Philippine special operations forces soldier fast ropes out of SH-60 Sea Hawk during training with U.S. and Australian SOF soldiers at Fort Magsaysay, Philippines, May 2014 (U.S. Marine Corps/Pete Thibodeau)

Strategic Development of Special Warfare in Cyberspace

By Patrick Michael Duggan

Today, small teams of special operators armed with asymmetric cyber-tools, irregular warfare tactics, and mass disinformation can have truly strategic effects.

—General Joseph L. Votel, USA[1]

Why are regional powers such as Iran and Russia better prepared for cyber-enabled special warfare operations than the United States? How do Iran and Russia empower their tactical operators, while the United States masses its cyber-authorities and cyber-capabilities at the strategic level? Why are U.S. policies, authorities, and doctrine for cyber-enabled special operations so immature despite their first announcement over 20 years ago?[2] Although these are serious questions, what is even graver for the Nation is addressing the root question: How does the United

Lieutenant Colonel (P) Patrick Michael Duggan, USA, wrote this essay while attending the U.S. Army War College. It won the Strategic Research Paper category of the 2015 Chairman of the Joint Chiefs of Staff Strategic Essay Competition.

States develop a strategic cyber-enabled special warfare capability?

As far back as 1993, cyber-thinkers John Arquilla and David Ronfeldt in their seminal study *Cyberwar Is Coming!* foreshadowed recent cyber–special operations forces (SOF) actions by Iran and Russia. The prescient notion that "numerous dispersed small groups using the latest communications technologies could act conjointly"[3] to master networks and achieve a decisive advantage over their adversaries has been played out repeatedly. As predicted by Arquilla and Ronfeldt, "We're no longer just hurling mass and energy at our opponents in warfare; now we're using information, and the more you have, the less of the older kind of weapons you need."[4] As senior leaders have recently recognized, groups of special operators armed with asymmetric cyber tools, irregular warfare tactics, and mass disinformation can have strategic effects.[5]

This article argues that Iran and Russia have already successfully employed cyber-enabled special warfare as a strategic tool to accomplish their national objectives. Both countries have integrated cyber-SOF that clearly demonstrate they understand how to leverage this tool's potential within the asymmetric nature of conflict. The countries' asymmetric innovations serve as powerful examples of an irregular pathway for aspiring regional powers to circumvent U.S. military dominance and secure their strategic interests.[6] The diffusion of inexpensive yet sophisticated technology makes it easier for potential adversaries to develop significant capabilities every year. Thus, the time has come for the United States to make a strategic choice to develop cyber-enabled special warfare as an instrument to protect and project its own national interests.

Russia

In February 2013, Russian Chief of the General Staff Valery Gerasimov published an article titled "The Value of Science in Prediction" in the obscure military journal *Military-Industrial Courier*. In the article, General Gerasimov heralded a game-changing new generation of warfare whose strategic value would exceed the "power of force of weapons in their effectiveness."[7] He called for widespread asymmetric actions to nullify enemy advantages through "special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[8]

In spring 2014, Russia successfully demonstrated its new understanding of how to integrate asymmetric technology into unconventional warfare (UW) operations by supporting paramilitary separatists in eastern Ukraine.[9] Russia dispatched small teams of unmarked *Spetsnaz*, or special forces, across the Ukrainian border to seize government buildings and weapons armories, and then turn them over to pro-Russian separatist militias.[10] Concurrently, Russia disconnected, jammed, and attacked digital, telephone, and cyber communications throughout Ukraine. Russia enlisted virtual "privateers" and bounty hunters to conduct cyber attacks against Ukrainian government information and logistic infrastructure, from Internet servers to railway control systems.[11] Russia bankrolled a "troll army" to wage *deza*, a Russian hacktivist term for disinformation, paying millions for each troll to post 50 pro-Russian comments a day on social media, blogs, and news sites that were critical of Russia's actions.[12] Russia surged epic streams of disinformation, both inside and outside Ukraine, not only to obscure its cyber-enabled UW campaign, but also to create complete political illusions: "Russia doesn't deal in petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with informational warfare. . . . It reinvents reality, creating mass hallucinations that translate into political action."[13]

In response, during a North Atlantic Treaty Organization (NATO) security summit in September 2014, the Supreme Allied Commander Europe, General Phillip Breedlove, USAF, proclaimed that Russia's "hybridized" UW in eastern Ukraine represented "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[14] General Breedlove urged the Alliance to develop new capabilities to counter Russia's mastery of UW, propaganda campaigns, and cyber assaults immediately.[15] NATO and the West were caught off guard by Russia's ability to advance its political objectives using nontraditional means in a manner once "not even considered warfare by the West."[16]

Russia did not use Spetsnaz, information operations (IO), or cyber capabilities in a piecemeal manner to accomplish its objectives. Instead, as General Gerasimov described, "Wars are no longer declared"; they simply happen when SOF armed with advanced technology and mass information create the conditions for conventional forces to achieve strategic objectives "under the guise of peacekeeping and crisis."[17] In other words, choreographed cyber disinformation and cyber attack bought time and space for laptop-carrying Spetsnaz to conduct unconventional warfare "between the states of war and peace."[18] Russia's cyber-enabled UW was a brilliant success, not simply for its cyber-SOF hybridization, but also for successfully invading a signature partner nation of the European Union without sparking any meaningful Western military response.

