# Next Generation ISR Dominance:

# Utilizing Lessons Learned from SOF ISR TTPs in the Global War on Terror for a Near-Peer Conflict

Author - Conrad Lutz

SOS 21G / Flight B23

19 October, 2021

**Abstract**

As the United States (US) military shifts it's focus away from counter-insurgency and counter-terrorism and towards near-peer competition, a new problem-set presents itself in terms of Intelligence, Surveillance, and Reconnaissance (ISR) utilization. Over the past decade, US ISR has enjoyed a largely uncontested environment, both in the air and space domains. It is no secret that the US military uses GPS capability to great effect, nor that the majority of ISR platforms, particularly the MQ-9, are vulnerable to attack both from the surface and the air. A conflict with a near-peer, however, will not offer the same freedom, as Russia and China continue to develop their anti-satellite capabilities as well as their air forces.

In the war on terror, US Special Operations Forces (SOF) have taken the lead, using networks of operators and intelligence analysts to find and fix enemy combatants, then remove them from the battlespace - all without the numbers required of a conventional force. ISR has played a significant role in this process, offering constant, near real-time characterization of the operational environment. This paper uses several of the Tactics, Techniques, and Procedures (TTPs) and concepts that SOF have utilized in terms of ISR and applies them to the problem set of a near-peer conflict where satellite communications are not guaranteed.

**Understanding the Task**

As Linda Dawson describes in her book, *War in Space: The Science and Technology Behind Our Next Theater of Conflict*, the first shots of the next major conflict might not be heard - they'll be in the vacuum of space.[1] What would the US military do, how would it react, if satellite communications were lost? And even if any secondary, non-satellite communications-based plans were effective, how would US military intelligence bring its weight to bear in the fight?

General Schwarzkopf, commander of US Central Command during the Gulf War, recalled the intelligence presented to him at the time as, "useless to him in the field and, two, bomb damage assessments done in Washington varied from those done in theater."[2] Years later, when SOF hunted Abu Musab al-Zarqawi, the founder of the group now known as ISIS, the resulting strike was a combined effort totaling 600 hours of Intelligence, Surveillance, and Reconnaissance (ISR), a robust Human Intelligence (HUMINT) network, and Signals Intelligence (SIGINT). All of the collection, analysis, and dissemination were part of a daily operations cycle that occurred successfully hundreds of other times - the Zarqawi strike was merely the most publicized.[3]

The US intelligence community has improved its ability to report valuable information to decision-makers over the past thirty-odd years, but those decades of conflict have been against technologically inferior opponents that lack the capability to disrupt standard US ISR TTPs. After the initial invasions of Afghanistan, Iraq, and to some extent, Syria, US air assets have

---

[1] Dawson, Linda. 2019. *War in Space: The Science and Technology Behind Our Next Theater of Conflict*. Cham: Springer International Publishing AG. 9783319930510.

[2] Keaney, Thomas A., and Eliot A. Cohen. 1996. "Revolution in warfare? Air power in the Persian Gulf." *Airpower Journal* 10, no. 2 (Summer): 88+. 0897-0823.

[3] Flynn, Michael T., Rich Juergens, and Thomas L. Cantrell. 2008. "Employing ISR: SOF Best Practices." *JFQ* 3rd Quarter, no. 50 (July): 56-61. 1070-0692.

largely enjoyed unrestricted freedom of movement under the umbrella of perpetual air supremacy. Contrasting the Global War on Terror (GWOT) to a potential conflict with China or Russia, who both have a capable air force and robust Integrated Air Defense System (IADS), demonstrates that the US's ability to achieve air supremacy, or even air superiority, will be challenged for a significant portion of any future conflict, but particularly at the onset.

