Reaching Forward in the War against the Islamic State

BY CHRISTOPHER THIELENHAUS, PAT TRAEGER, AND ERIC ROLES

Just like any other night…

The Iraqi Special Operations Forces (ISOF) Ground Force Commander surveys the farmland in front of him. His unit of ISOF soldiers has just captured two ISIL Commanders (Islamic State of Iraq and the Levant) at a house 50 kilometers from Baghdad—far enough away to put this unit in danger of being overrun if ISIL fighters respond quickly. He knows that his enemies must have received the call to arms only minutes ago, and are on the way to his location.

He commands his soldiers to be prepared for contact at any moment while he pulls out his cell phone. As cell phones go, this is a good one. He holds one of the newest Samsung Galaxy Note phones, but it is more than just a phone for this Commander—his device is securely linked back to U.S. special operations advisors. He quickly pulls up the MyTrax application and types out a quick message to his Operations Center: "Jackpot," he has captured his high value targets for this mission. As soon as he hits "send," he hears the staccato pop of gunfire to his left.

ISIL has arrived with what sounds like at least 20 fighters. Taking cover with his phone still in his hand, he taps a location for the enemy force and hits "share." An enemy infantry icon pops onto the screen on his phone, as well as every other connected phone that his subordinate leaders are carrying. The operations center receives this icon too, and the American special forces soldiers advising this mission in Baghdad start preparing for a close air support request. The Iraqi

Major Christopher Thielenhaus is a Special Forces Officer currently serving as a student at the Naval Postgraduate School. Mr. William Traeger is a retired Special Forces Sergeant Major currently serving as the Chief of Technology Operations at Special Operations Command Central (SOCCENT), where he has served since 2009. Major Eric Roles is a Special Forces Officer currently serving as a student at the Naval Postgraduate School.

Commander taps the screen on his phone again to bring up the 9-line air support request form, quickly entering the data for the enemy force and sending it immediately to his American advisors in the operations center. Fifteen minutes later, a Coalition F-16 arrives and drops multiple bombs directly on the target—all remotely and thoroughly coordinated by Coalition special operations advisors and fires elements. With the brief respite, the Iraqi Commander gathers his force, packs up his detainees, and returns to Baghdad before more ISIL fighters can arrive. His mission is a success.

Only 10 years ago, this brief vignette would have been consigned to the pages of science fiction or futurist military thrillers, but it is now the reality on the ground in Iraq. Similar scenarios play out every week with U.S.- and Coalition-advised ISOF troops taking the lead in combat operations using cellular communications systems that link them back to their Coalition advisors. This ability to "reach forward" by Coalition special operations forces (SOF) personnel represents a true evolution in the ability of U.S. and Coalition special operations advisors to be true force multipliers on the 21st century battlefield. Currently, this technology is in prototype phase in Iraq, but the current spate of low intensity conflicts makes this type of capability more important than ever.[1] The annually published Army Operating Concept describes an increasing dependence upon Special Warfare to contest irregular threats in the current resource and policy constrained environment.[2] The application of this technology increases U.S. SOF ability to respond to these threats. Like many technological achievements in the last 100 years, however, this requirement originated from military crisis: the relentless march of ISIL in the summer of 2014.[3]

Day Donaldson

In 2014, ISIL caught the world surprise, taking over large swaths of land in Iraq and Syria in an attempt to form a caliphate.

An Inauspicious Start

In June 2014 the Islamic State of Iraq and the Levant (ISIL) had just started its rampage across the northern and western provinces of Iraq. Iraqi forces were falling back on every front, yielding more and more ground to ISIL as it relentlessly marched to Baghdad. In this chaotic situation, a small special operations element that included less than 50 U.S. Army special forces soldiers deployed to Baghdad International Airport to support the U.S. embassy in the event of crisis escalation. Arriving on the ground, this force quickly realized the volatility of the environment and challenges in supporting the U.S. embassy, and immediately opened dialogue with their former ISOF partners to see what effects they could have to help slow the ISIL advance. Unlike their Iraqi conventional force brethren, the ISOF units were still mostly intact and regularly carrying out effective combat operations. ISOF at this time were clearly displaying the fruits of 10 years of U.S. special forces training and partnership, resulting in a professional, motivated, and battle-tested Iraqi special operations unit. Although low on personnel and equipment, the long relationship between ISOF and U.S. special operations had yielded a command climate within ISOF that valued mission success, efficiency, and the innovative use of technology to achieve unit objectives. ISOF Commanders desperately wanted the assistance, both technical and tactical, that U.S. special forces could bring, but U.S. policy at that time limited U.S. forces involvement in the fight against ISIL. The special forces soldiers on the ground would have to be creative.

