U.S. Navy E-2C Hawkeye 2000 aircraft assigned to "Wallbangers" of Carrier Airborne Early Warning Squadron 117 approaches flight deck of USS *John C. Stennis* while ship is underway in Pacific Ocean, July 13, 2006 (DOD/John Hyde)

Twenty-First Century Information Warfare and the Third Offset Strategy

By James R. McGrath

While the United States and our closest allies fought two lengthy wars over the past 13 years—the rest of the world and our potential adversaries were seeing how we operated. They looked at our advantages. They studied them. They analyzed them. They looked for weaknesses. And then they set about devising ways to counter our technological over-match.

—Deputy Secretary of Defense Robert Work

It is well established that both state and nonstate adversaries are gaining parity with current U.S. military-technological capabilities, and as a result adversaries are eroding the tremendous asymmetrical conventional warfare advantages once exclusively enjoyed by U.S. forces.[1] This leveling of the playing field has been enabled through decreased costs of modern information technology and low barriers of entry to attaining precision weapons; stealth capabilities; sophisticated commercial and military command and control (C2) capabilities; advanced intelligence, surveillance, and reconnaissance (ISR); and relatively cheap access to commercial and government-sponsored space and cyber capabilities.[2] As a result, in November 2014, then–Secretary of Defense Chuck Hagel announced the Defense Innovation Initiative to counter adversary technical and tactical progress that, if left unchecked, will ultimately hinder U.S. ability to project power across the globe and permanently challenge its aims of retaining its coveted status as a global hegemon.[3] While there are many aspects to this initiative, the Third Offset Strategy, as outlined in policy, does not adequately address the need for advanced information operations (IO), particularly IO wargaming, modeling and simulation (M&S), and training systems. The purpose of this article is to make the case that increasing the investment in joint live, virtual, and constructive (LVC) IO wargaming and simulations will generate lasting asymmetrical advantages for joint force commanders and will significantly contribute to the achievement of the Third Offset Strategy.

Military Problem

The Defense Innovation Initiative is aimed at solving the problem of ensuring that lasting power projection capabilities are available to the U.S. military in pursuit of the Nation's core and enduring national interests, most notably safeguarding national security, promoting democratic values, maintaining long-term economic prosperity, and preserving the current international order.[4] The solution to this problem—one that has yet to be fully articulated and bounded in scope, much less solved—has been named the Third Offset Strategy, meaning that there are a series of strategic capabilities that must be developed to give U.S. forces a decisive military-technological offset that generates lasting asymmetrical advantages over any potential adversary for the next 25 to 50 years. The strategy is so named because there already were two successful offset strategies in the 20th century.[5] The first was President Dwight D. Eisenhower's New Look Strategy during the 1950s, which sought to develop advanced nuclear weapons capabilities to offset the Soviet Union's overwhelmingly superior conventional forces and nascent nuclear capabilities. The second strategy was Secretary of Defense Harold Brown's Offset Strategy during the 1970s, which was aimed at countering recent Soviet advances in both numerical and technical parity regarding its nuclear arsenal, coupled with sustained numerically superior conventional forces deployed in Eastern Europe and elsewhere around the globe. Essentially, the U.S. Offset Strategy invested in stealth technologies, precision weapons, sophisticated C2 capabilities, and advanced airborne and space-based ISR that were ultimately revealed to the world during the first Gulf War.

As outlined by Secretary Hagel and currently being championed by Deputy Secretary of Defense Robert Work, the Defense Innovation Initiative emphasizes three key areas for sources of innovation: long-range research and development, new operating concepts, and reenergizing wargaming efforts and techniques.[6] Currently, most of the discussion regarding this initiative is overly focused on purely technical, materiel solutions, such as unmanned autonomous systems and sources of new global strike and ISR capabilities. Regrettably, the appeal for the development of new operating concepts and wargaming techniques seems to be overlooked in the media and most defense policy think tanks.

