Multi-Domain Information Operations and the Brigade Combat Team

Lessons from Cyber Blitz 2018

Maj. John P. Rodriguez, U.S. Army

Multi-domain operations is the Army's new future fighting concept, but what does this mean for the brigade combat team (BCT)? Cyber Blitz 2018 attempted to answer this question with a focus on identifying how a BCT integrates cyberspace operations, electronic warfare (EW), intelligence, and information operations (IO) to conduct operations across multiple domains, the electromagnetic spectrum (EMS), and the information environment against a regional peer.[1] Cyber Blitz demonstrated

the promise of BCT-level multi-domain operations. However, it also showed that the Army must ensure the proper doctrine and staff organization to reap the full benefit of multi-domain operations. The perceived divide between IO and cyber-electromagnetic activities (CEMA) is a major unresolved challenge. Many participants did not embrace the doctrinal view that IO functions as the integrator and synchronizer of information-related capabilities (IRCs), including CEMA, to affect an adversary's decision-making. A narrow focus on CEMA and a limited view of IO could increase stovepipes and prevent synchronized multi-domain operations. One solution to make BCT multi-domain operations more effective is to restore the IO officer position on the brigade staff and place more emphasis on the role of IO as an integrator at brigade level.

Multi-Domain Operations

The U.S. Army in Multi-Domain Operations 2028, released on 6 December 2018, describes the Army's concept for how to win future wars against near-peer competitors.[2] According to the "Summary of the 2018 National Defense Strategy," the joint force faces a more complex security environment "defined by rapid technological change, [and] challenges from adversaries in every operating domain."[3] Gen. Joseph Dunford, the chairman of the Joint Chiefs of Staff, wrote that "the U.S. military's long-held competitive advantage has eroded" as adversaries have adapted to counter U.S. capabilities.[4] The central idea behind multi-domain operations is that Army formations, as part of the joint force, must be able to fight across all domains (land, maritime, air, space, and cyberspace), the EMS, and the information environment. Due to resource constraints and more dangerous adversaries, Army formations must maximize every capability, synchronize operations across domains, and mass at the decisive point to win future battles.

Previous page: A soldier participates in Cyber Blitz 2018 on 21 September 2018 at Joint Base McGuire-Dix-Lakehurst, New Jersey. The Cyber Blitz exercise helped inform the Army on how to employ evolving cyber-electromagnetic activities and information operations during multi-domain operations. The series of experiments examined how the integration of cyberspace, electronic warfare, intelligence, space, and information operations could help a brigade combat team gain and maintain the advantage against a regional peer adversary in a decisive action training environment. (Photo by Steven Stover)

The Army must field formations at various echelons capable of operating across multiple domains. The Army cannot allow multi-domain convergence to occur only at the corps level or above. General purpose Army maneuver units must also be able to fight in a multi-domain fashion to win against near-peer threats. Even if higher echelons retain control of some national-level assets, select multi-domain capabilities must be pushed downward. More importantly, units at the tactical edge must be thinking in multi-domain terms so they can appropriately plan for outside support just as BCTs incorporate air assets into planning.

Cyber Blitz 2018

Through Cyber Blitz, which is a series of experiments co-led by the Communications-Electronics Research, Development and Engineering Center (CERDEC) and the Cyber Center of Excellence, the Army is bringing multi-domain operations to the tactical level. The experiments inform how the Army can employ CEMA and IO across the full spectrum of Army doctrine, organization, training, material, leadership and education, personnel, facilities, and policy.[5] CERDEC conducted Cyber Blitz 2018 at Fort Dix, New Jersey, over three weeks in September 2018.

Cyber Blitz adapted the decisive action training environment used in other Army training environments. CERDEC modified the scenario to increase adversary cyberspace and EW capabilities as well as to adapt the scenario to Fort Dix terrain. The scenario was set in 2025 to test emerging technologies, some still in research and development, and to experiment with force design updates and delegation of authorities. The experiment occurred in the friendly nation of Atropia, which was suffering from a separatist insurgency. Ariana, a neighboring country, supported the separatists and threatened to intervene with conventional forces. Most participants were familiar with the decisive action training environment scenario, which allowed them to focus on the CEMA and IO aspects of the scenario during Cyber Blitz.

