The Lessons of Mogadishu, Part II

The ODG in action

by Majs Joseph Montagna, USMC, & Lexi Plunkett, USAF

>Maj Montagna is the Director, Safety and Standardization, HMH-464.

>>Maj Plunkett is an Air Force Acquisition Officer. She currently works at the Air Force Rapid Capabilities Office, Washington, DC.

The original purpose of the ODG (operational decision game), available on the *Marine Corps Gazette* website at Appendix A, was to present an operational environment with a contemporary enemy possessing modern tools in order to conceptually evaluate how a non-state actor may fight an American military force in the future. The modern tools were meant to demonstrate how a non-state actor without the military-industrial complex of the United States may evolve with modern technology and employ its own version of MUM-T concepts using historical precedence as the background. Several people were asked to play the game and compile what thoughts they had. That feedback was subsequently compiled in Appendix B, available on the *Marine Corps Gazette* website, and used to augment independent research to develop a future concept of a non-state adversary's use of technology in urban and littoral terrain.

The ODG created for this case was specifically designed to mimic the Mogadishu operational environment of the early 1990s. While it was not based on actual current events, the ODG was thoughtfully crafted in a predictive way to build a situation roughly equivalent to that city during those years. Since the ODG was intended to help forecast and predict future enemy actions, however, a scenario with potentially more contemporary organizations and motives was used while trying not to alter the geographic precepts too greatly. Purely futuristic tools were not given to the enemy because that may produce forecasts that will never actually have a basis in reality. The game gave players tools that could be nearly approximated based on actual current and emerging technologies. This was less to evaluate the capabilities of the tool as it was to evaluate the decision cycle of the enemy, forcing us to think about how actors may connect humans in a hostile environment through unmanned machines or technological interfaces. Ultimately, the goal was to analyze various game plays and synthesize from those results how future enemy thought processes could evolve to shape a battlespace.

Design

The title of this game is "Boko Haram's Advance Toward the Islamic State of Nigeria," and it depicts a violent destabilization of the Nigerian city of Warri. After nearly a decade of intra-state strife, continually declining economic prosperity, and northern emigration to the south for various reasons, the military is unable to mass a response in Warri when Boko Haram begins taking control of portions of the city and massing attacks on its infrastructure.

The U.S. Embassy, Mogadishu, December 1992. (TSgt Perry Heiner, USAF; National Archives ID 6508294.)

A brief but violent battle with the Nigerian military in the city results in a military retreat that cedes ground and abandoned equipment to Boko Haram. The atrocities against Christians in Warri lead to a United Nations' Security Council Resolution, authorizing a forceful response against Boko Haram's leadership. A United States-led task force responds quickly with II MEF as the main effort. II MEF successfully remains 80 percent of the city's territory and its major infrastructure before redeploying and turning the mission over to the UN (United Nations)-led stability force called UNON (United Nations Operations in Nigeria). UNON is a CJTF (combined joint task force) made up of the Nigerian Army, other African nations fighting Boko Haram (Cameroon, Niger, and Chad), and the 24th MEU (Rein). Boko Haram still maintains authoritarian presence in the southeast quarter of Warri, making its population unreachable to the UN force. The 24th MEU (Rein) will support internal defense, development, and stability operations as part of a CJTF, to include counterinsurgency, foreign internal defense, and the support of adjacent special operations forces. Nigeria, Cameroon, Niger, and Chad's forces will provide security operations to maintain conditions for NGOs (nongovernmental organizations) to provide humanitarian relief.

The players represented a Boko Haram commander and were given several most-likely courses of action and basic force compositions for both sides of the fight. What made this game unique, however, were the three non-traditional systems/concepts that the players had at their disposal to create a low-end or low-cost A2/AD (anti-access/area denial) environment. These systems/concepts were meant to pair the non-state actors with technology in such a way that they could be reasonably predicted to create a MUM-T capability for an organization lacking the industrial backing that the United States enjoys.

