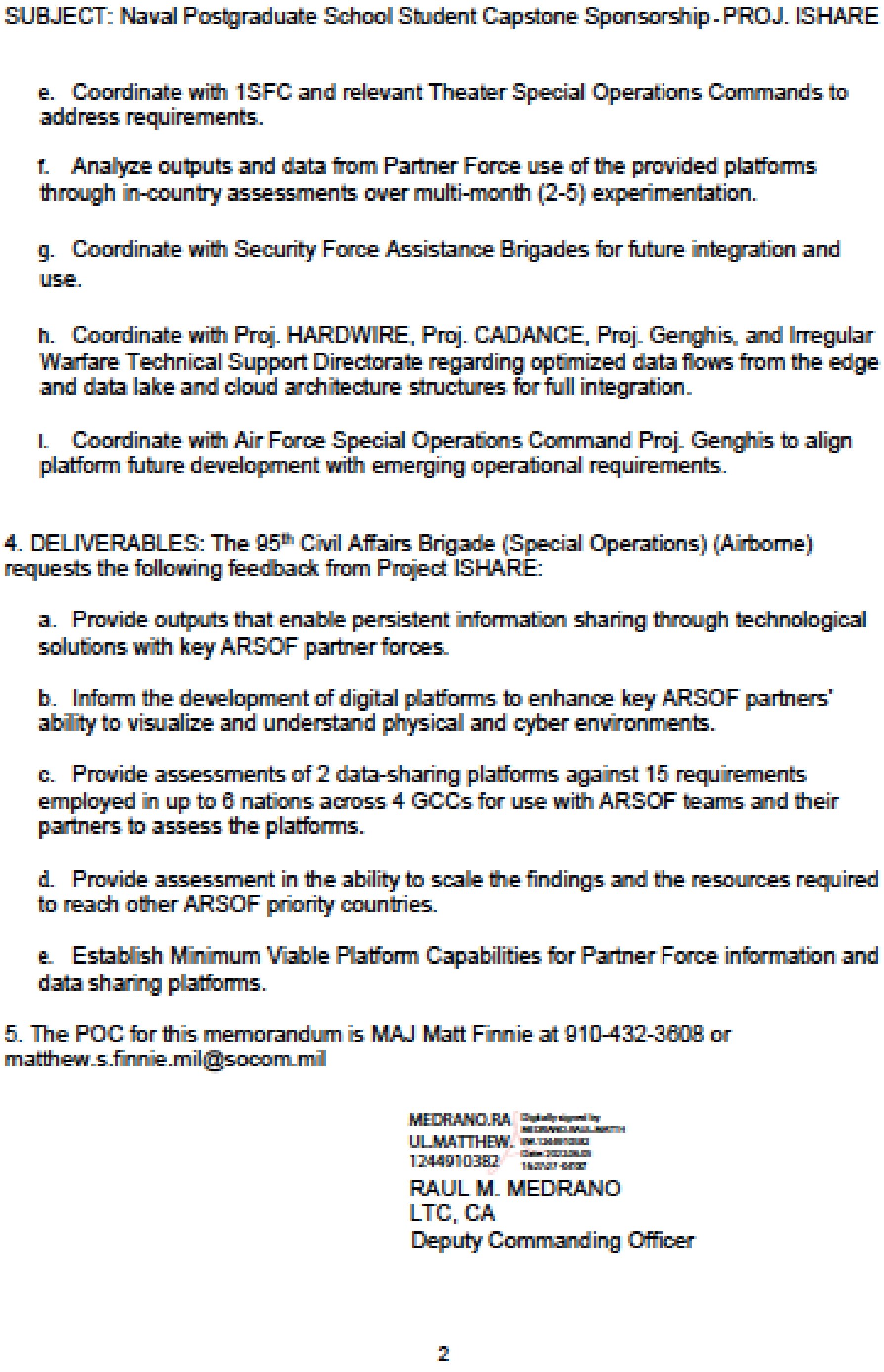
3. METHODOLOGY: The 95th Civil Affairs Brigade (Special Operations) (Airborne) supports the below methodology provided by the students:

a. Map the existing ecosystem of current and emerging information and data sharing, visual analytic, and digital COP tools available to U.S. and to Partner Forces.

