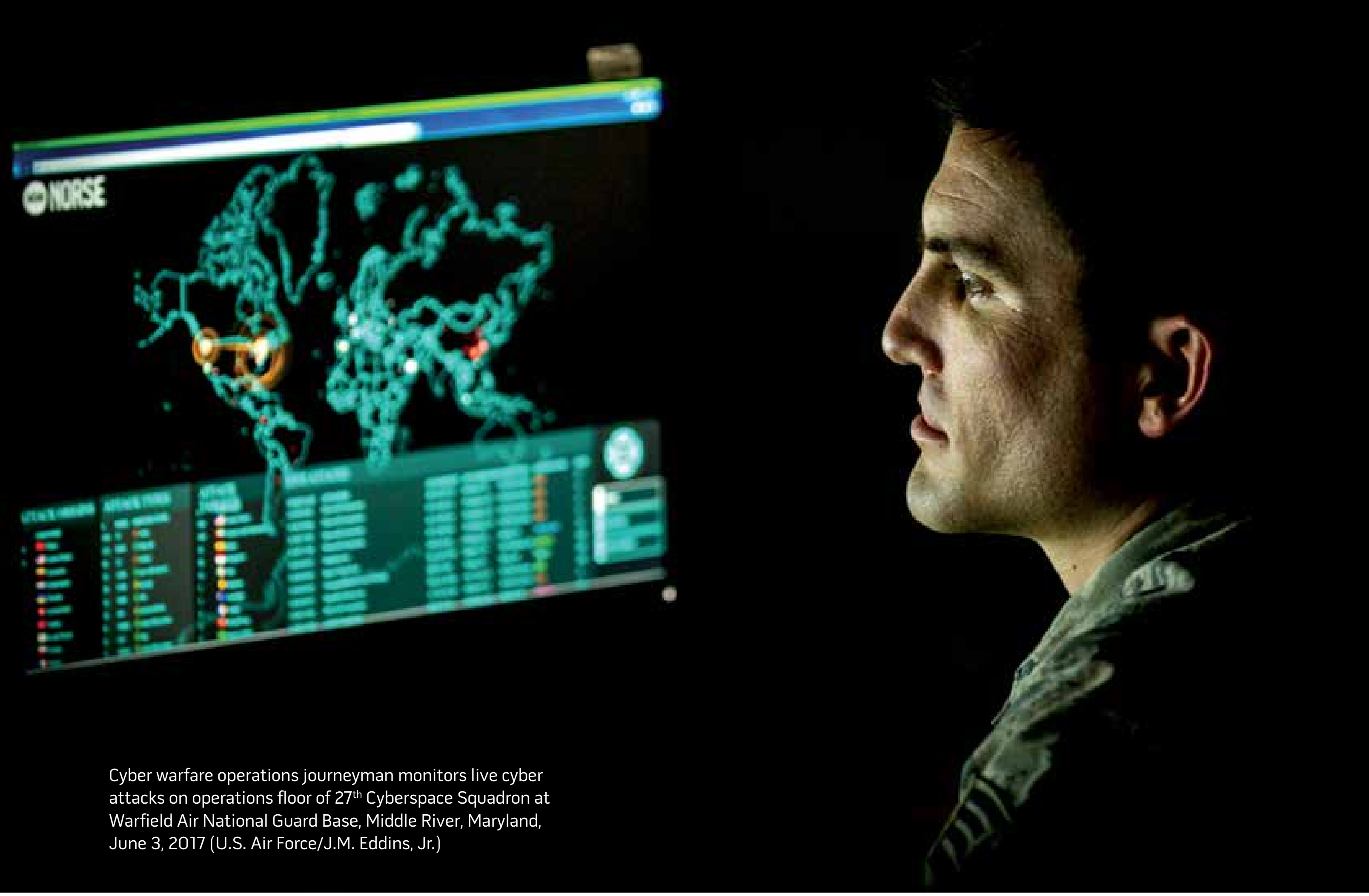

Cyber warfare operations journeyman monitors live cyber attacks on operations floor of 27th Cyberspace Squadron at Warfield Air National Guard Base, Middle River, Maryland, June 3, 2017 (U.S. Air Force/J.M. Eddins, Jr.)

