As part of Internet of Things display, booth of Deutsche Telekom at CeBit 2015 shows moving arms of robots holding magenta umbrellas, March 16, 2015 (Courtesy Mummelgrummel)

Information Warfare in an Information Age

By William R. Gery, SeYoung Lee, and Jacob Ninas

In the past week, how many devices have you used that were connected to the Internet or relied on an algorithm to accomplish a task? Likely, the number is upward of 10 to 15, and most of those devices are used daily, if not hourly. Examples may include a Fit-Bit, cell phone, personal computer, work computer, home monitoring system, car, Internet television, printer, scanner, maps, and, if you are really tech savvy, maybe your coffee pot or refrigerator.

The Internet of Things (IoT) is bound by a mesh network that is increasingly connected to every part of our lives, and those devices are becoming increasingly reliant on each other to perform their functions.[1] Computing devices, using advanced algorithms, are entering the machine-learning phase, a subset of computer science in which the computer is "learning" about the environment and presenting predictions based on available data and conditions.[2] Trends include machine-autonomy and self-learning. The idea of interconnectivity is not only about the IoT but also the information that

Major William R. Gery, USAF, is Program Manager for the U.S. Air Force Weapon System Evaluation Program at Air Combat Command. Major SeYoung Lee, Republic of Korea (ROK) Army, is a Student in the Military History Institution of ROK Army Headquarters. Lieutenant Colonel Jacob Ninas, USA, is a Branch Chief in the 704th Military Intelligence Brigade.

transits the Internet, and how it influences our daily decisions. The trend toward a worldwide mesh-network is nearing, and with the creation of an information technology (IT)-based domain comes increased understanding of the environment in which we live. There appears to be no deviation from Moore's law, developed in 1965, and popularized and demonstrated since its inception. If Moore's law continues to be upheld in the future, more apps, algorithms, and daily functions will link together each part of our lives, providing increased processing capability and a limitless stream of information creating maximum efficiency for humans.

The Westphalian design of society and order contributes to the human need to work within a set of logical models, whereas the principle of international law and orderly division of nations enables sovereignty over territory and domestic affairs. It is possible that globalization, which would be nearly impossible without a relatively high transfer rate of information, will play a critical role and may challenge global order. Assuming an information advantage is required to achieve nation-state and military objectives, and information superiority is not guaranteed because of the complex IoT, how does the U.S. Government present effective and integrated information warfare capability (IW) in the information age? Moreover, if wars are fought in the information space, can they be won with information alone? In other words, can information warfare provide the ways and means to fight wars, as well as the ends? Also, does the U.S. Government need to invest in an organization responsible for the coordination and integration of IW capabilities and effects?

To increase the U.S. Government's capability and capacity, a new organization should be created within the U.S. Government to focus on information warfare, with a fundamentally different organizational structure than our current governmental hierarchical structures. Specifically, the U.S. Government subscribes to the diplomatic, information, military, and economic (DIME) model but does not have an organization designed to lead the information functions of this model. The Department of State coordinates the diplomatic role, Department of Defense the military role, and Department of Treasury the economic role. Twenty-first-century challenges presented by the IoT require a more innovative organization that promotes adaptability and agility in the information space, akin to models used at Google, Facebook, or Apple.

Winn Schwartau, author of *Information Warfare* and recognized IW theorist, describes the information age as "computers everywhere."[3] The ultimate fact of the information age is the proliferation of IT, which "incorporates information systems and resources (hardware, software, and wetware) used by military and civilian decisionmakers to send, receive, control, and manipulate information necessary to enable 21st-century decisionmaking."[4] Additionally, the development of IT allows sharing of information in near real time, at an exponential rate, anonymously and securely. These advances can be used as an asset, but also pose a potential vulnerability to the United States, our allies, and our adversaries.[5] It takes seconds to upload pictures or comments on social media networks. At the same time, adversaries can use these systems to gain access to critical information. According to a *New York Times* article, "In July 2015, 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including social security numbers and some fingerprints."[6] The following list provides a general summary of the number of times systems have been attacked via cyber.[7] The number of attacks on information systems has increased each year, reinforcing the fact that warfare is currently being conducted in the information space via IT.

