KWar

Cyber and Epistemological Warfare—Winning the Knowledge War by Rethinking Command and Control

Mark Ashley*

In the movie *Patton*, George C. Scott, who plays Gen George S. Patton, outmaneuvers German field marshal Erwin Rommel, proclaiming, "Rommel, you magnificent bastard; I read your book!" That book, *Infanterie Greift An* (*Infantry Attacks*) (1937), gave Patton insight into how Rommel would behave in battle, and he used that knowledge to his ad-

*I would like to thank Robert Bivins and Richard Szafranski for their contributions to this article.

versary's disadvantage. This article takes that thinking a little further, asserting not only that we must understand our adversaries but also that we should become more agile than they by rethinking our whole approach to command and control (C2). To be more agile, we need to build synchronized and centralized situational awareness as well as decentralized C2 (DC2) and execution systems and concepts of operations.

Specifically, this article aims to give greater meaning to and provoke additional thought about a more recent war-fighting concept—knowledge-centric warfare (KCW), also known as "KWar"—which can produce strategic effects.[1] Ultimately, it seeks to convince the reader that in today's network-centric battlespace, the victor must not simply attack and exploit the enemy's cyber and communication systems at the tactical level but completely understand the information environment. The winner will use the knowledge gained from understanding that environment in a highly adaptive and responsive manner to attain a strategic advantage, doing so by means of synchronized and shared situational awareness together with a DC2 structure. These conditions occur when decision makers and war fighters fully understand and coordinate the commander's intent over a greater volume of space and time within an operating environment. After realizing this shared situational awareness, we can enable and accelerate DC2 and execution to stay inside the adversary's decision-and-action loop.

With Knowledge Comes Awareness

Today's military leaders continue to look for and advance new ways of making warfare highly adaptive to the forces of knowledge—of training soldiers to use their minds (brain force) to fight innovatively with novel (although still brute-force) weapons without a centralized, rigid C2 structure to get in the way. As the revolutionary driving force of the Third Wave "knowledge age," technology (more specifically, information technology) is changing the face of combat in the twenty-first century. This endless quest for information and knowledge stands to fundamentally change how we wage warfare. In conflict, victory will

belong to the side that acquires knowledge faster, understands its true value, and applies it more adaptively.

To make sense of the drastic technological progression occurring in today's "information age," we must have an appreciation for information and know its origins and value. For our purposes, we define information as a collection of facts or data that, when placed in context, provides meaning derived from the full range of sensory perceptions. In many cases, we use information as an asset that can improve the quality of life by connecting us to other people and events. We should also recognize, however, that people can use information today, even more so than in the past, to gain a strategic advantage: " 'In war information . . . is the single most significant military factor . . . for controlling the battlespace. . . . Information is the organizing principle of war and postmodernity."[2] Additionally, we must note that "even if one has perfect information it is of no value if it is not coupled to a penetrating understanding of its meaning. . . . Judgment is key. . . . It is not necessarily the one with more information who will come out victorious, it is the one with better judgment, the one who is better at discerning patterns."[3] Only when we can discern these informational patterns and associate them with other patterns can we create knowledge. When centralized, easily accessible, and consumable, this knowledge can generate shared situational awareness.

All of these dimensions of knowledge are changing simultaneously, at speeds never before encountered and thus "demand much faster, smarter decision-making under more and more complex, if not chaotic, conditions" (fig. 1).[4] Given the importance of information and its use in creating knowledge, we should more closely look at the origins of knowledge itself—the epistemological elements based on our observations and beliefs that allow us to interpret information, rightly or wrongly. Epistemology is just this, the study of the nature and origin of knowledge and its validity. According to Richard Szafranski, epistemology is, quite simply, "everything a human organism—an individual or a group—holds to be true or real, no matter whether . . . [it] was ac-

quired as knowledge or as a belief."[5] Based on whether we find something true or real, our knowledge foreshadows our behavior, and in order to understand human behavior, we must take into account what the environment does and how organisms react. To understand an adversary's systems and environment, we can take epistemology—the origins and evolution of our knowledge that include proven theories and observations—and then apply it to cybernetics, which focuses on how systems function, regardless of whether that system is living, mechanical, or social.[6]

