Information on the Twenty-First Century Battlefield

Proposing the Army's Seventh Warfighting Function

Capt. Charles M. Kelly, U.S. Army

In May 2013, Ukrainian artillery officer Yaroslav Sherstuk designed a smartphone application to decrease the artillery targeting process from minutes to less than fifteen seconds.[1] The application experienced initial success with upward of nine thousand Ukrainian soldiers using it to conduct fire missions against Russian forces.[2] However, the independent security firm CrowdStrike reported a Russian information attack on the application via malware offered Russian forces "the potential ability to map out a unit's composition and hierarchy,

determine their plans, and even triangulate their approximate location."[3] Russian forces presumably used the malware to target Ukrainian artillery units employing the application. This example aptly demonstrates the character of war confronting modern militaries in the information age. The U.S. Army's current warfighting model does not adequately reflect the reality of this evolution. The Army should adopt information as the seventh warfighting function because the rapid change in the character of war brought about by the advent of the internet enables the weaponization of information. Furthermore, the information warfighting function would enable the adequate integration of information in operational planning and execution and provide an improved ability to apply force below the threshold of lethal effects.

Current Model: The Elements of Combat Power

Prior to discussing the information warfighting function in detail, some background on the Army's current paradigm is necessary. The Army uses the term "combat power" to describe the "total means of destruction, constructive, and information capabilities that a military unit … can apply at a given time."[4] Combat power is comprised of eight elements: the six warfighting functions (command and control, movement and maneuver, intelligence, fires, sustainment, and protection) with the addition of information and leadership (see figure, page 64).[5] The warfighting functions provide structure for commanders and staffs to plan and execute operations. Army Doctrine Publication (ADP) 5-0, *The Operations Process*, states, "The staff … integrates forces and warfighting functions to accomplish the mission."[6] In the current model, commanders achieve battlefield effects using the warfighting functions, while information and leadership simply aid in the optimal application of these functions. Field Manual 3-13, *Information Operations*, defines information operations (IO) as "the integrated employment … of information-related capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[7] Examples of some of these IRCs are military deception, civil affairs operations, and cyberspace operations.[8] Information operations are currently listed as staff tasks under the intelligence and fires warfighting functions.[9] However, IO is rapidly exceeding the bounds of tasks already required of these two functions. The rapid developments in information technology have induced newfound importance and relevance of information on the twenty-first-century battlefield. This article demonstrates the increasingly important role of information in warfare and the subsequent necessity of elevating information to a warfighting function.