The 3rd Infantry Brigade (Patriot Brigade) Combat Team of the 10th Mountain Division provided the core of the forces for Cyber Blitz. The brigade formed an organic EW platoon by consolidating EW personnel from throughout the brigade to test a force design update. Additional personnel attached to the brigade rounded out the signal staff and the EW

platoon. An IO officer and a cyberspace planner also augmented the brigade staff.

The primary external support to the brigade was the expeditionary cyber team (ECT), which contained both offensive cyberspace operations (OCO) and defensive cyberspace operations personnel as well as an IO planner. The ECT had the capability to conduct remote operations and close target reconnaissance. The division retained operational control of the ECT during the experiment. However, the brigade was able to request cyberspace effects from the ECT through the division. The ECT conducted multiple missions for both the division and the brigade throughout Cyber Blitz.

The experiment almost entirely simulated maneuver forces while primarily conducting CEMA activities live with supplemental simulations. The ECT conducted cyberspace operations live on networks simulating the global internet and the brigade Secret Internet Protocol Router Network. CERDEC emplaced a range of emitters simulating enemy, friendly, and neutral emissions on various Fort Dix ranges. This allowed the EW teams to detect, characterize, geolocate, and jam a variety of signals.

The brigade's mission was to secure the area of operations (AO) and defeat enemy conventional forces to protect an adjacent unit AO.[6] The brigade's scheme of maneuver began with an air assault to secure an airfield and was followed by the buildup of combat power via air landing. After this, the brigade planned to secure key infrastructure in the sector and establish a defense.

The experiment planners dictated the scheme of maneuver, and the staff did not have to conduct detailed planning for the movements of the maneuver battalions. This simplified the task facing the brigade staff and freed them to focus on integrating CEMA into their maneuver plan. The brigade also planned to defend against enemy multi-domain operations. The brigade staff conducted an abbreviated military decision-making process during the first week of Cyber Blitz. The deputy brigade commander directed the staff to include CEMA and IO to the maximum extent possible.

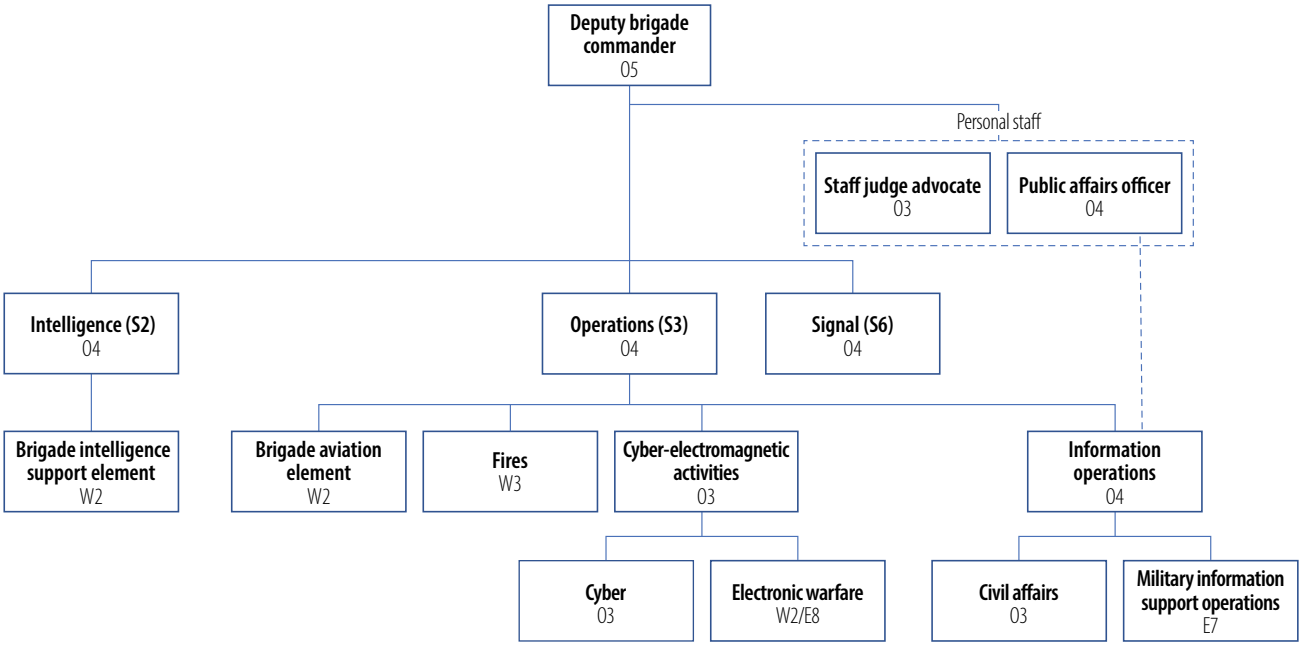
The brigade possessed multiple IRCs, but the organization of the staff split the IRCs between various sections (see figure, page 36). The brigade EW officer, a captain, served as the brigade's CEMA chief and an EW warrant officer and master sergeant supported her. The cyberspace planner attached to the brigade nominally worked for the CEMA chief. The attached IO major led a separate IO section including a civil affairs (CA) captain and a psychological operations (PSYOP) sergeant first class, who respectively planned operations for the CA and PSYOP elements notionally attached to the brigade. The brigade public affairs officer was also part of the IO section for all practical purposes. Additionally, the IO section assumed responsibility for deception and operational security (OPSEC) planning.