The first system/concept was a linked communications infrastructure using smartphones, applications, and pocket-sized antennas. This low-cost solution created a smartphone-to-smartphone network that did not require towers, routers, or satellites. It could create networks of communicators spanning several miles and could be established in less than a minute. The network was then able to transmit encrypted communications, use smart protocols, send software updates automatically to adjust frequency utilization, and share location information and data. The ODG players were asked to devise under what conditions they would employ this capability and how they would integrate it against U.S. forces.

The second system/concept was the use of commercially available UAS (unmanned aircraft systems). This technology is widely available on the commercial market and in myriad configurations and capabilities. Additional-

> *The results of the problem framing revealed that several players noticed the same problem presented to the Boko Haram commander ...*

ly, non-state actors are already tactically deploying these machines.[1] Low-cost UAS were incorporated in this game to evaluate how their use could be altered in the future based on observations of their capabilities, uses of more sophisticated systems, and how those evolving tactics could be employed against U.S. personnel and equipment.

The third system/concept was the utilization of worldwide communications systems, such as social media, available through the Internet. Again, like with UAS, the utilization of the Internet by non-state actors has already been observed and is a growing medium for recruitment and messaging.[2] Because the use of information sharing through the Internet has proven to be ever expanding since its inception, however, it was incorporated into this ODG as a capability set of Boko Haram so the ODG players could specifically utilize

it to imagine ways it could be used in an unmanned fashion to fight against U.S. military forces in the future.

ODG Results

Several themes emerged from the analysis of the ODG results. The players were familiar with the case study of Mogadishu, but all of them played the game individually. The games were completed by hand and with varying levels of input and detail. The results were compiled and input into a spreadsheet with four basic categories: Problem Framing, COA (Course of Action) Graphic and Narrative, Theory of Victory, and Future Concepts. Listed below are the trends that emerged from the various responses and a few outliers, which posed unique concepts of employment.

The results of the problem framing revealed that several players noticed the same problem presented to the Boko Haram commander; an overwhelming technical force had isolated Boko Haram and put them on the defensive. The conditions which would allow Boko Haram to resume its control of the city and the growth of its influence would be to force a withdraw of the U.S. military and to destabilize the local government. Opportunities for Boko Haram were access to the Internet and social media, time, and engagement in conflict that caused high casualty rates for both sides. Threats and limitations to Boko Haram were a better resourced U.S. military, the U.S.'s ability to conduct signals intelligence, and that there was no way for Boko Haram to gain air superiority.

The COA graphics and narratives also identified several trends. Within the mission and intent of the Boko Haram commander, the trends were to disrupt government legitimacy by disrupting infrastructure and sabotaging humanitarian aid missions, imposing cost restrictions on the U.S. military through loss of life and equipment, and lastly, ensuring all bloodshed and failed government missions were captured on the Internet and on social media. The concepts that emerged to support the missions and intents highlighted the need to push out from the defensive

and conduct clandestine attacks against the U.S. military, establish methods for reconnaissance and communications, establish integrated defensive positions around designed engagement zones, and distribute propaganda which highlights atrocities committed by the U.S. military and the death and wounding of its soldiers.

The theories of victory tended to have similar central ideas, but their necessary capabilities diverged. The agreed-upon central ideas were that defeating the U.S. military would be a strategic-level task that would primarily require destroying elements of the U.S. military, live streaming those events over the Internet, and filming and streaming the death of any civilian caused by an American. The necessary capabilities identified by the players to accomplish this central idea required the use of UAS, linked communications networks, cellular phones, Internet access, destroying U.S. military support assets and material, the ability to trap elements of the U.S. military in ambushes, and to avoid direct soldier-to-soldier engagements at all costs.

The future concepts that the players developed ranged from using each system/concept in isolation to joining all three together to maximize the use of each while complementing the capabilities of the others. In each case, however, they presented unique, deadly, and cost-imposing capabilities which could be employed against the U.S. military. The net effect of the concepts was an ad hoc or low-end anti-access environment at the tactical level that could lead to area denial at the strategic level if implemented repeatedly. The individual ideas presented by the players are listed in Appendix B, but a hybrid of their collective concepts will be presented in the following section.