A Smarter Approach to Cyber Attack Authorities

By Michael P. Carvelli

The highest levels of national power hold approval authority for any cyberspace operation that goes outside of a Department of Defense (DOD) network. An operational commander, who wants to conduct cyber attacks, submits a request seeking Presidential or Secretary of Defense approval.[1] If approved, the Chairman of the Joint Chiefs of Staff issues the authorization to U.S. Strategic Command, which then delegates execution to the commander of U.S. Cyber Command.[2] This process is inefficient, cumbersome, and needlessly complex. Operational commanders certainly shy away from cyber attacks because the authority to conduct them is restricted to national and strategic levels. The United States should delegate cyber attack authority to operational commanders, but it should impose restrictions on the authority based on the attack's effects. To be sure, understanding the full implications of any attack is never absolute, but this caution in this instance needs to be balanced against the significant advantages conferred by attacking effectively first in cyberspace. A system of nationally preapproved cyber attacks would likely ensure that commanders have access to a menu of appropriate attacks while balancing concerns of the national leadership.

This article seeks to illustrate how restricted cyber attack authority enables

Major Michael P. Carvelli, USA, is a Joint Engineer Planner at Headquarters U.S. Forces–Afghanistan.

Soldier conducts cyberspace operations while supporting 2nd Armored Brigade Combat Team, 1st Infantry Division, during Danger Focus exercise at Fort Riley, Kansas, February 2017 (U.S. Army/Alvaro Luna)

operational commanders to attack effectively while at the same time mitigate unintended consequences. It provides recommendations for the restriction of cyber attack authority. In the last few years, several defense professionals argued for pushing cyber attack authority to the operational level.[3] This article thus explains how the delegation of cyber attack authority could balance the advantages and risks. By incorporating some limitations, it would be possible to ensure that operational commanders could safely employ cyber attacks against an adversary, which would minimize the risk of unintended consequences.

Cyberspace is the newest domain that DOD operates in.[4] It consists of three layers: physical, logical, and cyber persona.[5] The physical layer is composed of the locations in land, sea, air, and space where elements of the network reside; the hardware, software, systems software, and infrastructure (wired, wireless, cabled links, satellite, and optical) that support the network; and the connectors (wires, cables, radio frequencies, routers, switches, servers, and computers). The logical layer consists of how the physical network components relate to each other (that is, multiple servers host a Web site, which is accessed through a single URL). The cyber persona layer is the most abstract because it uses the rules of the logical layer to develop a digital representation of an individual or entity. These three layers combine to form networks that, when aggregated, form the cyberspace domain. Cyberspace is complicated and it is difficult to employ military force in it precisely because the domain is constructed of physical and nonphysical components.[6] Moreover, the nature of the cyber domain is one where small changes or disruptions occur in unpredictable ways.[7] The decision to execute a cyber attack should be limited due to the complexity of cyberspace and the risks confronted when releasing a cyber weapon.

Recent Adversary Activities

Yet the United States faces adversaries who have already shown their ability to employ cyber attack capabilities and act without regard for the proliferation of unintended effects. Over the past two decades, America's adversaries have demonstrated increasing skill, speed, and agility in their use of cyber attacks.

In 1999, following the accidental bombing of the Chinese embassy in Belgrade, Chinese hackers targeted U.S. Government Web sites, resulting in a White House–directed shut down of its official site.[8] This attack showed the ability of adversaries to inflict damage through cyber attacks on U.S. Government systems.

In the Russo-Georgian War of 2008, Russia used cyber attacks to disable the Georgian leadership's communications network prior to the movement of Russian forces into Abkhazia and South Ossetia.[9] This cyber attack shut down much of the Georgian government's communication inside Georgia and to the outside world, as well as created fear and discontent within the Georgian population. In addition to Russian cyber attacks in a conventional conflict, the Russian Federal Security Service coordinated an attack with private software firms and criminal hackers targeting Ukraine's power grid and financial system in the ongoing Russia-Ukraine conflict.[10] This hybrid attack, in conjunction with the conventional attack on Georgia, shows Russia's willingness to use cyber attacks in war and in conflicts short of war. The so-called Islamic State conducted a cyber attack in 2015 when the group hacked into the U.S. Central Command Twitter account and posted an image of a masked militant.[11] This attack displayed the ability of nonstate actors to attack the United States and achieve strategic effects in cyberspace. General James Mattis, then commander of U.S. Central Command, stated, "Our enemies operate within cyberspace . . . to plan, coordinate, recruit, train, equip, execute, and garner support for operations against the [United States], its allies, and interests."[12] Clearly, state and nonstate adversaries possess the capabilities to degrade and disrupt U.S. domestic and foreign military and nonmilitary operations, so it is time for the national leadership to give operational commanders the authorities they need in this new environment.