Iran

In summer 2009, the Iranian regime strangled the Green Movement with the very tools that were supposed to liberate it: information and communication technologies (ICTs). The regime exploited "emancipating" ICTs to target activists, induce fear, and expand military and paramilitary suppression of cyberspace.[19] Shortly after the Green Movement began, the government dispatched its Islamic Revolutionary Guard Corps (IRGC) to break the "counter-revolutionaries." Charged with fighting domestic and foreign threats to the regime, the IRGC mobilized its subordinate Basij cyber units and its notorious clandestine paramilitary wing, the IRGC–Quds Force (IRGC-QF). The IRGC commander, Major General Mohammad Ali Jafari, quickly restructured and integrated Iran's cyber, paramilitary, and clandestine capabilities into a brutal national tool to terrorize Green Movement dissidents into "inaction and passivity."[20]

The Basij used various devious cyber-intimidation methods against activists, such as sending threatening emails and Internet messages, publishing activists' photos and offering rewards for their capture on government Web sites, infiltrating social media networks, seeding disinformation, sowing leader mistrust, and staging false events to arrest people who showed up.[21] The Basij also institutionalized cyber skills on "blogging, social networking sites, psychological operations, online spying . . . mobile phones and their capabilities, and computer games with the aim of targeted entry in the virtual world."[22] In concert with Basij cyber-targeting activities, the IRGC-QF tracked, imprisoned, tortured, or assassinated regime threats.[23] Iran had set in motion a new symbiotic cycle of misattributable/nonattributable cyber-targeting activities married to old-fashioned brute force. Iran would subsequently strengthen its marriage of counterinsurgency (COIN) and cyber activities in Syria.

Syria

In 2012, Iran dispatched IRGC-QF operators and ICT experts, who had mastered their craft in breaking the Green Movement, to Syria to advise pro–Bashar al-Asad forces.[24] Iran sent "several hundred members of the Revolutionary Guards al Quds force" to Syria armed with domestic COIN expertise, money, arms, and advanced equipment "designed to disrupt communications, the Internet, email, and cell phone communications."[25] Operations in Syria fell under the command of Major General Qasem Soleimani, an infamous figure described by General David Petraeus as "truly evil" and characterized by a senior Central Intelligence Agency officer as the "single most powerful operative in the Middle East."[26]

Under Soleimani's authority, Quds Force operators trained proxy Hizballah and Syrian elements in Iranian camps such as Amir Al-Momenin and integrated themselves into key command and control centers across Syria.[27] According to Dexter Filkins, "To save Assad, Soleimani called on every asset he had built since taking over the Quds Force: Hezbollah fighters, Shiite militiamen from around the Arab world and all the money and materiél he could squeeze out of . . . Assad's own besieged government."[28] Inside Syrian operation centers, Quds Force operators initially provided advice on techniques for suppressing social media and deterring civil disobedience, but soon escalated "with all kinds of kinetic options" to crush the rebellion, just like they had done at home.[29] The Quds Force showed a ruthless understanding of cyber-enabled COIN using "their intelligence networks to train the Syrian army how to fight people without killing; how to use force to cause injury, without being accused of a massacre . . . teaching them how to control Web sites and social media and how to jam television channels."[30]

As with the 2009 attacks on the Green Movement, the Quds Force backed up its cyber-targeting activities with brute force. By this time, however, operatives had learned to distance themselves from the Iranian-trained Syrian, Iraqi, and Hizballah proxies doing the dirty work. As a RAND paper pointed out, "Iran has skillfully employed its own special warfare capabilities as part of a long-term regional strategy, using state and nonstate proxies to advance its regional interests."[31] At the same time, the Syrian Electronic Army (SEA) benefited from Iranian expertise, money, and technology to attack anti-Assad social media and Web sites.[32] The SEA "aggressively engaged in a wide range of online activities to punish perceived opponents and to force the online narrative in favor of the Assad regime."[33] The SEA used distributed denial-of-service attacks, jammed online portals, overloaded networks, and used malware to thwart opponents' messages and actions.[34] Supporting the efforts from Iran, the Basij actively disseminated propaganda, developed increasingly advanced cyberspace capabilities, and professionalized offensive paramilitary hacker field training.[35] It seems that the Basij inundated the Internet with disinformation to obscure Iran's true complicity in Syria and redirect any blame as a Western conspiracy to overthrow Assad.