Future Concept of a Non-State Adversary's Use of Technology in Urban, Littoral Terrain

This section means to outline a synthesis of the results from the ODG and provide a future concept of how a non-state adversary of the U.S. military may employ current or future technologies in a MUM-T fashion that will construct a
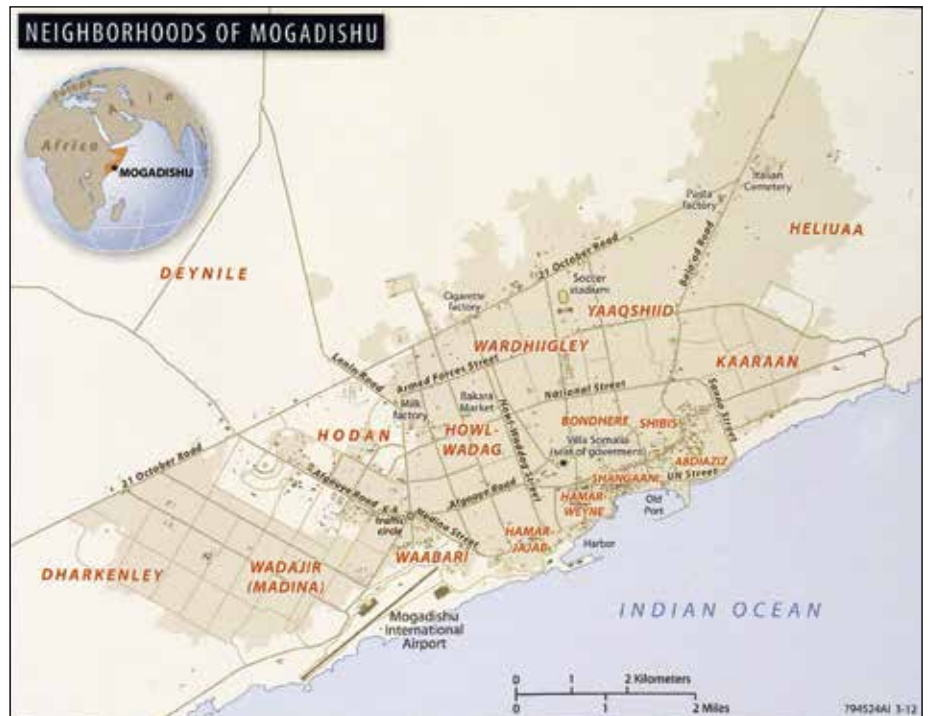
Map of the neighborhoods of Mogadishu. (Map from the Perry-Castaneda Library Map Collection, University of Texas.) (Map was produced by the CIA.)

low-end, but effective, A2/AD environment. As defined earlier in this article, the U.S. military generally sees MUM-T as the "relationships established between manned and unmanned systems personnel prosecuting a common mission as an integrated team." Though a non-state actor may not use the lexicon of the United States' military-industrial complex, they may very well adopt the principles of this tactic while employing the technologies they can afford and acquire. Since they will have access to machines, such as drones, which can be piloted by one person but offload information to another, both of whom are in communications with one another to achieve a common operating picture, they will be operating in a MUM-T fashion. It is important to remember that all adversaries will be thinking enemies and cannot be constrained to operate in accordance with paradigms set forth in U.S. military doctrinal publications. They will be seeking to exploit critical vulnerabilities and change the reality of the battlespace faster than U.S. commanders and policy makers can orient themselves to make credible decisions.

Problem Statement

Should the U.S. military find itself in a dense urban, littoral city fighting a non-state actor for control and to quell a humanitarian crisis, as it did in Mogadishu in the early 1990s, it should expect that the enemy commander will be problem framing and planning a campaign to defeat the United States. That commander's problem statement and list of assumptions may look something like the following: the presence of the U.S. military is preventing the natural and proper distribution of power, it has the backing of a multi-national coalition, and it has an overwhelming technical advantage and highly trained military with which it can achieve tactical victories.