Dividing IRCs into two separate sections made integration more difficult. The brigade treated the IO section and CEMA section as separate but equal entities. This meant CEMA and IO equities only formally converged at the brigade operations officer (S-3), creating a situation ripe for fragmented and disjointed planning. Therefore, the IO officer worked through the S-3 to develop overarching IO concepts of support to nest CEMA efforts with other IRCs. Fortunately for the S-3, the nature of Cyber Blitz, with its dictated scheme of maneuver, allowed him the time to focus on incorporating CEMA and other IRCs into the plan. The IO officer was also able to exert influence over the CEMA section due to his or her rank and experience despite having no formal authority over the section.

Information Operations at Cyber Blitz

The brigade successfully integrated and synchronized IRCs to support its scheme of maneuver throughout Cyber Blitz. Beyond individually supporting the scheme of maneuver, the brigade's IRCs often worked together in a mutually supportive manner achieving synergy. During an early phase of the operation, the IRCs focused on supporting an air assault. Later, when the enemy launched a powerful attack with both conventional and insurgent forces, a preplanned multi-IRC response delayed the attack and added friction into enemy mission command networks.

Maj. John P. Rodriguez, U.S. Army, is an information operations officer in the Maryland Army National Guard assigned to Plans and Policy Division, Intelligence Directorate, the Joint Staff. He holds a BA from Mount Saint Mary's University and an MA from Georgetown University. He served as the director of information operations for Combined Joint Task Force–Horn of Africa from 2017 to 2018 and participated in Cyber Blitz 2018.



(Figure by author)

Figure. Cyber Blitz Brigade Headquarters Organization

Initially, IO focused on supporting the brigade's decisive operation, an air assault to seize the airfield at Objective Desoto, located in the eastern portion of the AO. The deputy brigade commander sought to prevent the enemy from massing combat power against the air assault since it would take multiple lifts to get the whole assault force on the objective. The IO officer used OPSEC as the construct to synchronize the IRCs. The overarching concept was to protect the timing and location of the air assault. Ideally, this would cause the enemy to misallocate forces, but at a minimum, the goal was to disrupt enemy decision-making to prevent the enemy from massing combat power against the air assault.

The IO concept had two overlapping phases. The first phase was a feint to make the adversary believe the main friendly attack was occurring in the western portion of the AO. This required multiple mutually reinforcing elements. An airfield was located just outside the brigade's western boundary, which provided a realistic objective for the feint. There were also suitable landing zones in the vicinity of the false objective. EW, PSYOP, and OCO forces supported the feint. In addition to disrupting enemy communications, OCO delivered military information support operations (MISO) messages. This allowed PSYOP forces to influence broader target audiences and reinforce MISO messages delivered with other means. The feint did not give the enemy a windfall; instead, it presented the enemy with many different pieces that pointed to the decoy landing zone. The PSYOP planner also attempted to use EW platforms to deliver MISO messages, which was initially unsuccessful. In a later phase of the experiment, EW and PSYOP overcame these hurdles and did disseminate MISO messages with EW capabilities. EW also provided effects in the EMS to produce a signature consistent with an air assault and to degrade enemy collection assets and communication links that could discover or report on the feint.