b. Obtain and prioritize U.S. SOF requirements from across the force.

c. Establish CRADAs and/or contract usage agreements with selected platforms for use in research with Partner Forces and U.S. SOF teams.

d. Identify the extent of Partner Forces digital gaps and current requirements through surveys and interviews with foreign partners and U.S. SOF teams, during scoping trips to key nations. There is no expectation for the 95th to provide funding for such scoping trips. Future funding options by the 95th are not restricted and will be assessed upon request from the research team.



e. Coordinate with 1SFC and relevant Theater Special Operations Commands to address requirements.

f. Analyze outputs and data from Partner Force use of the provided platforms through in-country assessments over multi-month (2-5) experimentation.

g. Coordinate with Security Force Assistance Brigades for future integration and use.

h. Coordinate with Proj. HARDWIRE, Proj. CADANCE, Proj. Genghis, and Irregular Warfare Technical Support Directorate regarding optimized data flows from the edge and data lake and cloud architecture structures for full integration.

I. Coordinate with Air Force Special Operations Command Proj. Genghis to align platform future development with emerging operational requirements.

4. DELIVERABLES: The 95th Civil Affairs Brigade (Special Operations) (Airborne) requests the following feedback from Project ISHARE:

a. Provide outputs that enable persistent information sharing through technological solutions with key ARSOF partner forces.

b. Inform the development of digital platforms to enhance key ARSOF partners' ability to visualize and understand physical and cyber environments.

c. Provide assessments of 2 data-sharing platforms against 15 requirements employed in up to 6 nations across 4 GCCs for use with ARSOF teams and their partners to assess the platforms.

d. Provide assessment in the ability to scale the findings and the resources required to reach other ARSOF priority countries.

e. Establish Minimum Viable Platform Capabilities for Partner Force information and data sharing platforms.