Underlying this problem statement, the enemy commander may also hold the following assumptions. The U.S. military, with its superior military force, will have to be defeated at the strategic level by attacking its nation's will to fight. This can be quickly and effectively achieved by waging an information operations campaign that depicts a bloody war, the graphic death of U.S. soldiers, and U.S. soldiers committing violent acts against civilians. Another

assumption likely to be made is that the non-state force will have control of the local populations in which they are imbedded because of coercion or cultural, ethnic, or religious ties. Additionally, since the U.S. military will have to enter channelizing terrain to conduct its tactical operations, this will afford an adversary the ability to isolate it and inflict heavy casualties while using the same urban terrain to mask movements and minimize exposure. By using information operations and coercion in the local area, civilians may be lured into the engagement zone to hinder the ability of the U.S. military to distinguish between non-combatants and combatants or to simply overwhelm them physically and thus decrease their rate of movement.

Hypothesis

By using cheap and commercially available technology in unique and evolving ways, non-state adversaries will be able to develop MUM-T capabilities that will further their ability to communicate, control fires, maneuver against U.S. military forces, and conduct information operations in such a way as to establish an A2/AD environment that will have strategic effects on an opposing U.S. military campaign. Although the U.S. military may be able to win a series of tactical engagements, by locking them into a bloody campaign which can be broadcast to their policy makers, their nation's will to fight will be broken, and they will be ordered to withdraw. The situation can be further complicated for the U.S. military by spreading information that will cause the local population to have no trust in them or their espoused mission.

Capability Description

The assets a non-state actor will need to possess to make this hypothesis prove successful are commercial equipment, such as mobile phones for distribution throughout a command and control network; linked communications devices; unmanned vehicles (both aerial and ground); reliable access to the Internet; and a team of individuals who are capable of exploiting tools in that domain.[3] Each of these assets will offer

unique means to the user. The UAS in isolation can be flown by an operator for myriad missions, limited only by the imagination of the user, from simple reconnaissance profiles to dropping grenades on troop formations. Cell phones and the Internet simply connect two users via various mediums. Likewise, linked communications infrastructure just connects a varying number of users, albeit over varying ranges, but by itself, there is no unmanned component. Used in isolation, these technologies don't satisfy the definition of MUM-T. Ultimately, it will be their combined use that will leverage a MUM-T capability and facilitate the achievement of strategic ends. The ability to create battlefield relationships between decision makers, or manned systems personnel with unmanned personnel, through a shared asset to achieve a common operational mission objective, will create an ability to increase operational tempo and make a more complex reality for the U.S. military to react to.[4]

The capability of extending communications networks via mobile technology and the Internet may allow users to extend data-link distances to and from commercial UAS and allow for video feeds to be more widely disseminated more quickly. RADM Michael Manazir, the U.S. Deputy Chief of Naval Operations for Warfare Systems, said, at the Navy League's 2016 Sea-Air-Space Exposition, that networks will be the key to success in fifth generation warfare and that his office is less concerned with platforms than it is with capabilities.[5] Presumably, non-state actors will also be fighting in the fifth generation if they can achieve the paradigm of networking battlespace information and the prioritization of end-state effects over ways. Catch phrases like "turning a kill chain into a kill web"[6] will be state and actor agnostic. Non-state actors may not have encrypted "tactical clouds" meshing fifth generation fighter aircraft together with submarines, but they will understand that, by using readily available open networks, they will be able to maneuver in the information domain and increase the effectiveness of their warfighting capabilities.

Concept of Employment

The hybrid future MUM-T concept synthesized from the results of the ODG is a combination of all three of the concepts and systems presented to the players in the scenario. The UAS and its operator can stage at greater distances from the command and control hub to operate the machine. Then, to establish the relationship "between the manned and unmanned systems personnel prosecuting a common mission as an integrated team," they can be connected through a linked communications infrastructure and share or distribute videos, images, sound, or written messages through the same linked infrastructure, the cellular network, or the Internet. Using the Internet, the captured video or other propaganda can quickly be distributed to a worldwide audience. Figure 1 depicts a very simple MUM-T concept wherein a commander can communicate with unmanned personnel over a linked network and receive UAS position data while also viewing its video feed via an Internet connection. The operator is also in "direct voice communication between the participants [and able to] accurately depict each member's location with regard to the object being monitored." One of the benefits of a linked communications network is that, for one node to communicate with another, it can transmit throughout the entire linked network until the intended recipient ultimately receives the communication. Additionally, an added benefit to the non-state adversary in an urban environment is the ability to also rely on civilian communications networks as perhaps the primary, but most definitely as a secondary or even tertiary, means of communications. Figure 2 depicts the same information cycle as Figure 1 but is broken down by system and represents a single loop instead of the complete battlefield network displayed in Figure 1.

