2017 LtCol Earl "Pete" Ellis Essay Contest: Second-Place Winner

# War by Other Means

## Integrating modern technology

by Maj Nicola "Nick" Brunetti-Lihach

***>Maj Brunetti-Lihach is a Communications Officer currently assigned as a student to the U.S. Army Command and General Staff College in Fort Leavenworth, KS. His previous assignments include Marine Corps Forces Special Operations Command and Combined Joint Special Operations Task Force-Iraq.***

Armed with only a radio and a nine-line, a well-trained Marine can wreak havoc on enemy forces. During Operation IRAQI FREEDOM, lethal air and artillery fires destroyed, suppressed, or neutralized targets of all shapes and sizes. In that place and time, lethal combined arms were an effective means to an end. The standard has now changed. The ability to shoot, move, and communicate can no longer be taken for granted. Today's maneuver units do not have the tools to integrate lethal fires with non-lethal cyber (cyberspace) and EW (electronic warfare) fires at the tactical level in realtime to win a fight with a near-peer or contest cyber and the electromagnetic spectrum. Today's threats are no longer line-of-sight projectiles. Threats at the tactical edge may originate from anywhere in the world. In order to address the gaps in doctrine, organization, tactics, and technology, the MAGTF must adapt and evolve.

Marines should not fight with one hand tied behind their backs. For years, Russia has demonstrated the capability "to artfully converge and weaponize information operations, electronic warfare, and network warfare,"[1] yet the ability to produce non-lethal effects within the MAGTF lies largely with the CCDR (combatant commander) or JFC (joint force commander). Imagine a squad in Operation IRAQI FREEDOM marching up the Euphrates, waiting for fires clearance from the CCDR staff. Fortunately, the Marine Corps has not been idle. For instance, SPMAGTF 17.1 pushed the realm of the possible in developing a combined arms coordination center to collocate fires, intelligence, communications, and information warfare subject-matter experts.[2] Yet there remains little capability or capacity at the tactical level. The MAGTF information environment operations concept of employment recognizes there is "an inadequate mechanism in place for the MAGTF commander to comprehensively understand, plan, and execute Information Environment Operations as an integral component of MAGTF operations."[3]

While victory has many fathers, failure is an orphan. One reason for the MAGTF's inability to contest the spectrum of non-lethal effects is 17 years of operations against third-world powers and non-state actors or perhaps a lack of vision and complacency caused by a lack of resources and equipment. Yet, given the availability of modern technology and communications that "have lowered the barriers of entry for non-state actors,"[4] one need not look beyond the diverse application of munitions in tandem with hacking, propaganda, and commercial drones employed by the Islamic State to assess the realm of the possible. In order to harness lethal and non-lethal fires for tomorrow's fight, the MAGTF must possess the people, organization, and tools to create and exploit windows of opportunity at the tactical level through lethal or non-lethal means to ensure freedom of maneuver. The first step is to address the lack of institutional understanding of cyber and EW through realistic information environment operations training. The second step is to foster an environment of creative thinking among key leaders. The third step is to ensure the MAGTF is properly organized to execute tasks. Lastly, the MAGTF must rapidly integrate modern technology securely within existing systems.

Information environment operations span the depth and breadth of sea, air, land, space, and cyber domains, dependent upon the EMS. The Marine Corps defines information environment operations as "integrated planning and employment of MAGTF, Naval, Joint, and Interagency information capabilities, resources, and activities"[5] in order to win a contested operating environment. U.S. overmatch in traditional combined arms and high-end technology placed less consideration on this wider spectrum of warfare, and adversaries stole a march. Ironically, the democratization of information through the so-called information revolution and dispersion of cheap modern technology such as information technology (smartphones and software) is largely absent at the tactical level within the U.S. military. While the Services have approached tactical distributed mobile computing cautiously, its adversaries have proven far more sanguine as to its advantages and have aggressively applied cyber and EW capabilities against U.S. interests at home and abroad. At one time, cutting-edge information technology was the near-exclusive domain of the United States. No more.

