



Defeating Future Hybrid Threats

The Greatest Challenge to the Army Profession of 2020 and Beyond

Maj. John R. Davis Jr., U.S. Army

I would like to thank my research paper advisor at Air Command and Staff College, Dr. Sterling Pavelec, who continually empowered me to push the cutting edge and challenge conventional thinking when writing this article.

Maj. John R. Davis Jr., U.S. Army, is currently a student at the School of Advanced Military Studies, Fort Leavenworth, Kan. He holds a B.S. from Hampton University, an M.S. from Missouri University of Science and Technology, and an M.M.A.S. from Air Command and Staff College, Air University. He most recently served as a small group leader at the Engineer Captains Career Course, U.S. Army Engineer School. His other previous assignments include three combat deployments to Iraq as a platoon leader, company executive officer, and Multi-Role Bridge Company Commander.

PHOTO: U.S. soldiers leave their defensive fighting positions while preparing for an attack during a full-spectrum operations exercise at Fort Polk, La., 23 October 2010. The exercise trained the soldiers to defeat a hybrid threat comprised of insurgents and organized military forces. (DOD, D. Myles Cullen, U.S. Army)

“**W**E ARE AT a similar warfare inflection point; one that eclipses the introduction of nuclear weapons, the introduction of the air domain and the airplane, and the transition from battleship to aircraft carrier.”¹ Gen. Martin Dempsey’s statement captures the current moment in time with respect to changes in warfare facing the U.S. Army. Similar warfare inflection points in the transition to the air and nuclear domains produced lasting changes to the art of warfighting. New debates about warfare focus on how the evolution of the space and cyberspace domains will influence future conflict. Most defense analysts agree that the nature of the future security environment will be multi-polar (regionally focused) with inherent diversity and complexity. The future environment will present formidable challenges to the U.S. Army. One challenge resides in how to identify, understand, and combat the future threat. Defeating a hybrid threat, consisting of regular, irregular, and criminal elements synergistically working for a common end state, poses the greatest threat to the Army Profession of 2020 and beyond. Future hybrid warfare will test the military expertise, trust, and honorable service of the U.S. Army Profession. Furthermore, this form of warfare will evolve into a struggle to quickly learn, adapt, and out-think a changing hybrid threat.

The current Army Profession will endure. The crucible of combat, ground out in the jungles, deserts, mountains, and rolling plains of past battlefields, has forged the Army Profession that exists today. The near future security dilemma will be a continually evolving hybrid threat. The critical challenge facing the Army Profession of the future is determining what professional competencies to add or adapt in relation to the warfare inflection point that the force currently faces. One solution is the transition to a continually learning organization full of warrior-scholars. This will determine the success or failure of the Army Profession in a dynamic, challenging future. Throughout history, the force that learned more quickly maintained the initiative and

kept their adversary off balance. Another variable will be technology that accentuates the capabilities of the human element in warfare and presents an effective combat multiplier in a race to learn and adapt for the future.

Army Training Circular 7-100 describes the hybrid threat as three distinctly different forces working collectively toward a common objective.² The regular forces portion of the hybrid threat consists of national, uniformed military forces that engage in symmetric, conventional warfare. Regular forces will use identifiable military weapons and equipment with capabilities focused on battles reminiscent of high intensity conflict. Paramilitary forces consisting of insurgents, terrorists, and guerrillas represent the “irregulars” of the hybrid threat.³ Tactics including ambushes, terrorism, improvisation, information warfare, and other forms of asymmetric, unconventional warfare characterize their actions.

Hybrid Threat Constructs

Criminal elements, in the hybrid threat construct, create an enabling capability for adversary operations. Moisés Naím, an internationally renowned journalist and former editor in chief of *Foreign Policy* magazine, describes current global criminal acts as tactics criminal elements employ in a war enabled through globalization, including drug and arms smuggling, human trafficking, and money laundering.⁴ Criminal proceeds from these acts create funding for training and equipping hybrid forces. This presents a serious difficulty for the U.S. Army in an operational environment. The actions of criminal elements represent civil problems for a host nation government to address. However, if criminal actions support the combined efforts of regular and irregular forces, they necessitate a military response.