There are, of course, risks in granting operational commanders blanket cyber attack authority. Networks consist of physical (routers, switches, cables) and nonphysical (software, operating systems) elements that constantly and rapidly change. Likewise, obtaining full understanding of the second- and third-order effects of a cyber attack prior to execution is difficult, and joint task forces may not be able to determine fully the range of reactions that could occur.

Perhaps the most discussed instance of unintended consequences was Operation *Olympic Games*, more commonly known as the Stuxnet worm. The worm's designers intended to disable covertly Iranian centrifuges; however, it created irreversible damage to more than its intended target.[13] The worm spread and replicated itself globally creating irreversible damage to industrial control systems along the way. Although the United States and Israel allegedly created the weapon together with some of their best cyber teams, its effects were not fully known prior to its release.[14] The nature of the cyber domain—constantly changing in the physical, logical, and cyber persona layers—prevents fully understanding how a cyber attack will spread. Stuxnet is an example of a national-level cyber attack that authorities and designers resourced and built to create a specific effect, yet it unintentionally proliferated.

While Stuxnet offers an important cautionary lesson, it should not end the debate. Better balanced authorities could address the legitimate concerns of policymakers and the needs of the U.S. military. Limited cyber attack authority ensures that operational commanders can achieve operational objectives and account for the lack of complete knowledge of a cyber weapon's effects. Cyber attacks allow them to create positions of advantage to hasten the achievement of operational objectives. Commanders need the authority to employ cyber attacks in a constrained manner, even though they cannot be aware of every possible effect. The Stuxnet virus, designed with reversible effects, would have created the intended damage to Iranian centrifuges and left those affected with a way to prevent the virus's effects from creating further damage. When delegating cyber attack authority to operational commanders, they need to apply this lesson: account for unpredictable effects.

Design

Designing a cyber attack to create reversible effects is the best method to limit attack authority for operational commanders. Creating a cyber attack with reversible effects is possible. One example, a denial-of-service attack, floods a Web site with more traffic than it can handle, resulting in deterioration or temporary failure. When the attacker stops the deluge of Web traffic, he reverses the effects, resulting in normal operation.

Reversible cyber weapons offer considerable advantages over traditional kinetic weapons. Providing others (adversaries, allies, corporations, or the U.S. Government) the ability to reverse the damage allows them to mitigate a cyber attack's effects when these effects are unintended. Restricting an operational commander's authority to reversible damage ensures that if the cyber attack's effects reach catastrophic levels (for example, nuclear weapons command and control, national infrastructure), then the adversary could restore the system to the previous state. Limited cyber attack authority based on reversibility enables a commander to mitigate the cyber attack's unknowable propagation effects while maintaining his ability to attack effectively first. Operational commanders' authority, limited to reversible effects, allows any unintended consequences caused by the attack to change back to the status quo ante.

The current authorities' structure pushes commanders toward a bias in favor of using kinetic weapons due to the withholding of cyber attack authority at the highest levels of the U.S. Government. The following scenario demonstrates the methodology of approval for both weapon types.[15] Using an aerial-delivered munition to destroy a building or releasing a computer virus on a router can create the same desired effect. To attack the router, the commander requests approval from the President or Secretary of Defense. However, the operational commander has the vested authority to bomb the building. Additionally, the kinetic attack approval process is comparatively short due to several factors: "comfort" with traditional munitions, understanding of collateral damage, and standard operating processes. By contrast, the lack of cyber weapon understanding and longer approval time entice commanders to preselect the building. Because the operational commander has the authority to approve the bombing, approval takes only minutes, whereas the time to approve the cyber attack can take from hours to days. Lieutenant General Edward Cardon, the former head of U.S. Army Cyber Command, reinforced this notion when he stated, "it should not be harder to use cyber than it is to use kinetic to accomplish your goal. Right now, it is in some cases."[16] Delegating limited cyber attack authority eliminates this selection bias and encourages commanders to use cyber weapons because they possess the authority to approve both cyber and kinetic attacks. If some sort of limited authority were delegated, then operational commanders could make an equally informed choice between the bomb and virus. Delegation of authority creates parity between the building and router, allowing the commander to evaluate the advantages and disadvantages inherent in each. This creates an environment in which operational commanders do not continually chose kinetic weapons over cyber weapons.