A non-lethal information environment operation may operate and defend MAGTF $C^2$ (command and control) networks; provide information environment battlespace awareness; attack or exploit networks; or inform, influence, deceive, or control activities. Today most cyber and EW assets are dedicated to strategic or theater-wide targets or are in the hands of "big box" assets such as EW aircraft and remote cyber warriors. Cyber and EW capabilities should nest within traditional Marine Corps concepts of maneuver warfare at the tactical level. One method is, "if you build it, they will come," outlined by the *Marine Air Ground Task Force Information Environment Operations: Concept of Employment* and recent MIG (MEF information group) structure. Under this construct, the MAGTF develops the information environment operations capability, imbues its principles within the MAGTF, and offers the capability to CCDRs and JFCs. Yet without joint, combatant command, and theater special operations command acceptance, this concept may not get resourced or utilized. Hence, the Marine Corps requires viable methods to apply traditional tactics, techniques, and procedures to synchronize lethal and non-lethal fires with movement and maneuver on the battlefield.

A significant challenge to collective understanding and acceptance is visual. Commanders, riflemen, and pilots want to see a target and engage or defend directly. By its nature, information environment operations encompass physical and non-physical objectives which cannot be directly targeted or defended against by traditional means. Hence, any ability to visualize the information environment will lead to cognitive understanding to achieve effects in the battlespace.

Furthermore, the concept of multi-domain battle is nothing new to Marines accustomed to operating in all domains. As one author pointed out, "the individual Marine on the ground does not care about domains when trying to achieve an objective,"[6] only the effects. Yet for the MAGTF staff and subordinate commanders, organizing principles are important. If the mission objectives require fire and maneuver, key leaders should be well versed in the complementary nature of lethal and non-lethal fires and how the FECC (fires and effects coordination center) plans, coordinates, integrates, directs and monitors all organic and supporting lethal and non-lethal fires.[7] Because modern fights are joint and coalition in nature, this cannot be done by the MAGTF alone—it requires interoperable systems and complementary forces across the joint and coalition C4ISR (command, control, communications, and computers and intelligence, surveillance, and reconnaissance) network. In the information environment, the ability to achieve decisive effects is limited to the imagination. Fortunately, Marines excel at improvising and innovation.

For example, as a company with a battalion landing team advances ashore to its objective, it may launch multiple organic SUAS (small unmanned aerial systems) for ISR and sensor collection. The SUAS feed video and data to forward Marine targeteers and intelligence analysts armed with handheld TACROVER video receivers to view the video on tablets in realtime. The SUAS sensors detect hostile forces and multiple enemy reconnaissance drones ahead. Overhead, an F-35B detects the enemy drones and spots an armed, Chinese-manufactured CH-5 drone. The F-35B immediately transmits the data simultaneously to the MEU and combined air operations center over its MADL (Multi-function Advanced Data Link) and down to the company over the Link 16 network.

The company commander directs his JTAC (joint terminal attack controller) to request a pre-planned decoy mission through the FECC fires net, bypassing the FDC (fires direction center), which handles organic lethal fires. The company commander directs his platoons to "go dark" to reduce electronic emissions. Pre-rehearsed emissions control procedures are enforced as all non-essential communications are turned off and batteries removed, even from handheld, Iridium-based position location beacons. Only key personnel maintain tactical radios. A smaller group of Marines use specially configured smartphones connected to local host-nation cellular infrastructure, hiding among the common cellular signals in the area of operations. The company slows its advance and increases its use of terrain for natural cover.

The company commander asks for an intelligence update. The attached human intelligence Marine pulls out his smartphone and messages a source in the vicinity of the enemy maneuver element. The Marine's secure smartphone is running software to geo-fence his data with specialized security certificates for data in transit, allowing him to communicate securely with his source. The data is transmitted through proxy servers, which mask some of his electronic signature and simultaneously push the data to the MEU's classified networks. The device is preconfigured to feed critical cursor on target data in near-realtime for the BLT and MEU to process. A releasable version of enabling ATAK (Android Tactical Assault Kit) software is running on the source's device. The company radio operator has a tiny Raspberry Pi computer on his vest running a TAK server. If he loses connectivity with higher headquarters, he can still process, send, and receive data locally.

The source sends back realtime grids, pictures, and video of the enemy on the move, atmospherics, and other data. The intel Marine provides the company commander an update. The JTAC turns to the company commander, notifying him the FECC authorized the enemy drones be neutralized. The FECC confirms the F-35B engaged the CH-5 with its GAU-22/A four-barrel cannon. A thin streak of flame arching along the horizon confirms the same. The JTAC and targeteer launch an EW SUAS configured to engage the enemy surveillance drones, jamming their GPS signals and severing the links to their $C^2$ node. Some enemy SUAS fall from the sky; others wander away from the fight. The EW SUAS then form a screen, jamming known enemy proximity fuse frequencies in order to turn any potential shells into duds. The skies are now clear ahead for the company.