From this situation, the concept of "Remote Advise and Assist" (RAA) was born. The special forces soldiers realized that an "advise and assist" effort was necessary, but would only be possible by scaling up their forward reach with their partners; this could only be done remotely given the U.S. policies that restricted them from directly accompanying ISOF soldiers into combat. Incidentally, ISOF units already used several Android applications—Offline Maps, Google Earth, and Viber, to name a few—which allowed them to bring tablets and phones on their operations to help communicate, conduct reconnaissance and targeting, track their movements, and better navigate the old and complex road networks in the areas surrounding Baghdad. As a result, ISOF leadership was very well versed in using technology, especially cell phones, to assist both their planning and execution.

Fortunately, the special forces soldiers that had arrived in country were already trained in an Android cell phone program developed by the U.S. Government called "ATAK," short for "Android Tactical Assault Kit."[4] This program allows an android phone user to maintain collective situational awareness, communicate and coordinate with other users, quickly tap out commands, text messages, enemy/friendly locations, and even full 9-line calls for fire. It is an exceptionally powerful and user-friendly program that is rapidly evolving within the U.S. military, and specifically within the U.S. Special Operations Command. With this knowledge, the special forces soldiers quickly realized that a program like ATAK combined with the existing technical competence of the ISOF could yield significant battlefield results.

Stemming from this realization, the special forces Troop Commander in Iraq contacted the Special Operations Command, Central (SOCCENT) J3 Operations Technology Directorate with a request to fill an immediate

operational need for Remote Advise and Assist kits. In the meantime, the special forces soldiers in Baghdad assembled ad hoc kits using U.S., ISOF, and locally procured components. By using the very limited domestic terrestrial cellular networks, and by providing an alternate means of tracking with Frontier iridium GPS trackers that were linked into the system, these ad hoc kits provided an initial Remote Advise and Assist capability that enabled the special forces advisors to track, communicate, and share limited data with ISOF partners. The ad hoc capability greatly increased ISOF confidence during operations, as U.S. advisors were able to provide some measure of support to ISOF operations. Application of this ad hoc capability quickly resulted in the capture of several high-value ISIL targets.

Within 90 days of the request from Iraq, the SOCCENT J3 Operations Technology Directorate was able to prototype several "Virtual Accompany Kits" from off-the-shelf technology and deploy the kits to Iraq. The prototype kits used Samsung cell phones preloaded with the software program MyTrax, a multinational, releasable, International Traffic in Arms Regulations (ITAR) compliant version of ATAK. The phones worked on the Iraqi domestic cell phone network, but these kits also securely linked the forward cell phones with a portable Broadband Global Area Network (BGAN) satellite communications node, which is a standard issue piece of computer equipment that creates a local computer network for a special operations detachment. The BGAN would then transport data from the cell phones back to an operations center even when the phones were in austere areas out of Iraqi domestic cellular range. Armed with this system, and shortly after receiving authorization to conduct kinetic strikes in support of Iraqi forces, the special forces soldiers and ISOF units went to work. The first several operational employments of "virtual accompany kit" –enabled, U.S.-advised ISOF operations resulted in hundreds of ISIL enemies killed from coalition airstrikes. To date, the number of enemies killed from Remote Advise and Assist operations has grown into the thousands.

Combined Joint Task Force-Iraq Arrives on the Ground

Fast forward to February 2015: U.S. and Coalition forces have arrived in greater numbers to Iraq, and have partially succeeded in the primary task ordered by the Combined Joint Task Force (CJTF) Commander (the overall Commander in Iraq) which was simply to "stop the bleeding" of Iraqi forces.[5] There is now a demarcated front separating the regions controlled by ISIL and the Iraqi government. The situation is stable enough that U.S. and Coalition forces have set up headquarters at the Baghdad Airport and the U.S. embassy. It is at this time that special operations gets a major upgrade with the arrival of the 1st Special Forces Group, which assumed the role of Combined Joint Special Operations Task Force – Iraq (CJSOTF-I). This new CJSOTF was to take command of the myriad of coalition special operations task forces then operating in Iraq, as well as provide a legitimate planning and fires cell for on-going operations. Shortly after arrival, the fires cell specialists realized that they would not have the authority to deliver aerial ordnance at their level, so they re-prioritized their efforts. All the fires personnel from CJSOTF had been training with the ATAK application for the past year, and were very familiar with its use. Shortly after arriving, they received the briefings on the Remote

Advise and Assist kits and immediately realized that supporting the use of these kits would be their new priority effort.