Attacking an adversary first within clearly defined limited cyber attack authority enables an operational commander to fight from a position of advantage without creating unacceptable risk. If designers were to create only reversible effects in a cyber attack, the operational commander would attack the adversary first, thus reducing the possibility of damage that his subordinates cannot change. Creating reversible cyber weapon effects lowers overall operational residual risk. Predicting how a computer virus will outbreak is extremely difficult due to the human nature of the attack.[17] Humans create the cyber weapon and any alteration in the weapon causes the weapon's effects to change. In addition, any change to the three layers (physical, logical, and cyber persona) will affect the way in which the virus proliferates. These nuances make it difficult to predict the proliferation effects that the cyber weapon will cause once someone releases it. To account for this problem, cyber attack authority needs to be limited to design reversible effects thereby reducing residual risk. If the weapon's effects were to spread beyond the intended target, perhaps into the adversary's commercial sector, then the effects could be reversed, thereby lowering the possibility that widespread destruction would occur.

The difficulty in fully understanding a cyber attack risks creating disproportionate and indiscriminate effects from a cyber weapon's release. Cyber operations and weapons can cause more severe damage, or with consequences more widespread in space and time.[18] Using a cyber weapon within the context of the Law of Armed Conflict requires the weapon to be discriminate, distinct, and proportionate. Operational commanders and their staffs understand the relation between a bomb's effects on a target building and these three requirements. A cyber weapon's effects cannot be fully known; therefore, commanders need to find the cyber weapon's collateral damage acceptable when compared to the bomb. Designing the cyber weapon to have reversible effects ensures that if the anticipated effects are incorrect, then subordinates can control the effects. The same is not true for the bomb; once an airplane drops it, the bomb's effects are permanent. Designing the cyber weapon to generate reversible effects ensures that discriminate, distinct, and proportionate effects result when attacking an adversary.

Cyber attacks allow the United States to avoid the costs of kinetic destruction in terms of rebuilding or repairing infrastructure damaged in a conflict.[19] The costs of such damage can be staggering. However, if operational commanders had the authority to conduct limited cyber attacks, then they could lower the overall costs in comparison to destroying targets with kinetic weapons. For example, a commander could disrupt an electrical system with a cyber weapon instead of destroying it with a kinetic weapon. This allows the attacking agent to repair the damage through cyber means at a lower cost when compared to the kinetic weapon's physical destruction. Reversible cyber attack effects offer benefits that the kinetic weapon cannot match. They permit the commander to set favorable conditions without permanently destroying important infrastructure. Limited cyber attack authority translates into cost savings depending on the intended target.

Preapproved Cyber Authorities

From the point of view of policymakers, a preapproved set of authorities should offer some solace and confidence in granting greater authority to operational-level commanders because it offers national leaders greater insight and control than they would have in a kinetic operation. From the point of view of the U.S. military, operational commanders, armed with preapproved cyber attack methods, can attack faster and with the least cost of blood and treasure. Limited cyber attack authority increases the options available to national authorities who choose how best to serve vital, core, and peripheral national interests. Granting national authorities greater control over military operations enhances the ways in which the military can achieve strategic and political objectives. Limiting cyber attack authority to reversible effects enables national and strategic authorities to make choices to accept, transfer, avoid, or mitigate military operational risks.[20] Part of this greater control is the preapproval of specific military operations that generate reversible effects.