One of the primary hurdles the intelligence community will face should the US enter open conflict with a near-peer is how to communicate without much of the infrastructure on which it has become so dependent. The Distributed Common Ground System (DCGS) enterprise is a significant amount of analytic power that can be leveraged to inform decision-making, yet will be horribly hamstrung should satellite communications become degraded, as one of the primary premises of the enterprise is its reach-back capability - the analysts don't have to forward deploy, but are rather deployed in-garrison, slashing the logistical component of having them in-theater.

Special Operations Forces have, for the last decade or so, been the primary proponent of ISR collection in the counterinsurgency and counter-violent extremist organization fight. While their TTPs related to manhunting and dismantling terrorist networks are not directly applicable to a more conventional war, several of their intelligence architectures are.

**Last Calling Station, Have You Broken & Unreadable**

Even the most tactical and "small" (in terms of used forces) US military operations require a robust communications plan. While the ground force may be able to talk to any air assets overhead using line-of-sight radios, when communicating back to base or hailing assets elsewhere, satellite communications become the primary method.

Since the early 1990's, the US military has become increasingly reliant on the space domain and has, until now, been relatively unchallenged and unmatched by any other nation. It took 500,000 troops to invade Iraq during the Gulf War, yet less than half that just over a decade later. The large reduction in footprint is due in large part to the GPS capability and accuracy of standoff munitions.[4] Additionally, satellite communications now allow military units to communicate across vast distances and across domains, easing the coordination of joint air-ground operations and keeping headquarters elements better apprised of ongoing missions.

No matter the relevance and ability to take action on intelligence reporting, timeliness becomes unattainable the moment satellite communications are interrupted. Bringing the analysts forward answers one piece of the equation, but continuing collection to answer further requirements must still occur without the oversight of a larger headquarters like a Combined Air Operations Center (CAOC).

Unfortunately, the majority of US Unmanned Aerial Vehicle (UAV) assets operate primarily on a beyond-line-of-sight (BLOS) architecture, and of those that do operate solely on line-of-sight (LOS) links, most still require GPS. Currently, the Naval assets carrying low- to medium-altitude UAVs that are operated line-of-sight from the ship and processed, exploited, and disseminated (PED'd) from onboard the vessel best demonstrate a unit-organic process from control of the UAV to the ultimate analysis and dissemination of intelligence. While the reliability of many tactical UAVs is still debatable[5], there is still time to shift development focus towards increasing robustness. Assets like the MQ-27 Scan Eagle could still be used to good effect in a near-peer fight so long as a mindset shift occurs where the loss of these lower-cost

---

[4] BBC News. 2006. "Libya jamming 'exposed vulnerability.'" BBC News Channel. http://news.bbc.co.uk/1/hi/sci/tech/4602674.stm.

[5] Petritoli, Enrico, Fabio Leccesse, and Lorenzo Ciani. 2018. "Reliability and Maintenance Analysis of Unmanned Aerial Vehicles." *Senors* 18, no. 9 (September). 10.3390/s18093171.

systems becomes acceptable and a greater inventory amassed to rapidly resume collection upon any such loss.

Investing in tactical UAVs with an internal positioning capability then becomes a sub-requirement of maintaining UAV-centric collect that minimizes the risk to personnel that would be inherent against a near-peer with a significant IADS. Should ISR assets, regardless of manned, unmanned, or class (altitude, size & endurance), be able to collect, getting the data to a location where it can be properly exploited and have the subsequent analysis disseminated to decision-makers is the final hurdle.

**Humans Are More Important Than Hardware**

While the SOF Truths were developed as basic guidance for SOF units, the first can easily speak to the US military at large.[6] As evident by the initial effects of Millenium Challenge, a US military training exercise conducted in 2002 to test new warfighting concepts, fighting an enemy with a technological disadvantage does not guarantee victory - it's the human who has the ability to plan and outthink that is the most dangerous piece.[7]

The GWOT may very well go down as the heyday of the MQ-9 and other medium altitude ISR platforms, but all required humans for the actual intelligence production. At the first peak of ISR orbits over Afghanistan, SOF were operating "PED Sheds" on bases and forward operating bases (FOB's) in-country. Conventional forces adopted a similar construct, albeit at larger bases that carried less of a risk to personnel. Imagery Analysts, trained specifically to report on the full-motion video feeds being piped down from MQ-9's and other SOF platforms,

---

[6] Friberg, John. 2017. "SOF Truths." SOF News. https://sof.news/sof/sof-truths/.