What many analysts fail to realize is that the operating environment, specifically the information environment (IE),[7] has changed, and our adversaries are undermining our asymmetrical advantages through innovative use of the information space, particularly by operating in the informational and cognitive dimensions on a global scale.[8] What should be obvious—but unfortunately is not to many military and defense planners—is that IO is precisely the tool set that joint force commanders already have to attack our adversaries' newly found advancements in C2 warfare, ISR, and precision weapons. Unfortunately, for example, the Russians,[9] Chinese,[10] and the Islamic State of Iraq and the Levant,[11] to name a few, are now also demonstrating advanced forms of information warfare that continually undermine U.S. tactical prowess and enable successful antiaccess/area-denial (A2/AD) strategies that are the root cause of the problem.[12] For U.S. forces to achieve the Third Offset Strategy, the joint force must be able to achieve information superiority at the time and place of its choosing. To do that, the joint force must develop innovative operating concepts for IO, wargame them using a variety of computer-based methods, and then train to the newly discovered tactics, techniques, and procedures that are absolutely essential for 21st-century warfare—a type of warfare aimed at breaking the will of the adversary through control of the IE.

Currently, IO is often treated as an ad hoc, additive activity during most joint LVC training events; therefore, IO is routinely ignored or underutilized despite being a major component of every real-world joint operation since Operations *Desert Shield* and *Desert Storm*[13] and arguably in other forms, such as psychological warfare and deception, throughout all of human history.[14] Much of the reason for this routine omission and lack of prominence in major joint LVC exercises is that military information

Lieutenant Colonel James R. McGrath, USMC, is the Information Warfare Department Head for Expeditionary Warfare Training Group Atlantic.

support operations (MISO, formerly known as psychological operations), public affairs, electronic warfare (EW), cyber warfare, military deception (MILDEC), special technical operations, and other information-related capabilities (IRC)[15] are difficult to simulate over a relevant exercise time horizon. Even more challenging is the ability to realistically but sufficiently model the physical, technical, and cognitive complexities of the IE as a coherent whole whose sum is greater than its individual parts. If this can be achieved, U.S. joint forces would be able to train in synthetic environments that would ultimately enable them to effectively maneuver within the IE, counter recent adversary military-technological gains and newfound information warfare prowess, and provide the baseline for a newly defined technical, military, and psychological offset.

IO as the Solution

By acknowledging the fact that adversaries are reducing our operational advantages and conventional overmatch through innovative use of the IE, it becomes increasingly imperative that U.S. IO training, wargaming, and operating concepts be improved. It is also important to emphasize that this improvement should not only mirror-image the activities of our adversaries, but also provide joint force commanders with a comprehensive set of tools and concepts that allows them to outmaneuver adversaries within the cognitive, informational, and physical dimensions of the IE. As a starting point, a brief analysis of modern IO reveals at least six interrelated IO lines of effort (LOE), which if truly integrated with each other could facilitate the Third Strategic Offset. These primary LOEs or mission areas are psychological warfare, C2 warfare, denial and deception, cyber warfare, engagement, and IE situational awareness.[16]

While on the surface some of these IO LOEs appear well-established IRCs, that is not the intent or the case. These highly complementary and interdependent mission areas are IRC agnostic—meaning that no one particular IRC is necessarily required for a particular mission.[17] In fact, multiple IRCs applied in a combined arms fashion are a prerequisite to achieving success in any one of these critical mission areas. This idea is consistent with the accepted Department of Defense (DOD) IO definition and is precisely why they are considered germane to any serious discussion of future IO.[18] The following discussion briefly highlights the need for further development and implementation of these six mission areas, as well as their relevance to the future joint force.

Generally speaking, *psychological warfare* is defined as actions against the political will of an adversary, his commanders, and his troops, and includes inform and influence operations directed at any third party capable of providing sympathy or support to both the adversary or friendly forces.[19] This mission area directly targets the cognitive dimension of our adversaries' operations in the IE and ultimately attacks their will to resist. It should be the primary focus of the joint force in order to ensure lasting tactical, operational, and strategic success, especially while state and nonstate actors are simultaneously competing for dominance in this highly contested space. After all, by definition, war as a contest of political wills by other means is the primary basis of most warfighting philosophies.[20] Therefore, increasing the effectiveness of joint operations in this mission area would certainly require improved MISO, EW, cyber, and MILDEC capabilities and authorities at all levels of war.