The second phase was direct support of the actual air assault. Both EW and OCO attempted to disrupt enemy command and control on the objective and along the air corridor. The effects were overlapping to provide redundancy. This proved fortunate because some capabilities were unable to achieve the desired effects. However, staff swiftly communicated the setback, and other assets achieved the desired effects. The results were seamless for the assault force.

The enemy began a multi-domain attack during a later phase of the operation that stressed the brigade's

defenses. The enemy initiated insurgent attacks and popular uprisings as an enemy motorized rifle brigade began advancing. Enemy unmanned aerial systems and electronic attack platforms supported the advance and degraded friendly mission command. The enemy also attempted to disrupt critical infrastructure with OCO. This presented the brigade with multiple dilemmas. The situation became dire when enemy OCO penetrated the brigade network as enemy forces began to pressure the brigade's screen line.

The brigade executed a preplanned IO counterattack to delay the enemy advance. This allowed the signal staff to reestablish the network and the infantry battalions to finish preparing their defensive positions. The counterattack began with OCO against enemy mission command networks. OCO corrupted the integrity of the enemy systems and delivered MISO content. This induced friction into enemy decision-making, and the confusion caused the enemy to make mistakes. PSYOP elements exploited the enemy blunders with additional MISO messages to degrade cohesion and increase rifts between enemy conventional and insurgent forces. OCO continued attacking the mission command network and delivering MISO messages for the rest of battle.

Information Operations Lessons from Cyber Blitz 2018: The Good

The two most important lessons from Cyber Blitz 2018 are the importance of information operations to conduct multi-domain operations at the BCT level and how an antiquated view of IO impedes unified multi-domain operations. The brigade's operations were much more effective because the staff integrated and synchronized all available IRCs to affect the enemy's decision-making. The BCT faced a multi-domain threat throughout Cyber Blitz and responded in a multi-domain manner. The brigade achieved speed because it could plan and execute operations without always relying on outside support. However, this success occurred in spite of the brigade's staff organization and the framing of IO's role in the experiment.

During the air assault, the IO concept of support served to provide unity of effort across the IRCs allowing the brigade to mass effects. The IO approach ensured the IRCs were mutually supporting and identified opportunities for IRCs to collaborate, such as OCO and EW delivery of MISO messages. This presented the enemy with a more complex challenge and prevented the piecemeal employment of IRCs. The feint presented observables in multiple ways, including the EMS and social media, which targeted various conduits to enemy decision-makers. The feint was more likely to convince the decision-makers because it used diverse observables.

The brigade's counterattack created more friction for the enemy because it combined OCO and PSYOP. A purely OCO attack on enemy command networks would have had limited effects because it would have been a singular execution. Instead, the brigade's actions continued for the remainder of the fight as OCO continued delivering MISO messages. Additional MISO executions, not exclusively delivered by OCO, extended the duration of the effects and exploited every opportunity provided by enemy missteps. Furthermore, this counterattack was critical because it occurred at a decisive point in the battle. The brigade identified the enemy mission command network as a high payoff target during mission analysis and the ECT gained access early in the battle. The deputy brigade commander held this capability in reserve so he could use it for maximum effect. His patience carried risks because the ECT could have lost access in the interim, but in this case, it paid off.

The Bad

The biggest obstacle to effective IO during Cyber Blitz was that many participants and observers did not embrace the doctrinal definition of IO. Joint Publication 3-13, *Information Operations*, defines information operations as "the integrated employment, during military operations, of information-related capabilities 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] Many did not view IO as an overarching function that integrated all IRCs including CEMA. Instead, they treated IO as something separate and distinct from CEMA. While the new multi-domain operations concept advocates changing IO to information environment operations, it still emphasizes IO/information environment operations' role of synchronizing IRCs to achieve effects.[8]

The framing of the experiment reinforced the separation between CEMA and IO. The problem statement for the experiment was "how does an IBCT with external support in 2025 integrate cyberspace, electronic warfare, intelligence, space, and information operations to gain

and maintain the advantage in multi-domain operations against a regional peer?"[9] The brigade leadership had limited IO or CEMA experience, so this phrasing shaped how they approached their task. Their initial inclination was to ask in turn what each cyberspace operations, EW, and IO could do to support a phase of the operation. This approach increases the risk of disjointed approaches that do not mass effects on the enemy.

