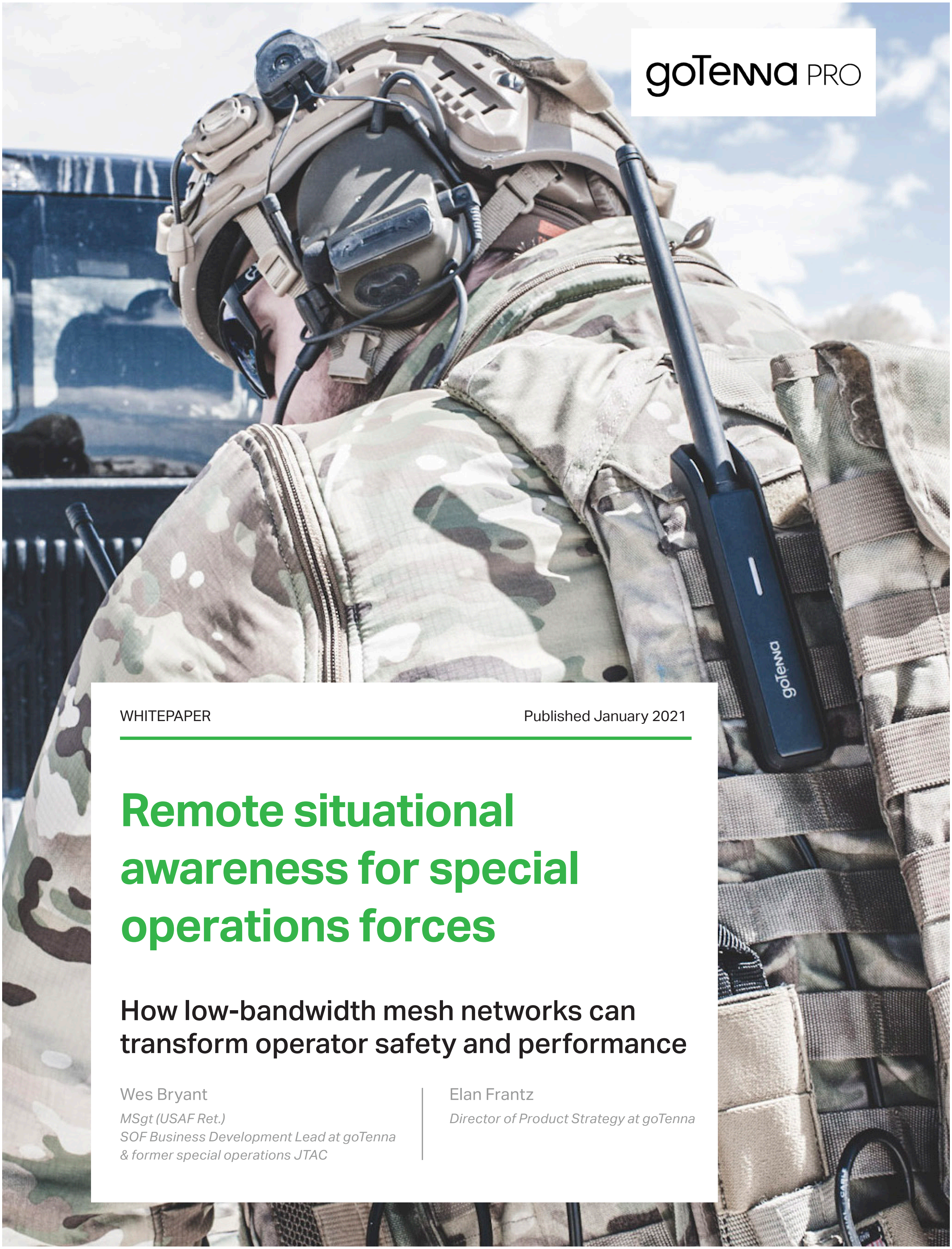


goTenna PRO

WHITEPAPER

Published January 2021

Remote situational awareness for special operations forces

How low-bandwidth mesh networks can transform operator safety and performance

Wes Bryant
MSgt (USAF Ret.)
SOF Business Development Lead at goTenna
& former special operations JTAC

Elan Frantz
Director of Product Strategy at goTenna

Overview

Today's connectivity allows each person to extend their scope of awareness well beyond their immediate environment. Without being physically present in a location, we can know the weather, check traffic, and receive updated news from nearly anywhere in the world. Remote situational awareness (RSA) — the ability to perceive beyond our immediate environment — is now fundamental to our everyday decision making.