The JTAC pulls RadioMap up on his tablet to analyze the spectrum in his area of operations. His multi-channel,

next-generation handheld radio serves multiple functions; one channel exchanges data through a high-performance line of sight waveform, enhanced by a radio relay embedded in each SUAS to expand coverage range. This relay is able to push the data back to the BLT 20 kilometers away. Fortunately, after his last deployment, the JTAC was able to get a seat at the updated JTAC course, which added cyber and EW tactics, techniques, and procedures.

The FECC receives approval from the joint task force for its pre-planned social media deception operation; the BLT meticulously planned target lists with the MEU FECC, which worked through the JFC CSE (cyber support elements) to begin vetting targets days before the mission began. Fortunately, the JFC and CCDR rules of engagement allowed the MEU to fully employ its lethal and non-lethal capabilities.

***"If we cease to refine, expand, and improve our profession, we risk becoming outdated, stagnant, and defeated."***

***—Gen Alfred M. Gray***

It stretches neither the imagination nor capabilities of existing technology to conceptualize a MAGTF integrating lethal and non-lethal fires on the battlefield. To do so, the MAGTF must ensure understanding of information environment operations among both leadership and rank and file through realistic training. The synchronization of lethal and non-lethal fires adds orders of difficulty upon a process already beset with complexity, friction, and limited resources. The ability to apply desired effects on targets will weigh heavily on MAGTF training, organization, structure, and pre-operational collaboration to ensure coordination, de-confliction, and responsiveness.

In the short term, Marine Corps training, particularly advanced schools such as JTAC and Advanced Communications Officers Course, but also the staff academies and intermediate-level schools, must incorporate cyber and EW instruction, to include capabilities and limitations, along with concepts of employment. Leveraging these courses will carry learning back to the MAGTF for realistic application and the desire to request the capabilities. Tactical formations must also train to simulations of cyber and EW offensive and defensive capabilities to incorporate more realistic lethal and non-lethal effects. This will force planning to occur in all aspects of training, among tactical formations and staffs alike. Predeployment exercises, such as the Integrated Training Exercise, should become laboratories of learning from failure. Each exercise or comparable predeployment event should feature MAGTF air and ground EW assets (e.g., F-35B) turning their non-lethal capabilities on our own maneuver forces. This will force small unit leaders to face degraded $C^2$ environments, to adapt, and above all, to gain an appreciation of the challenges ahead. As T.R. Fehrenbach observed, a "competent, adequately trained basic rifleman could be made in eleven months. Competent, well-schooled commanders and staffs could not."[8] Long term, a necessary MOS should be established to provide alternate career tracks for critical non-lethal fires planners within the intelligence, artillery, aviation, and communications fields.

Meeting an emerging near-peer threat requires creative thinking. Allied victory during World War II was as much due to innovations such as the Higgins boat and cracking of German and Japanese codes. Marines should be trained to fight at a disadvantage, to include a cyber- and EW-restricted environment. This will serve to improve critical and creative thinking and foster adaptation and innovation. It will further present dilemmas to commanders to assess and accept greater risk for potential greater opportunity. Maneuver elements should train to seamlessly shift among tactical—and commercial—networks during operations with degraded communications. Despite decades combating countless foes steeped in the arts of cunning, risk-taking, and asymmetric warfare, the U.S. military and the MAGTF continue to appear unprepared to assess and address a weaker foe.[9]

The MAGTF needs a framework to communicate this paradigm shift to all Marines to build a base of knowledge to initiate, request, and monitor lethal and non-lethal fires and to push this capability down to the lowest levels possible. Train squad, platoon, and company leaders to know when and how to request non-lethal fires, to include cyber and the range of EW (electronic attack, protection, support).