Previous page: Photo illustration by Justin Rakowski, U.S. Army

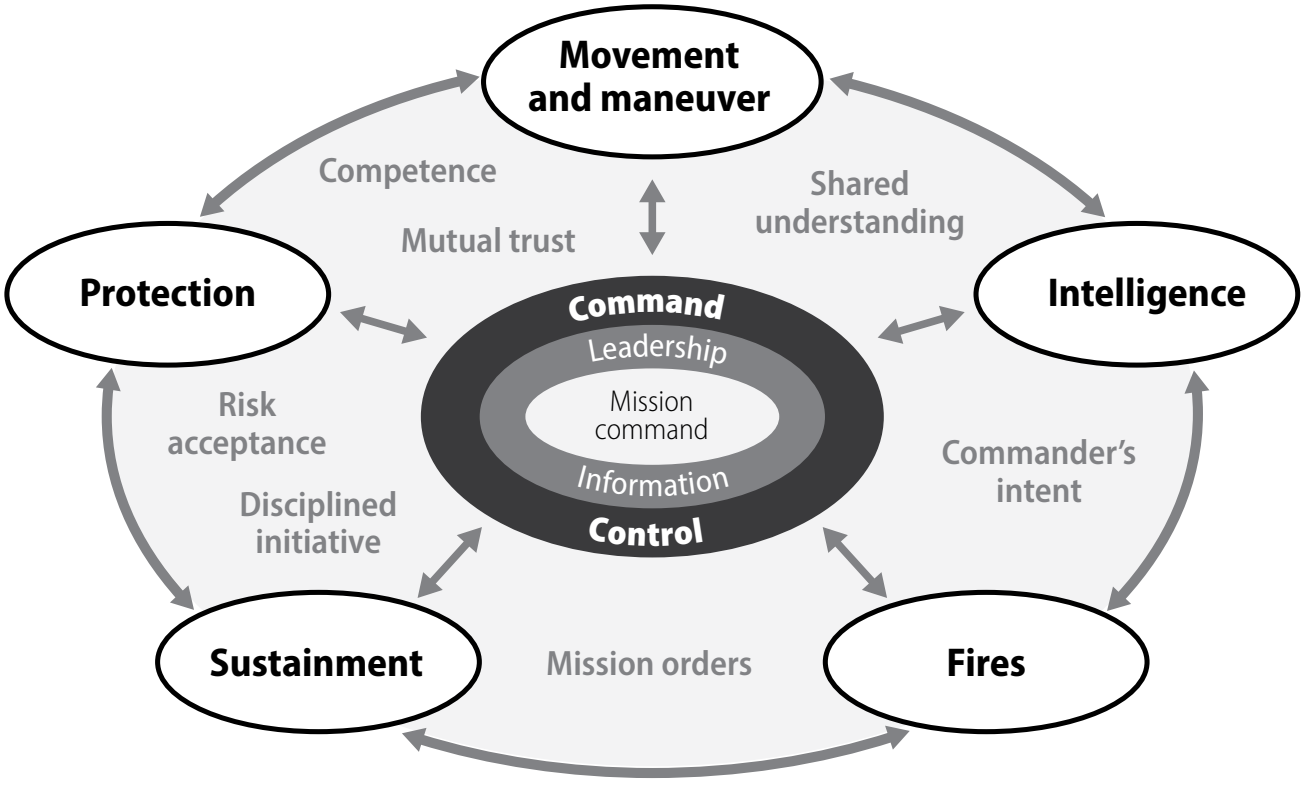
Information's Explosive Rise

The Army's current warfighting doctrine presents an antiquated view of the role of information in combat. History is replete with examples of the successful use of information in conflicts. During World War II, for example, the U.S. Army famously employed military deception using inflatable tanks and airplanes to deceive German forces in France. The rise in information technology increases the relevance and consequences of information in warfighting and offers opportunities for increased application. The North Atlantic Treaty Organization's Strategic Communications Centre of Excellence recently conducted an experiment in support of a large-scale military exercise using a simulated cyber red cell, "the opposing force in a war game," in order to evaluate friendly forces' signature in the online information environment.[10] Using only open-source information, social media, and sixty dollars, the red cell identified 150 soldiers, found the locations of several battalions, tracked troop movements, and compelled service members to engage in illicit behavior such as leaving their positions against orders.[11] The lack of institutional awareness of the effects and capabilities of information demonstrated by this example indicates the Army's current archaic model does not fully grasp the ramifications of information on today's battlefield.

Maintaining Supremacy

In order to maintain a competitive advantage

Capt. Charles Kelly, U.S. Army, is the commander of Company C, 2nd Battalion, 3rd Infantry Regiment, 1st Stryker Brigade Combat Team, 2nd Infantry Division, at Joint Base Lewis-McChord. He holds a BS in economics and a BS in Mandarin Chinese from the United States Military Academy. He previously served in 1st Battalion, 75th Ranger Regiment and 4th Brigade, 25th Infantry Division. He has deployed three times to Afghanistan in support of Operation Freedom's Sentinel.



(Figure from Army Doctrine Publication 3-0, *Operations*)

Figure. Elements of Combat Power

over our peer and near-peer adversaries, the Army must place a larger emphasis on the use of information as an instrument of war. Two decades of low-intensity conflict characterized by combating violent extremist organizations in the Middle East justifiably consumed much of the focus of the U.S. military. The relatively low sophistication level of the enemy enabled U.S. forces to become complacent on many of the tasks required to fight conventionally outfitted militaries in the twenty-first century. Former chairman of the Joint Chiefs of Staff Gen. Joseph Dunford stated, "The challenges of a decades-long campaign against violent extremism adversely affected our own modernization and capability development efforts."[12] Accordingly, participation in these wars presented America's peer and near-peer adversaries the opportunity to aim their force-modernization efforts on defeating U.S. tactics, techniques, and procedures. To further exacerbate this challenge, the concurrent meteoric rise in information technology enabled adversaries to integrate many of these advancements into their force-modernization efforts.