- *The Pentagon reports getting 10 million attempts a day.*
- *The National Nuclear Security Administration, an arm of the Energy Department, also records 10 million hacks a day.*
- *The United Kingdom reports 120,000 cyber incidents a day. That is almost as many as the state of Michigan deals with.*
- *Utah says it faces 20 million attempts a day—up from 1 million a day 2 years ago.*[8]

To meet the challenge that exists in the information age, organizational changes are required. Modern ideas and incorporating industry concepts may be one way to traverse the information space and create an advantage in future conflicts.

Within the IoT, actions take place in nanoseconds and occur billions of times daily. Big data concepts attempt to harness massive amounts of information and distill that information into something that a human can use to make a decision. In the near future, the information required to win the advantage over an enemy may be determined by who can extract data, identify key centers of gravity in the information space, and automatically take action though rule sets and computational criteria based on defined "rules of engagement." The ability to harness big data exists now and is only increasing. Consumer product companies are mining Facebook, Google, and other data to understand customer preferences, global trends, and public opinion on matters of interest. From a military standpoint, understanding the information terrain in relation to the potential adversaries is foundational to discerning points for information operations (IO) across the range of military operations. Big data concepts used in business could be advantageous and used in information warfare. It is possible that data-mining and subsequently an information advantage could achieve objectives purely through IW alone.

The United States has used various IW strategies, agencies, and professionals, with varying degrees of success. The U.S. Information Agency (USIA) was created in 1953 and was in service until 1999. USIA was designed to consolidate all information activities:

[USIA] *comprised all of the foreign information activities formerly carried out by the Department of State's International Information Administration (IIA) and Technical Cooperation Administration, and by the Mutual Security Agency. Overseas, existing United States Information Service posts became the field operations offices of the new agency. The exchange of persons program conducted by IIA remained in the Department of State, but USIA administered the program overseas. The Department of State provided foreign policy guidance.*[9]

Historically, information warfare was identified as critical to national security, and USIA was required to erode support for the Soviet Union during the Cold War.[10] Today, we usually consider IW as the means, or sometimes a way, to achieve an objective. But currently we rarely think of IW as an end, even though we live in an information age where we are all affected by the information environment every day. Brian Nichiporuk, the author of "U.S. Military Opportunities," discusses IW concepts and postulates:

The goals of an offensive information-warfare campaign are to deny, corrupt, degrade, or destroy the enemy's sources of information on the battlefield. Doing so successfully, while maintaining the operational security of your own information sources, is the key to achieving "information superiority"—that is, the ability to see the battlefield while your opponent cannot.[11]

In current and future warfare, information superiority could be the single most decisive factor. For instance, we could think about the China-Taiwan scenario. China is employing a robust IW strategy targeting the Taiwanese government in order to bring Taiwan under Chinese control, without engaging in kinetic war. They are simultaneously using information operations to delay U.S. involvement to the point where any outside interdiction occurs too late to affect the outcome.[12] This concept is fully realized by a dedicated focus on IW strategy, organization, and capabilities. This could be analyzed best by Sun Tzu's strategy: "To subdue the enemy without fighting is the acme of skill."[13] In another example, the Russian operations in Crimea provide a modern case study where the outcome of operations was directly attributed to IW principles and capability.