C2 warfare is about controlling the physical and informational dimensions of the IE by cutting off an enemy force from its commander, key decisionmakers, or automated control systems through attacking vulnerable control mechanisms or by simply attacking the commander and removing him or her from the C2 equation, ultimately resulting in the collapse of his or her subordinate forces.[21] Applying IRCs for C2 warfare purposes is one of the few ways to overcome the joint operational access and A2/AD problems. Using a combination of physical destruction, EW, cyber, MISO, and MILDEC capabilities would be indispensable to the process of systematically unravelling an adversary's integrated air and coastal defenses; undermining his ballistic and cruise missile standoff weapons; and blinding his advanced land, sea, air, cyber, and space-based ISR platforms. Furthermore, there is a defensive aspect of C2 warfare that requires advanced electromagnetic spectrum operations, information assurance, and defensive cyberspace operations to ensure assured C2 over friendly forces on a global scale. Without a modern, robust defensive C2 warfare capability, U.S. global power projection is nearly impossible.

Denial and deception operations are a combination of operations security and MILDEC activities, supported by a wide-range of IRCs, to protect critical information, facilitate surprise, and deliberately mislead an adversary to achieve a tactical, operational, or strategic advantage. Denial and deception operations provide force-multiplying advantages by enabling operational access and joint forcible entry operations under A2/AD conditions and contributing to the cognitive demise of an adversary as part of the psychological warfare effort. In addition, counter–denial and deception operations are critical to future conflicts, as demonstrated by our adversaries' skilled use of deception in Syria, Iraq,[22] and the Crimean Peninsula.[23]

Cyber warfare in the IO context is about controlling the content and flow of information within the information dimension of the IE. It includes the convergence of the cyber and EW IRCs, where cyber is enabled at the tactical level through radio frequency spectrum operations; cyber warfare in support of the other five IO mission areas; and offensive cyberspace operations in support of traditional kinetic operations. For instance, a prime example of this IO mission area in action is the Russia-Georgia war of 2008, during which the Russians executed the world's first synchronized cyber attack in concert with major combat operations, likely using both state cyber capabilities and nonstate hackers to attack key Georgian communications, finance, and government nodes prior to and during combat operations to control

Then–Secretary of Defense Chuck Hagel announces Defense Innovation Initiative and Third Offset Strategy during Reagan National Defense Forum at The Ronald Reagan Presidential Library in Simi Valley, California, November 15, 2014 (DOD/Sean Hurt)

the narrative and pace of the psychological war as well as demonstrate Russian resolve and future deterrence capabilities.[24] Furthermore, there is tremendous opportunity for future cyber warfare operations to: 1) support C2 warfare in A2/AD conditions by creating gaps and seams in an adversary's defensive system of systems from standoff ranges, especially during the early shaping phases of an operation; 2) enable the psychological warfare effort through focused and broad social media messaging; and 3) support both the engagement and IE situational awareness efforts as message delivery and ISR platforms.

The U.S. Army has recently established *engagement* as a concept for a seventh warfighting function and defines it as influencing people, security forces, and governments across the range of military operations to prevent, shape, and win in the future strategic environment.[25] While there are close similarities, in this context, engagement is an IO mission—not a warfighting function focused on the intersection between partnership activities and special warfare activities.[26] In this context, engagement is about operating in the cognitive dimension of the IE through informing and influencing partner and adversary nations using a wide range of IRCs, including but not limited to media operations using public affairs and MISO. Engagement as an IO mission also includes public affairs operations to harden the friendly force against adversary psychological warfare. Moreover, for the foreseeable future, engagement will remain a combatant commander's primary tool for Phase 0, steady-state, and theater security cooperation (TSC) operations, used to send signals to our adversaries and allies that we are committed to the current international order and a stable security environment. For instance, engagement could and should be used to amplify our TSC actions in the U.S. Pacific Command area of responsibility to ensure that Chinese psychological, media, and legal warfare[27] are countered with the overarching goal of ensuring that our regional allies are able to observe our actions and interpret them as U.S. commitment to defend our common interests.