There are several types of cyber attacks that national authorities need to preapprove: distributed denial of service, cryptographic, obfuscating, and resource-deception attacks. Distributed denial-of-service attacks use hundreds or thousands of compromised systems to force Web site failures and shutdowns or to deplete resources like bandwidth, memory, or processing capacities.[21] With either strategy, the attacker creates disruption ranging from inconveniences, to

Marine with Service Company, 7th Engineer Support Battalion, 1st Marine Logistics Group, participates in Exercise Deep Strike II, at Blythe, California, September 8, 2017 (U.S. Marine Corps/Timothy Shoemaker)

a lack of reliability for the Web site, and finally to a shutdown of the server and some delay until the restoration of Web services occurs.[22] Cryptographic attacks use encryption, which only the attacker knows, to encrypt key programs of the adversary; the attacker can later decrypt them.[23] Obfuscating attacks seek to rearrange the software and data of a computer system in a way known only to the attacker. After the attacker decides to end the attack, he can rearrange the system back to the status quo ante.[24] Resource deception deceives the adversary with illusory damage.[25] When the attacker reveals that he did not alter anything, this deception operation ends as the attacked party realizes what happened. These types of cyber attacks impart reversible damage to an adversary allowing the negation of the residual effects once the attack is complete. Preapproving these attacks grants national authorities greater oversight of specific military operations prior to execution.

In a scenario on the Korean Peninsula, operational commanders could use these four types of cyber attacks to mitigate risks of unintended consequences and provide options to restore North Korea's existing infrastructure at costs lower than those associated with kinetic weapons. A distributed denial-of-service attack, such as the one that U.S. Cyber Command allegedly conducted in 2017, provided temporary and nondestructive effects on North Korea.[26] U.S. Cyber Command turned off the attack, and there were no unintended consequences reported. Using a cryptographic attack aimed at North Korea's two oil refineries could disrupt the country's transport and agriculture production.[27] If the United States used this type of attack, it would disrupt North Korea's petroleum supply, affecting military vehicles and food production. When the United States decided to stop the effect, it could decrypt the attack to allow petroleum to return to normal supply levels. The United States could use an obfuscating attack, which would result in the same way as the cryptographic attack. Although the method is different, the effect is the same. Lastly, the United States could use a resource-deception attack if it decided to attack North Korea with military forces. The Nation could use this attack to deceive the North Korean military in a forced entry operation. If the United States seemingly attacked North Korean infrastructure in a resource-deception attack, the North Koreans might avoid certain routes because of perceived damage. This could provide the Nation with a marked advantage to use routes without the preponderance of North Korean military forces located near them. All of these examples of preapproved attacks mitigate unintended consequences because they are temporary and nondestructive.

Preapproved cyber attacks decrease operational costs and lower risk to Servicemembers while increasing costs to the adversary. An adversary who relies on Web-based commercial enterprises can lose money quickly, depleting his financial resources. From the attacker's perspective, most costs to conduct a cyber attack, such as a distributed denial-of-service attack, do not change because they are fixed. For example, the costs of electricity, connectivity, computers, and personnel are part of normal expenditures. When compared to the employment of a fixed-wing aircraft to bomb a building, cyber attack expenses are significantly lower. Cyber attacks also limit the exposure of Servicemembers to physical hazards. Manned and unmanned aircraft need to fly near the target to deliver ordnance, exposing Servicemembers and high-cost equipment to the dangers of enemy fire. Cyber attacks do not face such physical hazards. In addition, cyber attacks require lower maintenance and fewer logistical needs in comparison to aircraft. The features of cyber attacks decrease the risks and costs that national authorities incur when selecting military operations to achieve political objectives.

Counterargument

There have been many arguments against pushing cyber attack authorities down to the operational level, but these fail to address the change in this new domain. Some argue that cyber attacks are more dangerous than kinetic attacks because of the inherent unknowns in cyberspace. Cyber attacks require precision in targeting that is unachievable due to time and intelligence collection requirements in comparison to kinetic weapons. Decades of military operations have shown the high degree of accuracy and precision with the employment of kinetic weapons. A cyber weapon's collateral damage is inherently greater than a kinetic weapon because unintended consequences cannot be fully known prior to the cyber weapon's release. Employing a cyber weapon, even if designed with reversible effects, risks escalation if the weapon's effects target an adversary's sensitive networks. Yet this argument does not withstand scrutiny because the use and knowledge of cyber attacks are increasing exponentially in civilian and military circles. The time to develop the required precision in cyber targeting is decreasing rapidly. As cyber weapons proliferate, collateral damage estimates are becoming more accurate. Reversible effects ensure that collateral damage, when it occurs, can change to the status quo ante, thereby lowering escalation hazards. Lastly, kinetic weapons always result in death and destruction, while cyber weapons do not necessarily result in the same.