Information Warfare: The Russian Invasion of Crimea

The Russian incursion into eastern Ukraine, and eventual annexation of Crimea in 2014, serves as the current model of a sustained IW campaign and provides examples of successes and failures in these efforts. Russian IW, known as Reflexive Control, has its origins in Soviet doctrine and serves as a key component in their hybrid warfare operations.[14] Reflexive Control "relies . . . on Russia's ability to take advantage of preexisting dispositions among its enemies to choose its preferred courses of action."[15] During operations in Ukraine, Russia's primary impediments included Western European powers and the United States. Russia took multiple actions to seize the advantage of preexisting dispositions among its enemies in order to conduct successful operations in Ukraine and, at the same time, avoid a large-scale confrontation with the West.

As part of Reflexive Control, Russia utilized a well-coordinated denial-and-deception plan, called *maskirovka*, through the use of "little green men" to establish checkpoints and secure key terrain in Ukraine. These little green men operated with speed and efficiency, and wore no identifying patches or unit insignia. This lack of identification allowed Russia to deny any association with these forces, which were later acknowledged as Russian troops. By controlling information and being able to deny its involvement in the occupation of Ukraine during the early stages of the conflict, Russia was viewed as an interested party by the international community—as opposed to a belligerent. This fed directly into Russia's view that Western Europe and the United States did not desire a direct conflict and would not press the issue of Russian involvement, even if discovered.

The ability to operate in relative secrecy also allowed Russia to successfully mask its true desired endstate. By doing so, it allowed for almost any action to potentially be considered a successful mission to enemies and outside observers, due to a lack of understanding of Russian intentions. This also allowed for unchallenged Russian saber rattling and threats against the North Atlantic Treaty Organization and the West as Russia attempted to paint Western Europe and the United States as weak, especially in the eyes of developing nations. In addition to actions on the ground in Ukraine, Russia integrated and utilized television, print media, and social media to deflect and hide its efforts at occupation and annexation while reducing potential Western involvement.[16] The successful use of IW allowed Russian forces to occupy eastern Ukraine and annex Crimea without a large-scale response from the West.

As the world continues to move into the information age, the ability of nation-state and nonstate actors to employ successful IO tactics into their overall strategy will undoubtedly increase. To successfully deter and respond to these threats, the United States must innovate and develop organizations with expertise in both preventing and conducting such actions.

Russia's IW campaign in Ukraine enabled it to achieve the objective of annexing Crimea, but it was not a flawless strategy. One flaw was the effort that Russian leaders took to deny the existence of troops in Ukraine. Even after undeniable proof, including geotagged photographs on social media and captured Russian troops inside Ukrainian territory, Russian President Vladimir Putin continued to deny involvement. These excessive and continual denials served only to discredit Russian leaders and provide additional reason to believe that Russian forces were in fact operating inside Ukraine.[17] In addition, the lack of an overwhelming campaign of offensive cyber actions brings into question the overarching hybrid warfare campaign. Russia is arguably one of the most capable nation-state cyber actors.[18] The lack of a comprehensive offensive

Deputy Secretary of Defense Robert Work and Vice Chairman of the Joint Chiefs of Staff General Paul Selva meet with Commander of U.S. Pacific Command, Admiral Harry Harris, to discuss Third Offset Strategy and its implications for Indo-Asia-Pacific region, October 18, 2016, Camp H.M. Smith, Hawaii (U.S. Navy/Jay M. Chu)

cyber campaign, such as that observed in Estonia in 2007 and Georgia in 2008, raises questions about Russian IW and Reflexive Control strategy. While this may indicate a desire not to aggravate potential adversaries, it may also indicate Russia's inability to control all aspects of its offensive cyber actions such that it was concerned that actions could produce large-scale unintended consequences.[19] These consequences may have resulted in the Russians' inability to deny their involvement, or brought powerful enemies into the conflict. As discussed, the flaws noted in Reflexive Control doctrine serve as examples of how difficult it is currently, and will be in the future, to control the consequences of offensive actions and conduct information warfare in an information age. In an effort to better understand the capabilities and intentions of potential adversaries, understand their lessons learned, and use them to our advantage, the U.S. Government must ensure that the current organization of IW capabilities and strategic planning enables an integrated and cohesive National Security Strategy.

