The US Army War College Quarterly: Parameters

Volume 45
Number 1 *Parameters Spring 2015*

Article 10

Spring 3-1-2015

The Individualization of American Warfare

Glenn J. Voelz

The Individualization of American Warfare

Glenn J. Voelz

Abstract: Since 9-11, the United States has embarked on a decade of doctrinal and technical innovations focused on defeating networks and individual combatants rather than formations. This article examines this evolving model of individualized warfare within the context of current debates over the appropriate role of military landpower in an age dominated by persistent threats from non-state actors and unconventional adversaries.

In late 2014, the United States reached a milestone of the 500th non-battlefield targeted strike.[1] Beyond the numbers, this event is notable as one example of a new mode of state warfare based on military power being applied directly against individual combatants rather than formations. These so-called "targeted killings" are perhaps the most vivid example of the individualization of American warfare, particularly the Commander-in-Chief routinely reviewing and approving strikes against named combatants, a phenomenon "without precedent in presidential history."[2] However, this operational trend is by no means limited to high-level counterterrorism efforts. It represents a more systematic disaggregation of national security threats and the adoption of an individualized approach to military targeting that has dramatically transformed the American way of war. Within this paradigm, the targeting of "high value individuals" and networks has replaced conventional force engagement as the driving force of recent doctrinal change and technical innovation."

As the defining operational experience for a generation of junior leaders, this new mode of warfare reflects the culmination of a decade of tactical lessons, doctrinal adaptations, technical advances, and changes to the institutional cultures of the US military. Indeed, since 9-11 the US armed forces have "developed the fusion of operations and intelligence for the purpose of hunting high-value targets into a high art."[3] Yet even as these methods have been widely applied, there remains insufficient analysis as to their effectiveness and utility as an element of US military

Colonel Glenn J. Voelz is an Army Intelligence Officer and US Army War College Fellow at the Massachusetts Institute of Technology and MIT's Lincoln Laboratory. He most recently served with US Army Africa and prior to that was the Senior Duty Officer in the White House Situation Room. In summer 2015, he will join the International Military Staff at NATO Headquarters in Brussels, Belgium.

1 Micah Zenko, "The US Just Launched Its 500th Drone Strike," *Defense One*, November 21, 2014, *The New American Foundation*, *Long War Journal*, and *Bureau of Investigative Journalism* all monitor US drone strikes taking place outside the "active combat zones" of Iraq, Afghanistan, and Libya. The sum of 500 total strikes in Pakistan, Yemen, and Somalia represent an average among the range of estimates as of November 2014.

2 Jo Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *New York Times*, May 29, 2012.

3 Linda Robinson, Paul D. Miller, John Gordon IV, Jeffrey Decker, Michael Schwille, Raphael S. Cohen, *Improving Strategic Competence: Lessons from 13 Years of War* (Santa Monica, CA: RAND, 2014) 26

power.[4] This article describes the catalysts driving the individualization of American warfare and considers the implications for future national security strategy and the Army.

A Post-Westphalian Logic of Warfare

The rise of individualized warfare stands in stark contrast to the preceding Cold War era where focus of operational planning, intelligence analysis, and doctrine centered primarily on the conduct of large-scale conventional warfare against nation-state adversaries. The transition is even more profound as a departure from the foundational presumptions of the "Westphalian" system that defined the context of state warfare for over three hundred years. The end of the Thirty Years War was notable as the transition point from the age of private mercenary conflicts towards a modern construct of warfare in which combatants became instruments of the state, acting on behalf of political sovereigns rather than fighting for individual gain.[5] This period also marked the "depersonalization" of conflict as soldiers assumed collective identities as members of professional armies. Jean-Jacques Rousseau's seminal treatise on political power articulated the significance of this transition, noting modern warfare was no longer a "relationship between one man and another, but a relationship between one state and another, in which individuals are enemies only by accident, not as men, nor even as citizens, but as soldiers."[6] This shift provided the intellectual foundation for legal categorizations supporting the concept of lawful combatancy and the treatment of prisoners, wounded soldiers, and civilians on the battlefield.

As the Westphalian system depersonalized warfare, soldiers became "generic" members of their national armies in terms of legal status and appearance. Geo-political boundaries and national affiliations determined the application and scope of wartime protections, while uniforms emerged to distinguish soldiers from civilians and to provide the operational context for lawful targeting.[7] Within this mode of warfare, the treatment of soldiers became status-based, meaning that privileges, obligations and rules of engagement were no longer linked to individual identity but rather to the soldiers' generic status as part of a state formation.[8] This convention has come under challenge as a result of recent conflicts waged by "unprivileged enemy belligerents," disqualified from the privileges of combatant status as a result of joining or substantially supporting non-state armed groups in the conduct of hostilities. The ambiguous status of these combatants has led to a revolution in the logic

4 A recent paper by Austin Long, "Whack-a-Mole or Coup de Grace? Institutionalization and Leadership Targeting in Iraq and Afghanistan," *Security Studies* 23, no. 3 (July 2014) offers a useful overview of recent scholarship on the topic and thoughtful examination of leadership targeting in Iraq and Afghanistan. Separately, there is a significant body of literature on Israeli use of targeted killings and methods of precision targeting, particularly in relation to operations in Gaza. While potentially useful as a comparative case study, that discussion is beyond the scope of this article.