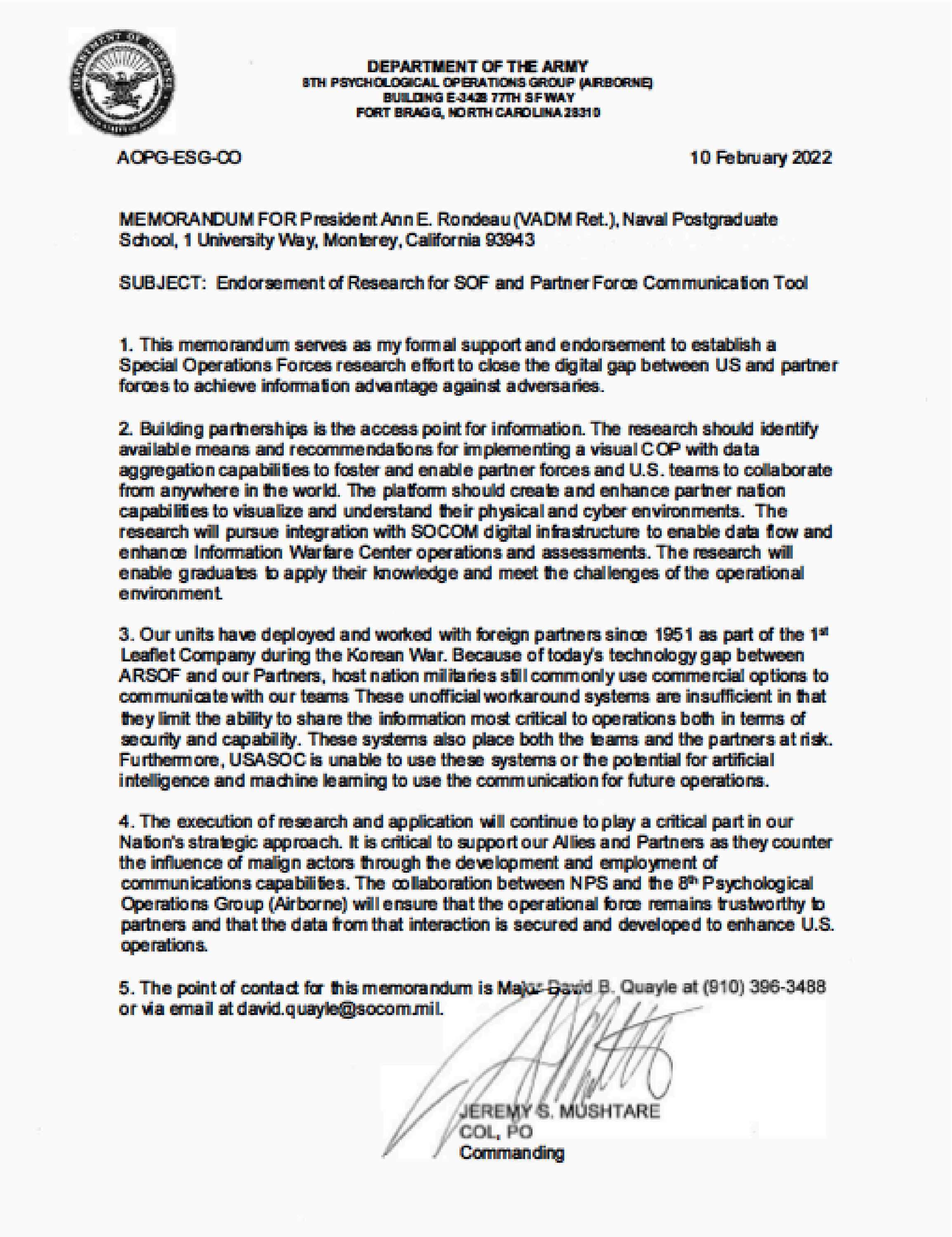
5. The POC for this memorandum is MAJ Matt Finnie at 910-432-3608 or matthew.s.finnie.mil@socom.mil

MEDRANO.RA
UL.MATTHEW.
1244910382

Digitally signed by
[illegible]

RAUL M. MEDRANO
LTC, CA
Deputy Commanding Officer

B. 8TH PSYCHOLOGICAL OPERATIONS GROUP (AIRBORNE)



DEPARTMENT OF THE ARMY
8TH PSYCHOLOGICAL OPERATIONS GROUP (AIRBORNE)
BUILDING E-3428 77TH SF WAY
FORT BRAGG, NORTH CAROLINA 28310

AOPG-ESG-CO 10 February 2022

MEMORANDUM FOR President Ann E. Rondeau (VADM Ret.), Naval Postgraduate School, 1 University Way, Monterey, California 93943

SUBJECT: Endorsement of Research for SOF and Partner Force Communication Tool

1. This memorandum serves as my formal support and endorsement to establish a Special Operations Forces research effort to close the digital gap between US and partner forces to achieve information advantage against adversaries.

2. Building partnerships is the access point for information. The research should identify available means and recommendations for implementing a visual COP with data aggregation capabilities to foster and enable partner forces and U.S. teams to collaborate from anywhere in the world. The platform should create and enhance partner nation capabilities to visualize and understand their physical and cyber environments. The research will pursue integration with SOCOM digital infrastructure to enable data flow and enhance Information Warfare Center operations and assessments. The research will enable graduates to apply their knowledge and meet the challenges of the operational environment.