By the time CJSOTF-I arrived in Iraq, the Remote Advise and Assist kits had been in the hands of the ISOF for over four months. In that short time, their U.S. and Coalition partners had tracked hundreds of sorties flown, missions executed, and thousands of enemies killed as a result of the kits' assistance.[6] The utility of the kits was not in question; they were performing at an extremely high level, to the point that their green force tracking ability was the primary method of battle-tracking being used by the ISOF on the ground in terms of verifying friendly locations when authorizing airstrikes. The CJSOTF-I fires personnel accordingly built a fires cell that could collate all of the information coming in from the kits. This allowed them to establish a common operating picture with far more granularity than what was standard at the time. In the timespan of only a little over a month, the common operating picture produced at CJSOTF-I came to be the most reliable source of information on ISOF partner movement in Iraq, providing a level of clarity that simply could not be reproduced through pure radio, cell phone, iridium tracker, or iridium phone contact with Iraqi partners.

CJSOTF-I paved the way for wide adoption of the Remote Advise and Assist concept by making it a key part of the special operations common operating picture. As operations evolved, such as the Iraqi attack on Tikrit and defense of Anbar, the CJSOTF-I was able to provide timely and relevant positional information to the overall U.S. commander that gave as clear a picture as was possible without American boots on the ground. This ability to better see and understand the Iraqi forces' situation greatly increased the ability of U.S. forces as a whole to support the Iraqi military. The concept of remotely advising and assisting partner forces had become a key portion of the CJSOTF-I strategy.

The success of the Remote Advise and Assist concept was the result of a multipronged effort by U.S. and Coalition special operations personnel to make an impact on the battlefield despite the limitations that they faced. This required creative adaptation of existing technology to fit an operational need. To successfully operate the equipment once it arrived, however, the special operations forces in Iraq had to develop a concept prior to even making a request. It was this concept, and its development process, that ultimately led to success.

The Remote Advise and Assist (RAA) Concept

At their core, the RAA kits are a system of integrated technologies that provide a vastly improved method for interfacing with and supporting a partner force. The current prototypes involve securely connected cellular and satellite communications technology, but the concept is not restricted to this particular construct. This concept structure is deceptively simple, but in execution it is highly technical. ATAK, MyTrax, and derivative programs provide the map technology, user interface, and a collaboration environment with additional military capabilities, such as the ability to text, call for fire, and share iconography among the phones and operations centers. Secure "backhaul" methods (that is, the method of transporting data from the phones to the remotely located operations centers, beyond line of sight) are the most important aspects of the kits. The technologies for all parts of the RAA

kits exist, but are not typically combined in the structure that the SOCCENT J3 Operations Technology Directorate put together in the prototype.

These systems, however, provide a level of clarity in the combined common operating picture that was infeasible with previous technology. With RAA kits, the U.S. advisors are able to communicate and receive immediate, up-to-the-second updates from their partner leaders during missions.

The commercial mobile devices integrated into the RAA nodes allow the leaders to carry the equivalent of an enhanced, user friendly Force XXI Battle Command Brigade and Below (FBCB2) system in the palm of their hands, as opposed to the bulky system that is confined to the passenger seat of military trucks. Similar to the functions that the FBCB2 system provides, ATAK, MyTrax and derivative programs allow users to generate a complete 9-line fires request for either aerial delivery or traditional artillery, all while doing the mathematical computations for the user. Combining this capability with a proficiently trained aerial fires specialist from the partner force leads to an unprecedented ability to deliver and control fire support in a reliable manner. This

U.S. Army

Applications like MyTrax and ATAK are replacing the original communications systems like the Force XXI Battle Command Brigade and Below FBCB2 computer and display, above in a Humvee.

capability is not confined to the partner force leader. With the current prototypes, the partner force leader is able to have multiple subordinates carry the enabled mobile devices as well, further increasing battlefield clarity.