For some, RSA is more than a way to optimize a daily routine, it is the difference between safety and danger. Every day, Special Operations Forces (SOF) are tasked with carrying out critical operations which are hazardous, require precise coordination between teams and resources, and demand that decisions are made in real-time.

While RSA is vital at multiple levels of the operation, from the commander to the operator, these missions are often conducted in off-grid, austere environments where standard connectivity is not possible between these entities. To address this connectivity challenge, low-bandwidth wireless technologies can provide essential communications where otherwise not possible.

In this whitepaper, we will overview how RSA tools and low-bandwidth connectivity are fundamentally impacting the safety and performance of SOF operations, and how RSA can be applied to core special operations activities in order to enhance team situational awareness, command and control, and survivability.

Remote Situational Awareness

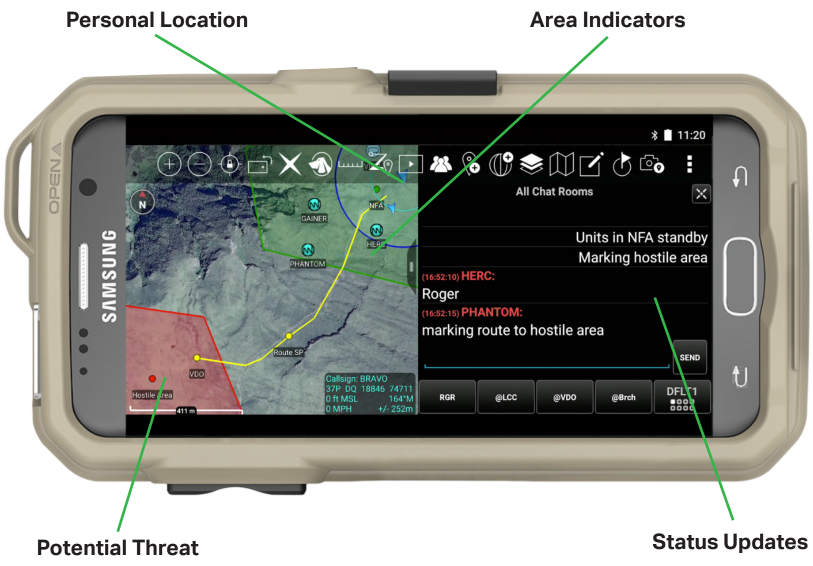
To ensure effective RSA, each team member on the ground, as well as at the command level, must share access to an updated common operating picture (COP). To execute their job effectively, there are distinct elements of the COP which must be known at the team and command levels.

Team-Level

In order to effectively conduct a mission, ground teams must be aware of the following information:

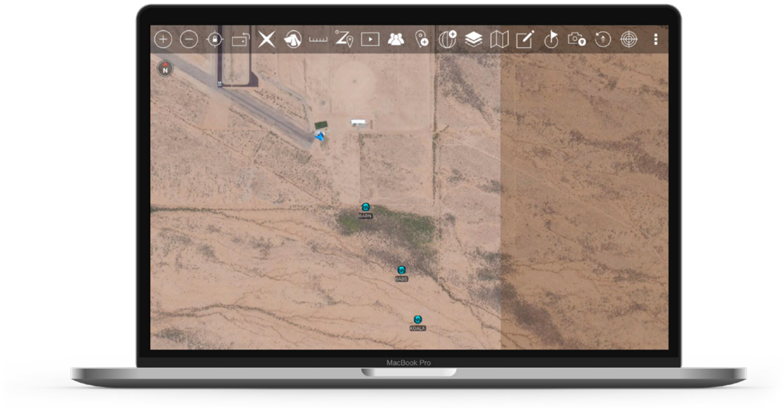
- Position of friendly forces
- Location of objectives and areas of interest
- Potential threats and enemy locations
- Permissive and restrictive boundaries (phase lines, no-fire areas, etc.)
- Status updates of people, equipment, and situation

To communicate this information to each operator, smartphones with situational awareness applications, are being deployed in the field. The key information is communicated through mapping and messaging features. With these tools, an operator can comprehend the current situation, project the likely outcomes and make decisions which improve the outcome of the operation.