In a 2013 article, Russian Chief of the General Staff Valery Gerasimov outlined what he believed to be the necessary approaches for twenty-first-century war. From his perspective, future conflicts must include an information element. He avers information asymmetrically lowers an adversary's combat potential and creates "a permanently operating front through the entire territory of an enemy state."[13] The ongoing Russian-Ukrainian conflict displays the practical application of his sentiments. When Russian forces entered the Crimean Peninsula on 2 March 2014, they preemptively shut down Crimea's telecommunications infrastructure, disabled major Ukrainian websites, and jammed the mobile phones of key Ukrainian officials.[14] Russian forces effectively isolated Crimea in the information environment, which contributed to setting the necessary conditions for the rapid physical attack.[15] While many factors contributed to Russia's ability to successfully annex Crimea, this example demonstrates how adversaries are leveraging the capabilities offered by information technology and meticulously integrating these capabilities in the planning

and execution of operations. Elevating information to a warfighting function enables the Army to exploit information capabilities to the degree that technology allows and that maintaining a competitive advantage requires.

The Adequate Integration of Information in Planning and Execution

The absence of information from the warfighting functions inhibits the complete and adequate integration of IO into planning and execution. In America's most recent conflicts, resource and technological overmatch against relatively unsophisticated enemies allowed the Army to sideline IO without perceived negative consequences. In future fights against peer adversaries, this approach is likely to produce devastating effects. Contemporary examples demonstrate the Army's challenges with IO integration. In a review of IO in "Information Operations in Operations Enduring Freedom and Iraqi Freedom – What Went Wrong?," Joseph Cox identified three factors inhibiting the effects of IO: (1) Army doctrine does not provide commanders adequate guidance for integrating IO, (2) intelligence doctrine and resourcing do not allow intelligence support to IO to be effective, and (3) the Army has not resourced itself to conduct IO effectively.[16]

Early IO against the Taliban and al-Qaida focused on the employment of kinetic engagements and "only later did commanders work to convince Afghans that attacks on Taliban fighters were not attacks on the Afghan populace."[17] Failure to adequately integrate IO into the planning with the early kinetic operations negatively impacted the U.S. military's ability to garner the local Afghan support required to secure long-term peace.[18] A 2012 RAND Corporation report on the use of information and psychological operations in Afghanistan stated, "The current disconnect between official IO doctrine and how it is practiced in the field is counterproductive" to effective and efficient operations.[19] Three years later, RAND Corporation published a follow-up perspective on the report and concluded, "It is evident that there is still a great deal of work that must be done to integrate and harmonize doctrine [with IO practice] to achieve the greatest results."[20] As noted in ADP 3-0 and ADP 5-0, warfighting functions are the mechanisms used to synchronize and integrate all available capabilities in an operational plan.[21] Without a warfighting function, the Army does not have the doctrinal means to sufficiently integrate information into operational planning and execution.

Beyond Physical: Expanding the Concept of War

The Army's narrow definition of tactical and operational conflict subverts attempts at strategic victory. In his seminal work, *The American Way of War: A History of United States Military Strategy and Policy*, Russell Weigley famously argues that with few exceptions, America's approach to war is aggressive, direct, and with an eye toward total annihilation.[22] Antulio J. Echevarria II argues this as proof that America only demonstrates a way of battle that has not yet matured into a complete and holistic way of war.[23] Although the American military touts the use of Clausewitzian principles, it seems the "American style of warfare failed to internalize Clausewitz's contention that war was the continuation of politics by other means."[24] The Army's failure to recognize the value of information further serves to support this point. The perception of war characterized by simply winning the physical battles, which overwhelmingly occupies the focus of the current warfighting functions, is not enough to win wars.

A Tool for "Gray Zone" Conflict

The Army's warfighting structure does not offer sufficient capabilities in the phases of conflict before and after the highly kinetic and lethal fight. "Gray zone conflict" and "hybrid warfare" are in-vogue terms frequently used to describe low-intensity conflicts or conflicts employing methods short of conventional war. Echevarria contends that this "new" form of war is, in fact, historically the norm and more common than the romanticized World War II style of fighting.[25] Failing to realize this phenomenon exposes America's unrealistic and self-limiting concept of war.[26] This style of warfare is also increasingly likely because it occurs below the North Atlantic Treaty Organization Article 5 threshold and below the level of violence necessary to prompt a United Nations Security Council resolution.[27] The near-exclusive orientation of the Army's warfighting functions toward lethal actions is an accurate reflection of this flawed concept.