When introduced to the RAA concept and the components of the kits, a common question among Coalition special operators and commanders is that of information security. While the practice of securely transporting data communications over unclassified and untrusted networks (such as cellular networks) may seem like a new concept to many, this practice is well established and widely executed within the realms of special operations units and among the wider U.S. intelligence apparatus. The information security methods used in the RAA kits comply with the Department of Defense (DOD) and National Security Agency guidance and fall within the theater commander's authority to operate. The primary means of information security are very similar to the methods standard to tactical communications networks used widely within the DOD such as commercial encryption and administrative management of network devices. The RAA nodes are susceptible to the same types of disruption and intrusion that most DOD networks are vulnerable to—particularly radio frequency interference and jamming. In the event that RAA kits or components fall into the hands of enemies or are otherwise compromised, RAA network administrators have the ability to revoke all network access on all devices from the nodes. In some cases, RAA network administrators may be able to remotely operate compromised devices, which in turn may provide exploitation options for Coalition and partner commanders.

A key aspect of the RAA concept is that, while it is a significant enhancement to the special operators' and partner force's ability to command, control, communicate, and integrate, it is not a replacement for a special operator on the ground. In fact, RAA is an enabling concept that is completely dependent upon highly developed relationships and extensive partner force mastery of fundamental military and technical skills. The RAA concept works exceptionally well in Iraq because the ISOF were highly trained throughout a 10-year U.S. investment and combat advisory relationship that is now bearing fruit. Conversely, for a force that has little training and experience, or is learning directly from the participation of U.S. special operations forces, such as a guerilla force in its infancy or a recently created commando unit, the RAA concept is not appropriate for sole, unaccompanied partner use.

In these cases, both the partner force and their accompanying U.S. partners would carry RAA technology on the ground. This construct increases the common operating picture clarity while enhancing the U.S. special operators' ability to directly command and control an advisory mission. In many ways, this is the ideal use of the technology, but there are few places in the world today where U.S. forces have full authorities to participate in combat operations in conjunction with their partners. In areas where the U.S. will assume the risks associated with U.S. special operators accompanying their partner forces, this incredibly powerful and scalable option also mitigates and reduces those myriad risks.

A second key aspect of the RAA concept, however, is that it can apply to a wide variety of potential mission sets that are not direct combat. There are multiple potential scales

and iterations of RAA kits that would be appropriate for different mission sets. For example, a "low visibility" kit can support 3-5 users with a small wireless router that could easily be hidden inside of a vehicle or other power source, while a "high visibility" kit can support more than 100 users and provides a very high quality signal using commercial satellite connective equipment that even works while driving. Hypothetically, a "very high profile" kit could potentially support hundreds of users by establishing a cell phone tower capability using a military balloon to elevate a long-range communications node. Missions for these kits could range from overt information or civil affairs operations, to clandestine low-profile missions, all the way up to major combat operations in support of hundreds or thousands of multinational partnered users. A limiting factor with these options is cost of the equipment: the highest level RAA prototype currently costs approximately $500,000 and serves more than one hundred users. The cost of a small low signature kit that serves three to five users is approximately $50,000, making it a very viable option for a low cost, high payoff operation. The RAA concept is ultimately limited only by the user's imagination, and can be a critical command and control multiplier in any type of operation where an advising unit needs better integration and communication with a partner force. In this way, the RAA concept supports Department of Defense efforts to better integrate both technology and international partners in line with stated national security objectives.

Staff Sgt. Adam Mancini, U.S. Army

1st Lt. Jared Tomberlin, left, and an interpreter pull security on top of a mountain ridge during a reconnaissance mission near Forward Operating Base Lane in the Zabul province of Afghanistan.

RAA in Support of National Security Objectives

The Department of Defense derivatives of the current National Security Strategy of the United States[7] specifically state that technologies like the RAA concept will be a key aspect of future U.S. conflicts. The Joint Chiefs of Staff September 2012 "Capstone Concept for Joint Operations: Joint Force 2020," endorsed by the current Chairman of the Joint Chiefs of Staff, explicitly states that the future security environment will be characterized foremost by irregular warfare.[8] Additionally, the Army Special Operations Forces Operating Concept and the U.S. Special Operations Command 2020 future force structure concept both emphasize special warfare capability enhancement as one of a myriad of options to combat irregular threats.[9] These sources characterize the future strategic operating environment as persistently unstable with growing irregular threats, reduced U.S. military forces and resources, and constrained policies.