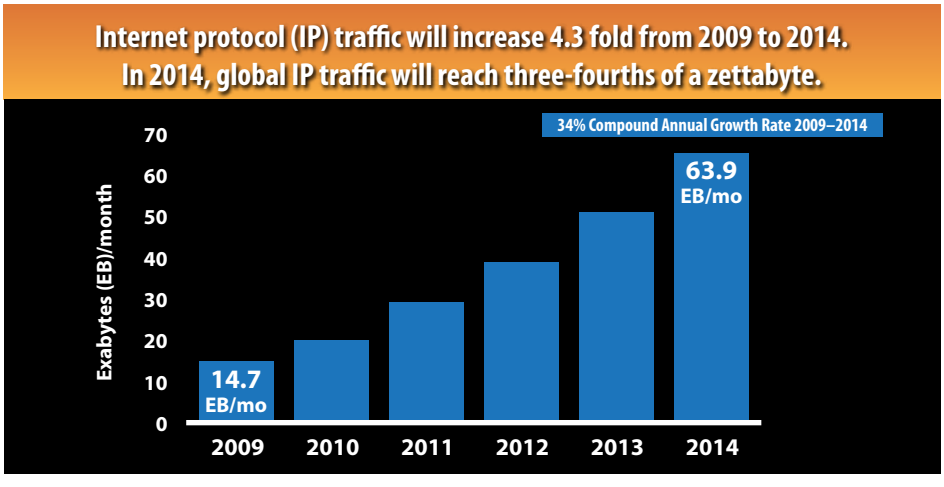

Figure 1. Global growth of Internet protocol traffic. (Adapted from Stacey Higginbotham, "The Zettabyte Era Is Getting Closer," GigaOM, 2 June 2010, http://gigaom.com/video/the-zettabyte-era-is-getting-closer. "A bit is a single binary digit, zero or one. A byte is eight bits. . . . An exabyte is 1024 petabytes which is about 1.15 * 10^18 [10^{18}] bytes. A zettabyte is 1024 exabytes which is about 1.18 * 10^21 bytes." Answerbag, 10 January 2005, http://www.answerbag.com/q_view/13291.)

The Concept of Knowledge-Centric Warfare

The final development of Third Wave war may well be the conscious design of something the world has not yet seen: competitive knowledge strategies.

—Alvin and Heidi Toffler

As it concerns the military's operating in today's information domain, "at the strategic level, the aim of a 'perfect' information warfare campaign is to influence adversary choices, and hence adversary behavior, without the adversary's awareness that choices and behavior are being influenced."[7] Thus, in any discussion of plans that emphasize manipulating adversary choices and behavior, we have the benefit of briefly revisiting John Boyd's observe, orient, decide, act (OODA) loop (fig. 2) and his supporting strategy, which "ties cognition to action designed to infiltrate the opponent's decision cycle."[8] Boyd posits that human behavior can be understood in terms of the mental processing of information, but he rejects the notion that we can see the brain as an information-processing device, "for the human mind thinks with ideas, not with information."[9] A closer examination of the cycle reveals

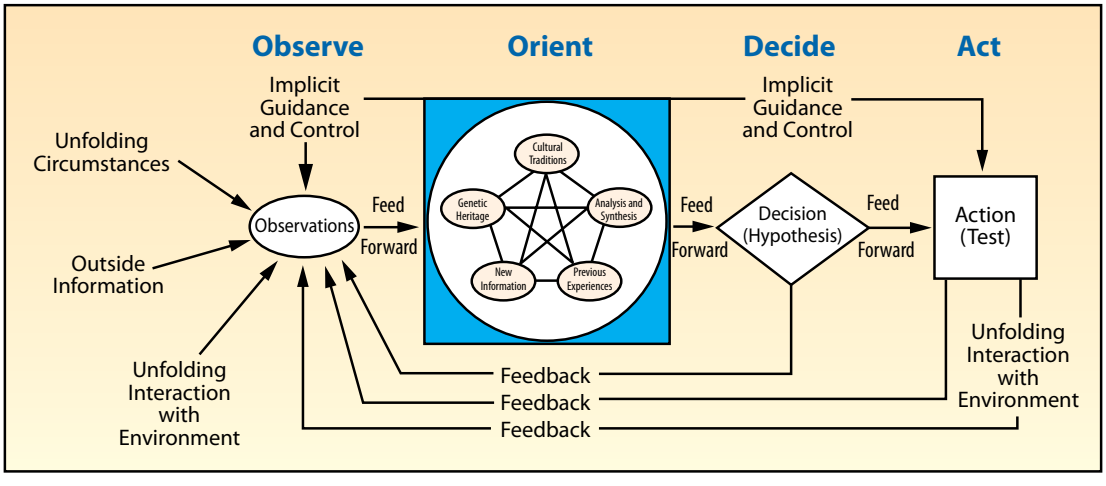

Figure 2. John Boyd's OODA loop. (Adapted from Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* [London: Routledge, 2007], 231.)