To assess future implications, a realistic future hybrid threat model is continually under development and review. Recent conflicts, like the wars in Iraq and Afghanistan, have various elements of hybrid warfare. However, the actions of Hezbollah in the 2006 Second Lebanon War represent one example of a future hybrid threat that encompasses the essence of hybrid warfare. At the start of the conflict, the Israeli Defense Forces (IDF) attacked into southern Lebanon in response to Hezbollah

rocket fire into Israel and the kidnapping of two IDF soldiers.⁵ The Israeli government firmly believed that their advanced conventional warfare technology, combined with precision firepower superiority, would quickly overwhelm Hezbollah forces and bring the conflict to a decisive conclusion.⁶ The IDF developed a technology-driven strategy, heavily focused on air power, based on exploiting Hezbollah’s assumed weaknesses and limited warfighting capabilities.⁷

However, Hezbollah’s tactics rapidly transitioned the nature of the conflict from conventional warfare to hybrid warfare, effectively negating the IDF’s technological advancements. Hezbollah developed a strategy that combined conventional warfare tactics and capabilities with guerrilla warfare operations. In one sense, Hezbollah’s actions departed from historical asymmetric, irregular operations and shifted toward conventional tactics. These tactics included defending terrain from fortified defensive positions and maneuvering in formations with conventional warfare weapons and equipment.⁸ On the other hand, Hezbollah personified an “information-age guerrilla force” employing asymmetric military methods atypical of past nonstate actors.⁹ These methods included higher-tech versions of sniping, ambushes, harassing indirect fire, and the use of civilians, including houses, as shields from attack.¹⁰

As the weaker force in the conflict, Hezbollah realized it could not destroy the IDF or break the Israeli will through large force on force engagements. Instead, at the strategic level, Hezbollah employed an approach to the war that aligned with Thomas Schelling’s strategy of coercion and Robert Pape’s strategy of coercion by punishment.¹¹ In contemporary international relations theory, coercion is persuading an adversary to stop or modify their actions by adjusting the cost-benefit analysis of their current campaign.¹² In essence, Hezbollah attempted to coerce the Israeli government by punishing the Israeli population with rocket barrages.¹³ In many ways this was reminiscent of some of the strategic bombing campaigns in previous wars, but with a different means of delivering the actual munitions.¹⁴ Hezbollah’s rockets served as an instrument of coercive pain inflicted to instill fear and break the resolve of the Israeli population.

From an operational framework perspective, Hezbollah used ground forces as an effective shaping operation to set the conditions for their decisive operation of rocket attacks into sovereign Israeli territory. In addition, ground forces prolonged the conflict in time and space, which forced the Israeli population to endure additional rocket volleys.¹⁵ Hezbollah's ground forces established an area defense in depth to protect their rocket launch sites from destruction and to disrupt a perceived IDF ground invasion. Hezbollah constructed complex conventional defensive sectors with fortified defensive positions, underground sustainment facilities, engagement areas, ambush sites, and firing points for Anti-Tank Guided Missiles (ATGMs).¹⁶ Although the main intent of these defensive arrays was to hold ground, at the tactical level irregular ambushes with small arms fire and ATGMs supported an indirect strategy of coercion by inflicting additional pain on the Israeli populace via IDF military casualties.¹⁷

Hezbollah's strategic, operational, and tactical efforts prevented a quick, decisive victory for the Israelis. Coordinated attacks prolonged the campaign long enough to allow a strategy of coercion by punishment through rocket attacks to achieve the desired end state of a stalemate. The Israeli government and populace grew tired of casualties and unsuccessful attempts at neutralizing Hezbollah rockets attacks. Furthermore, media coverage of the conflict publicized images of Lebanese civilian casualties and diluted international support for IDF offensive operations.¹⁸ On 12 August 2006, the United Nations Security Council unanimously accepted a resolution calling for an end to hostilities in southern Lebanon.¹⁹ On 13 August, amid continuing rocket barrages and mounting IDF casualties, Israel came to the bargaining table and eventually accepted the cease-fire agreement.²⁰ The conflict resulted in a deadlock where Hezbollah scored a psychological victory, viewed as a "Divine Victory" in Hezbollah's opinion, by both avoiding defeat and embarrassing the Israelis.²¹ The enduring significance of this conflict is "the combination by Shi'a militia of conventional military tactics with guerrilla and terrorist activities appeared to represent a novel approach to war that would revolutionize conflicts in the twenty-first century."²² Hezbollah did not wage a true guerrilla war or a true conven-