From an organizational standpoint, the MAGTF FECC must be tied into the joint task force's fires process, to include the CSE and CCDR joint cyberspace centers to ensure coordination and de-confliction. Authorities cannot be adjudicated by a MAGTF commander in the midst of an operation, but understanding of authorities is essential. Unfortunately, the process across the DOD simply has not adjusted to be responsive at the forward tactical edge. During operations, it matters not that a Marine necessarily conducts the attack but that the Marine unit receives the effects requested in a timely manner to support a tactical objective. In other words, it is less important for a MAGTF Marine to hack an enemy network than to understand how a cyber effect is nominated, vetted, and validated and how its effects will synchronize with other tactical echelons within the MAGTF.

Battalion-sized forces should have the capacity to task organize SMEs to companies to plan or execute lethal and non-lethal fires integration. This individual needs the requisite skill sets to understand, process, and direct lethal and non-lethal fires. This may be a JTAC or FAC with additional training or an intelligence or communications Marine with the requisite skill set. It may be more efficient to assign a necessary MOS to a range of specialties to deepen the talent pool.

Move authority to where the information is, as David Marquet espouses

within his intent-based leadership philosophy.[10] In addition to manpower and training, reorganizing units to improve training and flatten the lines of communications is worth consideration. For example, transferring the VMU (unmanned vehicle squadrons) to the Marine division or ANGLICO would bolster the ability to organically integrate ISR sensor capabilities with fires. Modern, commercial Group 2 UAS systems can be operated with significantly reduced manpower and equipment requirements of existing VMU detachments. Integrating longer-range Group 2 and Group 3 UAS assets is a unique discipline and is distinct from squads and platoons flying small commercial drones for overwatch. Flying drones can be taught relatively quickly, but the analytical ability to ingest, transmit, and process the video, data, and metadata cannot. Next generation Groups 2 and 3 UAS will be integrated with companies and battalions; this task organization should be reflected in garrison.

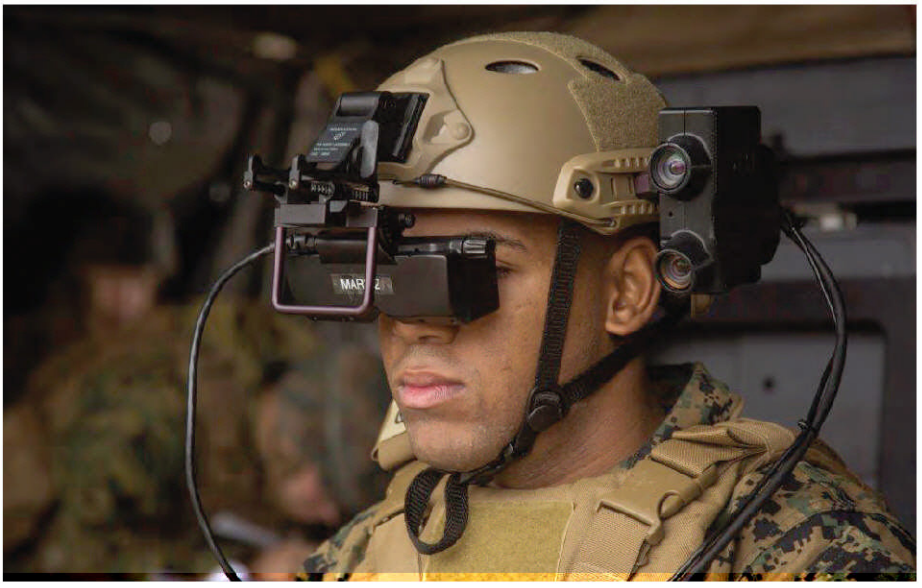
Access to information is essential to the decision-making process. The technology at the so-called last tactical mile must provide sufficient information to decision makers or target engagement authorities. Given the requirement for the MAGTF to process sensor data and share in realtime, persistent and interoperable communications is paramount. In any near-peer fight, the same requirement pertains to joint and coalition forces. There are plenty of technologies and capabilities available today to the MAGTF commander to meet or close this gap in analog and digital interoperability. Software such as Mobile Joint Effects Coordination Link and Android Tactical Radio Application Extension can process and translate disparate waveforms and protocols in near-realtime. Warfighting systems and platforms will likely never be "pure-fleeted" with all sensors operating on the same frequency and protocol. With the right technology, it's not even necessary for disparate MAGTF systems to use the same frequency or waveform when software can do the translation.

