

Member of coalition force surveys terrain in Kabul Province, Afghanistan (U.S. Army/Matthew Freire)



Combined Effects Power

By Ervin J. Rokke, Thomas A. Drohan, and Terry C. Pierce

The information revolution continues to recast how power is generated and how it can be used to achieve desired outcomes. Advanced technologies and novel communication tools are enabling individual and group actions to achieve truly disruptive effects. As recent events confirm, a single individual operating in the cyber domain can spark the stock market to lose billions of dollars, attack military infrastructures, and seize the initiative on key international and domestic political issues. Web-based social

networking can mobilize and align the power of group action with ease and speed. And individuals can be manipulated through the Internet to perform harmful acts.¹

The private sector, not the military, is driving this revolution. The Services are understandably looking for revolutionary ways to employ these information age technologies in warfare. The problem is that traditional combined arms warfare (CAW) doctrine used to generate maximum combat power in the natural domains of land, sea, air, and space is not

accommodating the broad range of novel power emerging in particular from the cyber domain. This article argues that a modified construct for how we think about the security challenge can enable our military to better observe, blend, protect, and project all types of power in the natural and cyber domains. In essence we recommend supplementing our current emphasis on traditional kinetic instruments of power with more explicit attention to desired effects.

Background

Combined arms warfare is the traditional concept that modern militaries use for maximizing combat power. It provides a lens through which to view the security arena and opens the door to a cognitive path for determining how

Lieutenant General Ervin J. Rokke, USAF (Ret.), is Senior Scholar in Residence in the Center for Character and Leadership at the U.S. Air Force Academy. Colonel Thomas A. Drohan, USAF, is Permanent Professor and Head of the Department of Military and Strategic Studies at the U.S. Air Force Academy. Captain Terry C. Pierce, USN (Ret.), is Director of the Center for Innovation at the U.S. Air Force Academy.



best to protect national security including economic interests.² CAW, in sum, is the prescribed doctrinal route that the joint force follows in developing strategies and force structures. It involves the “full integration of arms in such a way that to counter one form of armament the enemy must become more vulnerable to another.”³ Its historical legacy is impressive, dating back in the Western tradition as far as the Macedonian armies in the fourth century BC. Alexander the Great artfully combined phalanxes, cavalry, and dismounted runners in a novel way to conquer the Persian Empire.⁴ In Chinese history, CAW was employed during the Spring and Autumn Period from the eighth through the fourth century BC. Over a millennium later, Carl von Clausewitz’s *On War* offered a theoretical model of conflict that included the basic tenets⁵ of the CAW concept.⁶ Over time this combined arms construct has acquired nearly an immutable status as an unchangeable law of warfighting akin, perhaps, to Newtonian classical physics.

Quite clearly, CAW continues to enjoy substantial support among senior military leaders, particularly those in joint force. In 2008, for example, General James Mattis, USMC, then-commander of U.S. Joint Forces Command, issued guidance reaffirming the importance of using “time honored principles” in joint doctrine that have been “tested in combat” and “historically grounded in the fundamental nature of war.”⁷ He also made clear his strong preference for a combined arms approach as opposed to alternatives such as operational net assessment, effects-based operations, and system-of-systems approaches for developing security strategy and related force structure: “Our goal is to develop a joint force that acts in uncertainty and thrives in chaos through a common understanding of the essence and nature of the problem and the purpose of the operation.”⁸

We agree with General Mattis’s thoughtful goal statement as well as with his further assertion that we need operational concepts that link *ends* to policy and strategy through clear *ways* and *means*. We need to look no further than America’s longest war—Operation *Enduring Freedom* in Afghanistan—to see the impact of failing to connect and fully define desired ends with appropriate ways and means. We also believe, however, that it is time to rethink a theoretical construct when empirical evidence begins to mount and very different phenomena emerge that the construct cannot explain or predict. In this regard, the CAW concept is increasingly unable to adequately accommodate the disruptive striking and resisting power of emerging noncombat arms. Just as Newtonian physics, developed in the late 1600s, was unable to explain the quantum revolution of the early 1900s, the CAW construct is unable to appreciate the dynamics of cyber and social network instruments of power sufficiently, particularly the substantial effects they produce nonkinetically.