U.S. citizens evacuated from Lebanon disembark from a U.S. Air Force C-17 Globemaster III aircraft on the flight line at McGuire Air Force Base, N.J., 23 July 2006. (U.S. Air Force, Kenn Mann)

tional war. Instead, it waged something in between. The hybrid warfare phenomenon, even though it is not a new form of warfare in history, poses a daunting challenge to the U.S. Army of the future.

The game changer associated with the future hybrid threat is that hybrid warfare will likely adopt the best capabilities of both conventional and irregular forces involved to create a new, truly hybrid form. "Future wars will likely entail an increasingly vague distinction between the conventional and the irregular; indeed these forms will meld into one."²³ The hybrid threat will morph into a combination

of regular and irregular forces with the inclusion of criminal elements. The lines between all three elements will blur and they will become indistinguishable. The same unit will be capable of rapidly transitioning between operations and tactics that span the full range of military operations. A hybrid force will utilize conventional warfare capabilities to win symmetric battles at decisive points in a conflict and then quickly dissolve into the population to continue a protracted campaign of asymmetric tactics for steady state operations. In addition to symmetric and asymmetric operations, concurrent criminal activities will pose additional threats. A well-developed and detailed future hybrid threat model is difficult to create because each hybrid war will be unique. The evolution of the threat and its truly “hybrid” nature will always create new enemies for the U.S. Army to fight based on the actors involved.

Future Challenges

Future U.S. Army formations will face significant challenges combating and defeating a hybrid threat. Hybrid warfare will stretch existing capabilities of the U.S. Army in a struggle to continually learn and adapt. Furthermore, these challenges will indirectly stress the current and future Army Profession. The triple nature of hybrid warfare creates the need for complementary, but often exclusive, strategies to defeat a variety of foes. The essence of this dilemma rests in a strategy of mass versus dispersion. In order to effectively defeat a conventional force, an army must engage in a strategy of mass and concentration. In conventional warfare, victory is achieved by concentrating all the available effects of overwhelming combat power in offensive operations or massing all the available effects of overwhelming combat power for defensive operations.²⁴

However, in order to defeat an irregular force, an army must disperse to control and secure the operational environment. One objective for both forces in counterinsurgency warfare is control of the population.²⁵ A major focus in this form of warfare is separating the insurgent from the rest of the population.²⁶ These two strategies create a quandary where an army is vulnerable to conventional attack when it disperses to deal with enemy’s irregular forces, but cedes control of the operational environment and population to the enemy when an army keeps its forces concentrated.²⁷ A similar

condition emerged in the Vietnam War. American commanders found it difficult to fight regular North Vietnamese Army divisions while simultaneously trying to dislodge irregular Viet Cong formations from the South Vietnamese population.²⁸ Attempting to do both creates a case of trying to be strong everywhere that can easily result in being strong nowhere. This will create an ineffective strategy in future hybrid conflicts. Furthermore, neutralizing the criminal element of the hybrid threat will require the formulation of an entirely new strategy that includes close coordination with host nation civilian security forces and police to bring these groups to justice.

Complications with executing operational art and design to develop a coherent strategy for hybrid warfare, and actually implementing that strategy, will test the military expertise of the Army Profession. Army personnel are experts in “the employment of Landpower in a distinctly American military context.”²⁹ As experts, professional knowledge of doctrine, strategy, and tactics guide the use of Landpower to achieve decisive action. This knowledge transforms into a high-level competence in various military operations when coupled with unit and individual training.³⁰ The development of a balanced mass and dispersion strategy, coupled with devising ways to neutralize criminal elements, will be a daunting task for future Army planners, but provides an amazing opportunity for innovation.