Measures of Success

There are several ways in which this concept can be measured for success. First is whether combining several, otherwise separate and individual, systems and abilities can provide a non-state actor with a MUM-T capability or
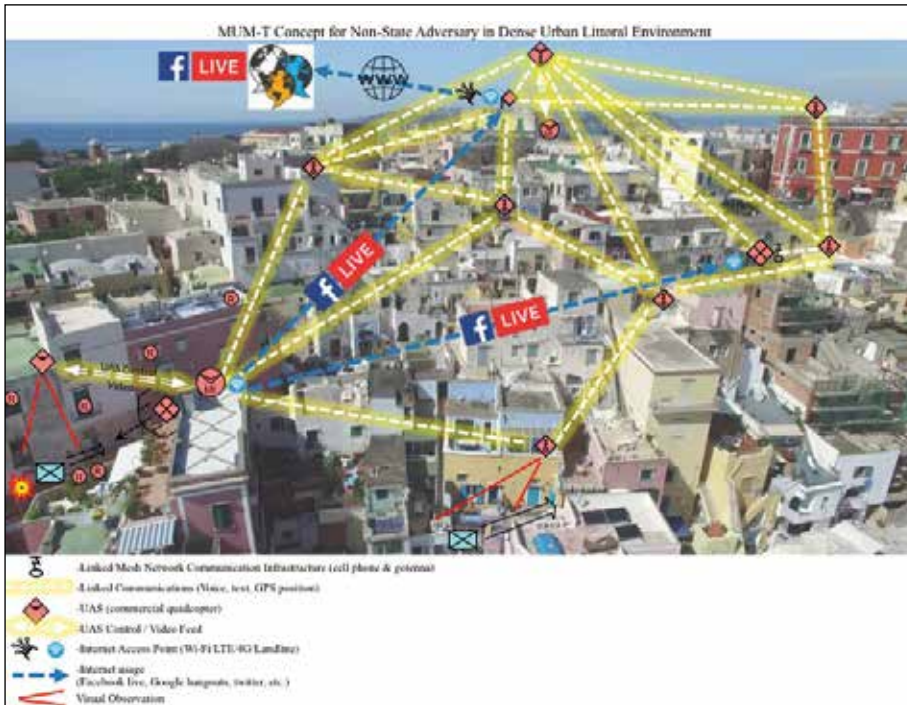
Figure 1. MUM-T concept for non-state adversary in dense urban, littoral environment. *(Photo by author.)*

not. Additionally, in this networked fashion, success can be measured by whether an otherwise technologically unmatched belligerent can operate in fifth generation warfare, bringing some level of symmetry to the battlespace. Cumulatively, this could allow a non-state commander to increase his operational tempo and further complicate the reality of the U.S. military. Lastly, success can be measured by whether this concept can increase the flow of information out of the battlespace effectively enough to negatively influence U.S. public opinion and ultimately break strategic policy makers' will to fight.

Tradeoffs

The utilization of this concept would impose a tradeoff for both the non-state adversary and for the U.S. military. The non-state actor would have to trade the opportunity to operate and fight in a technologically outmatched fashion. This could appear to not even be a question for many tacticians in a technologically superior military, but there could be some advantage gained by an opponent who chooses to operate totally off-grid, providing some level of asymmetry in a somewhat-reversed fashion. Someone can't be located and isolated on a domain in which they don't reside. So, this would have to be a tradeoff that the non-state commander

is willing to take. Once they chose to seek a MUM-T capability in a contemporary fashion, they would have to assume the risk that U.S. forces may be able to exploit them. The tradeoff which the U.S. military may face is if a non-state actor in a heavily populated, urban area begins developing widely linked communications schemes that operate on unsecure civilian networks, hidden in the mass of the Internet, it will have to develop countermeasures that may also disrupt the daily life of civilians and non-combatants. This could prove to be problematic if the U.S. military is trying to win the support of the local populace whose ability to communicate and conduct business gets restricted.