Lastly, *IE situational awareness* is defined as understanding past events within all three dimensions of the IE, tracking ongoing events, and being able to adequately model and reliably predict (or at the very least wargame) a wide variety of possible outcomes in support of the other five IO mission areas. These activities include not only all traditional intelligence disciplines but also the use of a broad range of IRCs operating on the battlefield as sensors, processors, and actors. In addition, IE situational awareness requires advanced M&S to aid IO planners and commanders in the extremely difficult task of understanding

the dynamic, nonlinear, and ever-changing IE. Furthermore, IE situational awareness requires a detailed understanding of individuals, social groups, behavior dynamics, communication architectures, exploitation of narratives, and target audience vulnerabilities, as well as the newly emerging techniques of real-time, live big data analytics, social media scraping, and memetic warfare.[28]

IO M&S Requirements

As discussed, there is a known gap for joint force commanders to exercise their IO cell within the six mission areas outlined above. There is also a gap for exercising both supporting organic and non-organic IRCs and then integrating them with traditional kinetic fires. Closing this gap with computer-based M&S would ensure that joint forces are well trained in a repeatable and expandable synthetic environment prior to employment across the full range of military operations. This is particularly important because IO mission areas and their supporting IRCs are highly sensitive in nature, and live IO training events are nearly impossible to conduct. For instance, certain EW, cyber, and special technical operations capabilities must be well protected to achieve any form of technical surprise, and MISO, EW, cyber, MILDEC, and special technical operations also have uniquely strict political and legal sensitivities.

Achieving repeatable, scalable, and fully integrated simulation of the IE is not an easy task. However, if the Third Offset Strategy is to be realized, the Services and DOD must invest in materiel solutions to enable the joint force to train its IO forces in a synthetic environment. There are several key additional requirements for any useful automated M&S of the IE and IO for advanced wargaming purposes:

- Must encompass a system-of-systems approach that includes training for individual IO and IRC mission essential tasks through the highest levels of a joint force's collective-level training events. Examples include a range of immersive virtual environments for individual and small-unit IRC tactical trainers through high-level constructive simulations supporting strategic- and combatant command–level wargaming, capable of seamlessly integrating with each other as well as other kinetic and legacy M&S systems.
- Must incorporate the full array of possible effects that can be generated by organic and non-organic IRCs from the strategic to the tactical level of warfare.
- Must be interoperable with other joint and Service-level LVC M&S networks and systems.
- Must be compatible with all major constructive M&S programs of record in order for IO M&S to be fully integrated into a single common tactical and operating picture.
- Must be interoperable with current command and control systems and classified intelligence systems up to Top Secret/Sensitive Compartmented Information and other high-level operational security control measures to be integrated into a single common tactical and operating picture.
- Must incorporate open source media and the replication or emulation of social and traditional media for analysis, using advanced forms of data analytic techniques to simulate actions in the IE.
- Must incorporate advanced decision support M&S techniques, including but not limited to artificial intelligence–enabled augmented reality, chatbots, and other expert systems to facilitate understanding of actions in the IE.
- Must leverage state-of-the-art artificial intelligence algorithms, machine-learning software, and advanced M&S paradigms, such as agent-based modeling, systems dynamics, and game-theoretic modeling in a federated architecture, to accurately model complex, adaptive systems with the goal of replicating the behaviors and communications conduits of a vast array of thinking target audiences and their highly automated information systems.

Ultimately, the desired endstate for developing an advanced IO M&S capability is to ensure that there are highly trained forces ready to design, plan, rehearse, execute, and assess operations within the IE, particularly when confronted with a sophisticated, technologically enabled 21st-century adversary. This can and should be implemented via a family of tactical- through strategic-level M&S systems that adequately model and simulate friendly, neutral, and adversary decisionmaking capabilities, behaviors, and information systems as well as the complex feedback loops that comprise all relevant aspects of the physical, informational, and cognitive dimensions of the IE.

IO Considerations

There are five prominent counterarguments that immediately come to mind for not developing advanced IO M&S capabilities. These arguments range from the cost of IO M&S materiel solutions, the presence of other existing solutions, widespread doubts regarding the efficiency and efficacy of IO across the full range and spectrum of military operations, and the complex framework of legal and policy restrictions governing most joint force IRC employment.

The first counterargument is that developing IO M&S systems would be expensive and that the technology for simulating the IE is not mature. However, this is exactly the type of investment that the Defense Innovation Initiative is calling for: an investment that leverages advanced technologies such as artificial intelligence, machine learning, agent-based modeling, and big data analytics that our adversaries would not likely have ready access to exploit. This investment in IO M&S would also lead to new operating concepts that would be tested during high-level joint wargames using the very same systems, which is precisely the intent behind the second and third key areas for innovation outlined by the Defense Innovation Initiative.