Reexamining CAW

Against this background we see a need for more critical thought about how the CAW concept can better relate ways

and means to desired ends. Indeed, we believe the paucity of such thought is a serious shortcoming, particularly if we fail to recognize that our enemies are increasingly comfortable operating beyond the traditional CAW concepts to employ the powerful new forces emerging, particularly in the cyber domain. Absent such rethinking, the emerging cyber forces—ours and those of potential adversaries—remain anomalous to our traditional CAW concept: their impacts are neither fully recognized nor anticipated in the context of struggle among adversaries of widely varying characteristics for equally disparate objectives. It is time to reexamine the CAW with a view toward retooling it to more effectively exploit these emerging power anomalies.

Cognitive psychologists tell us that because humans are frequently unable to grasp complex realities in a holistic sense, we craft simplifying “lenses, frameworks, or concepts” to help our understanding. Such is the role traditionally played by the CAW construct. It is a crucial role because it determines the extent to which we are able to view the breadth and depth of truly difficult problem sets; indeed, it is at the very heart of achieving an accurate understanding of our security predicament. We acknowledge that the CAW concept has worked well historically and continues to be helpful for assessing kinetic power in particular. As the late defense innovation chief Vice Admiral Arthur Cebrowski suggested, however, the information age has brought new forms of power from the cyber domain as well as nonkinetic aspects of power from the natural domains, which we believe the traditional CAW concept cannot accommodate effectively. The result is a cognitive tension—an incomplete view of power.

In response to this tension, we are “wired” to introduce new concepts or lenses that can proactively engage and adaptively shape the increasingly complex realities we face in the security arena. In his discussion of the evolution of principles of war, Lieutenant General James Dubik, USA (Ret.), former commander of the Multinational Security Transition

Command–Iraq, draws a parallel between the theories of a scientific revolution and the theories of warfare. He argues that when a substantial scientific theory faced difficulties, “the adherents of that view would treat the difficulties as *anomalies*.”⁹ At first they would try simply to “tweak” their existing theory to explain the anomalies. As the number of anomalies grew, however, they were forced to craft a new theoretical construct, which altered the perceived reality to accommodate the anomalies. In sum, General Dubik asserts, “the emergence of the information age has shifted the very foundations of the profession of arms. . . . Clearly the framework that guided decisions and actions in the past is just that, past.”¹⁰

Using Dubik’s metaphor, it seems we are in the tweaking phase of converting the challenges of operating in cyberspace “into a warfighting mold shaped by the four older domains.”¹¹ A recent literature review of the cyber domain, for example, offers recurring CAW themes: we must *dominate* cyberspace,¹² and we must determine how the cyber domain can be mainstreamed into the CAW model as an operational discipline alongside land, sea, and air warfare.¹³ In fact, Navy cyber leaders argue that the information technology “network and its components (information, intelligence, technology, and people) have become a combat system. In this form, they suggest, the network can serve as a platform from which to launch information as a weapon.”¹⁴ Some CAW pundits even assert that operating and fighting a network as a warfare platform will enable cyber networks to join existing platforms from the physical domains such as ships, aircraft, and infantry units and form combined arms teams.¹⁵

Such *tweaking* approaches are focused on translating the cyberspace anomalies into instruments compatible with a CAW concept conceived for dealing with the natural domains. We take strong issue with this approach. Ultimately, we are convinced that it will prove inadequate to force the anomalies of the cyber domain into the CAW concepts of mass, speed, fires, control, maneuver, dominance, superiority, and hierarchy.¹⁶ As a military

profession that has traditionally relied on platforms and combat arms for maximizing combat power, the “reality” we perceive when we look through the CAW lens at the many happenings in cyberspace today is random and unfathomably complex. The CAW lens’s focus on traditional instruments of warfare from the natural domains of land, sea, air, and space ignores important parts of the “reality picture.” Put simply, the CAW model is the wrong construct for conflicts that include action and reaction in the cyber domain (as nearly any conflict in the future will), and it is giving us fits.