that Boyd's strategic theory points to observation as the method used to reveal events and identify change, or the lack thereof, within other people's environments and the world around them. Orientation represents our perceptions of reality and observations—"the images, views and impressions of the world shaped by *genetic heritage*, *cultural traditions*, *previous experiences*, and *unfolding circumstances*" (emphasis in original)—which shape the way we interact with the environment.[10] Orientation, in other words, frames the way we observe, the way we decide, and the way we act.[11] Based on observations, we must then make appropriate decisions that correspond with our objective, ideally improving the capacity for action.

Ultimately, the strategic goal calls for constantly changing the enemy's perception of reality so much that he becomes mired in uncertainty and disorder due to the overwhelming contradictions of inconsistent ideas and interactions, thus causing him to make erroneous decisions. The aim of penetrating the enemy's OODA loop closely reflects military deception operations conducted at the strategic, operational, and tactical levels, defined in Joint Publication 3-14, *Space Operations*, as "those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests."[12] In essence we attack the adversary's ability to create knowledge from information, otherwise known as KCW.

Why is this critical, and what does all this have to do with cyber warfare? Focused primarily at the tactical level, cyber operations try to infiltrate and disrupt an adversary's computers and networks. However, although we continue to make great strides in improving both offensive and defensive cyber capabilities, we must now lift our sights from the tactical to the strategic level. We can do this by recognizing the full potential and strategic implications of utilizing our knowledge to suppress and reduce the enemy's knowledge and channels for information by penetrating his decision cycle and influencing his observations and perceptions. To do so, KCW needs to target and successfully distort

what Alvin and Heidi Toffler call "truth filters," used to validate one's observations and beliefs.[13]

A shift from information-centric warfare to KCW is now well under way, due in large part to the amazing new technologies appearing on and above the battlefield—a fact that we need to realize and embrace. Such technologies, though, have accelerated the decision cycle because, as massive amounts of data come in faster, we must make decisions more quickly. This dynamic change is not limited to the battlefield but transcends the chain of command to the highest levels, underlining the growing requirements for increased synchronization. Obtaining this shared and synchronized situational awareness requires greater trust from leadership and more empowerment of subordinate leaders as well as introductions of new, emerging technologies (fig. 3).[14]

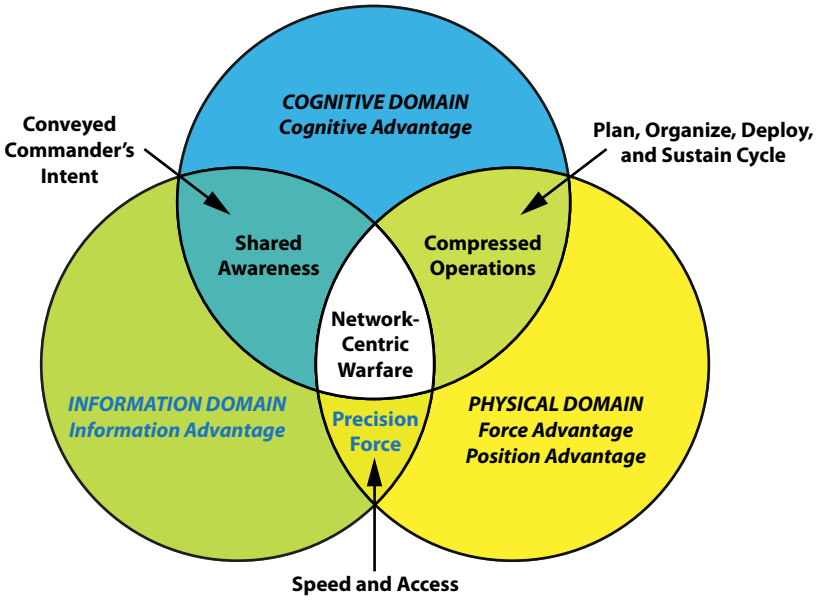

Figure 3. Information age warfare: Domains of conflict. (From Dr. Paul W. Phister Jr. and Mr. Igor G. Plonisch, *Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare* [Rome, NY: Air Force Research Laboratory, Information Directorate, n.d.], 7, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/188.pdf.)