Many participants seemed to believe IO focuses solely on themes and messages. This leads to pushing IO to concentrate on social media and publicly available information, which, while important, are not the only spaces IO should operate in. The old concept of inform-and-influence activities, which specifically mentioned themes and messages in its definition, may explain this belief.[10] This is a very human-centric approach drawing lessons from the last seventeen years of counterinsurgency operations. But IO must also focus on enemy mission command networks as the joint force focuses more on great power competition.

A reduced view of IO's role means the onus to integrate the IRCs falls on the S-3 if the IO officer in not empowered to do so. In Cyber Blitz, the organization of the staff meant the S-3 was officially fulfilling the IO officer's primary duty of integrating and synchronizing the IRCs. If the experiment had not dictated the scheme of maneuver, the requirement to coordinate both traditional fire and maneuver and IRCs likely would have overwhelmed the S-3. This would degrade synergy and result in diminished effects on the enemy. However, even if Army leaders embrace an expansive role for the IO function, the S-3 will still be the integrator since the Army no longer authorizes an IO officer on the brigade staff.

The Way Ahead

The brigade's multi-domain operations would have been much less successful without the attached IO officer. Even though in Cyber Blitz the S-3 had more bandwidth than usual to focus on integrating IRCs, this was no substitute for a trained IO officer. The IO officer's perspective on IO led him to fight to overcome the stovepipes between the IRCs. The cyberspace and EW planners were incredibly busy and focused on the detailed planning of their individual efforts. Successful EW and OCO require this concentration but also expecting IRC planners to develop a holistic IO plan to support the scheme of maneuver is impractical. However, the brigade would have missed many opportunities to multiply the effect of operations without a unified concept. The IO officer also ensured the incorporation of OPSEC and deception into planning. These are critical IRCs and can be great approaches to frame an integrated IO plan.

The Army should consider putting an IO officer back in the BCT. As brigades gain more IRCs and cyberspace operations increase supporting echelons below corps, the importance of an IO planner in the BCT will grow. Providing an OPSEC- and deception-trained IO officer will also ensure the routine incorporation of OPSEC and deception into operations. A BCT that does not plan for multi-domain OPSEC will increasingly be vulnerable against near-peer adversaries with advanced collection capabilities.

A division IO officer, or one in an ECT, is no substitute for an IO officer within the brigade. It is ideal to incorporate IO into military decision-making processes from the start and the best way is an IO officer on staff. A division IO officer will likely only have an opportunity to inject ideas late in the decision-making process when path dependency may have already set in. Similarly, the IO planner in the ECT was ineffective at influencing BCT plans during Cyber Blitz. Mission command relies upon trust to speed decision-making and ensure we seize and retain the initiative. Unfortunately, it is very difficult for brigade leadership to trust a planner outside their organization, especially if they are using capabilities new to brigade leadership.

An IO officer should lead a consolidated information warfare section within the S-3. The information warfare section could plan cyberspace operations, EW, MISO, OPSEC, and deception. Instead of a discreet CEMA section, an IO section consolidates IRC planners under one field grade officer who reports directly to the S-3. The brigade public affairs officer is an exception and should remain on the personal staff to maintain credibility with the press and public. Combined Joint Task Force–Horn of Africa successfully used a similar staff organization by having all primary IRCs, including CEMA, fall under the IO directorate except CA and public affairs. This greatly increased the unity of effort.