Integration of commercial cellular/wireless networks through secure means is an untapped resource for information sharing and redundancy to enable lethal and non-lethal fires fusion. Today, over half the people on earth have smartphones and two thirds have a mobile phone. Mobile connection speeds are on the rise and expanding, with increased access to 3G/4G across the Middle East and Asia.[10] There is enormous potential for MAGTF C4ISR systems to leverage this bandwidth at least to supplement or provide redundant means of communications. With powerful, small form-factor computers such as Raspberry Pi, the MAGTF can scatter de-centralized mesh networks with their own organic virtual servers, providing minimal required computing power across the area of operations to ensure de-centralized C4 capabilities.[11] If the link to the distant MEU commander is severed, the BLT or company can still send/receive analog and digital information. Fortunately, efforts to integrate disparate software are also currently underway.[12]

While technological overmatch is critical, the back door cannot be left open. The Services have become complacent in securing communications over the past two decades, given the threat environment. This will be untenable in a near-peer fight. All communications, to include ISR, must be secured properly at all times. This extends to the use of Selective Availability Anti-Spoofing Module GPS encryption often overlooked in existing systems. There are also promising new capabilities to better secure antennas against jamming[13] and other initiatives to explore ISR jamming and counter-drone capabilities to small UAS.[14] Future 5G networks further promise faster speeds, less latency, and better encryption, with the added ability to operate in a GPS-denied environment.[15]

The stigma against employment of commercial mobile devices (e.g., smartphones) must be mitigated. This is largely a matter of education and configuring mobile devices to securely communicate using technology available today. A smartphone with the requisite software applications on the right network with the right security features in the hands of a local/partisan source is a force multiplier. The device does not need MAGTF bandwidth and is not connected to secure MAGTF networks, but it can be configured to send or receive mission-essential data military networks in near-realtime to collect and share information and enhance the MAGTF or JFC common operating picture.

Reliance on satellite terminals for data connectivity must be reduced. While the military will gain a capability upgrade around 2020 when the Mobile User Objective System satellites are fully operational,[16] it will provide only



***The Augmented Immersive Team Trainer provides a virtual training experience, in this case for fire support training.*** *(Photo by LCpl Juan A. Soto-Delgado.)*

***Communications equipment capabilities are continually improving because of lessons learned in training exercises and during deployments.*** *(Photo by Cpl Timothy Valero.)*

limited bandwidth and continue to be over reliant on satellites for connectivity. There are existing high performance waveforms today which offer high-speed video and data well beyond the range of ANW2 or SRW, such as TrellisWare, Wave Relay, and Silyus, to name a few. This technology has been available in small form-factor radios for years.

There is something to be said about brilliance in the basics. Within the MAGTF, preparedness should translate the "weapons, gear, self" mantra into accuracy and currency of firmware and software on tactical radios, tablets, phones, and drones. Failure to do so in a near-peer battle is akin to a Marine falling asleep at his post. Maintenance and currency of MAGTF C4ISR nodes should be placed on the same footing with weapons systems accountability.

The *MOC* (*Marine Corps Operating Concept*) reminds us we are not properly "organized, trained, and equipped"[17] for the complexities of the future operating environment, highlighting proliferation of technology, control of electromagnetic signatures, and effective employment of information warfare. With the advent of cyberspace as a fifth domain, the interdependency of worldwide communications (and access to the EMS) is inextricably linked. The consequences of degraded $C^2$ due to lack of communications were illustrated by T.R. Fehrenbach, describing conditions during the initial North Korean assault:

> Casualties among officers of high rank of the U.S. Army were greater in proportion to those of any fighting since the Civil War. They had to be. There were few operable radios with the regiments in Korea, and almost no communication from command posts down to the front positions.[18]

Commanders could not command and control and thus traveled to company and platoon areas to personally direct actions. There should be no presumption of asymmetric C4ISR advantage in future conflict, but the MAGTF should be as prepared as possible with robust, secure, and resilient networks in place.[19] Even given advanced systems, it should not be overlooked that battles are "won not by weapons, but by men."[20]

Six decades removed from the Korean War, Air Force LtCol Josh Koslov, 43rd Expeditionary Electronic Attack Squadron, echoed the point more succinctly: "If you can't talk, you can't fight."[21] If the MAGTF goes to war lacking interoperability, security, and resiliency, it will meet the same result. Hence the need for air/ground assets to communicate across the spectrum is essential, as is the need to deny the same to the enemy. Thinking outside the box, such as recent Defense Innovation Unit Experimental efforts to develop software to manage dynamic strikes in lieu of Microsoft Word and Excel, is one example.[22]