Because decisions increasingly depend upon the constant barrage of data and information, we must know what is real and what is not. Consequently, the Tofflers contend that individuals in certain cultures and societies use any of six accepted criteria, or filters, to validate their beliefs:

1. Consensus: something deemed true through conventional wisdom.
2. Consistency: something that assures truth if the supporting facts harmonize with other facts.
3. Authority: something authenticated by a leadership figure.
4. Revelation: something assumed true and not subject to debate.
5. Durability: something that confirms inherited facts which have stood the test of time.
6. Science: something that ascertains truth through rigid tests and experiments.[15]

The utility of certain truth filters lends to the unique orientation of different cultures. We should note here that increases in the distance between two distinct cultures make the orientation of those cultures more difficult to understand. For instance, American citizens of European descent would find it easier to grasp how the British orient themselves, as opposed to the Arabs, Iranians, or Chinese.[16] In fact, with regard to cyberspace, the Chinese provide a clear example of how our orientations differ in that they approach "information security" as a broad concept that involves regulating content, whereas we narrowly concentrate on "cyber security" to protect our communications and critical networks.[17] Thus, to fully prepare ourselves against present and future threats projected from an ever-growing array of asymmetric capabilities, we must truly understand not only which criteria our adversaries use but also (and more importantly) how the selection of such truth filters validates certain beliefs on which their cultures are built and oriented.

If senior officers wish to have a better understanding of the enemy's orientation, they must improve their grasp of local conditions on the

ground. As P. W. Singer explains, "new technologies may give them an unprecedented view of the battlefield and the ability to reach into it as never before, but this view remains limited," creating danger because "you get too focused on what you can see, and neglect what you can't see. . . . And a lot of the time, what's happening elsewhere is more important."[18] Additionally, given the higher operational tempo demanded on today's battlefield, the enemy no longer affords the general several hours to watch video and analyze information prior to making a decision.[19] Commanders now need to make decisions in real time, as fast as the situation arises.

Acquiring a better understanding of our adversaries' orientation, which shapes the local context on the periphery of the battlefield, demands that we give stronger consideration to creating a more agile DC2 structure, allowing generals to give field officers greater initiative to supply a more comprehensive picture of the battlespace. This image, in turn, enables the desired synchronized and shared situational awareness that generals must have to make more effective strategic decisions. The current austere environment of US defense investment, caused by budget constraints, means that we must do more with less. For that reason, we have to think beyond cyber-based maneuvers at the tactical level and focus on adapting and perfecting our KCW capabilities at the strategic level in order to compete effectively. In KCW, the victor will strategically target and successfully affect the opponent's truth filters, which the latter uses to validate beliefs and knowledge that guide his decisions. We can produce this effect only by means of synchronized and shared situational awareness as well as DC2 and execution.

Social media can greatly aid in the development of in-depth understanding of adversarial truth filters. Social media tools for using "science" to affect the other truth filters—consensus, consistency, authority, revelation, and durability—abound, and few are "military." One social media information organization lists more than two dozen such tools, which include (1) online profiles and online connections; (2) people,

online groups, and new media; (3) e-mail; (4) websites; (5) e-commerce; (6) web conferencing; (7) online video; (8) instant messaging; (9) online communities; (10) podcasts; (11) mobile phones; (12) wikis; and (13) blogs.