Strategic Planning Guidance to Tactical Execution?

In the joint planning process, IO planning is typically a supporting effort. If we prescribe to the idea that all wars are fought on the cognitive plane, at least at some point, then it is logical to assume that, at one point or another, IW courses of action (COAs) should be the supported effort. Moreover, "information operations support themes" are sometimes developed after military kinetic COAs are.[20] While the current planning process and traditional planning structure provide the formal links between national strategy and the tactical level, they do not prescribe a way in which to gain the information advantage in future conflicts. Arguably, from a national perspective, an information strategy should drive subsequent actions and be integrated from the President to the individual Servicemember. The information strategy should be integrated with strategic communications efforts of the U.S. Government. However, as noted in the 2008 report from the Defense Science Board, "Strategic Communications is a dynamic process with responsibility held by those at the highest levels of government—the President and senior government leaders. . . . But to do so requires a commitment not yet seen,

Routers and switches inside Google's campus network room at Council Bluffs, Iowa, allow data centers to talk to one another, with fiber-optic networks that run at speeds more than 200,000 times faster than typical home Internet connections (Photo courtesy Google Inc.)

though some steps have been taken."[21] In fact, the report recommends the creation of a nonprofit, nonpartisan Center for Global Engagement as a focal point for strategic communication activities.

In 2010, Joseph Biden provided the President a report on strategic communications that urged synchronization and defined the overall concept.[22] An interagency policy committee, led by the National Security staff, was a recommended solution; however, a committee is made up of individuals with allegiances to their own organization and likely with other responsibilities, not fully being dedicated to integrated strategic communications. The little IW capability that exists is based on the current and legacy organizational structure, which hinders effective IO planning and execution.

If information space can be considered a way and means to fight and win wars, then a framework is required to assist in prioritization and planning and to present ends that may be achieved through information warfare. Planners must articulate why a specific action is being taken and when it should occur based on commander's intent, the operational environment, and the operational approach designed to solve the problem. Decades of trial and error in warfare have led to institutional doctrine and rule sets. While there is an argument that these rules should be applied to both kinetic and nonkinetic effects, it is important to realize that there are certain unique factors associated with both. For example, targeting fundamentals are largely agreed upon and accepted for offensive force-on-force operations, but do the theories of targeting need to adjust for information warfare?

Some argue that the center of gravity (COG) for the Islamic State of Iraq and the Levant (ISIL) is the Internet. If we accept this idea, how does the United States target ISIL? Does the U.S. Government shut down Internet Service Providers (ISPs) (that is, the target) that ISIL is using? Does the government conduct a distributed denial-of-service attack against certain Web sites? Does it put influential messages onto ISIL message boards on the Internet? All options are plausible, but many times are not executed due to lengthy and unsynchronized plans. The lack of leadership and a focal point in the U.S. Government who can articulate the second- and third-order effects of information operations often contributes to a lack of action. The ability to understand how the information space will be influenced by the outcome of a U.S. action is not effective because there is no lead organization.

In addition to the tactical-level information effects, how are strategic communications vetted and targeted? Do the processes differ or are they the same? If the view of this process were to change, and targeting were to become a

process within which information targets are held at risk (for example, the ISP example or building a strategic weapon to deter an enemy), then it is possible that realistic options could be presented to a combatant commander in a crisis action scenario. To execute a concept where the United States holds information targets at risk, it must have access to the target. Access for information-related effects delivered through the information space is no different than for physical effects delivered by airplanes or ships. The delivery method could be news, a cyber capability, a military action, or even a comment by the President. The path to employ information-related capabilities (IRCs) requires access from the sender to the receiver, and that targeting path must be sustainable. Without sustained access, a target cannot be held at risk because gaining access to the receiver could take an extended amount of time, with relation to the operation.