Callsign: BRAVO
37P DQ 18846 74711
0 ft MSL 164°M
0 MPH +/- 252m

Units in NFA standby
Marking hostile area
(16:52:10) HERC:
Roger
(16:52:15) PHANTOM:
marking route to hostile area



Command-Level

In order to maintain oversight and effectively direct a mission, command-level entities must understand:

- The current and historical position of units
- Objectives and areas of interests being pursued
- Status of units in terms of MWE (men, weapons, and equipment)
- Intelligence from ground teams or external sources

To best support rear-area command and control, operations centers must be connected to all deployed teams and accurately convey the real-time operating picture. These command posts, whether vehicle-based or fixed, are where information from disparate sources converges to support informed decision making.

Remote Situational Awareness Data Types

The COP for ground teams and command is supported by reliable information transfer between all entities. The type of information transferred will vary greatly on the requirements of the operation, but can include visual, audio, text, sensor feeds and more. These information types can be separated into "low" and "high" bandwidth based on the size of the data files. Below, we classify the information types commonly involved with RSA into these two high-level categories:

Low-Bandwidth

- Short Message Service (SMS)
- Position Location Information (PLI)
- Map Objects (points & polygons)
- Voice-to-text Messages
- Low Resolution Images
- Sensor Information

High-Bandwidth

- High Resolution Images
- Streaming Video
- Large File Transfers

Connectivity Solutions

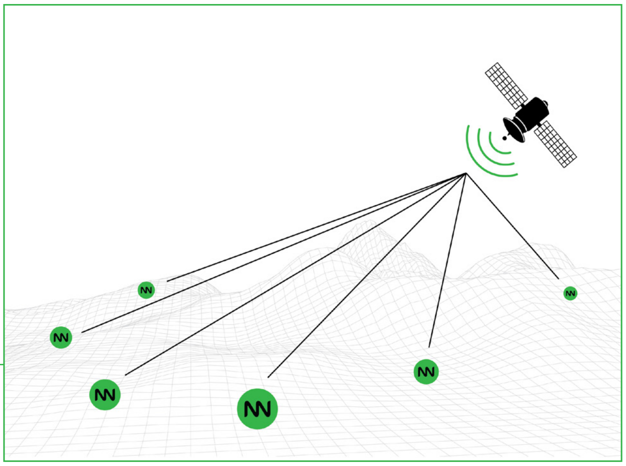
There are fundamental differences in the resource and equipment required to support high-bandwidth and low-bandwidth off-grid connectivity, in that high-bandwidth requires a significantly higher C-SWaP (Cost, Size, Weight and Power). For this reason, high-bandwidth technologies are typically limited to operational leaders, delegating only one device per team or platoon. While the long-term initiative for SOF is to utilize high-bandwidth technologies for each team member, there is an opportunity to equip individuals at every level of the operation with low-bandwidth, low C-SWaP technology to support a holistic COP from the command level down to the operator.

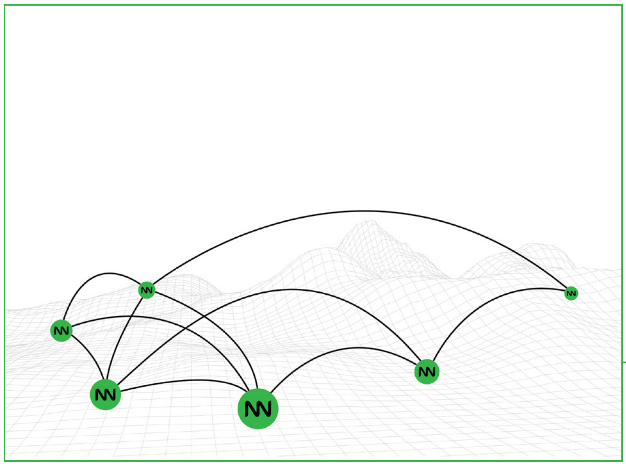
The wireless mesh network and backhaul solutions required to support low-bandwidth RSA are available today. While many of these solutions are commercial-off-the-shelf (COTS), these devices have been vetted by military, federal, and state & local authorities and are actively deployed in operation. Low-bandwidth COTS devices tend to be significantly cheaper than military-specific high-bandwidth options while maintaining a level of ruggedization and security commensurate with the types of critical operations for SOF.