3. Our units have deployed and worked with foreign partners since 1951 as part of the 1st Leaflet Company during the Korean War. Because of today's technology gap between ARSOF and our Partners, host nation militaries still commonly use commercial options to communicate with our teams These unofficial workaround systems are insufficient in that they limit the ability to share the information most critical to operations both in terms of security and capability. These systems also place both the teams and the partners at risk. Furthermore, USASOC is unable to use these systems or the potential for artificial intelligence and machine learning to use the communication for future operations.

4. The execution of research and application will continue to play a critical part in our Nation's strategic approach. It is critical to support our Allies and Partners as they counter the influence of malign actors through the development and employment of communications capabilities. The collaboration between NPS and the 8th Psychological Operations Group (Airborne) will ensure that the operational force remains trustworthy to partners and that the data from that interaction is secured and developed to enhance U.S. operations.

5. The point of contact for this memorandum is Major David B. Quayle at (910) 396-3488 or via email at david.quayle@socom.mil.

JEREMY S. MUSHTARE
COL, PO
Commanding

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. LIMITED PURPOSE-COOPERATIVE RESEARCH AND DEVELOPMENT AGREEMENTS

A. KESTREL TECHNOLOGY GROUP, LLC.

The Limited Purpose-Cooperative Research and Development Agreement (LP-CRADA) identified the responsibilities of KTG to be provided to the Naval Postgraduate School research team. The LP-CRADA guaranteed the proper support for this research initiative including technical support, capability briefs, platform familiarization, and equipment. The legal framework also included stipulations to grant KTG access to the findings and recommendations from research.

B. RAYTHEON TECHNOLOGIES BBN

A legal review by multiple parties determined that a Limited Purpose-Cooperative Research and Development Agreement (LP-CRADA) was not required with Raytheon BBN. Raytheon BBN is under contract with the Irregular Warfare Technical Support Directorate (IWSTD) within DOD to produce the CKI-TAK plug in. Under the perimeters of this existing contract, the 95th CA BDE (SO) (A) and IWTSD are permitted to grant use and access to the platform to any group or organization they deem necessary for the purposes of testing and evaluations. This was confirmed with IWTSD representatives on April 8, 2022, and confirmed by Raytheon BBN representatives on the same day. These confirmations were provided via email correspondence. The existing contract between IWTSD and Raytheon BBN identified the responsibilities of Raytheon BBN. The agreement included details of what equipment, software, accounts, and technical support would be provided to IWSTD, the 95th CA BDE (SO) (A) and all other assessment teams. The sponsorship agreement with the 95th CA BDE (SO) (A) served to agreement the Raytheon BBN contract to outline responsibilities of the NPS research team within that framework, including the documents and feedback due back to Raytheon to enhance further research and development of information-sharing technologies.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL 1. SURVEYS

A link is available to this supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

A. NPS U.S. STUDENT PRE-USE QUESTIONNAIRE

The questionnaire requested the facts and organizational information that describe partner force information-sharing platforms and practices. The questions also elicited information to understand factors that contribute to globally connected information-sharing platforms.

B. NPS INTERNATIONAL STUDENT PRE-USE QUESTIONNAIRE

This set of questionnaires, given to over 25 nations, inquired about information-sharing practices and platforms in use by international units represented at NPS. The questionnaires also requested information regarding inter-organizational communication of armed forces and the extent of foreign technology in use within host-nation countries. Questions were based on 15 criteria listed in Supplemental 5. Criteria to assess institutional effectiveness of information sharing. This pre-use questionnaire was used with international participants both at NPS and in the Philippines.

C. CKI-TAK POST-USE QUESTIONNAIRE

This questionnaire allowed respondents to assess CKI-TAK platform functionality for operational use based on organizational, intelligence, and targeting requirements. Data-sharing platforms were compared to alternate methods of information sharing. Participants were asked to evaluate use of the tools through questions developed based on the 15 assessment criteria the research team developed in consultation with subject matter experts and SOF personnel. The assessment criteria can be found in Supplemental 5. Criteria.