Additionally, the capability must be attainable. Software development can be a potential strategic advantage. Driving education and training for software development down to the tactical level empowers young Servicemembers to create capabilities linked to the target, reduce cost, and create efficiencies. For example, a Soldier is taught how to use a rifle, the foundations are built in training, and he is able to utilize the weapon through the employment of various tactics, techniques, and procedures on the battlefield as the situation dictates. If the situation changes, he adjusts to the enemy in an instant. From an IW perspective, software is but one tool, as is the rifle. Foundations are built, skills are honed, but it is left to the tactical level to ensure the capability is "tuned" to the target because the tactical-level operator should have the most accurate knowledge of that target. Additionally, as accesses change, the tactical and operational level should ensure consistent and reliable access to the target. Indeed, the Soldier does not develop the strategy; the national security staff, President, and combatant commanders do. But what organization is responsible for coordinating the strategic message throughout the national security apparatus? Furthermore, what organization is responsible for providing information operation COAs for the President, specifically designed as an end?

The contrarian viewpoint to the idea of driving development down to the operator level (that is, the Soldier) is that authorities do not come with capability. This is true. A tactical-level unit should not have authority to execute operations in the information space, just as the Soldier with the rifle would not fire without orders. There should be a strategy with clear and precise guidance for operational and tactical targeting. This does not require "execution authorities," but it does require guidance from national-level leadership on the issue. In other words, because technical acumen is required, the U.S. Government cannot afford to have a disjointed IW strategy in which progress is slowed due to an overly complicated and bureaucratic hierarchical structure. A lack of unity of effort results, and risk to mission and risk to force increase. Developers, operators, and analysts need flexibility and agility to solve problems quickly with innovative technology and an understanding of the information age, just as a Soldier does when in battle.

Is the World Organizationally Changing?

Military organizations have generally followed hierarchical models as early as the Greeks in 400 BCE for organizing and equipping. It is possible that global IT trends will require a foundationally different way of thinking and organizing IRCs in the U.S. Government to maintain pace with the speed of information. Largely, from the time of the Greeks to that of the current U.S. Government, militaries have been designed around a hierarchical system. As IW becomes increasingly more important during the conduct of government or military operations, a lattice framework and system may be a logical way to organize information warfare–based capabilities and personnel.

This concept prescribes basic guidance and a certain rule set (that is, authorities) but empowers individual members to develop solutions unabated by personnel unfamiliar with the technical situation. The concept capitalizes on meritocracy-based principles and focuses on a federated approach as well as crowd-sourcing solutions internally to the military, or even in the public sector, to arrive at solutions. Within the U.S. Government, it is unlikely that a lattice organization would be wholly integrated; however, a hybrid concept that captures the value of a legal and hierarchical framework along with realizing the potential benefit of a lattice organization would be valuable, as globalization and IT increasingly integrate our world. Additionally, a lattice framework would more closely align conceptually with the mass-network IT environment in which we live. Ideas presented in the corporate world are potential solutions that can be used or modified for complicated IW concepts within the U.S. Government. In a thought piece from business, Cathleen Benko and Molly Anderson from *Forbes* magazine highlight a few key benefits of a lattice organizational structure:

With employees working in geographically dispersed teams, the old ways of communicating [are] *no longer served. Lattice ways to participate moved the organization toward more interactive, transparent communication. In one instance, the finance division gave a role traditionally reserved for management—identifying improvement priorities—to employees, by launching a "pain points" portal where they can voice their views of current challenges for everyone to see. The company appoints teams to address the highest priorities.*

At Deloitte, our annual employee survey shows that 90% of workers who experience all three lattice ways are engaged. Contrast that with the results of a major global workforce study by Towers Perrin in 2007–2008 that found just over 60% of employees in surveyed companies were engaged.[23]

Not only does a lattice framework promote internal integration and idea-sharing, the concept also promotes the use of solutions from external sources. In many cases, members of a lattice-type

USS *Freedom* and USS *John C. Stennis* are under way conducting Independent Deployer Certification exercise in surface warfare, air defense, maritime-interception operations, command and control/information warfare, C4 systems intelligence, and mine warfare, April 28, 2015 (U.S. Navy/Ignacio D. Perez)

organization are encouraged to look for nonstandard solutions to difficult problems, even if that means branching outside of organizational norms.