The U.S. Army will face challenges in cultivating units that are experts in executing both strategies. In the resource constrained future fiscal environment, the Army will face tough budgetary choices. The allocation of funds to train for multiple mission sets will be a hard budgetary sell; the Army may find itself strained to find innovative ways to train for more, with less resources. Units will face adversity training for both conventional warfare and irregular warfare to be considered experts in both disciplines. The knowledge of doctrine, strategy, and tactics for both forms of warfare will still exist, but the individual and unit training required to convert that knowledge into expertise may not.

The IDF faced a similar situation in the 2006 Second Lebanon War. Prior to the war, Israeli ground forces engaged in years of counterinsurgency operations against bordering Arab nations. These operations significantly degraded conventional, symmetric warfare capabilities within

the IDF.³¹ Although knowledge of conventional warfighting still existed in the IDF, the lack of training in that area created a shortage of military expertise in conventional operations. Israeli ground forces found themselves at a tactical disadvantage when fighting Hezbollah in a hybrid war. Swinging the U.S. Army training pendulum too far to the right (the conventional paradigm) or too far to the left (the irregular paradigm) has the potential to create similar issues for future U.S. Army forces engaging in hybrid warfare. Composite risk management will be critical to identify acceptable risks and well-developed controls to help maintain a high level of military expertise across the range of military operations in the future.

Extended Nature of Conflict

Another challenge to winning a hybrid war is the extended nature of the conflict. Hybrid warfare is inherently protracted. No quick solutions exist in these wars. In most cases, the U.S. Army will possess technological, organizational, and professional military advantages in relation to its adversaries. In order to overcome the U.S. Army's technological advantages, potential adversaries will wage hybrid warfare to extend conflicts in time and space. Also, adversaries will expand wars to include indigenous populations. A hybrid war eventually devolves into a protracted battle of wills to control a population and test the strategic patience of a hybrid threat's opponents.³² Throughout history, numerous technologically superior nations failed to achieve lasting, decisive victory due to the protracted nature of hybrid war.

Temporal and spatial protraction of hybrid conflicts will strain the public's trust in the Army Profession. As regards the importance of trust in the Army Profession, Gen. Robert Cone stated that, "trust can be considered the life blood of our profession."³³ Trust permeates throughout the whole organization and enables the Army to successfully employ Landpower across the globe in response to current and future contingency operations. Trust from soldier to soldier, soldier to officer, civilian leaders to Army leaders, and between citizens and the Army creates mutual bonds of confidence in the actions of the other. As a hybrid conflict protracts, civilians, political leaders, and military personnel in combat begin to question the approach to war as

the achievement of objectives bogs down. The lack of quick and tangible results in a hybrid war raises questions of confidence in the military strategy to the conflict. Measures of effectiveness and timelines for termination of the conflict can be hard to gauge and then explain to the public. Waning popular support for the war inevitably follows.

Skepticism and doubts have the potential to erode the bonds of trust critical for the Army Profession to fully function. In the 2006 Second Lebanon War,

A hybrid war eventually devolves into a protracted battle of wills to control a population ...

broken trust between the IDF and the Israeli people were voiced in the media. Television newscasts "denounced the IDF and what it called idiotic maneuvers."³⁴ Front page stories in newspapers questioned the IDF decision-making process, failing goals in the war, and army performance.³⁵ By the end of the conflict, historical consensus among experts maintains that the Israeli public was demoralized and frustrated. They felt betrayed by pre-war IDF predictions of a quick, decisive victory and the actual outcomes of the conflict.³⁶ Widespread Israeli discontent after the 2006 Second Lebanon War provides a contemporary example of popular unrest similar to Americans in the 1970s after the Vietnam Conflict. This portion of U.S. Army history has become a repressed and overlooked memory tucked away in literature and post-war studies. However, if it has happened before, it can happen again.