The second counterargument is that the Joint Staff and the Office of the Secretary of Defense are already investing in IO M&S through the use of the Joint IO Range and other cyber and EW

Soldiers from Britain's Royal Artillery train in virtual world during Exercise Steel Sabre 2015 (MOD/Si Longworth)

initiatives. While that is a first step, the Joint IO Range is only a stovepipe capability for cyber warfare effects rather than a capability that truly exercises all relevant IRCs in support of joint operations—that is, something more than cyber and EW operations are required to realize the true potential for full-spectrum IO, specifically how to assemble a relevant array of IRCs aimed at placing an adversary on the horns of a dilemma and then inducing a complete collapse of their will to resist our aims and objectives. Without being able to model and integrate the cognitive, informational, and physical aspects of the IE in a coherent simulation, influencing adversary decisionmakers and their supporting systems would not be achievable to the level of what is required for the Third Strategic Offset.

The third counterargument is that IO is not suited for major combat operations, and thus many military planners perceive it as a tool only for counterinsurgency or irregular warfare, whereby keeping the violence threshold low or controlling the attitudes and the behavior of the local populace is paramount. This is not the case, however, since IO and IRCs have routinely been employed by U.S. forces throughout all phases of operations and all types of conflict, from World War II through Operations *Enduring Freedom* and *Iraqi Freedom*. Additionally, there is considerable evidence that increasing the lethality of operations using information warfare is central to the strategy of our 21st-century adversaries, most notably and recently demonstrated by the Russians operating in Ukraine and Syria.[29]

The fourth counterargument is that IO is not well suited for the strategic shaping and deterrence missions required by the Third Offset Strategy, or at least not as effectively as the physical advantages that the Second Offset capabilities have provided. However, in some sense, the luxuries that were afforded by the unprecedented freedom of movement, maneuver, and firepower that successfully held our adversaries in check for the past 25 years are also the root cause of our current military problem—namely that U.S. joint forces routinely win tactically and sometimes operationally, but continuously have their victories ultimately overturned at the operational and strategic levels, such as in Iraq and Afghanistan. Ironically, it has been the overdependence on our physical, conventional superiority that has led the U.S. military to neglect the mental and moral aspects of warfighting, a deficiency that IO, by definition and if sufficiently raised to the appropriate level of prominence within U.S. warfighting doctrine, can immediately address.[30] In addition, to further discredit the notion that IO is an ineffective strategic shaping and deterrence tool, it is a well-accepted fact that due to international legal, diplomatic, and political constraints, IO and a handful of select influence-oriented IRCs are our military's only available tools to successfully prevent, deter, initiate, or close a conflict.

Soldiers from U.S. Army's 350th Tactical Psychological Operations, 10th Mountain Division, drop leaflets over village near Hawijah, Iraq, on March 6, 2008, promoting idea of self-government (U.S. Air Force/Samuel Bendet)

The fifth and final counterargument is that there are insurmountable legal and policy restrictions for the joint force to conduct full-spectrum IO. This is simply not the case. However, the two primary supporting counterarguments either revolve around U.S. Code Title 10, *Armed Forces*, versus Title 50, *War and National Defense*, arguments, or claim that the current review and approval processes for IRCs are too complicated to achieve timely and relevant effects in the IE. The first supporting argument is false because Title 10 and Title 50 issues have already been solved and are deconflicted on a daily basis using a highly complex but extremely effective ISR and strike network. This network is enabled by intelligence professionals and operators working side by side, both physically and virtually, and allows the lowest tactical formations to receive the benefits of strategic assets and vice versa. There is some truth to the second supporting counterargument that the review and approval processes are overly complex. Many IRCs do, in fact, require DOD- and national-level approvals. This is not true for all IRCs, however, and there are numerous IRC-unique programs already in place for military planners to immediately implement. In addition, all IRCs can be and already are implemented with great effect for those commanders with well-trained IO staffs. Hence, developing an IO M&S and training capability is actually part of the solution to the military problem and not an impediment. Lastly, as joint forces continue to demonstrate their increased proficiency for fighting and winning in the IE—and as our adversaries do the same—it is inevitable that over time, many of the authorities for certain sensitive IRC activities, currently held at the strategic level, will naturally be delegated to operational and tactical commanders.