D. FIST POST-USE QUESTIONNAIRE

This questionnaire allowed respondents to assess FIST platform functionality for operational use based on organizational, intelligence, and targeting requirements. Data-sharing platforms were compared to alternate methods of information sharing.

Participants were asked to evaluate use of the tools through questions developed based on the 15 assessment criteria the research team developed in consultation with subject matter experts and SOF personnel. The assessment criteria can be found in Supplemental 5. Criteria.

SUPPLEMENTAL 2. QUESTIONNAIRE RESULTS

A link is available to this supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

Supplemental 2. Questionnaire Results is a spreadsheet compilation of raw numbers and comments recorded from survey participants. These survey results provided the foundation of data for the project metrics, and proved foundational for creating Supplemental 3. Data Charts. All possible individual identifiers were omitted from the spreadsheet. Sheets include average score comparisons for applicable individual questions.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL 3. DATA CHARTS

A link is available to this Supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

Supplemental 3. Data Charts contains over 60 charts to show the raw data-aggregation comparisons from each of the pre-use and post-use survey data sets. The charts represent responses from many of the questions asked to U.S. NPS, International NPS, and Philippine study participants.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL 4. SCENARIO PACKET

A link is available to this Supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

Supplemental 4. Scenario Packet contains a cover sheet and nine scenarios that describe Civil-Military response and evaluation situations. Each scenario was used in conjunction with demonstration and assessment to validate platform utility, and to allow participants to get experience with each platform.

THIS PAGE INTENTIONALLY LEFT BLANK

SUPPLEMENTAL 5. CRITERIA

A link is available to this Supplemental file with the main thesis's catalog entry in the NPS Institutional Archive, Calhoun, or by contacting the NPS library.

Supplemental 5. Criteria describes the assessment criteria that inform acquisition and evaluation of unclassified digital common operation picture systems by capability. The spreadsheet gives operations professionals a rubric for evaluating the types of actions performed by information sharing platforms, and the subcomponents of each category.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Allison, Graham T. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston: Houghton Mifflin Harcourt, 2017.

Bacon, John. "Someone in China Could Be Reading Your Texts." *USA Today*, November 16, 2016. https://www.usatoday.com/story/tech/2016/11/16/someone-china-could-reading-your-texts/93951846/.

Bandy, Daniel W., Jay D. Parsons, Aaron L. Goldan, and Eric A. Mitchell. "Joint Operations Center Tactical Assault Kit (JOCTAK): Evolution Toward Scalable Multilateral SOF C4I." Master's thesis, Naval Postgraduate School, n.d. http://hdl.handle.net/10945/61230.

BBC News. "Taiwan Says 19 Chinese Warplanes Entered Air Defence Zone." BBC News, September 6, 2021. https://www.bbc.com/news/world-asia-58459128.

Biden Jr., Joseph R. *Interim National Security Strategic Guidance*. Washington, DC: White House, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

———. *National Security Strategy*. Washington, DC: White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Blanken, Leo, Romulo G. Dimayuga II, and Kristen Tsolis. "Making Friends in Maker-Spaces: From Grassroots Innovation to Great-Power Competition." War on the Rocks, January 12, 2021. https://warontherocks.com/2021/01/making-friends-in-maker-spaces-from-grassroots-innovation-to-great-power-competition/.

Boot, Max. *War Made New: Weapons, Warriors, and the Making of the Modern World*. New York: Gotham Books, 2007.

Brodie, Bernard. *The Anatomy of Deterrence*. RR-RM2218. Santa Monica, CA: RAND Corporation, 1958. https://www.rand.org/pubs/research_memoranda/RM2218.html.

Brose, Christian. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York: Hachette Books, 2020.

Brunnstrom, David, and Trevor Hunnicutt. "Biden Says U.S. Forces Would Defend Taiwan in the Event of a Chinese Invasion." Reuters, September 19, 2022. https://www.reuters.com/world/biden-says-us-forces-would-defend-taiwan-event-chinese-invasion-2022-09-18/.