5 Martin van Creveld, *The Rise and Decline of the State* (New York: Cambridge University Press, 1999), 162-163.

6 Jean Jacques Rousseau, "The Social Contract," in *The Social Contract and Other Writings*, ed. Victor Gourevitch (New York: Cambridge University Press, 1997), 51.

7 Gabriella Blum, "The Individualization of War: From War to Policing in the Regulation of Armed Conflicts," in *Law and War: An Introduction,* eds. Austin Sarat, Lawrence Douglas, and Martha Merrill Umphrey (Redwood City, CA: Stanford University Press, 2014), 52.

8 For elaboration on this concept see Gabriella Blum, "The Dispensable Lives of Soldiers," *Journal of Legal Analysis* 2, no. 1 (Spring 2010): 115-147.

of military targeting and a shift towards highly individualized assessment of threats. This new operational paradigm reflects a personalized form of warfare where the legitimate use of military force has become "tied to quasi-adjudicative judgments about the individual acts and roles of specific enemy figures."[9]

Doctrine and Individualized Warfare

The individualization of American warfare is readily apparent in contemporary doctrine and operational practices, specifically in applications of counterterrorism and counterinsurgency strategies. Debates over these war-fighting theories have led to doctrinal incoherence with regard to specific methods; however, on a conceptual and operational level they share the important commonality of systematically individualizing the adversary. One of the early lessons of campaigns in Iraq and Afghanistan was "conventional warfare approaches often were ineffective when applied to operations other than major combat, forcing leaders to realign the ways and means of achieving effects."[10] The central challenge, as the Army's targeting manual notes, was in "contrast to major theater operations where the purpose is to find and destroy ships, tank formations, or infrastructure, the most difficult task in insurgencies is finding the enemy."[11] Over the last decade the US military has demonstrated remarkable adaptability towards this end, marked by a major evolution in doctrinal methods and war-fighting approaches focused on the problem of identifying and targeting individual combatants. While counterinsurgency doctrine pointedly emphasizes a broad range of governance and stability measures, much of the tactical focus in recent campaigns gravitated towards highly refined kinetic and non-kinetic targeting efforts designed to "identify and separate the reconcilables from the irreconcilables."[12] This effort included aggressive efforts to identify key actors within insurgent networks and conduct kill/capture operations against top-tier targets.[13] Over the last decade, doctrinal methods evolved in direct response to these operational priorities and strategic approaches.

The "find, fix, finish, exploit, analyze, and disseminate" targeting approach evolved specifically as the preferred methodology for identifying and engaging high-value individuals.[14] US forces in both Iraq and Afghanistan applied this find-and-fix approach with great success against insurgent networks and terrorist cells. In Iraq, these network-based targeting approaches were used to develop "all-source intelligence to provide situational awareness of the local environment, its social

9 Samuel Issacharoff and Richard Pildes, "Targeted Warfare: Individuating Enemy Responsibility," *New York University Law Review* 88, no. 5 (November 2013): 1521.

10 US Joint Chief of Staff, Joint and Coalition Operational Analysis Division (J7), *Decade of War Volume 1: Enduring Lessons from the Past Decade of Operations* (Washington, DC: US Joint Chiefs of Staff, June 15, 2012), 2.

11 US Department of the Army, *The Targeting Process*, Field Manual 3-60 (Washington, DC: US Department of the Army, November 26, 2010), Appendix B-1.

12 General David Petraeus, Commander, US Central Command, Multi-National Force-Iraq, "Counterinsurgency Guidance," June 21, 2008.

13 One may arguably identify precursor models of individualized targeting in the Phoenix Program from Vietnam or from other counterinsurgency examples. However, these cases are significantly different from recent US experience in terms of the scope of application, as well as the broader intellectual, technical and doctrinal impact on war-fighting strategy.