Future Innovation

In the long run, creating the necessary technical innovation in the field of advanced IO M&S and training would no doubt lead to the maturation of capabilities and tactics needed to achieve the goals of the Third Strategic Offset. Furthermore, the gaps that IO M&S could immediately close are also the first steps in the necessary research, design, and development of an integrated global effects network that could and should act as the primary intellectual engine for an advanced, semi-autonomous global strike and ISR network—a network that has been considered the "holy grail" by those who already offer solutions to the Third Strategic Offset problem and that is a solution that is eerily similar to nefarious systems of science fiction literature and movies, such as *The Terminator*'s self-aware "SkyNet" and "Genisys" programs.[31] The flaw in this popularized global strike and ISR network solution—other than the obvious science fiction connotations—is that it is shortsighted and deals only with the current problem within the physical dimension of the operating and information environments. The real solution is something far more complicated and worthy of the forward thinking required by the Third Strategic Offset problem set.

A better solution is an advanced, semi-autonomous hybrid kinetic and nonkinetic weapons system fully enabling the warfighter to, at a moment's notice, conduct highly integrated, cognitively focused operations that are also simultaneously synchronized with other ongoing joint actions across the globe, as well as concurrently facilitating long- and short-term influence campaigns. Continuously and consistently striking at the will of our adversaries through the use of carefully selected physical, information, and cognitive-related capabilities should be the ultimate goal of this advanced weapons system concept. This system would facilitate maneuver warfare and mission command by integrating, synchronizing, and coordinating many different capabilities by different commanders at all levels directly against an adversary's physical, moral, and mental critical capabilities. Again, this is something that clearly cannot be accomplished without advanced IO M&S accurately and continuously modeling the complex, nonlinear, and ever-changing IE. While the fusing of kinetic and nonkinetic modeling into a semi-autonomous global effects network might seem like material for science fiction, in the current era of machine-based learning and artificial intelligence–enabled autonomous vehicles, these capabilities are not too far over the horizon and are worthy goals for the ambitions of the Third Offset Strategy.

The military-technological gains of our adversaries over the past several decades are apparent and alarming. To counter this

threat and meet the intended objectives of the Defense Innovation Initiative, a robust set of research and development programs, concept development activities, and wargaming efforts has begun to uncover a series of technologies required to achieve the Third Strategic Offset. While an advanced family of IO LVC M&S systems is not the only capability required to achieve this ambitious offset strategy, failing to recognize the prominence of IO in this new era would be a serious mistake. In addition, these IO M&S capabilities should be the foundation and focus of any future advanced, semi-autonomous global effects system. Therefore, advanced IO M&S is an absolutely indispensable capability that will fully enable the joint force to achieve lasting asymmetrical advantages over our newly emerging, emboldened, and technologically savvy 21st-century adversaries. **JFQ**

Notes

[1] James R. Clapper, Opening Statement to the Worldwide Threat Assessment Hearing, Senate Armed Services Committee, February 9, 2016, available at <www.dni.gov/index.php/newsroom/testimonies/217-congressional-testimonies-2016/1314-dni-clapper-opening-statement-on-the-worldwide-threat-assessment-before-the-senate-armed-services-committee-2016>.

[2] Robert Martinage, *Toward A New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection* (Washington, DC: Center for Strategic and Budgetary Assessment, October 2014).

[3] Chuck Hagel, "Secretary of Defense Memo: Defense Innovation Initiative," November 2014.

[4] *National Security Strategy* (Washington, DC: The White House, February 2015), available at www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>.

[5] Martinage.

[6] Hagel.

[7] The *information environment* is an environment that is an aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information as defined by Department of Defense (DOD) Directive 3600.01, *Information Operations* (Washington, DC: DOD, May 2013), available at <www.dtic.mil/whs/directives/corres/pdf/360001p.pdf>.

[8] The *information environment* is comprised of three interrelated dimensions: cognitive, information, and physical. See Joint Publication 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 20, 2014), x.