This era of renewed great power competition necessitates a mechanism for employing nonlethal force. Adversaries seek to win battles below the threshold of America's narrow definition of war in order to score victory before the United States even realizes the conflict

has begun. The elevation of information to a warfighting function provides the Army with the practical flexibility and means to employ capabilities and address adversarial actions occurring below the threshold for lethal force. The Army must "account for more than just the use of kinetic military force during wartime, and it must accommodate more than just the goal of dominating an adversary through decisive operations."[28] The Army needs to develop its warfighting style to reflect the reality of war's political context as opposed to a struggle for domination of wills devoid of broader implications.[29] The information warfighting function would provide the capabilities to influence adversarial actions outside of lethality and would help to serve as a catalyst for the required institutional mindset change.

Evaluating Adversaries

Analysis of the Chinese People's Liberation Army (PLA) indicates an astute understanding of the asymmetric potential of information. Long before the information age and the advent of the internet, Mao Tse-tung worked to instill the notion of the military as a body to carry out the political will, not solely a physical fighting entity. In his 1929 resolution, titled "On Correcting Mistaken Ideas in the Party," Mao stated that members of the party who held a purely military view "think the task of the Red Army … is merely to fight. They do not understand that the Chinese Red Army is an armed body for carrying out the political tasks of the revolution … The Red Army fights not merely for the sake of fighting but in order to … help establish revolutionary political power."[30] Mao's expression also seems to closely follow Sun Tzu's famous maxim: "Supreme excellence consists in breaking the enemy's resistance without fighting."[31] This idea was further codified into Chinese military doctrine in 2003 when the Communist Party's Central Committee and Central Military Commission approved a new warfare concept for the PLA titled "three warfares." These are public opinion warfare (media), psychological warfare, and legal warfare.[32]

The Chinese information strategy focuses on using stratagems to build and maintain information superiority in order to compensate for its deficiencies in technology-based weapons.[33] According to a report to the U.S. Congress, the PLA views the United States as a militarily superior foe whose advantages can be overcome through strategy and information operations. The report, which cites *Unrestricted Warfare: China's Master Plan to Destroy America*, states, "The U.S. reliance on technology … creates a vulnerability that can be exploited, along with 'theoretical blind spots' and 'thought errors,' such as the absence of a comprehensive theory in DOD doctrine that combines all elements of information warfare."[34] These are exactly the sort of asymmetries Mao referred to nearly nine decades ago. The Army uses the warfighting functions to not only structure friendly planning and execution but also to assess the capabilities of the enemy. Failing to include information as a warfighting function hinders the Army's ability to comprehensively understand our adversaries' capabilities and mentality.

Embracing the Burdens of Change

Some may argue the addition of the information warfighting function is an unnecessary institutional burden. Making a change of this nature has complex implications across doctrine, organization, training, materiel, leadership and education, personnel, and facilities. Information is already an element of combat power, and Field Manual 3-13 and Army Techniques Publication 3-13.1, *The Conduct of Information Operations*, give specific guidance on applying and using information.[35] Therefore, the focus should be on better applying information as it currently exists in the Army's lexicon. However, based on the evolving technology and the adversarial capabilities, it is clear that the status quo is not adequate. In its current form, "many continue to skeptically view it [IO] as a marginal military activity or as a failing enterprise."[36] This mindset must change if the United States is to maintain supremacy on future battlefields. Military professionals have a responsibility to achieve an objective reality of war and adapt accordingly. Imagine if the U.S. military did not institute the Air Force after World War II due to institutional inconveniences. The burdens of change and inconvenience outweigh the consequences of strategic defeat.