The June 2015 National Military Strategy is, perhaps, the foremost military document that most explicitly identifies technology challenges to the United States. The document emphasizes:

> *"Global disorder has significantly increased while our comparative military advantage has begun to erode. We now face multiple, simultaneous security challenges from traditional state actors and transregional networks of sub-state groups – all taking advantage of rapid technological change. Future conflicts will come more rapidly, last longer, and take place on a much more technically challenging battlefield. Success will increasingly depend on how well we enable our network of allies and partners."*[10]

This National Military Strategy clearly recognizes the gravity of effects of technology and the required utility of enabling partners to support U.S. national interests.[11] Though all of the cited national security documents clearly state that international partnership is the only way to overcome current challenges, none provide new ways to achieve a requisite scale of partnership. The RAA concept is one method to bridge that gap. It provides the "middle option" that makes special warfare a more viable alternative to solving national security crises.

RAA Research and Way Ahead

Understanding why RAA works and how it could be applied to missions outside of Iraq are the two fundamental subjects driving ongoing research efforts. To this end, the Naval Postgraduate School (NPS), supported by Special Operations Command Central (SOCCENT) and in conjunction with the Defense Advanced Research Projects Agency (DARPA), is executing a twofold study to examine the ideal conditions that determine successful application of the RAA concept as well as conducting an experiment by inserting and observing the effects of improved prototypes of the equipment into the battlefield. Specifically, the first aspect of this study will examine SOCCENT's recent application of the RAA concept in Iraq, identify conditions for U.S. and partner or surrogate forces that drive success, identify best practices, and catalyze the implementation of the concept and proliferation of requisite skills and equipment among special operators and their partners and surrogates. The second aspect of the study plans

will be an experiment to analyze the utility, scalability, and disproportionate effects of RAA by inserting advanced developments of RAA prototype nodes into active combat, simultaneously supporting SOCCENTs efforts to apply RAA regionally and to fight ISIL.

The study intends to answer three fundamental questions: (1) What are the conditions under which RAA is best utilized by special operators to fight effectively in an ever-increasing number of irregular wars with indigenous or partner nation personnel? (2) What conditions and prerequisites make RAA prone to succeed or fail? (3) What are the fundamental conceptual, physical, and technical frameworks for RAA?

This study is unique: the RAA concept is in active, limited, and ad hoc use on the battlefields of Iraq. However, no systematic research exists about the conditions and mechanisms that enable the concept to be effective. The study will gain atmospherics, technical data, and results of field experimentation directly from operators utilizing the prototype equipment in the field against an active enemy. The resulting yield of information has the potential to be exceptionally valuable, with a possibility of supporting expanded application of RAA. While the scope of the study is limited to the special operations application of RAA prototypes in several separate cases in Iraq, there is a high level of interest throughout the special operations community in this technology, as well as consideration for further application of the RAA concept in many other hot spot areas around the globe.

Conclusion

The RAA concept is not limited to improving partnered operational connectivity. In fact, it provides a breakthrough to address a systemic challenge facing special operations forces writ large. Special operations forces today face a difficult paradox: there is a growing need for scalable options to cope with an increasing number of irregular conflicts coupled with national policy constraints that limit the presence and effects that special operators can have on the ground.[12] The birthplace of the Remote Advise and Assist concept is certainly not the only applicable scenario for this technology. Irregular threats today are growing in scope and scale. RAA could be used to assist the Ukrainian military in combating Russian aggression by providing real time updates on separatist enclaves, battlefield movements, and other applications similar to how ISOF uses the technology against ISIL. For a more intelligence based approach, low visibility kits could accompany intelligence agents as they try to identify Iranian sponsored resistance groups, using the kit's suite of photographic, video, and reporting tools to send updates to a national intelligence center. From a defensive standpoint, the Republic of Korea could use this technology to track and neutralize North Korean clandestine activities below the 38th parallel. These are just a few examples, but they demonstrate the width and breadth of activity possible with this technology.

RAA provides a solution to this paradox by making special warfare a viable option even when direct boots-on-the-ground combat advisory missions are inappropriate or infeasible. The key strength and uniqueness of special warfare is working with and through partners or surrogates. The discreet, precise, scalable, and economic nature of Special Warfare makes it a more attractive option than large force structures that are often high cost, inappropriate, counterproductive, infeasible, or may incur significant political risk. When used effectively,

special warfare strategies yield disproportional benefits.[13] The RAA concept makes special warfare options more feasible for U.S. policymakers than ever before. A properly resourced RAA effort can bridge the gap between a direct combat advisory mission, such as the U.S. involvement with the Afghan Commandos, and one where U.S. forces are prohibited from being involved directly.[14] The potential type of operation is limited only by the Commander's imaginative use of the technology. RAA represents an evolutionary step forward in U.S. special operations forces' ability to reach forward and influence partners. **PRISM**

Mention of any commercial product in this paper does not imply DoD endorsement or recommendation for or against the use of any such product. No infringement on the rights of the holders of any registered trademarks is intended.