Yet each of these tools, to one degree or another, can have a "military" instantiation to create arsenals of superior knowledge and affect an adversary's truth filters. To what degree was nascent KWar evident during the Arab Spring? According to Kate Taylor,

> After analyzing more than three million tweets, gigabytes of YouTube content and thousands of blog posts, a new study has concluded that the Arab Spring truly was fueled by social media. "Our evidence suggests that social media carried a cascade of messages about freedom and democracy across North Africa and the Middle East, and helped raise expectations for the success of political uprising," says Philip Howard, an associate professor in communication at the University of Washington.[20]

Knowledge-Centric Warfare Applied

Successful application of KCW depends upon its organization. Adm Arthur Cebrowski and John Gartska, who introduced the notion of network-centric warfare (NCW) in 1998, observe that synchronization is the "operating of entities in the absence of traditional hierarchical mechanisms for command and control," serving as the "link between shared situational awareness and mission effectiveness." Synchronization "is the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up."[21] Their creation of NCW has certainly had strong theoretical merit over the years; nevertheless, we continue to have difficulty operationalizing the concept of synchronization, perhaps because the traditional hierarchical, top-down structure among the strategic, operational, and tactical levels still remains.

Rather than the NCW bottom-up approach, KCW seeks to obtain and expand synchronized situational awareness across a wider landscape of the battlefield, offering a more detailed picture of the operating en-

vironment. The use of new operating concepts and technology facilitates a shared understanding of that environment across a DC2 structure that enables delivery of more relevant and timely information to the participants anywhere and at any time, yielding the desired effect of synchronized situational awareness (fig. 4). In decentralized systems, "there is no one central executive or leader directing every aspect of the battlefield, but rather responsibilities are distributed, culminating in an emergent coordination structure based on input from many different perspectives of global terrain. This functionality comprises a general organizational strategy applicable over a wide range of complex tasks."[22] The concept of DC2 envisions a learning organization, shifting from the traditional top-down hierarchy towards a more cylindrical framework that permits greater agility in the face of constantly changing circumstances. In this new arrangement, generals trust their subordinates to adapt to new concepts and technologies, thereby establishing a fully synchronized situational awareness.

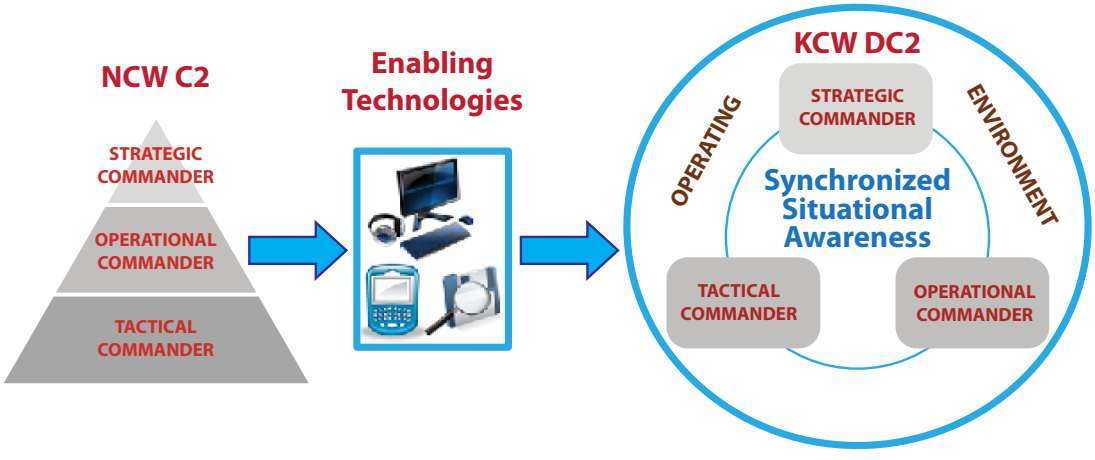

Figure 4. Decentralized command and control

Building on the thesis of Phillip Kao's article "Operationalizing Knowledge," we see that the utility of DC2 resides in the concept of a closer, more coordinated fusion of the strategic and operational levels that support the tactical level in an effort to execute strategic, high-level

functions in a flexible and adaptive manner.[23] The success of military operations depends on assured, reliable, and effective synchronized situational awareness facilitated through DC2 at every military echelon, from the continental United States to the forward-deployed war fighter.