Strategic Objectives

In addition to protraction, hybrid warfare requires a detailed understanding of the strategic objectives of the enemy. Sun Tzu proposed the timeless theory, "know the enemy and know yourself; in a hundred battles you will never be in peril."³⁷ In Sun Tzu's view, it was critical to understand the enemy (their strengths, weaknesses, and motivations) as well as yourself to ensure victory. This theory is applicable

to any war, but is critically important to combating a dynamic and evolving hybrid threat. A deep understanding, bordering on empathy, of a hybrid threat will help to develop an effective strategy to combat it. This understanding must include the threat's powers of resistance, ideology, resolve, history, and culture.³⁸ A thorough understanding of the enemy will lead to a clear strategy with significant chances for success.

Attempts to gain intelligence superiority over a hybrid threat will also strain the military expertise of the Army Profession. The U.S. Army currently possesses a significant array of Reconnaissance, Intelligence, Surveillance, and Target Acquisition (RISTA) systems.³⁹ Properly employed RISTA systems can provide Army forces with real time operational data, time sensitive targeting, and a detailed representation of the threat and operational environment. However, this system is based on layers of sensors to gather information. By overwhelming and saturating RISTA system sensors with false information, a hybrid threat can negate

a U.S. Army technological advantage.⁴⁰ From a strategic perspective, this condition represents an A-type military deception where a hybrid threat increases ambiguity surrounding its operations by saturating U.S. RISTA sensors with false and irrelevant information.⁴¹ Intelligence analysts could draw false conclusions from conflicting data and pass incorrect information to Army leaders. Decisions would then be made based on false information and intelligence.

Knowledge and training inculcates Army leaders with military expertise to exercise mission command and required discretionary judgments without close supervision.⁴² An incomplete understanding of a hybrid threat and an operational environment will complicate an Army leader's decision-making cycle. Clausewitz described a state of psychological fog (unpredictability and uncertainty) that clouded the judgment of the military commander.⁴³ RISTA saturation by a hybrid threat aligns with Clausewitz's theory and will create a psychological fog in Army leaders that obstructs military expertise. In



(U.S. Army, D. Myles Cullen)

U.S. Army Gen. George W. Casey Jr., Army chief of staff, participates in an after-action briefing following a full-spectrum operation exercise at Fort Polk, La., 23 October 2010.

the 2006 Second Lebanon War, Israel struggled to execute intelligence collection that assembled a full understanding of conflict and threat characteristics.⁴⁴ This intelligence gap exacerbated Israel's difficulties in developing a comprehensive strategy to defeat Hezbollah in a hybrid conflict.

A vital part of understanding a hybrid threat is grasping the lack of moral or ethical restraint displayed in the execution of adversary operations. Rule of law and Geneva Conventions will not limit a hybrid threat's operations. This adversary fails to acknowledge and abide by both the legal and military concepts. In hybrid warfare, "the enemy does not fight fair and is fighting not only a fight in theater, but also in the living rooms of America."⁴⁵ Hybrid threats will use information warfare to achieve a marked advantage during critical times in a conflict to sway indigenous and international support in their favor.

The U.S. Army dedicates itself to honorable service to the Nation. The Army employs Landpower in a manner that upholds U.S. laws and American values.⁴⁶ Hybrid warfare entails engaging in an unfair fight. The hybrid threat will fight "dirty" in an attempt to draw U.S. Army forces into compromising situations. During the 2006 Second Lebanon War, Hezbollah employed operational shielding to protect key components of its force from IDF attack and interdiction.⁴⁷ On numerous occasions Hezbollah used operatives dressed in traditional Lebanese attire and carrying white flags to redistribute ATGMs among different fighting positions.⁴⁸ For larger resupply operations, Hezbollah used "ambulances and other rescue vehicles for cover in its movements."⁴⁹ "Everything in war is very simple, but the simplest thing is difficult," Clausewitz once espoused in reference to the fog and friction of war.⁵⁰ Hezbollah's resupply operations were no different in regard to this theory. The operational shielding tactics employed by Hezbollah made targeting, disrupting, and interdicting their sustainment operations problematic for the IDF. The psychological fog in war once again challenged Israeli military commanders by forcing them to make moral and ethical decisions on engaging questionable military targets.