Bush, Richard C. *The United States Security Partnership with Taiwan*. Washington, DC: Brookings Institution, 2016. https://www.brookings.edu/research/the-united-states-security-partnership-with-taiwan/.

Business Wire. "Palantir Awarded $111m Contract to Provide Mission Command Platform for the United States Special Operations Command." Business Wire, May 28, 2021. https://www.businesswire.com/news/home/20210528005069/en/Palantir-Awarded-111m-Contract-to-Provide-Mission-Command-Platform-for-the-United-States-Special-Operations-Command.

Cancian, Matthew. "Stop Undermining Partners with 'Gifts.'" War on the Rocks, December 13, 2021. https://warontherocks.com/2021/12/stop-undermining-partners-with-gifts/.

CBS News. "Biden Tells 60 Minutes U.S. Troops Would Defend Taiwan, but White House Says This Is Not Official U.S. Policy." CBS News, September 18, 2022. https://www.cbsnews.com/news/president-joe-biden-taiwan-60-minutes-2022-09-18/.

Central News Agency. "U.S., Taiwan Launch Disaster Preparedness Cooperation." Focus Taiwan, March 11, 2021. https://focustaiwan.tw/politics/202103110004.

Cerulus, Laurens. "EU Commission to Staff: Switch to Signal Messaging App." *POLITICO*, February 20, 2020. https://www.politico.eu/article/eu-commission-to-staff-switch-to-signal-messaging-app/.

Chang-Liao, Nien-chung, and Chi Fang. "The Case for Maintaining Strategic Ambiguity in the Taiwan Strait." *Washington Quarterly* 44, no. 2 (2021): 45–60. https://doi.org/10.1080/0163660X.2021.1932088.

Chen, Kelvin. "US Special Forces to Train Taiwan Soldiers after Annual War-Games." *Taiwan News*, May 31, 2021. https://www.taiwannews.com.tw/en/news/4213647.

Cheravitch, Joe. "Cyber Threats from the U.S. and Russia Are Now Focusing on Civilian Infrastructure." *The RAND Blog* (blog), July 23, 2019. https://www.rand.org/blog/2019/07/cyber-threats-from-the-us-and-russia-are-now-focusing.html.

Crombe, Katie, Steve Ferenzi, and Robert Jones. "Integrating Deterrence across the Gray—Making It More than Words." *Military Times*, December 9, 2021, sec. Commentary. https://www.militarytimes.com/opinion/commentary/2021/12/08/integrating-deterrence-across-the-gray-making-it-more-than-words/.

Daniels, Tommy, and Aaron Honn. "To Keep Pace with Rivals, Analyze the Competition Space." *War Room* (blog), October 20, 2022. https://warroom.armywarcollege.edu/articles/competition-space/.

Defense Security Cooperation Agency. “Humanitarian Assistance and Disaster Relief.” DSCA AT 50, September 14, 2021. https://www.dsca.mil/50th-anniversary/humanitarian-assistance-and-disaster-relief.

Department of Defense. *Online Information Management and Electronic Messaging*. DoDI 8170.01. Washington, DC: Department of Defense, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf.

Dorasamy, Magiswary, Murali Raman, and Maniam Kaliannan. “Knowledge Management Systems in Support of Disasters Management: A Two Decade Review.” *Technological Forecasting and Social Change*, Planning and Foresight Methodologies in Emergency Preparedness and Management, 80, no. 9 (November 2013): 1834–53. https://doi.org/10.1016/j.techfore.2012.12.008.

Hamel, Brian. “Using MAGE to Facilitate Mission Command in USSOUTHCOM’s Response to Hurricane Eta.” *Eumonia Journal*, September 23, 2021. https://www.civilaffairsassoc.org/post/using-mage-to-facilitate-mission-command-in-ussouthcom-s-response-to-hurricane-eta.