For this whitepaper, we will focus on the hybrid use of mesh networking and backhaul (satellite and cellular) to provide all-purpose, affordable, redundant communications to all levels of the organization for SOF operations.

Satellite

Satellite communications devices may be built into a UHF/VHF radio or be a standalone unit. These devices communicate directly with the satellite while an online server manages the distribution of information to all the ground nodes and to command. Outside of federal use, satellite service typically requires a usage-based subscription.



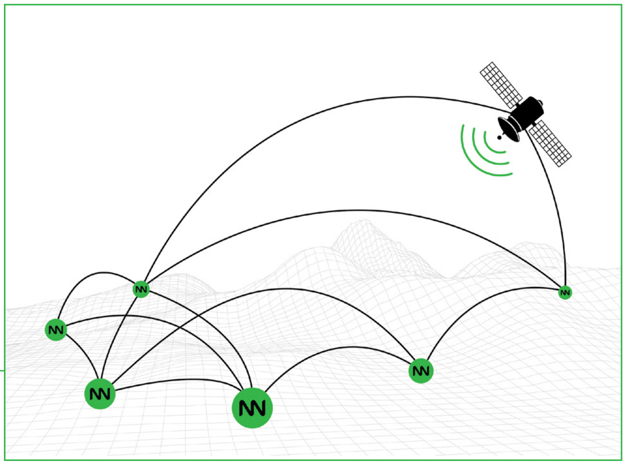


Low-bandwidth Mesh Networking

Nodes communicate to and through each other so that all broadcasted information is received by the entire group. As a fundamentally decentralized network, mesh is resilient, can adapt to diverse terrains, and does not require a subscription. The mesh network is not inherently connected to the internet.

Hybrid Low-bandwidth Mesh & Backhaul

All individuals are equipped with low-bandwidth mesh while some also have satellite or cellular devices where connectivity is available. This enables the online connectivity with command, network coverage and resiliency of mesh, and built-in redundancy for critical communications.



Implementation

The tools to achieve operational excellence through low-bandwidth RSA are available and actively being deployed in diverse settings.

Low-bandwidth RSA can greatly enhance core special operations activities by increasing ground team situational awareness and interoperability and strengthening command and control capabilities; therefore heightening survivability. Specific core special operations activities[1] directly benefited by low-bandwidth RSA include:

- Direct Action
- Hostage Rescue and Recovery
- Special Reconnaissance
- Counterterrorism
- Counterinsurgency
- Unconventional Warfare
- Foreign Internal Defense
- Security Force Assistance
- Foreign Humanitarian Assistance

Direct Action (DA) and Hostage Rescue and Recovery

Direct Action (DA) and Hostage Rescue and Recovery involve small-scale offensive actions that rely heavily on speed and surprise. In DA operations, special operations teams seek to “seize, destroy, capture, exploit, recover, or damage designated targets in hostile, denied, or diplomatically and/or politically sensitive environments.” Hostage rescue and recovery operations are “sensitive crisis response missions” often taking place within the same environments.[2]

In both activities, although small in scale, the operational make-up of the executing forces are often diverse and include many separate elements that will remain non-co-located during mission execution.

In conjunction with the main force, there will often be a supporting force, a cordon element, a combination of one or more security or blocking elements, and a quick reaction force (QRF) standing by. RSA can enable each element within the operation.

All operators in both the main and supporting elements and the cordon will maintain continuous inter-team situational awareness on individual operator locations simply by glancing at their ATAK screen. Every operator will have the ability to send cursor-on-target data and SMS messages through ATAK real-time in order to keep the entire team aware of targets of opportunity, threat locations, areas of interest, and so on. Subsequently, the need for line-of-site (LOS) voice radio transmissions is massively reduced and team situational awareness, down to the individual operator level, is exponentially increased.

Security and blocking forces can also be tied into the network, ensuring that the main force is continuously aware of the exact location of supporting forces outside the immediate vicinity of the objective where “actions on” is taking place. And the quick reaction force can be equipped in order to enable rapid sync with friendly forces in the event they are called in to support the mission, thereby mitigating risk of a “fog of war” situation upon arrival.