Information Beyond the Joint Level

In September 2017, then Secretary of Defense James Mattis signed a memorandum elevating information to a warfighting function at the joint-force level.[37] Critics may argue against the idea of an information warfighting function at the service level because information is viewed as a strategic capability that belongs centralized at the Department of Defense. It is certainly useful for the joint force to integrate information into operational and strategic plans, and some of the decisions germane to IRCs belong at that level. However, as evident by the

An inflatable OH-58C Kiowa helicopter and inflatable fuel blivets simulate a forward arming and refueling point during a deception operation on 10 November 1990 carried out by the XVIII Airborne Corps Deception Cell in the Eastern Province of Saudi Arabia approximately forty-five kilometers northwest of An Nuariya. (Photo by Pfc. Randall R. Anderson, XVIII Airborne Corps)

examples above, information is already proving useful in tactical scenarios. Additionally, as technology continues to improve, the tactical solutions will continue to emerge. The information warfighting function provides the Army with a method to integrate these critical capabilities and help drive a change in the self-limiting centralization of IRCs when able.

The role of information in future conflicts is becoming exceedingly important given the explosive rise of information technology. Our adversaries are using information to achieve effects and secure their political objectives. Russian military sources even go so far as to claim the "role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force or weapons in their effectiveness."[38] While the elevation of information is not a panacea for all the Army's warfighting challenges, it provides a method to better integrate these rising technological advances and offers the flexibility to apply force in conflicts occurring below the appetite for lethality. The last eighteen years of conflict characterized by extreme technological overmatch lulled the American military into a sense of complacency and hubris, which precipitated the marginalization of information capabilities.[39] If the U.S. Army wants to maintain supremacy in this era of renewed great power competition, it must adapt to the challenges brought on by the changing character of war. ■

Notes

1. CrowdStrike Global Intelligence Team, "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," CrowdStrike, updated 23 March 2017, accessed 31 July 2019, https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/.
2. Ibid.
3. Ibid.

4. Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 5-1, accessed 3 October 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18010_ADP%203-0%20FINAL%20WEB.pdf.

5. Ibid.

6. ADP 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 31 July 2019), 4-5, accessed 3 October 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18323_ADP%205-0%20FINAL%20WEB.pdf.

7. Field Manual (FM) 13-3, *Information Operations* (Washington, DC: U.S. GPO, 6 December 2016), 1-2, accessed 31 July 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/FM%203-13%20FINAL%20WEB.pdf.

8. Ibid., 1-3.

9. ADP 3-0, *Operations*, 5-3–5-4.

10. "A Guide to Red Teaming: DCDC Guidance Note" (Shrivenham, UK: The Development, Concepts and Doctrine Centre, February 2010), lexicon-2, accessed 5 August 2019, https://www.act.nato.int/images/stories/events/2011/cde/rr_ukdcdc.pdf.

11. Sebastian Bay et al., *Responding to Cognitive Security Challenges* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, January 2019), 13–14, accessed 31 July 2019, https://www.stratcomcoe.org/responding-cognitive-security-challenges.

12. Joseph Dunford, "The Character of War and Strategic Landscape have Changed," *Joint Force Quarterly* 89 (2018): 2, accessed 5 August 2019, https://ufdc.ufl.edu/AA00061587/00089.

13. Valery Gerasimov, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows* (blog), 6 July 2014, accessed 31 July 2019, https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/.

14. Azhar Unwala and Shaheen Ghori, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *The Journal of the Military Cyber Professionals Association* 1, no. 1 (2015): 1, accessed 31 July 2019, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1001&context=mca.

15. *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: U.S. Army Special Operations Command, n.d.), 51, accessed 31 July 2019, https://permanent.access.gpo.gov/gpo107669/14-02984_LittleGreenMen-UNCLASS-hi-res.pdf.

16. Joseph L. Cox, *Information Operations in Operations Enduring Freedom and Iraqi Freedom - What Went Wrong?* (Fort Leavenworth, KS: United States Army Command and General Staff College, 2006), iii, accessed 31 July 2019, https://fas.org/irp/eprint/cox.pdf.

17. Walter E. Richter, "The Future of Information Operations," *Military Review* 89, no. 1 (January-February 2009): 106–7, accessed 31 July 2019, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20090228_art001.pdf.

18. Ibid., 107.

19. Arturo Muñoz, "U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001–2010" (Santa Monica, CA: RAND Corporation, 2012), xx, accessed 23 September 2019, https://www.rand.org/pubs/monographs/MG1060.html.