Others argue that operational commanders and their staffs cannot possibly design cyber attacks without vast resources to achieve reliable results with reversible effects. They say that operational staffs cannot reliably design reversibility into a cyber weapon. These critics might point to the error in the Stuxnet code that let it unintentionally spread and replicate itself globally.[28] They argue that the Intelligence Community and strategic commanders have the niche capabilities, resources, and knowledge to understand the complexities of the design of cyber weapons. The constantly evolving nature of cyberspace makes the quick design of a cyber weapon almost impossible. This argument does not stand because most countries communication systems, electric grids, and so forth use commercially available software and systems well known throughout the world, and "off the rack" cyber weapons could conceivably meet such needs. Not every cyber weapon requires individual construction to achieve desirable effects against an adversary. Operational staffs have robust intelligence, operations, and communications sections capable of assessing adversary networks. If existing staffs were unable to conduct cyber planning and targeting, U.S. Cyber Command has two types of support teams to augment their cyber planning and targeting capabilities. There are 27 combat mission teams generating integrated cyberspace effects in support of operational plans and contingency operations in their support to combatant commands.[29] In addition, 25 support teams provide analytic and planning support to the national mission and combat mission teams.[30] Both teams could augment and aid operational commanders and their staffs to conduct cyber attacks through their assigned combatant command. Preapproved cyber attack methods provide operational commanders the ability to attack adversaries within existing resource limitations.

The nature of cyberspace challenges military leaders to apply force within legal, ethical, and resource limitations. Many unknowns exist and persist that certainly provide operational commanders with challenging but surmountable obstacles in the application of military force in cyberspace. It is in the best interest of policymakers to grant, yet limit, cyber attack authority to hedge greater risks in operational-level decisions that use cyber weapons. Operational commanders face adversaries capable of degrading and destroying military capabilities; they need to be armed with as many tools as possible to achieve objectives. Limited cyber attack authority expands the available set of tools. Cyber weapons need to be made available to operational commanders to pursue national interests through military operations. In cyberspace, offense has the upper hand.[31] The best way to provide operational commanders with the ability to attack an adversary includes providing them with limited cyber attack authority based on the reversible effects of the cyber weapon. Reversible effects lower the risk inherent in military operations and mitigate unintended consequences. National authorities gain greater control over military operations in preapproving cyber attack methods. They also gain access to more military options to select in the event of a crisis. National authorities need to grant limited cyber attack authority to operational commanders so they can achieve operational, strategic, and political objectives aligned with vital, core, and peripheral national interests. **JFQ**

Notes

[1] The Department of Defense (DOD) includes cyber attacks in a larger category referred to as "offensive cyberspace operations." This article refers to all offensive cyberspace operations as cyber attacks. DOD defines *offensive cyberspace operations* as "Missions intended to project power in and through cyberspace." See Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, June 8, 2018), GL-5.

[2] Maren Leed, *Offensive Cyber Capabilities at the Operational Level* (Washington, DC: Center for Strategic and International Studies, 2013), available at <www.csis.org/analysis/offensive-cyber-capabilities-operational-level>.

[3] Rosemary M. Carter, Brent Feick, and Roy C. Undersander, "Offensive Cyber for the Joint Force Commander," *Joint Force Quarterly* 66 (3rd Quarter 2012), 22–27, available at <http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-66.aspx>; James E. McGhee, "Liberating Cyber Offense," *Strategic Studies Quarterly* 10, no. 4 (Winter 2016), 46–63, available at <www.airuniversity.af.mil/SSQ/>; Musa A. Samad, "Cyber Operations: Putting MAGTF Commanders in Control," *Marine Corps Gazette* 99, no. 7 (July 2015), 20–23, available at <www.mca-marines.org/gazette/2015/07/cyber-operations>.

[4] DOD defines *cyberspace* as a "global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." See JP 3-12, GL-4.

[5] Ibid., I-2–I-4.

[6] Paul W. Phister, "Cyberspace: The Ultimate Complex Adaptive System," *The International C2 Journal* 4, no. 2 (2010), 13, available at <www.dodccrp.org/files/IC2J_v4n2_03_Phister.pdf>.

[7] Ibid.