[9] Jolanta Darczewkska, *The Anatomy of Russian Information Warfare* (Warsaw: Centre for Eastern Studies, May 2014), available at <www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study>.

[10] Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: Strategic Studies Institute, March 2014), available at <www.strategicstudies-institute.army.mil/pubs/display.cfm?pubID=11901>.

[11] U.S. Army Training and Doctrine Command (TRADOC) G-2 Intelligence Support Activity, Complex Operational Environment and Threat Integration Directorate, *Threat Tactics Report: Islamic State of Iraq and the Levant* (Fort Leavenworth, KS: TRADOC, November 2014), 1, 13–15, available at <https://drakulablogdotcom3.files.wordpress.com/2015/04/trisa_threat_tactics_rpt_isil_141101-cdr-137271.pdf>.

[12] *Joint Operational Access Concept, Version 1.0* (Washington, DC: DOD, January 17, 2012), available at <www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%20 2012_Signed.pdf>; and *Joint Concept for Entry Operations* (Washington, DC: The Joint Staff, April 2014), available at <www.dtic.mil/doctrine/concepts/joint_concepts/jceo.pdf>.

[13] John Broder, "Schwarzkopf's War Plan Based on Deception," *Los Angeles Time*s, February 28, 1991, available at <http://articles.latimes.com/1991-02-28/news/mn-2834_1_war-plan>.

[14] Jon Latimer, *Deception in War* (New York: Overlook Press, 2001), 6.

[15] *Information-related capabilities* are tools, techniques, or activities employed within the dimensions of the information environment and can be used to achieve specific ends as defined by DOD Directive 3600.01.

[16] Martin C. Libiki, *What Is Information Warfare?* (Washington, DC: NDU Press, 1995); Darczewkska; Wortzel; TRADOC.

[17] Agnostic in this sense is based on the information technology context, where software and other processes are independent of hardware or various platforms. In this case, for example, psychological warfare objectives could be achieved outside the traditional doctrinal military information support operations construct with kinetic effects, maneuver, and other information-related capabilities (IRCs). Similarly, cyber objectives and denial and deception objectives could be achieved or supported outside the current cyber and joint military deception doctrinal framework using a variety of IRC effects—not to circumvent current DOD policy and authority framework but to simply acknowledge that there are other, perhaps more innovative means and ways to achieve the same ends.

[18] *Information operations* are generally defined as the integration, coordination, and synchronization of IRCs to deny, degrade, disrupt, or usurp an adversary's decisionmaking capabilities, people, and systems in support of a commander's objectives as defined by DOD Directive 3600.01.

[19] Libicki, 34.

[20] Carl Von Clausewitz, *On War*, trans. J.J. Graham (London, 1909), chapter 1, available at <www.gutenburg.org>.

[21] Libicki, 9–15.

[22] TRADOC, 12.

[23] Lucy Ash, "How Russia Outfoxes Its Enemies," *BBC.com*, January 29, 2015, available at <www.bbc.com/news/magazine-31020283>.

[24] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 2011, available at <www.smallwarsjournal.com>.

[25] TRADOC Pamphlet 525-8-5, *Functional Concept for Engagement* (Fort Eustis, VA: TRADOC, February 28, 2014), available at <www.tradoc.army.mil/tpubs/pams/tp525-8-5.pdf>.

[26] Ibid.

[27] Wortzel.

[28] Memetics and memetic warfare are used in the context of discrete ideas or units of culture being rapidly transferred to wide audiences, particularly over social media—that is, things "going viral" and their influence on cognition and behavior. See Jeff Giesa, "It's Time to Embrace Memetic Warfare," *Defense Strategic Communication* 1, no. 1 (Winter 2015), available at <www.stratcomcoe.org/download/file/fid/3956>.

[29] David Stupples, "How Syria Is Becoming a Test Zone for Electronic Warfare," *CNN.com*, October 9, 2015, available at <www.cnn.com/2015/10/09/opinions/syria-electronic-warfare-russia-nato/index.html>.

[30] Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: Headquarters Department of the Navy, June 7, 1997). Mental, moral, and physical aspects of maneuver warfare and the Marine Corps' warfighting philosophy are discussed throughout the text.

[31] Martinage.