20. Arturo Muñoz and Erin Dick, "Information Operations: The Imperative of Doctrine Harmonization and Measures of Effectiveness (Santa Monica, CA: RAND Corporation, 2015), 3, accessed 23 September 2019, https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE128/RAND_PE128.pdf.

21. Ibid., 5-2; ADP 5-0, *The Operations Process*, 4-5.

22. Russell F. Weigley, *The American Way of War: A History of United States Military Strategy and Policy* (Bloomington, IN: Indiana University Press, 1973), xxii.

23. Antulio J. Echevarria II, *Toward an American Way of War* (Carlisle, PA: Strategic Studies Institute, 2004), 1, accessed 31 July 2019, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=374.

24. Antulio J. Echevarria II, *Reconsidering the American Way of War: US Military Practice from the Revolution to Afghanistan* (Washington, DC: Georgetown University Press, May 2014), 46.

25. Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Carlisle, PA: Strategic Studies Institute, April 2016), xi, accessed 31 July 2019, https://ssi.armywarcollege.edu/pubs/display.cfm?pubID=1318.

26. Ibid., 40.

27. Charles T. Cleveland, Shaw S. Pick, and Stuart L. Farris, "Shedding Light on the Gray Zone: A New Approach to Human-Centric Warfare," Association of the United States Army, 17 August 2015, accessed 31 July 2019, https://www.ausa.org/articles/shedding-light-gray-zone-new-approach-human-centric-warfare.

28. Ibid., xii.

29. Echevarria, *Operating in the Gray Zone*, 41.

30. Mao Tse-tung, "On Correcting Mistaken Ideas in the Party," in *Selected Works of Mao Tse-tung*, vol. 1 (Beijing: Foreign Languages Press, 1965), accessed 31 July 2019, https://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_5.htm#s1.

31. Sun Tzu, *The Art of War*, trans. Lionel Giles, Project Gutenberg, updated 14 January 2012, accessed 24 September 2019, http://brainab.com/site_images/files_books/war_sun.pdf.

32. Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare* (Carlisle, PA: Strategic Studies Institute, 2014), 29, accessed 31 July 2019, https://publications.armywarcollege.edu/pubs/2263.pdf.

33. Catherine A. Theohary, *Information Warfare: Issues for Congress*, Congressional Research Service (CRS) Report No. R45142 (Washington, DC: CRS, 5 March 2018), 11, accessed 31 July 2019, https://fas.org/sgp/crs/natsec/R45142.pdf.

34. Ibid.

35. FM 3-13, *Information Operations*, iv; Army Techniques Publication (ATP) 3-13.1, *The Conduct of Information Operations* (Washington, DC: U.S. GPO, 4 October 2018), v, accessed 31 July 2019, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN13138_ATP%203-13x1%20FINAL%20Web%201.pdf.

36. Scott Thompson and Christopher Paul, "Paradigm Change: Operational Art and the Information Joint Function," *Joint Force Quarterly* 89 (2nd Quarter, 2018): 11.

37. Secretary of Defense Memorandum, "Information as a Joint Function," 15 September 2017, accessed 31 July 2019, https://www.rmda.army.mil/records-management/docs/SECDEF-Endorsement_Information_Joint%20Function_Clean.pdf.

38. Ben Sohl, "Influence Campaigns and the Future of International Competition," The Strategy Bridge, 12 September 2017, accessed 31 July 2019, https://thestrategybridge.org/the-bridge/2017/9/12/influence-campaigns-and-the-future-of-international-competition?rq=Gerasimov.

39. Nick Brunetti-Lihach, "Information Warfare Past, Present, and Future," The Strategy Bridge, 14 November 2018, accessed 31 July 2019, https://thestrategybridge.org/the-bridge/2018/11/14/information-warfare-past-present-and-future.

Next page: Chinese Defense Minister Wei Fenghe salutes 21 October 2019 after delivering his opening speech for the Xiangshan Forum, a gathering of the region's security officials, in Beijing. Wei issued a stinging rebuke of the United States at the defense forum, saying China was not fazed by sanctions, pressure, and military intimidation. (Photo by Andy Wong, Associated Press)