Heath, Timothy R. *The Consolidation of Political Power in China under Xi Jinping: Implications for the PLA and Domestic Security Forces.* Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/testimonies/CT503z1.html.

iNewswire. “Trace Systems Awarded All Partners Access Network Support Task Order by the Defense Information Systems Agency in Support of the United States Air Force.” Digital Journal, January 24, 2022. https://www.digitaljournal.com/pr/trace-systems-awarded-all-partners-access-network-support-task-order-by-the-defense-information-systems-agency-in-support-of-the-united-states-air-force.

Irregular Warfare Technical Support Directorate. “Full Spectrum—Remote Advise and Assist—Virtual Accompany Kit.” Irregular Warfare Technical Support Directorate, February 1, 2022. https://www.tswg.gov/Projects/I2C/Remote_Advise_Assist.html.

Kim, Giyoon, Soram Kim, Myungseo Park, Younjai Park, Insoo Lee, and Jongsung Kim. “Forensic Analysis of Instant Messaging Apps: Decrypting Wickr and Private Text Messaging Data.” *Forensic Science International: Digital Investigation* 37 (June 2021): 1–11. https://doi.org/10.1016/j.fsidi.2021.301138.

Lead Inspector General. *Operation PACIFIC EAGLE-PHILIPPINES: Lead Inspector General Report to the U.S. Congress*. Washington, DC: Lead Inspector General, 2022. https://oig.usaid.gov/sites/default/files/2020-11/OPE-P_Philippines%20Lead%20Inspector%20General%20Report%20to%20the%20Congress%20of%20the%20United%20States%2C%20July%201%2C%202020%20-%20September%2030%2C%202020_Q4_Sep2020.pdf.

Leister, Janice. "Pacific Partnership 2021 Mission Concludes in Palau." U.S. Indo-Pacific Command, August 13, 2021. https://www.pacom.mil/Media/News/News-Article-View/Article/2731776/pacific-partnership-2021-mission-concludes-in-palau/.

Lendon, Brad. "Chinese Threat to Taiwan 'closer to Us than Most Think,' Top U.S. Admiral Says." CNN, March 24, 2021. https://www.cnn.com/2021/03/24/asia/indo-pacific-commander-aquilino-hearing-taiwan-intl-hnk-ml/index.html.

Lewis, James Andrew. *National Security and the Innovation Ecosystem*. Washington, DC: Center for Strategic & International Studies, 2021. https://www.csis.org/analysis/national-security-and-innovation-ecosystem.

Lynch, Justin. "Yet Another Article about Information Technology and the Character of War." War on the Rocks, September 2, 2020. https://warontherocks.com/2020/09/yet-another-article-about-information-technology-and-the-character-of-war/.

Mazza, Michael. "Imagining a New U.S. Military Presence in Taiwan." American Enterprise Institute Op-Ed, May 17, 2020. https://www.aei.org/op-eds/imagining-a-new-us-military-presence-in-taiwan/.

Moore, Blake, and Jan E. Tighe. "Insecure Communications Like WhatsApp Are Putting U.S. National Security at Risk." Nextgov.com. Accessed January 31, 2022. https://www.nextgov.com/ideas/2020/12/insecure-communications-whatsapp-are-putting-us-national-security-risk/170577/.

Moore, Blake, and Jan E. Tighe. "Insecure Communications Like WhatsApp Are Putting U.S. National Security at Risk." Nextgov, December 8, 2020. https://www.nextgov.com/ideas/2020/12/insecure-communications-whatsapp-are-putting-us-national-security-risk/170577/.

National Intelligence Counsel. *Global Trends 2040: A More Contested World*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.dni.gov/index.php/gt2040-home.

Nye, Joseph S. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs, 2004.

O'Hanlon, Michael E. "An Asymmetric Defense of Taiwan." *Order from Chaos* (blog), April 28, 2021. https://www.brookings.edu/blog/order-from-chaos/2021/04/28/an-asymmetric-defense-of-taiwan/.