[7] "Millennium Challenge: The Real Story of A Corrupted Military Exercise and Its Legacy." 2015. War on the Rocks. https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/.

sat in small conex boxes within walking distance of the decision making nexus at the tactical level, whether it be a Joint Operations Center (JOC) or Tactical Operations Center (TOC). Over time, as US taxpayer appetite for the cost of the war on terror began to decline, these positions were removed and fulfilled using the ever-growing over-the-horizon architecture, where all data was sent through a communications infrastructure from in theater to units in the states for its initial exploitation. In a future conflict where our over-the-horizon capability is degraded or altogether untenable, however, the forward deployment of enabler personnel may be required. The Analysis and Exploitation Team (AET) construct that next-gen DCGS has postured to support SOF targeting requirements, where, contained within the team, all intelligence disciplines are covered and able to be fused in order to provide timely, accurate, and actionable intelligence, is a strong basis for such a forward deployment.[8] While the weight of various intelligence sources would shift drastically from a counter-insurgency fight to that of a near-peer, having each discipline represented reduces the risk that certain elements are missed or inaccurately reported. Additionally, having the braintrust of a multi-disciplined node creates an environment where innovative solutions may be presented to mitigate unforeseen collection problems. "The enemy gets a vote" is often quoted throughout military planning, lending itself to the idea that not all plans survive first contact - posturing our people is the best way to ensure we can quickly adapt and overcome.

But who would staff such an intelligence node? Arguably, the most effective solution would be a joint force, as the nature of collect in a truly contested environment would dictate both an unpredictable Air Tasking Order (ATO) and one in which all platforms, regardless of

[8] Borukhovich, Kelly, and Tyler Morton. 2020. "DCGS Next Generation: Accelerating Change to Deliver Decision Advantage." Over the Horizon Multi-Domain Operations and Strategy. https://othjournal.com/2020/09/26/dcgs-next-generation-accelerating-change-to-deliver-decision-advantage/.

branch, would be called upon. While the Air Force flies the preponderance of ISR platforms currently utilized, members from the sister services would bring irreplaceable experience on the capabilities their branch maintains as well as specific collection requirements that may be unique to their service's needs. For consideration, the creation or repurposing of a career field may also fit the bill - a functional rewrite and follow-on plus-up of ISR Liaison Officer (ISRLO) positions comes to mind, where the career field centers on becoming not only the embedded ISR subject matter expert, but also the officer in charge of joint force intelligence nodes.

An architecture of forward-staged joint analysts would require a few objectives to be met in order to be effective. First, intelligence personnel must be properly equipped for the operating environment. While the increased threat due to proximity of the conflict is of some concern, the risk can be mitigated with small changes to force readiness that would inherently come with an imminent large-scale conflict. The primary focus of this objective lies in the actual intelligence equipment itself. While humans are indeed more important than the hardware they utilize, any intelligence analyst would be severely degraded in analysis and production capability without the proper systems. SOF intelligence analysts are known to wield systems pre-loaded with the most up-to-date data and software, allowing them to rapidly stage at any location and join the local network without need for massive downloads.

The second objective relates to the first, requiring that the physical space be rapidly constructible and have the ability to tap into a LOS-primary communications network. Even if satellite communications would be degraded or disabled, the infrastructure to connect the space over-the-horizon (OTH) back to CONUS is still desirable for when full communications are reestablished. The node would need to be able to function separate from others like it, protecting itself from any communications pathway dependencies, but sync with the other nodes whenever

the pathways are restored, thereby ensuring all nodes maintain the current common operating picture.