Analyzing a recent case, the iPhone encryption issue surrounding the San Bernardino terrorist attack is an example of a federated approach to problem-solving. The Federal Bureau of Investigation (FBI) was able to crack the iPhone's encryption, despite Apple's unwillingness to support. Apple's fear stemmed from the idea that if it provided the requested support, the government would then own the key to all encryption security measures for iPhones around the world.[24] When the international media reported and publically debated the issue, the FBI received calls from individuals and companies claiming to possess the tools necessary to break the encryption. In fact, one company was able to break the encryption and allowed the FBI to retrieve the desired data from the terrorist's phone. This example shows the power of information in multiple ways; the first is the fact that the government was unable to use traditional methods of gaining support from a private company. Second, media, as the primary driver, brought attention to the problem and forced a public debate, which worked in favor of the government. There were arguments on both sides of the issue, but it should be assumed that the challenge in and of itself was enough to stimulate a solution, whether right or wrong. The key point to this example is that the proliferation of information drove a solution, regardless of Apple's standpoint, the FBI's authority, and even despite popular public opinion for or against the FBI. If the power of information can easily dictate the outcome of such an example, what are the long-term implications for warfare? The U.S. Government can take measures now, organizationally, to harness IW concepts and be positioned to maintain the information advantage in a dynamic and unsure information age.

Future IW solutions will also need to involve multidomain skills from individuals with varying backgrounds. In today's military, once a Servicemember is branded with a specific skill set, it is challenging to break from that community and maneuver effectively between communities, while still maintaining upward mobility. To achieve greater effectiveness in IO planning and execution, cross-domain and diverse IRC careers should become a desired career path option for future leaders.

Amazon Meets the U.S. Government

To harness the information age and enable IW capability toward the success of future U.S. conflicts, a new organiza-

tion should be created within the U.S. Government. The Cold War has passed, and so has USIA; however, it is possible that a new version of USIA is required as Russia continues to test its limits of power. As in the case of Ukraine, Georgia, and Estonia, as well as the need to combat terrorist groups such as ISIL, a renewed effort on U.S. information warfare is required. The dynamic and ever-changing environment requires a fundamentally different organizational structure than that of current government hierarchical structures in order to be flexible and adaptable for 21st-century problems. Additionally, as we move forward in the information age, our lives will be increasingly intertwined and connected with information systems. This information environment will continue to play a critical role in how the U.S. Government and military interact with allies, partners, and adversaries in all of the operational domains.

To shape the environment to meet our desired endstates, we must recognize the importance of information warfare and work to ensure that IO concepts are properly integrated into all actions and operations, if not become an end themselves. We must also search for innovative ways to build and employ IO concepts. Our IO experts must have the required training and expertise necessary to meet these requirements by way of strategic guidance. Operators must have flexibility and agility engrained into their ethos through a lattice-type organizational structure, which honors a multidomain career path. The ability to carry out all IW requirements must be done in a timely and succinct manner that allows for the fastest possible action with the most flexibility. If we are not able to achieve these objectives, we will most definitely fall behind in the fast-paced and constantly changing world of IT and IW, and we will likely be ineffective in identifying and combating enemy COGs, such as ISIL's reliance on IT. It is time to implement ideas that exist in industry, and force change, before change is unattainable—through a sustainable and repeatable process and organization within the U.S. Government. **JFQ**

Notes

[1] "A mesh network is a Local Area Network (LAN), Wireless Local Area Network (WLAN), or Virtual Local Area Network (VLAN) that employs one of two decentralized connection arrangements: full mesh topology or partial mesh topology. In a full mesh topology, each network node is connected directly to others. In a partial mesh topology, some nodes are connected to all the others, but are only connected to those nodes with which they exchange the most data." See "Mesh Network Topology (Mesh Network)," *IoTAgenda.com*, available at <http://internetofthingsagenda.techtarget.com/definition/mesh-network-topology-mesh-network>.