War today goes well beyond the kinetic campaign maneuvers of the battlefield and has a much broader scope that includes postconflict objectives, joint training exercises, economic development, and nation building, all of which require military commanders to serve as both advisers and consultants with supporting subject-matter experts and ad hoc entities. In terms of shaping KCW and related efforts to create DC2 that fosters improved intelligence analysis and effective situational awareness, numerous consulting engagements that run advanced analytics across the commercial and public sectors have enjoyed great success. Given that intelligence analysis concerns itself with knowledge competition, efforts such as these have directly contributed to creating the shared and synchronized situational awareness of the environment. They do so by utilizing methodologies that not only focus on identifying the adversary's unknown biases and values but also aim to answer the key intelligence question in an effort to provide critical insights in a compressed time frame.

With regard to cyber warfare, the fact that commercial and military systems are not impervious to viruses and data corruption by way of sabotage makes the thrust towards developing KCW capabilities all the more pertinent. Some of the key technology areas of KCW include advances in (1) cognitive reasoning, which deals with understanding human-technology interactions and strives to grasp the cognitive skills underlying behavior, such as problem solving, decision making, and assessment; (2) behavioral modeling, which involves the study of how the human brain functions, reasons, and assesses data, information, and knowledge—a process that machines can mimic, offering more human-like alternatives for a decision maker to consider; and (3) self-learning knowledge extraction, which attempts to develop an automated capability to reason, infer, and discover knowledge implicit in extracted information.[24]

As these capabilities become more integrated, we might foresee something similar to IBM's Watson computer put to use in military cyber, network, and knowledge domain operations. Watson could search and process a tremendous amount of data in less than six seconds per question, outthinking even the smartest contestants on the trivia game show *Jeopardy!* Imagine how this computer's advances in deep analytics and its ability to process unstructured data as well as interpret natural language could be tailored to fit the requirements of new solutions in obtaining knowledge dominance in the cyber battlespace.[25]

Here, we envision a scenario in which a remotely piloted vehicle photographs insurgent activity and then forwards the image to Watson for what one might call an "übersource" assessment—a fusion of all-source intelligence (e.g., human, signals, electronic, geospatial, etc.) augmented by predictive analysis on related environmental, political, economic, and cultural conditions—thus providing the precise, shared situational awareness needed for commanders to make more efficient and better-informed decisions. Lt Gen Michael Flynn, nominated by President Obama to become director of the Defense Intelligence Agency, advocates looking beyond the collection of battlefield intelligence and insurgent activity. Specifically, he urges that we investigate the possibility of successfully attaining the desired full-spectrum intelligence and situational awareness that accounts for all relative environmental conditions in a decentralized command structure.[26]

How Do We Implement Knowledge-Centric Warfare?

Herein lies a working theory and construct that offers an approach to a new strategic command framework that will better accommodate and accelerate the acquisition and distribution of information and knowledge across the battle sphere. The fact that conflicts are becoming more globally interconnected demands new conceptual thinking from military leadership and subject-matter experts, presenting a unique opportunity to embrace a new C2 structure for greater success across future complex conflicts.

The Department of Defense's fiscal circumstances have changed our strategic priorities and made our joint force smaller and leaner. To maintain our military superiority in a world where complex conflicts occur across a greater expanse of the globe, we will need new operating concepts, one of which calls for a more dispersed and decentralized command structure across all domains. This creates the agility necessary to respond to a myriad of contingencies at any given time. A flatter command framework that demonstrates agility with an emphasis on human behavior will gain the competitive advantage in knowledge in a rapidly changing, complex environment.

This emphasis on human behavior remains central to KCW, attained by creating knowledge derived from a comprehension of what people value and why they value it within their environment. By completely understanding the adversary's truth filters—what shapes their perceptions, observations, biases, and beliefs—and by using this knowledge adaptively, we gain the desired situational awareness demanded at all levels of command. We will dominate the knowledge sphere once we have a genuine understanding of what our adversaries value and how those values drive their intentions and motivations within their environment.

In the networked-connected wars of the twenty-first century, new operating concepts and advanced war-fighting technologies are shaping "an environment 'where the strategic, operational, and tactical levels of war can at times be so compressed as to appear virtually as a single function.' "[27] Winning in this environment necessitates the speed of execution based on a shared knowledge that enables the commander to contest the enemy in each of these levels in near-simultaneous fashion.