CAW Anomalies

In anomaly theory research, the focus is on discovering anomalies and understanding why the current theory does not explain their existence. It is only when we can identify such anomalies that an opportunity exists to improve the relevant theory.¹⁷ Understanding how and why anomalies are emerging is how new constructs are built. Against this background, let us look at several anomalies with a view toward identifying ways to improve the CAW construct’s capacity for accommodating and exploiting the emerging forces from the cyber domain in particular.

Cyber Soft Power. Unlike the natural domains, the cyber domain is a man-made entity consisting of networked systems. It is, in a sense, the world’s largest ungoverned space with its own medium and constantly changing rule sets.¹⁸ Significantly, it is also shifting the concentration of power—most of which is nonkinetic, or “soft”—from combined arms forces to individuals.¹⁹ It generally does not use physical force in a coercive sense, but rather tends to use networked systems to influence and to persuade behavior by attracting and co-opting. It is distinctive in its capacity to enable single individuals to exert uncommon soft power and private commercial entities to exert far greater influence over the domain than governmental authorities do.

The resulting easy access to this domain by both governments and private individuals creates an abundance of lucrative targets for serious mischief

as well as legitimate endeavors, most of which fall outside the CAW focus on traditional instruments of power associated with natural domains. The Stuxnet Cyber Worm, for example, is a powerful instrument, but it remains an anomaly for CAW because it is neither a platform nor a combat arm, and its effects can go far beyond traditional calculations about destruction. Cyber attackers are successfully compromising the network security of banks. In another example, the self-proclaimed Izz ad-Din al-Qassam Cyber Fighters have claimed responsibility for several attacks against American financial institutions that have taken these corporations offline intermittently, costing millions of dollars.²⁰

Social Network Power. Cyber technology platforms operating in cyberspace, such as Google and Facebook, are providing a powerful destructive tool to conduct Wiki War.²¹ The power of such social networks comes from their ability to scale like spreading viruses and create a rapid and direct impact on societal action.²² For example, the WikiLeaks story of a U.S. Soldier and recent events involving a National Security Agency contractor stealing and releasing hundreds of thousands of government digital secrets have done considerable harm to our nation.²³ In another example, the so-called Syrian Electronic Army hacked into an Associated Press Twitter feed and reported a fake White House attack that briefly wiped out \$136.5 billion of the Standard and Poor’s 500 Index value.²⁴ Our CAW focus on ways and means (traditional arms) overlooked the critical factor of ends (effects) and the resulting anomalies were significant.

Virtual Reality Power. As demonstrated by the Boston Marathon bombing, the cyber domain enables terrorists to recruit, radicalize, train, and execute in the virtual world in a far more rapid and precisely targeted manner.²⁵ Indeed, it enables terrorists to live physically in different regions of the natural domain of land but to operate virtual cells for collaboration and execution in a carefully crafted distributive virtual world. When it suits their purposes, terrorists can shift from the soft power cyber

domain to hard power natural domains for destructive attacks. Once again, our CAW concept does not provide a lens sufficient for understanding or predicting such activities.

Crowdsourcing. Finally, the marathon bombing incident demonstrated the capability of social networking tools to build collaborative virtual communities and then harness the resulting “wisdom of crowds” for constructive purposes.²⁶ The Federal Bureau of Investigation’s public release of two poor-quality images of the suspects with a request for assistance resulted in the mobilization of hundreds of private citizens who reviewed their own photography of the event and provided a flood of helpful images to the police. A similar phenomenon explains how the killing of a young woman in Iran resulted in a powerful mobilization of public opinion by private citizens who used their smart phones to photograph the event and quickly distribute the pictures worldwide.

The above examples of power emerging from the cyber domain demonstrate a common capacity for producing desired effects by directly influencing the perceptions and behavior of adversaries whether they are individuals, nongovernmental organizations, or nation-states. In short they provide measurable outcomes in efficient ways for the battle of wits. Regrettably, most of their outcomes are shielded from view by the CAW lens’s focus on traditional instruments of warfare associated with the natural domains.