[1] Joint Publication 3-05 Special Operations. x-xi. 16 July 2014. Joint Chiefs of Staff. Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_05.pdf.

[2] Ibid.

Special Reconnaissance (SR)

Special Reconnaissance (SR) actions involve small teams operating in a "clandestine or covert manner to collect or verify information of strategic or operational significance."[3]

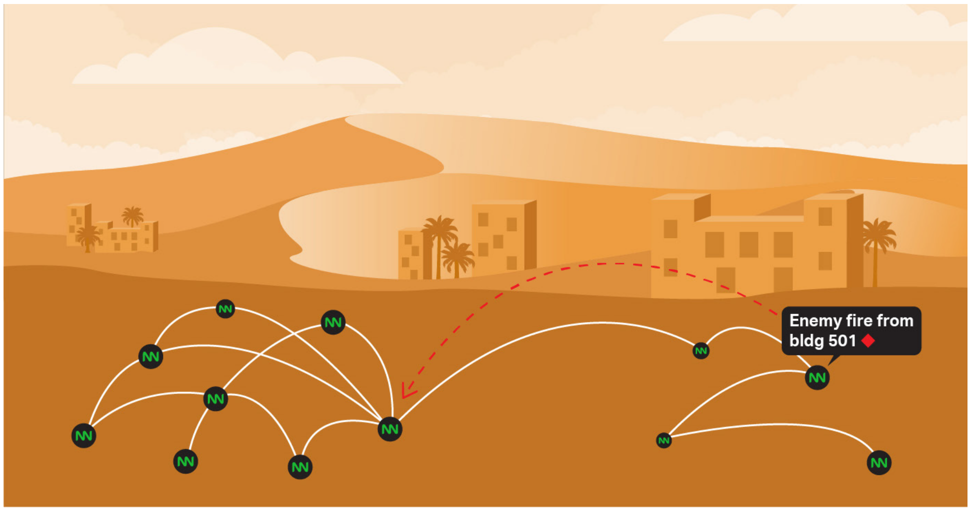
SR operations, by their very nature, rely on operators remaining undetected. LOS voice communications are not optimal for such mission, for several reasons: 1- they present a risk of operators being audibly detected by enemy forces; 2- they reduce an operator's external hearing awareness, as their ears are typically engulfed by a headset or internal earphones; 3- they carry a significantly increased radio frequency (RF) signature as compared with low-bandwidth RSA networks; 4- they are bulky and not concealable. Outfitting each operator with low-profile RSA capabilities significantly reduces, if not eliminates, the need for voice communications on SR operations. It provides a silent and concealable option for team situational awareness and communications throughout any given mission.

Counterterrorism (CT) and Counterinsurgency (COIN)

Counterterrorism (CT) and Counterinsurgency (COIN) operations incorporate a host of missions to "neutralize terrorists and their networks" and "defeat and contain insurgency."[4]

Low-profile RSA devices can significantly enhance CT and COIN activities in any theatre of operation. Missions ranging from ground offensives and clearing operations to close air support (CAS) to reconnaissance and presence patrols to combat search and rescue (CSAR) and personnel recovery (PR) will see benefit from low-bandwidth RSA capability. As well, it is optimal for many forms of infiltration and exfiltration, to include static-line parachuting and military freefall, helicopter insertion and extraction methods such as fastroping and rope ladders, and vehicular or dismounted overland operations.

In all uses, operators will have the ability to quickly reference team positions on their moving map within ATAK and send and receive cursor-on-target data such as targeting, boundary lines, areas of interest, rally points, routes, and casualty collection points. They will be able to transmit both CAS and medical evacuation (MEDEVAC) 9-lines, and will have at their disposal a secondary mode of communication to add to their communications PACE plan via SMS messaging capability.



[3] Ibid.

[4] Ibid.

Unconventional Warfare (UW) and Foreign internal Defense (FID)

Unconventional Warfare (UW) activities are to "enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power." While Foreign Internal Defense (FID) activities "support a host nation's internal defense and development strategy...to protect against subversion, lawlessness, insurgency, terrorism, and other threats to their internal security, and stability."[5]

For both UW and FID, low-bandwidth RSA enables an encrypted and closed network between US advisors and partnered forces. Partnered forces and US handlers can then communicate with one another via their smartphone applications completely independent of the host nation or other operating environment's communications or cellular networks.