The very essence of this article concerns the need to know what and why. A new, decentralized command structure that delivers accurate and timely intelligence will give modern commanders a fuller awareness of their environment. When we attain such awareness and always know the answers to what and why, we will have achieved the knowledge dominance that we seek. ✪

Notes

1. For the idea of KWar, see Alvin Toffler and Heidi Toffler, *War and AntiWar: Survival at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993), 8, 9.
2. Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (London: Routledge, 2007), 244. I am grateful to Dr. Frans Osinga for his profound understanding and eloquent articulation of John Boyd's thinking.
3. Ibid., 36.
4. Alvin Toffler and Heidi Toffler, *Revolutionary Wealth* (New York: Knopf, 2006), 104, 105.
5. Col Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 60.
6. Osinga, *Science, Strategy and War*, 57, 72.
7. Szafranski, "Theory of Information Warfare," 60.
8. Osinga, *Science, Strategy and War*, 8.
9. Ibid., 77.
10. Ibid., 84.
11. Ibid., 193, 230.
12. Joint Publication 3-14, *Space Operations*, 6 January 2009, GL-6, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.
13. Toffler, *Revolutionary Wealth*, 123.
14. Dr. P. W. Singer, "Tactical Generals: Leaders, Technology, and the Perils of Battlefield Micromanagement," *Air and Space Power Journal* 23, no. 2 (Summer 2009): 78–87.
15. Toffler, *Revolutionary Wealth*, 123–28.
16. Szafranski, "Theory of Information Warfare," 59.
17. Adam Segal, "Chinese Computer Games: Keeping Safe in Cyberspace," *Foreign Affairs* 91, no. 2 (March/April 2012): 14–20.
18. Singer, "Tactical Generals," 81.
19. Ibid.
20. Kate Taylor, "Arab Spring Really Was Social Media Revolution," *TG Daily*, 13 September 2011, http://www.tgdaily.com/software-features/58426-arab-spring-really-was-social-media-revolution.
21. B. J. A. van Bezooijen, P. J. M. D. Essens, and A. L. W. Vogelaar, *Military Self-Synchronization: An Exploration of the Concept* (Netherlands: Tilburg University, n.d.), 2, 4, http://www.dodccrp.org/events/11th_ICCRTS/html/papers/065.pdf.
22. Jamie Gorman, Nancy Cooke, and Jennifer Winner, "Measuring Team Situation Awareness in Decentralized Command and Control Environments," *Ergonomics* 49, nos. 12–13 (October 2006): 1312–25.
23. Philip Kao, "Operationalizing Knowledge: A New Chapter in the Saga of US War Fighting and Cognition," *Air and Space Power Journal* 26, no. 3 (May–June 2012): 31–44, http://www.airpower.au.af.mil/digital/pdf/issues/2012/ASPJ-May-Jun-2012.pdf; and Gorman, Cooke and Winner, "Measuring Team Situation Awareness."
24. Dr. Paul W. Phister Jr. and Mr. Igor G. Plonisch, *Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare* (Rome, NY: Air Force Research Laboratory, Information Directorate, n.d.), 14, 16, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/188.pdf.

25. "Watson—A System Designed for Answers: The Future of Workload Optimized Systems Design," IBM, accessed 19 May 2012, https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=stg-600BE30W.

26. Maj Gen Michael T. Flynn, USA; Capt Matt Pottinger, USMC; and Paul D. Batchelor, DIA, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Washington, DC: Center for a New American Security, January 2010), http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

27. Singer, "Tactical Generals," 83.

Mark Ashley

Mr. Ashley (BA, George Washington University; Graduate Certificates, Texas A&M University) is a consultant with Toffler Associates. He originally worked as a cameraman in the film industry shooting high-profile movies such as *The Perfect Storm* and television shows such as *The X Files*. After the terrorist attacks of 11 September 2001, he earned a degree and certificates in international affairs and advanced international affairs with concentrations in counterterrorism and intelligence studies. He has studied at the Middle East Institute and the US Foreign Policy Institute in Washington, DC, and attended the Arabic Language Institute and Al-Akhawayn University in Ifrane, Morocco. Prior to joining Toffler Associates, Mr. Ashley worked as an artificial intelligence engineer with the MITRE Corporation in the Center for Integrated Intelligence Systems and with the MASY Group, supporting the US intelligence community by conducting surveillance training and practical exercise assistance related to antiterrorism and countersurveillance. His present focus area is military and business competitive strategies, especially as they relate to China. Mr. Ashley resides in Arlington, Virginia.

Let us know what you think! Leave a comment!