**Conclusion**

In the face of a near-peer conflict where the communications and air environments will be heavily contested, the US military and intelligence community must posture themselves to ensure that actionable intelligence can reach the hands of decision-makers at the lowest level. Over-reliance on CONUS-based or OTH analysis, especially in the critical moments of a conflict where the US is not the instigator, leaves the intelligence community unable to inform or fulfill any form of collection request. Learning from the SOF ISR TTP's developed throughout the Global War on Terror, the use of pre-packaged analysis nodes to create a forward hub-and-spoke network able to immediately react to new priorities and continue to function when isolated from the network is of great value. The modular and inter-connected architecture could rapidly expand or shrink to meet the demand and, depending on the severity of communications degradation, the nodes could even follow the forward line of own troops (FLOT), increasing the single-hop reach of LOS-based connections. The end result is enabler personnel postured and equipped to give decision-makers and warfighters the flexible support needed to continually pressure the enemy with informed targeting in the most challenging of environments.

## References

BBC News. 2006. “Libya jamming 'exposed vulnerability.'” BBC News Channel. http://news.bbc.co.uk/1/hi/sci/tech/4602674.stm.

Borukhovich, Kelly, and Tyler Morton. 2020. “DCGS Next Generation: Accelerating Change to Deliver Decision Advantage.” Over the Horizon Multi-Domain Operations and Strategy. https://othjournal.com/2020/09/26/dcgs-next-generation-accelerating-change-to-deliver-decision-advantage/.

Byman, Daniel, and Ian Merritt. 2018. “The New American Way of War: Special Operations Forces in the War on Terrorism.” *Washington Quarterly* 41, no. 2 (June): 79-93. 10.1080/0163660X.2018.1484226.

Dawson, Linda. 2019. *War in Space: The Science and Technology Behind Our Next Theater of Conflict*. Cham: Springer International Publishing AG. 9783319930510.

Deptula, David A., James R. Marrs, and NATIONAL DEFENSE UNIV WASHINGTON DC INST FOR NATIONAL STRATEGIC STUDIES. 2009. “Global Distributed ISR Operations: The Changing Face of Warfare.” *JFQ* 3, no. 54 (January): 110-115. ADA515567.

Eaton, Derek, Angela O'Mahony, Thomas S. Szayna, and William Welser IV. 2017. *Supporting Persistent and Networked Special Operations Forces (SOF) Operations: Insights from Forward-Deployed SOF Personnel*. Santa Monica, CA: RAND Corporation. RR-1333-USSOCOM.

Flynn, Michael T., Rich Juergens, and Thomas L. Cantrell. 2008. “Employing ISR: SOF Best Practices.” *JFQ* 3rd Quarter, no. 50 (July): 56-61. 1070-0692.

Friberg, John. 2017. “SOF Truths.” SOF News. https://sof.news/sof/sof-truths/.

Keaney, Thomas A., and Eliot A. Cohen. 1996. “Revolution in warfare? Air power in the Persian Gulf.” *Airpower Journal* 10, no. 2 (Summer): 88+. 0897-0823.

Kiras, James D. 2018. *Routledge Handbook of Air Power*. 1st Edition ed. London: Routledge.

“Millennium Challenge: The Real Story of A Corrupted Military Exercise and Its Legacy.” 2015. War on the Rocks. https://warontherocks.com/2015/11/millennium-challenge-the-real-story-of-a-corrupted-military-exercise-and-its-legacy/.

Myers, Grover E. 2003. “Millenium Challenge 2002: Setting the Mark.” *JFQ* Winter 2002-03 (33): 23-29. 1070-0692.

Petritoli, Enrico, Fabio Leccesse, and Lorenzo Ciani. 2018. “Reliability and Maintenance Analysis of Unmanned Aerial Vehicles.” *Senors* 18, no. 9 (September). 10.3390/s18093171.