With low-bandwidth RSA, partnered forces can be battle-tracked real-time by all members of the US team without any action required on part of the partnered force operators. This will enable more timely, effective, and secure command and control of partnered forces than the common reliance on unencrypted, line-of-sight voice communications or cell phones operating on a host nation network. They will also be able to send cursor-on-target data and secure text messages in order to relay targeting, surveillance, and other vital data, enabling US teams to more effectively advise and shape operations.

Security Force Assistance (SFA) and Foreign Humanitarian Assistance

Security Force Assistance (SFA) activities support the "reform, restructure, or reestablishment" of a host nation's armed forces. Foreign Humanitarian Assistance involves "a range of DOD humanitarian activities conducted outside the US and its territories to relieve or reduce human suffering, disease, hunger, or privation."[6]

Teams conducting either of these activities, which sometimes are concurrent, often find themselves in offgrid situations, where host nation communications infrastructure is entirely decimated. Their operating environment could be any combination of benign, hostile, or completely unpredictable; but will likely always involve a large number of civilians.

In these scenarios, low-bandwidth RSA enables a layer of team independence and situational awareness even in the most austere and fluid of situations. Teams will maintain awareness on each other's locations and be able to mark and transmit vital location information such as points of impact for humanitarian airdrops, medical aid stations, food and water distribution points, refugee areas, large civilian concentrations, and so on.

All of this will be enabled entirely off the grid without need for host nation cellular infrastructure, WiFi, or satellite communications.

> "Running ATAK over a mesh network means that the team can still have and share that kind of information even if other, traditional communication infrastructure like cell towers are down."
>
> — Kelsey D. Atherton
> C4ISRNET[7]

[5] Ibid.

[6] Ibid.

[7] Atheron, K.. (2019, April 2). Can this off-the-shelf platform mesh with tactical network needs? Retrieved from C4ISRNET: https://www.c4isrnet.com/it-networks/2019/04/02/gotenna-hopes-new-platform-meshes-with-tactical-networking-needs/.

Summary

To execute missions effectively when high-bandwidth communications like WiFi, cellular, or larger MANET radios are not an option or not desired, special operations forces can create an effective common operating picture utilizing low-bandwidth mesh networking.

In addition to interteam situational awareness and communications, low-bandwidth mesh networking enables a single operator to automatically become a backhaul node by tying the network to a TAKServer via satellite communications or cellular network—providing rear area command and control with real-time friendly force tracking down to the individual operator.

Low-bandwidth RSA devices are an easy-use, low-profile communications option to enable inter-team situational awareness and provide a common operating picture between special operations teams, and command and control elements. With these unique capabilities, low-bandwidth RSA is directly impacting a diversity of operations, and will continue to grow in relevance throughout a broad scope of SOF operations.

About the authors

Wes J. Bryant is the Military and Special Operations Forces (SOF) Business Development Lead at goTenna. He served over 20 years as a special operations joint terminal attack controller in the U.S. Air Force, and is co-author of the book Hunting the Caliphate — a first-person account of America's war on ISIS written alongside former Army Major General Dana PIttard. Wes holds a bachelor's degree in Asian Studies from the University of Maryland and is currently working towards his masters in Professional Studies at The George Washington University.

Elan Frantz directs Product Strategy at goTenna. Elan has a wide range of technical and product experience bringing advanced technologies to market, including drones, communications devices, cutting-edge materials, and more. Today, Elan works to discover how low-bandwidth mesh networking can have the greatest impact in the private and public sectors. Elan holds a Bachelor's degree Mechanical Engineering from UC, Santa Barbara.

About goTenna

goTenna is the world's leading mobile mesh networking company and provider of off-grid connectivity solutions for smartphones and other devices. In the public sector, goTenna's innovative mesh networking protocol is embedded into lightweight, low-cost tactical radio devices and paired with easy-to-use mobile apps enabling mobile, long-range connectivity even without cell, wifi, or satellite.

The goTenna vision to create a resilient communications system was ignited during Hurricane Sandy in 2012, when approximately a third of cell towers and power stations were knocked out. Based in Brooklyn, goTenna now supports mission-critical law enforcement, public safety, and defense operations around the world. For more information on goTenna's solutions for disaster response, please visit www.gotennapro.com.