Consequences of these decisions surfaced in the international media and degraded the honorable merits of the Israeli campaign. "Throughout the 2006 war, the Lebanese news media reported, and the international news media largely repeated, that

Israel was attacking hospitals, health care facilities, and ambulances; schools, mosques, and churches."⁵¹ By broadcasting attacks on Lebanon's infrastructure and inadvertent civilian casualties, the media swayed international opinion away from Israel and helped to foster a UN resolution for a cease-fire.⁵² In this conflict, Israel viewed itself as an honorable nation with high moral and ethical standards. However, the negative strategic communication narrative that Hezbollah, who openly committed war crimes by attacking Israeli civilians and using their own population for operational shielding, crafted against the IDF brought Israeli's honorable intentions under significant scrutiny.⁵³ Historians argue that Israel did not lose the information war and honorable cause case because they had poor strategic communication techniques. Instead, the Israelis lost because "they had to tell the truth while Hezbollah told lies."⁵⁴ These Hezbollah lies created a public bias against the IDF.

Lt. Gen. Robert Caslen stated that "today's hybrid threats seek complex environments, where the actions of leaders at all levels could and do have strategic consequences."⁵⁵ Actions (both positive and negative) at the tactical level can have an immediate, overarching impact. Through technological advancements, media sources and individuals can instantaneously transmit unvetted military actions, with strategic implications, to the world. A hybrid threat will exploit this condition *by utilizing information warfare. Isolated cases of a lack in judgment (Abu Ghraib, a kill team in Afghanistan) and collateral damage from justified military action will have far reaching second and third order effects felt around the world. Similar cases, like the aforementioned IDF and U.S. Army examples, have the potential to degrade the future honorable service of the U.S. Army.*

Warrior-Scholars

The ambiguous future security environment may challenge the Army Profession, but its core attributes will endure. However, is the Army Profession, in its current form, strong enough to defeat the future hybrid threat and achieve victory in future hybrid warfare? To ensure success, the U.S. Army Profession will need to adapt. One possible shift is the transition to a continually learning organization full of warrior scholars. Peter Senge describes a learning

organization as one where “people continually expand their capacity to create the results they truly desire, where new and expansive patterns of thinking are nurtured, where collective aspiration is set free, and where people are continually learning how to learn together.”⁵⁶

This construct fits well with the U.S. Army. Every member of the Army Profession—the Army soldier, NCO, officer, and civilian—possesses a strong sense of pride in the service they provide to the Nation. In addition, as Army professionals, their focus is always toward finding new and innovative ways to solve problems and improve the organization. Some scholars argue that recent operational challenges in OEF and OIF forced the U.S. Army to learn and adapt to achieve success in counterinsurgency operations.⁵⁷ In this regard, the U.S. Army may already exhibit some characteristics of a learning organization.⁵⁸ However, this concept may only be superficial; the Army has not yet fully embraced the idea. Influential leaders like Maj. Gen. H.R. McMaster and Maj. Gen. Sean MacFarland are examples of warrior-scholars who transitioned their commands into learning organizations focused on thinking and adaptation.⁵⁹ Internalizing the idea of a learning organization in the Army Profession will help to reduce barriers to learn and adapt for the future. Establishing an environment focused on learning will create a climate that promotes scholarly study, critical analysis, and reflection. In this environment, individual learners can flourish and thrive for the greater benefit of the organization.

Another important idea in Senge’s book is the principle of personal mastery.⁶⁰ This principle forms “the essential cornerstone of the learning organization.”⁶¹ In this construct, people commit to their own life-long learning, expand their ability to recognize problems, and then develop plans for success. Over time, individuals increase their work performance as they become vested in achieving goals they helped to shape. This logic incorporates the concept of the warrior-scholar into the Army Profession and increases the collective military and leader expertise of the U.S. Army.