Areas for Future Research

From this point, there are many areas for future research, which may lead to a better understanding of how non-state actors may approach the concept of MUM-T capabilities. The three highlighted in this section attempt to focus on considerations from the tactical to the strategic level. The first is how quickly, how diversely, and how uniquely application software for mobile
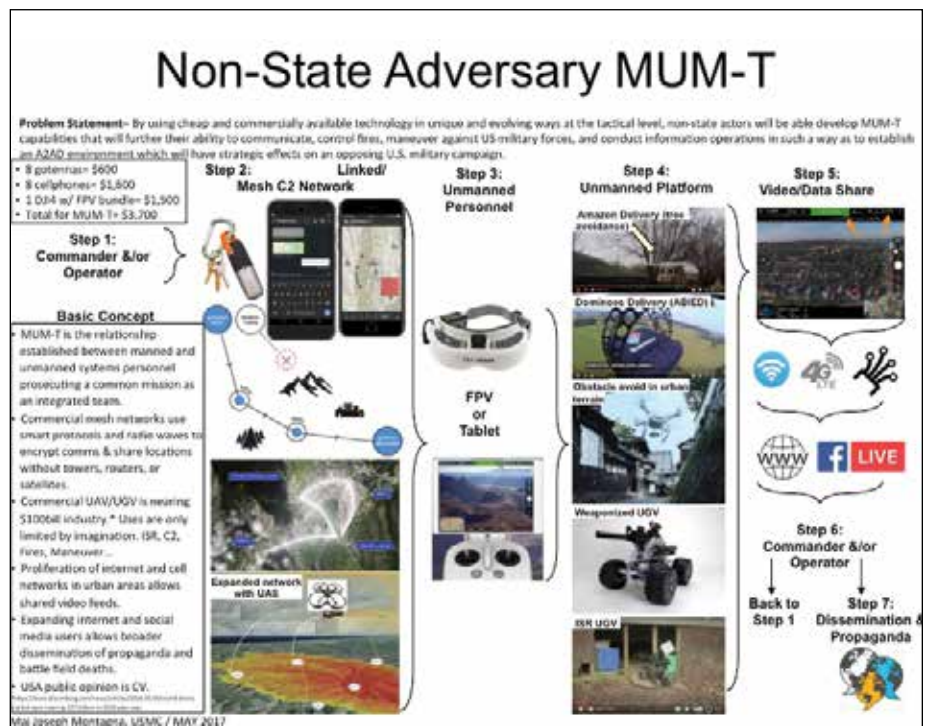

Figure 2. Non-State adversary MUM-T system components. *(Photo by author.)*

phones, linked communications infrastructure, and UAS can get updated and refined to stay ahead of countermeasure attempts and maintain control of a MUM-T capability. The second is if the benefit of developing and maturing a MUM-T capability for use in an urban environment outweighs the social costs which come once a population begins living under a siege mentality, in that death may come at any time from a machine that is watching them from the sky.[7] Lastly is whether a non-state actor is best suited to fight a technologically superior force by focusing on material progress or on its own cognitive progress and how to out-think its enemy.[8] Air Vice-Marshal, United Kingdom's Royal Air Force, Jon Lamonte, astutely noted that the world's largest military powers' ever expanding use of UAS controlled from bases at home may become an impetus for their adversaries to transfer the battlefield away from their homelands and to the control points of those machines.[9]

Conclusion

MUM-T is less about platforms than it is about creating relationships between people to increase information sharing. Inherent in the nomenclature, however, is the fact that an unmanned system is vital to this process and that without it, the operational objective would have to be accomplished with other means. As the U.S. military pursues a third offset strategy that leverages technology to gain battlefield advantages, it is important to remember the basic concept of MUM-T: the machine is simply used to connect people to one another. This is a significant point because "machines don't fight wars … humans fight wars."[10] If the United States pursues ways to remove human cognition from the observation and orientation steps of the OODA loop at the tactical level,[11] commanders' decision-making cycles will be stalled or flawed, thus allowing the enemy to shape the battlefield and achieve victory.