The Marine Corps is perennially focused on the tactical level of war. As lethal and non-lethal warfighting functions have converged, a tangible concept of how to leverage such capabilities for tactical effects has become abstract. Much as a rifleman trains his sights on a target or a maneuver unit masses firepower on an objective, the Marine Corps has determined in its MAGTF information environment operations concept of employment that fusion of traditional fire and maneuver with emerging cyber and EW capabilities are essential to the MAGTF translating orders into specific effects. Technological and organizational shortfalls have led to needed overdue research, development, and experimentation as the information environment becomes operationalized. In order to fully realize this goal, the MAGTF must ensure understanding of information environment operations through training, foster an environment of creative thinking among key leaders, ensure formations are properly organized to execute the tasks, and rapidly integrate modern technology into existing systems.

"War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously."[23]

---

**Notes**

1. Rodney D. Harris and Jeffery D. Morris, "Cyber Talent for Unified Land Operations," *Small Wars Journal*, (Online: January 2016), available at www.smallwarsjournal.com.

2. Rich H. Robinson III, "Beyond the Strong Point," *Marine Corps Gazette*, (Online: August 2017), available at www.mca-marines.org.

3. Headquarters Marine Corps, *Marine Air Ground Task Force Information Environment Operations Concept of Employment*, (Washington, DC: July 2017).

4. Department of Defense, *Strategy for Operations in the Information Environment*, (Washington, DC: June 2016).

5. *Marine Air Ground Task Force Information Environment Operations Concept of Employment.*

6. Brian E. Russell, "Cyberspace Operations and Electronic Warfare Convergence, Part I," *Marine Corps Gazette*, (Online: July 2017), available https://www.mca-marines.org.

7. Joint Staff, *JP 3-09, Joint Fire Support*, (Washington, DC: June 2010).

8. T.R. Fehrenbach, *This Kind of War: The Classic Korean War History*, (Lincoln, NE: Potomac Books, March 2001).

9. Jim Greer, "The Weaker Foe," *The Strategy Bridge*, (Online: March 2017), available at https://thestrategybridge.org.

10. Inno-Versity, "Inno-Versity Presents: 'Greatness' by David Marquet," YouTube video, 9:47, (Online: October 2013), available at https://www.youtube.com.

11. Simon Kemp, "Digital In 2017 Global Overview," *We Are Social*, (Online: January 2017), available at https://wearesocial.com.

12. Joseph Trevithick, "The U.S. Army Wants to Call in Cyber Attacks Like Artillery Fire," *The Warzone*, (Online: April 2017), available www.thedrive.com.

13. Katherine Owens, "Navy Seeks Lightweight, Jam Resistant Antennae," *Defenses Systems*, (Online: August 2017), available at https://defensesystems.com.

14. Colin Clark, "ThunderDrone: Best Name Ever, But What Is It?" *Breaking Defense*, (Online: August 2017), available at https://breakingdefense.com.

15. Kris Osborn, "Samsung Works with U.S. Military to Prototype New High-Speed 5G Network," *Defense Systems*, (Online: November 2017), available at https://defensesystems.com

16. Stew Magnuson, "Army One Step Closer to On-the-Move Satellite Comms," *National Defense*, (Online: August 2017), available at https://www.nationaldefensemagazine.org.

17. Headquarters Marine Corps, *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*, (Washington, DC: September 2016).

18. *This Kind of War.*

19. Ian Brown, "When the Unblinking Eye Closes," *War on the Rocks*, (Online: October 2017), available at https://warontherocks.com.

20. Michael Howard, "Men Against Fire: The Doctrine of the Offensive in1914," in *Makers of Modern Strategy*, ed. Peter Paret, (Princeton, NJ: Princeton University Press, 1986).

21. Joseph Trevithick, "America's Electronic Attackers May Have a Secret Mission," *The Warzone*, (Online: June 2017), available at www.thedrive.com.

22. Anthony Capaccio, "Pentagon's Silicon Valley Unit Helps Target Terrorists," *Bloomberg*, (Online: August 2017), available at https://www.bloomberg.com.

23. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: July 1997).