In a recent *Joint Force Quarterly* magazine, Gen. Martin Dempsey introduced concepts on adapting the force. He highlights that military power in the last century focused on measures of weapons and munitions.⁶² However, the future will focus on adapting smartly, and ranking people, in agile organizations, over platforms.⁶³ Gen. Dempsey goes on to highlight that

adapting smartly really means “we have to out-learn and out-think our adversaries.”⁶⁴ The warrior-scholar concept directly aligns with the CJCS’s argument. By investing in the scholarly aspect of the soldier and leader, the U.S. Army can begin to emphasize and invest in human capital instead of platforms. Promotion of life-long learning throughout a soldier’s career from an institutional, experiential, and personal level will pay dividends in an uncertain future. Combating a hybrid threat in a fluid future operational environment will require soldiers and officers who are comfortable in the uncomfortable. Soldiers and leaders who can out-learn and out-think the adversary and adapt more quickly, will prove decisive in hybrid warfare for the U.S. Army.

In a race to adapt smartly, technology presents an effective combat and learning multiplier. Integration of technology into initial entry training, professional military education, and unit level training exercises will greatly enhance the overall learning continuum. Gen. Dempsey, while serving as the TRADOC commander,

Combating a hybrid threat in a fluid future operational environment will require soldiers and officers who are comfortable in the uncomfortable.

commented that “we must make the scrimmage as hard as the game in both the institutional schoolhouse and at home station.”⁶⁵ In an effort to create realistic, future combat conditions for training, technology may well be the key. Within the last few years, TRADOC created the Training Brain Operations Center (TBOC) with this purpose in mind. This center uses technology to gather real world data from current theaters of operations, declassify it, and then manipulate it to replicate the current operational environment to support home station training for units throughout the Army.⁶⁶ In addition, TBOC can use the flexible capabilities of technology to create virtual realities of real-world scenarios from current operations.⁶⁷ This will enable and empower soldiers through training in realistic combat-like environments. Actual, real world scenarios developed with technology can help a warrior-scholar internalize concepts introduced in a traditional classroom environment. The U.S. Army

Engineer School is currently working to push the technology envelope by integrating Virtual Battlespace 2 scenarios and TBOC products into the Engineer Officer Basic and Captains Career Courses. As technology, TBOC, and other organizations like TBOC continue to evolve into the future, the U.S. Army may realize it is just scratching the surface for integrating technology into military education.

What does the future hold? This question is a common one organizations and individuals regularly use for reflection to develop a shared vision for the future. The U.S. Army is no different when it contemplates what is the greatest threat to the Army Profession of 2020 and beyond. The current U.S. security environment is full of uncertainty and unpredictability, with no foreseeable shift in the future. Combating future adversaries will prove

to be the greatest threat to the Army Profession as warfare evolves into a more lethal and aggressive hybrid form. Defeating a hybrid threat and waging hybrid warfare will stretch and strain the *U.S. Army Profession's essential characteristics of military expertise, trust, and honorable service* into a thinking man's war. The experience of the IDF fighting Hezbollah in the 2006 Second Lebanon War serves as an ominous example of how hybrid warfare can test the fundamentals of a professional military. In a race to adapt smartly, the U.S. Army should transition to a learning organization full of warrior-scholars to ensure the vigilant employment of Landpower in the future. The vast possibilities of technology can also provide flexible options to challenge the future generation of U.S. Army Professionals in preparation for the next conflict. **MR**