Price, Ned. "PRC Military Pressure against Taiwan Threatens Regional Peace and Stability." U.S. Department of State Press Releases, September 12, 2021. https://www.state.gov/prc-military-pressure-against-taiwan-threatens-regional-peace-and-stability/.

Rogin, Josh. “To Avoid Conflict, the United States Must Deter Chinese Aggression: The U.S. Must Adjust Its Strategy as China Races Forward.” *Washington Post*. 2019. https://www.washingtonpost.com/opinions/global-opinions/to-avoid-conflict-the-united-states-must-deter-chinese-aggression/2019/06/06/400b8ef0-8899-11e9-98c1-e945ae5db8fb_story.html.

Sacks, David. “China’s Huawei Is Winning the 5G Race. Here’s What the United States Should Do to Respond.” *Net Politics* (blog), August 8, 2021. https://www.cfr.org/blog/china-huawei-5g.

Schupp, Phil, Sverre Wetteland, and Paddy Ferriter. “ADAPT: Tactical Assault Kit: Collaborative Mission Planner.” Monterey, CA: Naval Postgraduate School, November 2017. http://hdl.handle.net/10945/56573.

Serbu, Jared. “DOD’s New R&D Chief Prioritizes Moving Prototypes to Real-World Applications.” Federal News Network, October 25, 2021. https://federalnewsnetwork.com/on-dod/2021/10/dods-new-rd-chief-prioritizes-moving-prototypes-to-real-world-applications/.

Singer, P. W., and Emerson T. Brooking. *Likewar: The Weaponization of Social Media*. Boston: Houghton Mifflin Harcourt, 2018.

Sullivan, Kyle. “Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure.” *Cyber Defense Review* 6, no. 3 (Summer 2021): 109–18. https://www.jstor.org/stable/48631158.

Thesys. *Humanitarian Assistance and Disaster Relief (HADR) Health Support NMD*. Taipei: Medical Affairs Bureau, 2021. http://mab.mnd.gov.tw/.

Thielenhaus, Christopher, and Eric Roles. “Virtual Accompany Kits Return to Baghdad: A View from the Front Lines.” *Special Warfare* 30, no. 2 (June 2017): 26–29. http://hdl.handle.net/10945/55178.

Thompson, Loren. “Taiwan Tripwire: A New Role for the U.S. Army In Deterring Chinese Aggression.” *Forbes*, August 25, 2021. https://www.forbes.com/sites/lorenthompson/2021/03/26/taiwan-tripwire-a-new-role-for-the-us-army-in-deterring-chinese-aggression/.

Tian, Yew Lun, and Yimou Lee. “China Drops Word ‘peaceful’ in Latest Push for Taiwan ‘Reunification.’” Reuters, September 12, 2021. https://www.reuters.com/article/us-china-parliament-taiwan/china-drops-word-peaceful-in-latest-push-for-taiwan-reunification-idUSKBN22Y06S.

Tidwell, Alan. “Being a Better Partner in the Pacific.” War on the Rocks, January 28, 2022. https://warontherocks.com/2022/01/being-a-better-partner-in-the-pacific/.

U.S. Army Combined Arms Center. “Army Knowledge Management Proponent (AKM).” U.S. Army Combined Arms Center, September 14, 2021. https://usacac.army.mil/organizations/mccoe/akm.

Williams, Brad D. “To Transform Tech, DOD Must Stop Being An ‘Innovation Tourist:’ Report.” *Breaking Defense* (blog), July 29, 2021. https://breakingdefense.sites.breakingmedia.com/2021/07/to-transform-tech-dod-should-stop-being-an-innovation-tourist-report/.

Zember, Christopher, and Peter Khooshabeh. “Defense Innovation Is Falling Short.” War on the Rocks, December 15, 2021. https://warontherocks.com/2020/09/defense-innovation-is-falling-short/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California