14 Also sometimes referred to as F3EAD.

networks, key decision-makers, and their motivations," most famously applied during the successful effort to track, target, and kill terrorist leader Abu Musab al-Zarqawi.[15] In Afghanistan, such individualized approaches were used extensively in targeting insurgent networks, resulting in a five-fold increase in raids between 2009 and 2011 designed to capture or kill high-level insurgents.[16] Beyond targeting active combatants, similar methods were applied against drug producers and criminal networks as a means to undermine financial support to insurgencies. Over the last decade, this find-and-fix approach has migrated into conventional targeting doctrine and the Army's institutional training programs.[17] Attack-the-Network theory (AtN) offers another example of the doctrinal trend towards individualized warfare. This theory emerged specifically for defeating improvised-explosive-device networks in Iraq and Afghanistan, and over time has been applied to a broad range of missions such as tracking Joseph Koni and Lord's Resistance Army in Uganda, analyzing the spread of Boko Haram influence in Nigeria, and understanding threat finance patterns of narcotics networks in Latin America.

Both find-and-fix and Attack-the-Network methodologies reflect an evolution in analytical approaches related to the adoption of Social Network Analysis for military targeting. Application of Social Network Analysis to complex networks predates recent campaigns with significant scholarly research dating back to the 1960s, notably Stanley Milgram's early work on network theory and structural disintermediation.[18] Admiral Arthur Cebrowski's influential "network-centric warfare" expanded the notion to distributed sensor systems and precision targeting; however, he did not conceive of such methods being used specifically against individual combatants. These concepts were more directly articulated in John Arquilla and David Ronfeldt's, *Networks and Netwars*, where they described the rise of non-state actors organized as decentralized networks.[19] Under the guise of "fourth generation warfare," William Lind, T.X. Hammes and others, foresaw such networks and individual actors supplanting the state as primary drivers of a new security environment, an idea later sensationalized by Thomas Friedman's thesis on "super empowered individuals."[20]

Operational Social Network Analysis techniques were introduced directly in the influential 2006 publication of FM 3-24, *Counterinsurgency*, and have since matured into a foundational component of doctrinal

15 Christopher J. Lamb and Evan Munsing, *Secret Weapon: High-Value Target Teams as an Organizational Innovation* (Washington, DC: National Defense University Press, March 2011), 33.

16 Carlotta Gall, "Night Raids Curbing Taliban, but Afghans Cite Civilian Toll," *New York Times*, July 8, 2011; and Tom Peter, "Afghanistan: NATO's Night Raids Cause More Harm Than Good, Report Says," *Christian Science Monitor*, September 19, 2011.

17 Charles Faint and Michael Harris, "F3EAD: Ops/Intel Fusion Feeds The SOF Targeting Process," *Small Wars Journal*, January 31, 2012.

18 Steve Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present and Future Research," *Homeland Security Affairs* 2, no. 2 (July 2006).

19 John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001).

20 Thomas L. Friedman, *The Lexus and the Olive Tree* (New York: Anchor Books, 2000).

thinking.[21] These techniques provided the framework for identifying individual roles, organizational positions, and influential actors within given networks. At the tactical level, Social Network Analysis supported the practical need for conducting "pattern of life" analysis, identifying associations, habits, locations, movement routes, financial transactions, and overall visualization of network dynamics down to the level of individual actors. Information obtained from this network analysis often focused on personalized details such as physical descriptions of suspects, their biographic histories, familial relations, biometric data, and forensic evidence in support of operational targeting.[22]

The recent emergence of Identity Intelligence (I2) and methods for personality-based targeting offers another example of the doctrinal evolution towards individualized warfare.[23] Identity Intelligence is not an intelligence process, per se, but rather tailored products derived from the fusion of identity attributes (biologic, biographic, behavioral, and reputational information) into operational planning processes. Identity Intelligence integrates the technical disciplines of biometrics, forensics, document and media exploitation, with other all-source data for the purpose of "connecting individuals to other persons, places, events, or materials" and analyzing patterns of life.[24] Only in the last few years has Identity Intelligence matured as part of recognized doctrine; however, its use in support of military operations evolved rapidly due to the challenges of identifying and targeting individuals in environments where positive identification has been problematic due to unverifiable documentation or intentional evasion. Recognizing these challenges, the DoD formally established biometrics as a core function in 2012 and directed combatant commands to integrate biometrics into mission planning.[25]

What is remarkable about the evolution of counterinsurgency and counterterrorism practices is the degree to which operational targeting has not only become individualized, but also *personalized* through the integration of identity functions. The greatest weapon of insurgent networks in Iraq and Afghanistan was anonymity, specifically the ability of fighters to blend in with, and disappear into, local populations. Population-centric approaches of counterinsurgency, therefore, placed Identity Intelligence activities at the center of efforts "to positively identify, track, characterize, and disrupt threat actors."[26] In Iraq the targeting of high-value individuals became closely integrated with

21 For example, Social Network Analysis techniques feature prominently in the most recent version of US Department of the Army, *Intelligence Analysis,* Army Techniques Publication 2-33.4 (Washington, DC: US Department of the Army, August 2014), as a methodology in US Joint Chiefs of Staff, *Joint Intelligence Preparation of the Operational Environment*, Joint Publication 2.01-3 (Washington, DC: US Joint Chiefs of Staff, June 2009), and in US Department of the Army, *The Targeting Process*, Field Manual 3-60 (Washington, DC: US Department of the Army, November 2010).