[8] Jeffrey Hunker, *Cyber War and Cyber Power: Issues for NATO Doctrine*, Research Paper No. 62 (Rome: NATO Defense College, November 2010), 3, available at <www.files.ethz.ch/isn/124343/rp_62.pdf>.

[9] Richard M. Cromwell, *War in the Information Age: A Primer for Information Operations and Cyberspace Operations in 21st Century Warfare* (Newport, RI: U.S. Naval War College, 2010), 18.

[10] Natalia Zinets, "Ukraine Charges Russia with New Cyber Attacks on Infrastructure," Reuters, February 15, 2017, available at <www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>.

[11] Helene Cooper, "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts," *New York Times*, January 12, 2015, available at <www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html>.

[12] *Statement of General James N. Mattis, U.S. Marine Corps, Commander, U.S. Central Command, Before the Senate Armed Services Committee on the Posture of U.S. Central Command*, 112th Cong., 1st sess., March 1, 2011, 39, available at <www.armed-services.senate.gov/imo/media/doc/Mattis%2003-01-11.pdf>.

[13] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, 2012, available at <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>; Kim Zetter, "Report: Obama Ordered Stuxnet to Continue after Bug Caused It to Spread Wildly," *WIRED*, June 1, 2012, available at <www.wired.com/2012/06/obama-ordered-stuxnet-continued/>; John Naughton, "Stuxnet: The Worm That Turned Obama into a Hypocrite?" *The Guardian*, June 9, 2012, available at <www.theguardian.com/technology/2012/jun/10/stuxnet-us-internet-freedom-policy-john-naughton>; Rowan Scarborough, "In Classified Cyberwar against Iran, Trail of Stuxnet Leak Leads to White House," *Washington Times*, August 18, 2013, available at <www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/>.

[14] Ibid.

[15] This scenario was adapted from the one provided by Carter, Fieck, and Undersander, "Offensive Cyber," 25–26.

[16] Lieutenant General Edward Cardon, USA, panel member, "CMF #11: The Future of Army Public-Private Partnership and Cyberspace," Association of the United States Army, Washington, DC, October 5, 2017, available at <www.dvidshub.net/video/486234/cmf-11-future-army-public-private-partnership-and-cyberspace>.

[17] Bimal K. Mishra and Dinesh Saini, "Mathematical Models on Computer Viruses," *Applied Mathematics and Computation* 187, no. 2 (2007), 929.

[18] Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict," in *2012 4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2012), 323, available at <https://ccdcoe.org/cycon/2012/proceedings/d1r3s2_fanelli.pdf>.

[19] Leed, *Offensive Cyber Capabilities at the Operational Level*, 8.

[20] Norman T. Sheehan, "A Risk-Based Approach to Strategy Execution," *Journal of Business Strategy* 31, no. 5 (2010), 31–32, available at <www.researchgate.net/profile/Norman_Sheehan2/publication/242020919_Making_risk_pay_The_board's_role/links/559eefee08ae03c44a5cdef5.pdf>.

[21] Lech Janczewski and Andrew M. Colarik, *Cyber Warfare and Cyber Terrorism* (Hershey, PA: Information Science Reference, 2011), 263.

[22] Ibid.

[23] Neil C. Rowe, "Towards Reversible Cyberattacks," U.S. Naval Postgraduate School, Monterey, CA, available at <http://faculty.nps.edu/ncrowe/rowe_eciw10.htm>.

[24] Ibid.

[25] Ibid.

[26] Karen DeYoung, Ellen Nakashima, and Emily Rauhala, "Trump Signed Presidential Directive Ordering Actions to Pressure North Korea," *Washington Post*, September 30, 2017.

[27] Tony Munroe and Jane Chung, "For North Korea, Cutting Off Oil Supplies Would Be Devastating," Reuters, April 13, 2017, available at <www.reuters.com/article/us-northkorea-nuclear-china-oil/for-north-korea-cutting-off-oil-supplies-would-be-devastating-idUSKBN17F17L>.

[28] Rowe, "Towards Reversible Cyberattacks."

[29] *The DOD Cyber Strategy* (Washington, DC: DOD, April 2015), available at <www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

[30] Ibid.

[31] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (2010), 99, available at <www.dtic.mil/dtic/tr/fulltext/u2/a527707.pdf>.