The lessons learned from Mogadishu in the early 1990s reveal that a technologically outmatched adversary will be constantly thinking and evolving with the intent of locating and exploit-ing U.S. military critical vulnerabilities. This was not an isolated incident relevant only to the technologies of a 1993 battlefield; it is an observable trend throughout history. Whether it was David fighting Goliath in ancient times, Egypt fighting Israel in the 1973, or the SNA fighting the U.S. military in 1993, technologically outmatched forces will find gaps and maneuver around their enemies' surfaces to turn tactical actions into strategic victories.

By using cheap and commercially available technology in unique and evolving ways, non-state adversaries will be able to develop MUM-T capabilities that will increase their ability to communicate, control fires, maneuver against U.S. military forces, and conduct information operations in such a way to establish an A2/AD environment which will have strategic effects against an opposing U.S. military campaign. Too many forecasts of future conflict predict that U.S. military actions will occur in the world's urban, littoral landscape against non-state adversaries for a third offset strategy to focus solely on how to create overmatch against another industrialized military. If the third offset strategy does not account for the full spectrum of conflict and the threats therein, adversaries using low-end technology will defeat the U.S. military by using tactics and equipment that allow them to maneuver more effectively despite costing far less, much like David, a shepherd boy with a rock and a sling, defeating Goliath, covered in armor, wielding large weapons, and expecting to battle another prized fighter.

>*Editor's Note: Part I of "The Lessons of Mogadishu" appeared in the January issue of the* Marine Corps Gazette *online. Briefing slides for the Boko Haram Operational Decision Game can be accessed at: https://www.mca-marines.org/gazette/boko_harams_advance_towards_the_islamic_state_of_nigeria.*

Notes

1. Conducting a simple Internet search on the topic reveals a variety of sources which report on the issue. For a particularly interesting report on the matter, see Chris Abbott, et al., "Hostile Drones: The Hostile Use of Drones by Non-State Actors Against British Targets," *The Remote Control Project*, (Online: January 2016), available at https://www.files.ethz.ch.

2. Charlie Winter, "Documenting the Virtual 'Caliphate,'" *Quilliam*, (Online: October 2015), available at www.quilliamfoundation.org.

3. Though legacy systems like radio remain prolific in countries like Nigeria, where this ODG took place, the Internet, especially in littoral areas, is gaining more users and is becoming more available for home use. For example, according to the report, "Contemporary Media Use in Nigeria," published by the Broadcasting Board of Governors, from 2012 to 2014, while radio and television usage both declined, Internet usage increased.

4. Department of Defense, *Unmanned Systems Integrated Roadmap FY2011–2036*, (Washington, DC: 2011).

5. Megan Eckstein, "Manazir: Networked Systems are the Future of 5th-Generation Warfare, Training," *USNI News*, (Online: May 2016), available online at https://news.usni.org.

6. Ibid.

7. David Kilcullen and Andrew McDonald Exum, "Death From Above, Outrage Down Below," *The New York Times*, (Online: May 2009), available at http://www.nytimes.com.

8. To highlight this point, it is beneficial to reference the 1973 Arab-Israeli War. Albeit, that war was a state-on-state contest, but the point remains the same. Egypt knew it could not match the material assets and technological capabilities of Israel, so it focused its effort instead on achieving political success, without a military victory, by out-maneuvering Israel in the cognitive domain.

9. Jon Lamonte, "Address on the Future of UAVs to the Royal United Services Institute," *Royal Air Force*, (Online: June 2009), available at http://www.raf.mod.uk.

10. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War*, (Boston: Little, Brown and Company, 2002).

11. "Manazir: Networked Systems are the Future of 5th-Generation Warfare, Training."