22 US Department of the Army, *The Targeting Process*, Appendix B-1.

23 Identity intelligence (I2) appeared for the first time as part of US doctrine in October 2013 as part of the updated version of US Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2.0 (Washington, DC: US Joint Chiefs of Staff, October 2013).

24 US Joint Chiefs of Staff, *Counterterrorism*, Joint Publication 3-26 (Washington, DC: US Joint Chiefs of Staff, October 24, 2014), V-5

25 Deputy Secretary of Defense, *Authority to Collect, Store, and Share Biometric Information of Non-US Persons with US Government (USG) Entities and Partner Nations*, Memorandum, Washington, DC, January 13, 2012.

26 US Joint Chief of Staff, *Counterinsurgency,* Joint Publication 3-24 (Washington, DC: US Joint Chiefs of Staff, November 2013), XVI.

efforts against broader facilitation networks (finance, recruitment, training, logistics, media, command and control). This integration included non-kinetic targeting against specific individuals using such methods as leaflets, "most wanted" posters, text messaging, and hotline tip numbers to create a "spotlight effect" for denying insurgents access to particular operational areas.[27] Identity Intelligence tools and techniques were also integrated into a wide range of missions dependent on the ability to identify and distinguish specific actors on the battlefield such as focused raids, checkpoint and area security, border control operations, and detailed mapping of "human terrain." In sum, the commonalities among these diverse missions are doctrinal approaches and war-fighting techniques focused on the lowest common battlefield denominators of identifying and targeting individual combatants.

Technology and Individualized Warfare

The individualization of warfare has been fueled by several key technical innovations over the last decade, including advances in persistent surveillance, standoff precision strike, data analytics, biometrics, and forensics capabilities. These tools directly enabled what has been described as a "patient and relentless man-hunting campaign" waged by the US military against non-state actors.[28] Certainly, the most visible technology of this new mode of warfare has been the use of unmanned aerial vehicles, or drones. Prior to 9-11, their operational use was limited primarily to reconnaissance missions in the Balkans and Afghanistan; they were not tested as a weapons platforms until early 2001, and then were rapidly adapted for kinetic targeting in Afghanistan. Early in the campaign, General Tommy Franks called the Predator "my most capable sensor in hunting down and killing al Qaeda and Taliban leadership."[29]

These platforms soon emerged as a central component in the military's high-value targeting programs, and their number increased more than 40-fold between 2002 and 2010.[30] In Afghanistan there were a total of 74 military drone strikes during all of 2007; yet by 2012, that number averaged 33 strikes *per month*.[31] Over time, improved sensors and software packages enabled analysts to "recognize and categorize humans and human-made objects," providing unprecedented real-time surveillance and detailed granularity for targeting individual combatants.[32] Perhaps more significant has been the degree to which such drone strikes "have gone from a relative rarity to a relatively common practice" as a tool of US counterterrorism.[33] Indeed, unclassified estimates suggest

27 Joint Center for Operational Analysis, *Operation IRAQI FREEDOM, January 2007 to December 2008 The Comprehensive Approach: An Iraq Case Study* (Norfolk, Virginia: US Joint Forces Command, February 2010), 14.

28 Robert O. Work and Shawn Brimley, *20YY Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), 17.

29 Mark Mazzetti, *The Way of the Knife* (New York: Penguin Books, 2014), 94-101; also, Andrew Callam, "Drone Wars: Armed Unmanned Aerial Vehicles," *International Affairs Review* 18, no. 3 (Winter 2010).

30 Jeremiah Gertler, *US Unmanned Aerial Systems* (Washington DC: Congressional Research Service, January 3, 2012).

31 Amitai Etzioni, "The Great Drone Debate," *Military Review* 93, no. 2 (March-April 2013): 2.

32 Andrew Callam, "Drone Wars: Armed Unmanned Aerial Vehicles," *International Affairs Review* 18, no. 3 (Winter 2010).

33 Stimson Center, *Recommendations and Report of the Task Force on US Drone Policy* (Washington, DC: Stimson Center, 2014), 11.

over 98 percent of non-battlefield targeted killings over the last decade have been conducted by these platforms.[34]

However, the expanded use of persistent surveillance introduced new challenges for analysts with a deluge of sensor data making it "nearly impossible to track and identify suspicious activities and potential security threats solely through human analytical processes."[35] A separate analytical challenge has evolved from the need to collect and interpret different signatures from those of the doctrinally coherent, state-based adversaries of the Cold War era. Analysts must now process and correlate multiple streams of disparate, unstructured data such as cell phone numbers, biographic data, digital communications, biometric signatures, and forensic evidence in support of lethal and non-lethal targeting. This requirement has produced new data processing techniques specifically designed to leverage Social Network Analysis methods, including tools such as Analyst Notebook and the Distributed Common Ground System (DCGS), enabling data integration and advanced network analysis. Other database systems employed in Iraq and Afghanistan, such as the Combined Information Data Network Exchange, a massive repository of tactical reporting, evolved in response to the immense data processing challenge of analyzing insurgent activities, individual identities, and operational patterns.