NOTES

- 1 Martin E. Dempsey, *Joint Education*, White Paper (Washington, DC: Joint Chiefs of Staff, Department of Defense, 2012), 3.
- 2 U.S. Army, Training Circular (TC) 7-100, *Hybrid Threat* (Washington, DC: U.S. Government Printing Office [GPO], 2010), 7.
3. *Ibid.*, 15-16.
4. Moisés Naim, "The Five Wars of Globalization," in *International Security Studies Coursebook* (Maxwell AFB, AL: Air Command and Staff College, 2012), 85.
5. Itai Brun, "The Second Lebanon War, 2006," in *A History of Air Warfare*, edited by John Andreas Olsen, 297-324 (Washington, DC: Potomac Books, Inc., 2010), 297.
6. Williamson Murray, "What the Past Suggests," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, edited by Williamson Murray and Peter R. Mansoor, 289-307 (Cambridge: Cambridge University Press, 2012), 290.
7. William M. Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War* (Maxwell AFB, AL: Air University Press, 2007), 54.
8. Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and The Future of Warfare: Implications for Army and Defense Policy*, Monograph, U.S. Army War College, (Carlisle Barracks, PA: Strategic Studies Institute, 2008), 5.
9. *Ibid.*, xi.
10. *Ibid.*, 4.
11. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996), 12-13. Pape describes one type of coercion as coercion by punishment. This form of coercion raises the costs or risks to the civilian population through direct attack by strategic bombing. Coercion by punishment also adjusts the costs by exploiting a civilian population's sensitivity to large numbers of military casualties. In theory, exposure to constant pain and punishment will force an adversary to accept the coercer's terms and make concessions.
12. *Ibid.*, 12-13.
13. Biddle and Friedman, 49-50.
14. *Ibid.*, 73.
15. *Ibid.*, 50-51.
16. Brun, 302.
17. Biddle and Friedman, 52.
18. Brun, 312.
19. *Ibid.*, 313-14.
20. *Ibid.*, 314.
21. Collin S. Gray, *Airpower for Strategic Effect* (Maxwell AFB, AL: Air University Press, 2012), 259.
22. Murray, 290.
23. Cited in Peter R. Mansoor, "Hybrid Warfare in History," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, edited by Williamson Murray and Peter R. Mansoor, 1-17 (Cambridge: Cambridge University Press, 2012), 13-14.
24. U.S. Army, Army Doctrine Reference Publication 3-90, *Offense and Defense* (Washington, DC: GPO, 2012), 39,64.
25. David Galula, *Counterinsurgency Warfare: Theory and Practice* (New York: Praeger Publishers, 2006), 4.
26. Michael Walzer, *Just and Unjust Wars* (New York: Basic Books, 1977), 186.
27. Murray, 293.
28. Karl Lowe, "Hybrid Warfare in Vietnam," in *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, edited by Williamson Murray and Peter R. Mansoor, 254-88 (Cambridge: Cambridge University Press, 2012), 256.
29. U.S. Army, Army Doctrine Publication (ADP) 1, *The Army* (Washington, DC: GPO, 2012), 26.
30. *Ibid.*, 26.
31. Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*, The Long War Series Occasional Paper 26, U.S. Army Combined Arms Center (Fort Leavenworth, KS: Combat Studies Institute, 2008), 63.
32. Mansoor, 7, 9.
33. Robert W. Cone, "Enduring Attributes of the Profession: Trust, Discipline, and Fitness" *Military Review* (September 2011): 5.
34. Matthews, 47.
35. Cited in *Ibid.*, 47.
36. Brun, 315.
37. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 84.
38. Murray, 307.
39. TC 7-100, 32.
40. *Ibid.*
41. Defense Intelligence Agency, *Intelligence Warning Terminology* (Washington, DC: Joint Military Intelligence College, 2001), 5.
42. ADP 1, 26.
43. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1989), 108.
44. Brun, 321.
45. Jack D. Kem, *Campaign Planning: Tools of the Trade*, Monograph, U.S. Army Command General and Staff College (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2009), 85. Note: Modified for grammar and syntax.
46. ADP 1, 28.
47. TC 7-100, 34.
48. Arkin, 49.
49. *Ibid.*
50. Clausewitz, 119.
51. Arkin, 75.
52. Matthews, 47-48.
53. Arkin, 150.
54. *Ibid.*
55. Robert L. Caslen and Nathan K. Finney, "The Army Ethic, Public Trust, and the Profession of Arms," *Military Review* (September 2011): 17.
56. Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (New York: Doubleday, 1990), 3.
57. Gray, 249.
58. *Ibid.*
59. Mark Moyar, *A Question of Command: Counterinsurgency from the Civil War to Iraq* (New Haven: Yale University Press, 2009), 233-34, 239-42.
60. Senge, 7.
61. *Ibid.*
62. Martin E. Dempsey, "Sustaining Our Edge," *Joint Force Quarterly* no. 68 (1st Quarter 2013): 4.
63. *Ibid.*
64. *Ibid.*
65. Martin E. Dempsey, "Leader Development," *Army Magazine* 61, no. 2, February 2011, 26.
66. *Ibid.*, 27.
67. *Ibid.*