Notes

[1] Examination of data collected on conflicts between 1775 and 2012 illustrates an increase in irregular conflict. Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (WW Norton & Company, 2013), 557-590.

[2] Department of the Army, Army Operating Concept, i, 14, 17, 22, 24, 25, 41.

[3] MAJ Keith Carter explores the history of technology integration since the Industrial Revolution and its correlation to the execution of war in his Master's Thesis. One of his hypotheses specifically states that "Periods of Adversity and Intense Strategic Competition will Increase Pressure to Integrate Revolutionary Technology, Whereas Periods of Stability will Promote the Continuation of Evolutionary Integrated, and Potentially Evolutionary and Disintegrated Technology." Please see his full thesis for further research on this topic: Keith L. Carter, "Technology Strategy Integration," (Master's Thesis, Naval Postgraduate School, 2012).

[4] "ATAK is a mapping engine developed for the Android Operating System which allows for precision targeting, intelligence on surrounding land formations, navigation, and generalized situational awareness. ATAK is under continuous development by various government laboratories to include the Air Force Research Lab, the Army Research Laboratory and the Defense Advanced Research Projects Agency. It enables users to navigate using GPS and National Geospatial Agency map data overlayed with real-time situational awareness of ongoing events." from "What is ATAK?," Android Windows Tactical Assault Kit, <https://atakmap.com/>.

[5] Bryan Dominique, "Never out of Reach: ARCENT's 15 month fight against ISIL," *The Official Homepage of the United States Army*, September 27, 2015, <http://www.army.mil/article/156142/Never_out_of_Reach__ ARCENT_s_15_month_fight_against_ISIL/>.

[6] The exact numbers of sorties directly affiliated with Remote Advise and Assist kit positional data and ISOF efforts are only available from classified sources; however, unclassified data does exist on the overall number of air missions flown against IS . For the purposes of this article, the *Operation Inherent Resolve* fact sheet provides a good metric of the overall air campaign. "Targeted Operations against ISIL terrorists," Department of Defense – *Operation*

Inherent Resolve website, <http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve>

[7] "United States National Security Strategy," February 2015, <https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

[8] Joints Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, (2012): 1, <http://www.defenseinnovationmarketplace.mil/resources/JV2020_Capstone.pdf>.

[9] United States Army Special Operations Command, ARSOF Operating Concept, 1–3; and United States Special Operations Command, *SOCOM 2020*, 3, 5.

[10] Joints Chiefs of Staff, *The National Military Strategy of the United States of America*, June 2015, i, 1.

[11] The National Military Strategy acknowledges the profound effects and role of technology: "The spread of new technologies enables a global information environment and empowers people to see more, share more, create more, and organize faster than ever before. This is challenging competitive advantages long held by the United States." It also further identifies the importance of partners and implies the role of SOF: "Regional partners are vital. The U.S. military contributes select combat forces, enabling technologies, and training in support of local partners… in a politically, financially, and militarily sustainable manner." Ibid, 1, 8.

[12] The Uppsala Conflict Data Program has collected data on violent conflicts since 1970. Analysis indicates a clear increase in irregular conflicts. "UCDP Conflict Encyclopedia" and "UCDP Data for Download," Uppsala University, Department of Peace and Conflict Research, Uppsala Conflict Data Program, last modified July 21, 2015, <http://www.pcr.uu.se/research/UCDP/>. Data collected on conflicts between 1775 and 2012 illustrates the same trend; and Boot, 557-590.

[13] Department of the Army. F*ield Manual 3-18, Special Forces Operations*, 2.

[14] The U.S. Special Operations mission in the Philippines has been characterized by training and advising, but not participating in combat operations with Philippine counterparts . It is an example of the type of mission that could have benefited from RAA . The following article from *Small Wars Journal* gives a brief overview of the scope of the mission, as well as its long term strategic importance to U.S. strategy: Mark Munson, "Has Operation Enduring Freedom Been a Success?," *Small Wars Journal*, April 5 2013.

Photos

Page 98. Photo by Day Donaldson. 2014. Can the US actually defeat ISIS? the limits of "limited war". From < https://www.flickr.com/photos/thespeakernews/15715981259/>. Licensed under Creative Commons Attribution 4.0 International <https://creativecommons.org/licenses/by/4.0/>. Photo unaltered.