Of all the technical advances emerging in recent years, biometrics and forensics are perhaps the most vivid examples of the central role of technology in waging individualized warfare. The need to verify identity and distinguish adversaries from the larger population led to the expansion in the use of biometric systems on the battlefield.[36] As with drone technology, there had been no significant operational use of biometrics by the US military prior to Iraq and Afghanistan. In early 2001, the Army began developing the Biometric Automated Toolset (BAT), offering an initial capability to collect, match and store biometric and personal identifying information. The first major combat employment of biometrics occurred in 2004 by Marine Corps units in Iraq where the technology was used to quarantine an insurgent safe haven in Fallujah through biometric screening.[37] Use of this technology grew as part of the 2007 "surge" as the primary means of identity verification and separating insurgents from the larger population. Biometrics, linked with operational forensics, was also used extensively for analyzing and penetrating cells employing improvised explosive devices, and by the end of operations in Iraq the US had complied a biometric database of some 3 million files on Iraqi citizens.[38]

Similarly, in Afghanistan, over 7,000 biometric collection devices have been employed in support of detention operations, execution of

34 Micah Zenko, *Reforming US Drone Strike Policies* (Washington, DC: Council on Foreign Relations, January 2013), 8.

35 Sandra I. Erwin, "As Defense, Intelligence Agencies Drown in Data, Technology Comes to the Rescue," *Nation Defense Magazine*, November 2014.

36 US Department of Defense, *Defense Science Board Task Force on COIN and ISR Operations* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, February 2011), 65.

37 Thom Shanker, "To Track Militants, US Has System that Never Forgets a Face," *New York Times*, July 13, 2011.

38 Spencer Ackerman, "US Holds on to Biometric Database of 3 Million Iraqis," *Wired Magazine*, *Danger Room Blog*, December 21, 2011, http://www.wired.com/2011/12/iraq-biometrics-database/.

high-risk warrants, and targeted raids against identified insurgents.[39] Between 2004 and 2011, US forces collected biometric data on more than 1.1 million individuals - equivalent to roughly one of every six fighting age males - and used this data to identify thousands of known enemy combatants.[40] This measure was of particular importance in Afghanistan, a country with limited institutional capacity for identity verification, few birth certificates, drivers' licenses and citizenship documents, exacerbated by an active black market in forged identity papers. For similar reasons, biometric technologies have spread to other theaters where identity cannot be reliably verified by available documentation, such as counter-piracy operations in East Africa.[41] As an Identity Intelligence specialist at the Army's Training and Doctrine Command explained, "biometrics puts a uniform on the enemy" and enables the categorization of actors even in the absence of traditional status-based signatures.[42]

Expeditionary forensics is another technical area that evolved rapidly in direct response to the shift towards individualized warfare. Forensic tools and analysis supported evidenced-based targeting methods used to individualize, identify, associate, and scientifically link people, places, things, intentions, activities, organizations, and events. In late 2004, US forces in Iraq began collecting battlefield forensic materials to identify suspected insurgents by cross-referencing evidence with detainee biometrics in support of follow-on targeting and prosecution. By 2006, this capability expanded to include numerous expeditionary forensic facilities analyzing ammunition, clothing, latent fingerprints, and DNA, among other materials. By 2010, the United States had deployed a total of seven forensic laboratories to Iraq and eight to Afghanistan.[43] During that year alone, expeditionary forensics enabled the capture of over 700 high-value individuals associated with improvised explosive devices, or suspected terrorist and criminal activities.[44] According to one report, this fusion of forensic and biometric information into actionable intelligence directly enabled "precise fires to shape the operational environment, including supply chain interdiction, counter-threat finance operations, information operations, cache destruction, and the capture of high-value individuals."[45] The task force responsible for detainee operations in Afghanistan estimated that some 70 percent of key individual targets captured on the battlefield had been

39 David Pendall and Cal Sieg, "Biometric-Enabled Intelligence in Regional Command–East," *Joint Forces Quarterly* 72, no. 1 (January 2014): 70

40 US Government Accountability Office, *Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan* (Washington, DC: US Government Accountability Office, April 2012), 1.

41 David Axe, "CSI Somalia: Interpol Targets Pirates," *Wired Magazine*, *Danger Room Blog*, June 18, 2009, http://www.wired.com/2009/06/csi-somalia-interpol-targets-pirates/.