Newtonian Physics and CAW Anomalies

These and multiple other elements of power that are in large part emerging from the cyberspace domain cannot be accommodated adequately by the CAW construct. The cyber domain is challenging previously conceived theories of power by spawning a host of anomalies. This anomaly challenge resembles a similar problem the physics community faced in the early 1900s. Just as the CAW construct has explained hard power in the natural domains for several centuries, Newtonian physics offered a powerful conceptual model



Kandahar PRT security force leads team member through Shur Andam Industrial Park in Kandahar City (U.S. Air Force /Richard Simonsen)

for explaining the fundamental forces of nature for several hundred years. Then came Ernest Rutherford’s early experiments with the atom, which revealed that nature sometimes did not behave in accordance with Newtonian theory. Put simply, Newton’s theory of motion and gravitation had an anomaly; it simply did not accurately predict the physical principles that governed the behavior of electrons orbiting the nucleus of the atom. Niels Bohr, August Heisenberg, and others met the challenge with a new concept for atomic behavior: quantum mechanics.

This article proposes a more modest solution for the CAW anomalies. It is a complement to the CAW concept that accommodates the behavior of participants in the cyber domain as well as soft power participants from the natural domains. We call it the Combined Effects Power (CEP) construct. We are not jettisoning the CAW model. Just as Newtonian classical theory still explains gravity and the

mutual attraction of the planets, CAW remains a valid model for understanding hard power in the natural domains. We believe, however, that our proposed CEP concept can serve, like the concept of quantum mechanics for Newtonian anomalies, as a remedy to explain the CAW anomalies.

But unlike the classical and modern physics analogy, we believe CEP is a unifying construct that can amplify and preserve the deepest tenets of CAW’s hard power while integrating the critically important soft power behavior we are observing in the natural as well as cyber domains. As a new way of thinking, the CEP construct is capable of accommodating and exploiting these forces in a single, all-encompassing, coherent framework. The integrating tenet for this framework is *effects*. Focusing on effects allows measurement of both hard and soft power. The CEP construct thus effectively overcomes the soft power anomalies generated by our traditional

focus on arms and puts the cyber domain on the same playing field as the natural domains.

The CEP construct also has the ability to accommodate not only first- and second-order effects from the CAW construct, but also to align (or harmonize) them with n^{th} -order effects resulting from soft and hard power regardless of the parent domains. For example, while the CAW construct enables understanding of the first-order effects of “sequestration,” the more significant n^{th} -order effects on subjective aspects of capability, morale, and complex interactions of human networking, for example, are better understood through the broader lens of CEP. This is equally relevant for distributed operations beyond the range of traditional CAW supporting forces as well as for distributed tactical groups self-organizing (or self-coordinating) for reaction to fleeting opportunities in accordance with commander’s intent. In other words, the CEP construct would enable us to rack and stack the different orders of first- through n^{th} -order effects of both hard and soft power more effectively. Indeed, we would see a flattening and simplifying of the command and control hierarchy as well as a wider horizontal span of understanding and control for combat operations.

Combined Effects Power

Once again, we note that atoms existed in 1687 when Newton published his *Principia Mathematica* and that the physical science community believed his laws adequately explained atomic behavior. They did not, however. Only with the quantum revolution in modern times were we able to understand the nuclear atom. And so it is that the CAW model has existed for thousands of years as the intellectual construct for understanding power. But however effective it may have been for understanding the effect of destroying opposing force structures in the natural domains, it is increasingly beset with challenges emerging from the cyber domain as well as nonkinetic forces from the natural domains. Furthermore, we are also concerned that most commanders today

are using the CAW mental construct in attempting to understand cyber power. Such an approach is analogous to using reading glasses to observe a distant object.

Then what is CEP? Combined effects power is essentially a way of thinking—a cognitive path that looks at a complicated security problem set through a quite different lens and addresses a new question at the outset: What effects do we want to achieve using both hard and soft power? It expands our frame of reference beyond the traditional CAW lens, which for centuries has focused on natural domain weapons systems and asked the question: How do we most effectively create a coherent, flexible force structure and strategy? With CEP’s wider lens and new question, the door is opened for leaders and commanders to better understand the human dimension of conflict—the thinking of our opponents (and allies). Most importantly, perhaps, it recognizes that the information age revolution has dramatically changed the means of application, speed, breadth, and potential impact of soft power.