[2] Machine-learning is a subfield of computer science that evolved from the study of pattern recognition and computational learning theory in artificial intelligence. Machine-learning explores the construction and study of algorithms that can learn from and make predictions on data.

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

[4] Ibid.

[5] Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: The Joint Staff, November 27, 2012), I-1.

[6] Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," *New York Times*, July 9, 2015.

[7] Brian Fung, "How Many Cyberattacks Hit the United States Last Year?" *National Journal*, March 8, 2013, available at <www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/>.

[8] Ibid.

[9] U.S. Information Agency, available at <www.archives.gov/research/foreign-policy/related-records/rg-306.html>.

[10] Alvin A. Snyder, *Warriors of Disinformation: American Propaganda, Soviet Lies, and the Winning of the Cold War* (New York: Arcade Publishing, 1995).

[11] Brian Nichiporuk, "U.S. Military Opportunities: Information-Warfare Concepts of Operation," in *The Changing Role of Information in Warfare*, ed. Zalmay Khalilzad and John White (Santa Monica, CA: The RAND Corporation, Project Air Force, 1999), 181.

[12] Eric A. McVadon, "Systems Integration in China's People's Liberation Army," in *The People's Liberation Army in the Information Age*, ed. James C. Mulvenon and Richard H. Yang (Santa Monica, CA: The RAND Corporation, 1999), available at <www.rand.org/content/dam/rand/pubs/conf_proceedings/CF145/- CF145.chap9.pdf>.

[13] Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), 77.

[14] Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report 1 (Washington, DC: Institute for the Study of War, September 2015), 7, available at <http://understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare>.

[15] Ibid.

[16] Ibid.

[17] Dimitry Gorenburg, "Crimea Taught Us a Lesson, But Not How the Russian Military Fights," *War on the Rocks*, May 19, 2014, available at <http://warontherocks.com/2014/05/crimea-taught-us-a-lesson-but-not-about-how-the-russian-military-fights/>.

[18] LookingGlass Cyber Threat Intelligence Group, *Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare*, CTIG-20150428-01 (Reston, VA: LookingGlass Cyber Solutions, Inc., April 28, 2015), available at <https://lookingglasscyber.com/wp-content/uploads/2015/08/Operation_Armageddon_FINAL.pdf>.

[19] David Talbot, "Watching for a Crimean Cyberwar Crisis," *MIT Technology Review*, March 4, 2014, available at <www.technologyreview.com/s/525336/watching-for-a-crimean-cyberwar-crisis/>.

[20] JP 5-0, *Joint Operation Planning* (Washington, DC: The Joint Staff, August 11, 2012), II-9.

[21] *Report of the Defense Science Board Task Force on Strategic Communication* (Washington, DC: Department of Defense, January 2008), available at <www.acq.osd.mil/dsb/reports/ADA476331.pdf>.

[22] *National Framework for Strategic Communication* (Washington, DC: The White House, 2010).

[23] Cathleen Benko and Molly Anderson, "The Lattice that Has Replaced the Corporate Ladder," *Forbes.com*, March 16, 2011, available at <www.forbes.com/2011/03/16/corporate-lattice-ladder-leadership-managing-hierarchy.html>.

[24] Pierre Thomas and Mike Levine, "How the FBI Cracked the iPhone Encyption and Averted a Legal Showdown with Apple," ABC News, May 29, 2016, available at <http://abcnews.go.com/US/fbi-cracked-iphone-encryption-averted-legal-showdown-apple/story?id=38014184>.