42 Antonia Greene, "Including Biometrics in Deployment Training Helps Soldiers Identify the Enemy," *Army*, April 30, 2012.

43 US Government Accountability Office, *Additional Planning and Oversight Needed to Establish an Enduring Expeditionary Forensic Capability* (Washington, DC: US Government Accountability Office, June 2013), 4.

44 Oliver Herion, "Expeditionary Forensic Support to Joint Force Commanders: What Changes or Considerations are Warranted?" (Quantico, VA: US Marine Corps Command and Staff College, April 2012), v.

45 Thomas B. Smith and Marc Tranchemontagne, "Understanding the Enemy: The Enduring Value of Technical and Forensic Exploitation," *Joint Forces Quarterly* 75, no. 4 (October 2014): 124.

identified with the help of biometrics and forensics technologies.[46] A study by the Army Audit Agency similarly concluded the conflicts in Iraq and Afghanistan had revolutionized expeditionary forensics and operational use of latent fingerprints and DNA, in particular.[47] In sum, the introduction of these technologies enabled a fundamental paradigm shift in targeting whereby combatants were no longer "generic" soldiers on the battlefield, but rather targeted as individuals based on identity attributes and evidentiary analyses (see table below).

Key Characteristics of Industrial & Individualized Warfare

	Industrial Warfare	Individualized War
Political Context	Westphalian; professional armies fighting as political proxies with defined geo-political objectives; recognizes *Jus in Bello* constructs	Post-Westphalian; individual combatants fighting for ideological causes and ambiguous objectives; challenges *Jus in Bello* constructs
Adversary Characteristics	State armies comprised of "generic" professional soldiers applying doctrinal methods and a depersonalized, bureaucratic logic	Non-state entities; "unprivileged" combatants using anonymity for operational advantage; idiosyncratic, highly personalized networks
Operational Environment	Contested primarily in the physical domain (land, sea, air, space); engagements within a contiguous, linear battle-space with explicit operational boundaries	Contested primarily in the informational domain (influence and identity); spatially and temporally unbounded; fusion of military and domestic security spheres
Theories of War-fighting	Influenced by traditional tenets of maneuver warfare, mass, firepower, destruction of enemy forces and seizure of key terrain	Influenced by counterinsurgency and counterterrorism doctrines; stability concerns, governance, and population-centric approaches
Analytical Approach & Tools	Order of Battle analysis, doctrinal templating, traditional Indications and Warning, conventional ISR and technical signatures	Social Network Analysis, Attack the Network, Identity Intelligence, biometrics and forensic signatures, document and media exploitation
Targeting Paradigm	Status-based targeting against units, formations and equipment	Identity-based targeting against individuals, cells and networks
Objectives & Measures of Effectiveness	Physical attrition/destruction of the adversary war-fighting capability; predominantly quantitative assessment - units destroyed, terrain seized, kinetic effects and technical BDA	Slowing the regeneration of key leadership and operators; predominantly qualitative assessment - kill/capture high value individuals, measures of network centrality, influence and cohesion
Success Criteria & End State	Defeat of adversary military force compels political capitulation, orderly demobilization and repatriation of combatants	Risk mitigation rather than military victory; legal limbo for detained combatants and fighter recidivism presents enduring challenge

46 Anthony Iasso, "A Critical Time for Biometrics and Identity Intelligence," *Military Intelligence Professional Bulletin* (July-September 2013): 39-40.

47 US Army Audit Agency, *Workforce Requirements for Expeditionary Forensics*, Audit Report No. A-2012-0031-FFD (Alexandria, VA: December 27, 2011)

Policy Imperatives and Strategic Choices

While new doctrine and supporting technologies have provided the methods and tools of individualized warfare, ultimately this paradigm shift resulted from specific policy preferences and strategic choices in response to the threats posed by non-state actors. The 2001 Authorization for Use of Military Force (AUMF) established the initial legal context for waging war against individuals and geographically dispersed networks with broad language authorizing the use of force against "nations, organizations, or *persons*."[48] CIA Director John Brennan articulated what might be considered the "trickle-down" logic of this approach, describing how these methods have gradually expanded to wider networks of individual actors, noting that "in this armed conflict, individuals who are part of al-Qaida or its associated forces are legitimate military targets."[49] Yet this strategic approach has expanded far beyond "leadership strikes," and now reflects a new paradigm of war waged by "precise attacks against individuals" as the centerpiece of US counterterrorism approaches in Pakistan, Yemen and elsewhere.[50]