Regularly attaching Army Reserve and National Guard IO officers to BCTs is another solution if manpower constraints prevent adding an active duty IO officer. Reservists could supplement BCTs during deployments. This would mitigate the tendency to

Maj. Alex J. Duffy, 3rd Brigade Combat Team, 10th Mountain Division operations officer (*right*), and Capt. Jacob M. Allen, assistant operations officer, use a map overlaid with operational graphics to back-up digital mission command systems and provide redundancy 17 September 2018 during Cyber Blitz 2018 at Joint Base McGuire-Dix-Lakehurst, New Jersey. This alternate method to battle track temporarily became the primary method when an enemy cyberattack knocked the digital systems off-line. (Photo courtesy of U.S. Army Communications-Electronics Research, Development and Engineering Center [CERDEC])

misuse IO planners and saddle them with additional duties unrelated to IO in garrison. Ideally, the reservists would also support the BCTs at combat readiness center rotations in addition to deployments so units could train as they would fight. However, it could place a strain on reservists to support month-long training center rotations habitually while already attending many schools and supporting numerous exercises in addition to regular deployments. Relying on reservists to fill this gap could further stress the force and be impractical.

Conclusion

The Army must embrace IO's integration function to institutionalize the Patriot Brigade's success at Cyber Blitz 2018. Cyber Blitz demonstrated that, while new equipment and organizations are necessary to enable BCT multi-domain operations, without the proper doctrine and staff organization, these capabilities will not be used to their full potential. It also showed how an IO officer on the brigade staff can drastically improve the brigade's effectiveness. The Army cannot accept piecemeal employment of IRCs and a divide between CEMA and IO. The U.S. military "has no preordained right to victory," and we must relentlessly improve our capabilities to win the multi-domain battles of tomorrow.[11] ■

FUTURE WARFARE WRITING PROGRAM

Call for Speculative Essays and Short Works of Fiction

Military Review calls for short works of fiction for inclusion in the Army University Press Future Warfare Writing Program (FWWP) for 2019. The purpose of this program is to solicit serious contemplation of possible future scenarios through the medium of fiction in order to anticipate future security requirements. As a result, well-written works of fiction in short-story format with new and fresh insights into the character of possible future martial conflicts and domestic unrest are of special interest. Detailed guidance related to the character of such fiction together with submission guidelines can be found at https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/Future-Warfare-Writing-Program-Submission-Guidelines/. To read previously published FWWP submissions, visit https://www.armyupress.army.mil/Special-Topics/Future-Warfare-Writing-Program/.

Army University Press

Notes

1. Cyber Blitz Team, "Cyber Blitz 2018 (CB18) Distinguished Visitor Day" (PowerPoint presentation, Fort Dix, NJ, 26–27 September 2018).

2. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Washington, DC: U.S. Government Publishing Office [GPO], 2018), accessed 21 March 2019, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

3. Office of the Secretary of Defense (OSD), "Summary of the 2018 National Defense Strategy of the United States of America" (Washington, DC: Department of Defense, 2018), accessed 21 March 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

4. Joseph Dunford, "Gen. Dunford: The Character of War & Strategic Landscape Have Changed," DoDLive, 30 April 2018, accessed 21 March 2019, http://www.dodlive.mil/2018/04/30/dunford-the-character-of-war-strategic-landscape-have-changed/.

5. Steven Stover, "Cyber Blitz 2018 Gives ARCYBER Opportunity to Test New Concepts, Capabilities and Techniques," Defense Visual Information Distribution Service, 3 October 2018, accessed 21 March 2019, https://www.dvidshub.net/news/295282/cyber-blitz-2018-gives-arcyber-opportunity-test-new-concepts-capabilities-and-techniques.

6. Cyber Blitz Team, "Cyber Blitz 2018 (CB18) Distinguished Visitor Day."

7. Joint Publication 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 27 November 2012).

8. TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, GL-5. Information environment operations is defined as "integrated employment of information related capabilities (IRC) in concert with other lines of operation to influence, deceive, disrupt, corrupt, or usurp the decision-making of enemies and adversaries while protecting our own; to influence enemy formations and populations to reduce their will to fight; and influence friendly and neutral populations to enable friendly operations."

9. Cyber Blitz Team, "Cyber Blitz 2018 (CB18) Distinguished Visitor Day."

10. Field Manual 3-13, *Inform and Influence Activities* (Washington, DC: U.S. Government Printing Office, 2013 [obsolete]). Revised to Field Manual 3-13, *Information Operations* (Washington, DC: U.S. GPO, 2016).

11. OSD, "Summary of the 2018 National Defense Strategy."