Put simply, the CEP construct is a way to maximize and harmonize hard and soft power. It allows for the full integration of all effects generated from power arising in both the natural and manmade domains. It rejects the traditional notion that the “supported effort” is always an arm or platform; cyber domain soft power is no longer the default choice for supporting or secondary efforts. The CEP construct’s new question and wider lens allow for a level playing field—an accessible battlespace—on which all domains can participate as appropriate. Whereas the aim of CAW was to use all available resources to generate maximum hard power, the aim of CEP would be to use all available resources to generate power relevant to desired effects whether it is hard or soft. The units for measurement of effectiveness would reflect increments of desired effects, not necessarily levels of physical destruction.

Prospects for Change

We are realistic about the difficulties of effecting disruptive changes in so

fundamental a construct as CAW. Most certainly we are aware of the rich and intense dialogue during the past decade among Marine Corps leaders such as General Mattis and Lieutenant General Paul Van Riper, who supported the traditional CAW construct, and their Air Force contemporaries such as Lieutenant General David Deptula and Major General Thomas Andersen, who led in developing an effects-based approach as a way of thinking about and executing operations.²⁷ The passionate commitments of these strategists to quite different ways of thinking about our security challenges were not reconciled, but nevertheless they allowed sufficient flexibility on both sides for joint effectiveness in such practical matters as the Operation *Desert Storm* air campaign. More important for our purposes, the substance of this dispute showed remarkable foresight about the doctrinal imperatives of the emerging and future weapons systems with which we must deal today. As Lieutenant General Deptula explains:

*Effects-based operations provide a useful construct on how to conduct war that can bridge the gap between the weapons of today and the weapons of the future. It allows useful application of current weapon systems as we acquire a new generation of tools needed to fully exploit the concept. . . . The ability to achieve effects directly against systems without attacking their individual components would allow a preferable application of the concept of parallel war [or CEP] than we are capable of today. Indeed, the ultimate application of parallel war [or CEP] would involve few destructive weapons at all—effects are its objective, not destruction.*²⁸

As the late Admiral Cebrowski suggested, the long-held principles underlying theories of war were “chafing against new realities on the battlefields . . . and when this happens, rules change.”²⁹

Against that background, an emerging group of strategic thinkers such as Martin Libicki of the RAND Corporation and Major Kris Barcomb, an Air Force cyberspace strategist, is looking at the

cyber domain quite differently than simply as new high ground for *natural domain* warfare.³⁰ For example, Major Barcomb asserts that “hard power will be secondary to soft power in cyberspace for the foreseeable future” and calls for a new paradigm to better understand the proper role of the military in the cyber domain.³¹ Using our vernacular, both Libicki and Barcomb seem intent on substantially modifying the traditional CAW model for understanding cyber domain capabilities. We do not know whether Libicki and Barcomb would agree, but we believe this new framework could well focus on what we refer to as the CEP construct.

Once again, implementing such new thinking will not be easy. Despite de facto movement toward more acceptance of effects-based approaches to operations and planning,³² there remains a tendency throughout all the U.S. Services for continuing their traditional efforts to push the soft power capabilities of cyberspace as well as those emerging from the natural domains through the CAW hard power construct.³³ Cyber experts such as Libicki and Barcomb, intent on crafting a new paradigm for strategic thinking about the critical cyber domain, struggle to overcome such efforts.³⁴ The major challenges they face include the substantial cultural identity that the CAW model reinforces in our thinking about power as well as its capacity to provide legitimacy for the major weapon systems associated with each of the natural domains.

At the same time, however, the emerging anomalies associated with the cyber domain and other soft power capabilities from the natural domains have an increasing momentum of their own. Their force is significant, particularly for the United States with its great dependence on the cyber domain. If history is a guide, theoretical constructs such as CAW will ultimately give way to adaptations to exploit anomalies emerging from an increasingly complex security environment. The issue is not *whether* CAW will adapt, but rather *when* natural forces will overcome its grip on how we think about our security predicament.

Finally it has not escaped our notice that the CEP construct offers an

alternative path for sorting through research and development challenges associated with force structure. We are left with the critical question of whether policymakers and strategists are willing to grapple with a fundamentally new way of thinking about complex and messy issues. Whatever the case, it is clear that our potential opponents are increasingly comfortable in this thicket. JFQ

Notes

¹ Gary Strauss et al., “SEC, FBI probe fake tweet that rocked stocks,” *USA Today*, April 24, 2013, available at <www.usatoday.com/story/news/nation/2013/04/23/hack-attack-on-associated-press-shows-vulnerable-media/2106985/>; Nicole Perlroth and David Sanger, “Cyberattacks Seem Meant to Destroy, Not Just Disrupt,” *The New York Times*, March 29, 2013, B1; Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2008).