The trend towards such individualized approaches seems a logical path for a liberal democracy dealing with the threat of terrorism while balancing the rights of citizens. Public discomfort with profiling techniques in the aftermath of 9-11 created political pressure to focus targeting against individuals with legitimate connections to terrorism rather than applying categorical measures against entire suspect groups (racial, ethnic, religious, or otherwise). More recently, public outcry over broad application of domestic intelligence gathering by the NSA suggests similar disapproval of dragnet-like approaches to counterterrorism. However, Americans have expressed few reservations with focused intelligence collection and lethal targeting based on evidentiary approaches and presumptions of culpability, thus presenting few political liabilities.[51]

Beyond the domestic audience, international opinion has also pushed the US toward an individualized, and increasingly personalized approach to warfare. Perhaps the best example has been the broad condemnation of US "signature strikes" directed against detected patterns of adversary behavior, or signatures, rather than specific individuals.[52] This approach closely resembles conventional targeting methods applied against formations, equipment and facilities where technical signatures generally offer reliable categorization of intended targets. However, this technique has produced numerous incidents of misidentification and unintended civilian casualties with significant political repercussions, notably in Pakistan and Yemen, but also during military operations in

48 *Authorization for the Use of Military Force* (AUMF), Joint Resolution 23, 107th Cong., 1st sess. (September 14, 2001). Also, Public Law § 2(a), 115 Stat at 224.

49 John O. Brennan, "The Efficacy and Ethics of US Counterterrorism Strategy," Transcript of Remarks at the Wilson Center, April 30, 2012.

50 John Yoo, "Assassinations or Targeted Killings Since 9/11," *New York Law School Review* 57 (2011): 63.

51 Sarah Kreps, "Do Americans Really Love Drone Strikes?" *Washington Post*, June 6, 2014, and Pew Research, Global Attitudes Project Survey, "Global Opinions of US Surveillance," (Spring 2014), http://www.pewglobal.org/2014/07/14/nsa-opinion/.

52 Steve Coll, "The Unblinking Stare: The Drone War in Pakistan," *The New Yorker*, November 24, 2014.

Iraq and Afghanistan.[53] In response, the Obama administration has reportedly moved towards increased use of "personality" strikes only against confirmed individuals in order to avoid diplomatic fallout from unintended causalities. This process has been formalized by the creation of a "disposition matrix," a dynamic, individualized targeting database consisting of biographies, locations, associations and operational profiles of high-value targets.[54] The administration has also suggested a policy preference for capture and prosecution of individual suspects, when feasible.[55]

In terms of military strategy, the individualization of warfare has also exposed an inherent tension between traditional military activities and law enforcement functions when today's targeting packages have more similarities with police arrest warrants than with conventional targeting folders of the Cold War-era. During the later phases of operations in Iraq and Afghanistan, high-value targeting increasingly involved such "evidence-based" methodologies, relying on identity verification and forensic science to produce probable-cause-like adjudications as the basis of actionable intelligence. One observer noted, the find-and-fix paradigm evolved into a "police-like investigate, arrest, convict" model of non-lethal targeting.[56] Indeed, the current preference for such individualized approaches will continue to obfuscate traditional concepts of state warfare and raise difficult procedural questions as technology enables ever-greater disaggregation of the battlefield—and increasingly personalized targeting methods.

Challenges for the Future

The US response to threats from non-state actors has evolved into a new mode of warfare placing the individual combatant at the center of the analytical and operational challenge. The question remains as to whether this paradigm shift represents a transient diversion from the military's traditional focus on large-scale conventional conflict, or if the experiences of the last decade will have a lasting influence on approaches to land warfare and development of future capabilities and doctrine. Certainly the Army's natural inclination suggests a return to familiar ground of thinking about, and preparing for, conventional land force engagements. However, the catalysts of individualized warfare may not allow a full return to more traditional operating methods. The recent National Intelligence Council *Global Trends* report depicts a near-future security environment characterized by terrorism, subversion, sabotage, insurgency, and criminal activities; while others predict continuing outbreaks of "hybrid" wars similar to the ongoing conflicts in Syria and Ukraine.[57] The commonality among these diverse scenarios is that they

53 Danya Greenfield, "The Case Against Drone Strikes on People Who Only 'Act' Like Terrorists," *The Atlantic,* August 19, 2013. Also, Lawfare Staff, "Civilian Casualties & Collateral Damage," *Lawfare*, http://www.lawfareblog.com/wiki/the-lawfare-wiki-document-library/targeted-killing/controversy/.

54 Greg Miller, "Plan for Hunting Terrorists Signals US Intends to Keep Adding Names to Kill Lists," *Washington Post*, October 23, 2012.

55 Brennan, "The Efficacy and Ethics of US Counterterrorism Strategy."

56 Lamb and Munsing, *Secret Weapon: High-Value Target Teams as an Organizational Innovation*, 53.

57 US National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington DC: US Director of National Intelligence, December 2012), 59–60.

are all likely to involve targeting against decentralized, individual combatants who use anonymity to operational advantage.