² Kris Barcomb, “From Sea Power to Cyber Power,” *Joint Force Quarterly* 69 (2nd Quarter 2013), 79; also see Paul G. Kaminski, “Dealing with the Cyber Threat to Our National and Economic Security,” speech, Pittsburgh, PA, January 10, 2013.

³ Robert Leonard, *The Principles of War for the Information Age* (New York: Ballantine Books, 2009), 67.

⁴ Jonathan M. House, *Combined Arms Warfare in the Twentieth Century* (Lawrence: University of Kansas Press, 2001), 1–2.

⁵ Carl Von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1989), 4, 291.

⁶ Clausewitz, 285–291, 295–296.

⁷ James N. Mattis, “Memorandum for U.S. Joint Forces Command: Assessment of Effects Based Operations,” *Parameters*, August 14, 2008, 22.

⁸ *Ibid.*; attachment with “USJFCOM Commander’s Guidance for Effects-Based Operations,” August 14, 2008.

⁹ James Dubik, “Get on with It,” in *Rethinking the Principles of War*, ed. Anthony D. McIvor, 2 (Annapolis: Naval Institute Press, 2005).

¹⁰ *Ibid.*, 8.

¹¹ Martin C. Libicki, “Cyberspace Is Not a Warfighting Domain,” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012), 328.

¹² Kendall Card and Michael Rogers, “The Navy’s Newest Warfighting Imperative,” U.S. Naval Institute *Proceedings* 138, no. 10 (October 2012), 23.

¹³ *Ibid.*

¹⁴ *Ibid.*

¹⁵ *Ibid.*

¹⁶ Richard Hundley, *Past Revolutions Future Transformations* (Santa Monica, CA: RAND, 1999), 11–12; Paul Carlile and Clayton Christensen, *The Cycles of Theory Building in Management Research* (Boston: Harvard Business School, January 6, 2005), 4; Barcomb, 80; Libicki, “Cyberspace.”

¹⁷ Carlile and Christensen, 4.

¹⁸ Eric Schmidt and Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations, and Business* (New York: Borzoi Knopf of Random House, 2013), 3, 6; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), iii.

¹⁹ *Ibid.*, 6.

²⁰ Perlroth and Sanger.

²¹ For a discussion of modern technology platforms as paradigm shifts in soft power, see Schmidt and Cohen, 9.

²² *Ibid.*, 10.

²³ *Ibid.*, 10, 162.

²⁴ Alina Selyukh, “Bogus ‘Obama injured’ tweet upsets US Markets,” *Mail & Guardian* (Johannesburg, South Africa), April 24, 2013, available at <<http://mg.co.za/article/2013-04-24-false-tweet-from-hacked-ap-account-irks-us-markets>>; Dan Goodin, “Hacked AP Twitter feed reporting fake White House attack rocks markets,” *ArsTechnica.com*, April 23, 2013, available at <<http://arstechnica.com/security/2013/04/hacked-ap-twitter-feed-rocks-market-after-sending-false-news-flash/>>.

²⁵ Schmidt and Cohen, 151.

²⁶ James Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station: Texas A&M Press, 2012), 178.

²⁷ John Correll, “The Assault on EBO,” *Air Force Magazine*, January 2013, 51.

²⁸ David Deptula, *Effects Based Operations: Change in the Nature of Warfare* (Washington, DC: Aerospace Education Foundation, 2001), 21–22.

²⁹ Anthony McIvor, ed., *Rethinking the Principles of War* (Annapolis: Naval Institute Press, 2005), ix, xii.

³⁰ Libicki, “Cyberspace,” 328.

³¹ Barcomb, 83.

³² See, for example, Air Force Doctrine Document 3-0, *Operations and Planning* (Washington, DC: Headquarters Department of the Air Force, November 9, 2012).

³³ Card and Rogers, 23.

³⁴ Barcomb, 79.