However, current operations against the Islamic State may well prove a frustrating test case for the effectiveness of individualized targeting in the absence of significant ground forces and robust local intelligence networks. Unclassified reports of target selection during the early phases of Operation Inherent Resolve reveal patterns closely resembling conventional approaches, with a clear majority of strikes focused on facilities, fighting positions and vehicles, and far fewer against specific individuals and key leadership.[58] Yet, even success in this effort may have a potential downside. As the military continues to identify and strike individuals from greater distances and with higher accuracy, it should be expected that adaptive adversaries will move towards locations (megacities) or modes of operation (cyber) where US targeting advantages are less asymmetric.

While there is little debate as to the awe-inspiring tactical efficiency of US techniques for waging individualized warfare, it is less certain these methods have been effective in achieving larger political objectives. The perpetual regeneration of terrorist threats inside Pakistan, Yemen and Somalia offer little evidence these techniques have been fully successful as a centerpiece of counterterrorism strategy. Likewise, deteriorating conditions in Iraq and Afghanistan suggest limits as to what these approaches deliver to counterinsurgency efforts. The inherent ambiguity in the data raises the more difficult question as to whether one can evaluate the utility of specific tactics and tools separately from the overall strategic outcomes they produce. As General H. R. McMaster, Director of the Army's Capabilities and Integration Center, has cautioned, "targeting does not equal strategy."[59] This area should one be of continuing research and professional debate.

As President Obama recently observed during an address to National Defense University, "we must define the nature and scope of this struggle, or else it will define us."[60] Indeed, this has been the case for an entire generation of soldiers socialized under this operational paradigm and now highly skilled in the art of waging individualized war. As one senior US officer recently noted, the task of "putting warheads to foreheads" has become a core military function. The challenge ahead will be creating a context whereby the experiences and tools refined over the last decade can evolve and mature as an integrated component of full-spectrum operations. The risk is that this expertise will be lost in a rush back to focus on conventional warfare, or marginalized as some exotic, niche function within a narrowing scope of strategic utility for American land forces.

The goal should be full integration of these capabilities into a flexible landpower concept enabling rapid transition along the operational continuum from conventional conflict against state adversaries to

58 Kedar Pavgi, "Five Months of Air Strikes in Iraq and Syria in Four Charts," *Defense One*, January 8, 2015, http://www.defenseone.com/threats/2015/01/5-months-air-strikes-iraq-and-syria-4-charts/102495/?oref=d_brief_nl.

59 Sydney J. Freedberg, "Raiders, Advisors And The Wrong Lessons From Iraq," *Breaking Defense,* March 20, 2013, http://breakingdefense.com/2013/03/gen-mcmaster-raiders-advisors-and-the-wrong-lessons-from-iraq/.

60 President Barrack Obama at National Defense University, May 23, 2013.

individualized warfare in hybrid scenarios against non-state actors. To this end, several specific recommendations are offered.

Recommendations

First, ensure that the technical capabilities refined over the last decade continue to evolve even in the absence of a persistent operational targeting mission. The challenge of future hybrid scenarios, such as the situation in Ukraine, will be in detecting and exploiting non-standard signatures and data sources (cyber, open source, social media, biometrics and forensics) and integrating them with conventional collection streams in support of situational awareness and targeting. This task will require continuing advances in data processing and tools for analyzing large amounts of unstructured information with the ultimate goal of cross-domain integration, automated tipping and queuing, and improved network visualization. These represent enormous technical challenges that cannot wait for the next crisis.

Second, continue efforts to empower soldiers down to the lowest level with real-time integrated data from national level sources. Current biometrics technologies represent one useful example where a squad leader on patrol can rapidly access national-level watchlist information and biographic data on a subject encountered during tactical questioning. Within the contemporary threat paradigm there is no clearly bounded battlespace; therefore, an individual of interest encountered in a combat zone may also have relevance to a customs agent at an international airport, a police officer conducting a routine stop in Tucson, or a counterterrorism analyst at the CIA. Bureaucratic interests, technical barriers, and over-classification must not inhibit robust information sharing between such entities. Informational empowerment downward to the tactical level must be the ultimate goal so situational awareness is not limited to the operations center.

Finally, continue to integrate concepts such as Identity Intelligence and Network Analysis fully into the doctrinal canon and operational usage. By all indications, various forms of hybrid or irregular warfare will persist in the near future. These scenarios are likely to include lethal and non-lethal targeting against networked entities operating in ungoverned spaces with weak identity regimes and adversaries determined to leverage anonymity for operational advantage.

The techniques of individualized warfare and need for identity verification on the battlefield will only grow in importance. The Army, in particular, cannot afford to squander the hard lessons it has already learned about waging this kind of war.