Iran succeeded against the Green Movement and anti-Assad forces by interweaving ICT efforts to identify key human and information networks with brute force. Beginning with Jafari's reorganization of the IRGC, Iran's cyber-enabled COIN was later perfected with Soleimani's operations in Syria. Throughout both campaigns, the Basij cyber force was a "core state instrument of suppression," honing its techniques to provide cover for Iran's ruthless actions.[36] Iran's cyber-enabled COIN is a stunning success, not only for its cyber-SOF hybridization but also for crushing two separate rebellions and never triggering any meaningful Western military response.

Lessons Learned

There are four primary lessons learned from the actions of Iran and Russia that inform a conceptual framework for aligning cyber capabilities to U.S. special warfare operations.

1. There is a distinction between the offensive cyber tools the IRGC-QF and Spetsnaz employed at the tactical level and those that exist at the strategic level. Iranian and Russian operators targeted tactical-level "circumscribed or closed networks,"[37] such as local communications, social media, and regional Internet and logistic infrastructure, while seemingly keeping their more sophisticated open network tools in reserve.

2. Cyber-enabled special warfare is primarily a proxy-executed endeavor that values minimal source attribution. As described by General Gerasimov, "Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[38] Cyber-enabled SOF generally avoid direct force-on-force engagement and strive to operate in the gray areas between peace and war. As observed in Ukraine and Syria, cyber-enabled violence seeks to retain a modicum of deniability, letting proxies execute the dirty guerrilla tactics of assassination, sabotage, and

Insurgents in Donetsk, Ukraine, May 9, 2014 (Wikipedia/Andrew Butko)

ambush. Russia and Iran retained the strategic flexibility to cut and run should things go awry.

3. ICT exploitation, cyber attack, and IO play significant roles in cyber-enabled irregular campaigns. Properly conducted, traditional special warfare campaigns extend to far more than SOF; "they involve the comprehensive orchestration of broader capabilities to advance policy objectives."[39] Likewise, for these campaigns to work, expertise from other arenas must be integrated and synchronized.

4. Cyber-enabled special warfare could both deter conflict and be applied throughout the spectrum of conflict because it "is well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction."[40] Even though Iran and Russia have operated at the malicious end of the spectrum, cyber-enabled special warfare has a constructive side, too. The proliferation of low-cost information and communication technologies benefits partner nations in the building of security, thereby helping to keep conflicts from breaking out.

Cloud-Powered Foreign Internal Defense

Cloud-powered foreign internal defense (FID) is both a technical computing concept and a metaphor for building partner capacity and trust through virtual means. Although not yet fully defined, FID clouds link cross-disciplined communities together to better understand human, geographic, and virtual arenas, and then act conjointly on targeted overlaps. Technically speaking, FID clouds strengthen partner relationships through federated architectures that share data in real time, enhance automation, and diffuse analytic processes. Clouds have adjustable configurations that can take the shape of private, public, community, and hybrid models, each characterized by different software, platform, and infrastructure architectures.[41] FID clouds power encrypted mobile applications, analytic tools, and pooled data through smart technology in the hands of those involved with building security. Although data are virtually tethered to a cloud, the real value lies in enabling the diffusion of timely information to elements at the tactical level. FID clouds are also a metaphor for persistent and vibrant partnerships because, like the technology, the data never rest and the networks do not go idle. This technology is simply a vehicle to empower a deeper, broader, and more contextual community of understanding for the sociocultural, political, and historical factors that all too frequently fuel strife. Instead of reactive relationships characterized by intermittent FID deployments, which achieve a spotty understanding, FID clouds are metaphors for building a more persistent form of capability, capacity, and trust between partnered nations.

Senior Airman from 21st Special Tactics Squadron conducts air traffic control operations on edge of Geronimo Landing Zone at Fort Polk, Louisiana, during Joint Readiness Training Center rotation 13-09, August 2013 (U.S. Air Force/Parker Gyokeres)

FID clouds lay a virtual foundation for future growth of diverse institutions, centers, and laboratories that can help close the seams between U.S. interagency community interests in a country. From a strategic U.S. Government perspective, FID clouds are a pragmatic "partner-centric approach to design campaigns around a partner's core interests, rather than hoping to transform them in ways that have frequently proved to be ephemeral."[42] FID clouds also provide strategic discretion "when a public relationship of a U.S. partner state is problematic because of the partner state's domestic politics."[43]

FID clouds provide other opportunities as well. The technology and relationships that they foster across communities can be quickly scaled up to respond to sudden emergencies such as humanitarian assistance/disaster relief operations, counter-genocide, or noncombatant evacuation missions. They can save money, time, and manpower by feeding information to decisionmakers when time is of the essence. For partner-building efforts, FID clouds can store information hosted by indigenous non-U.S. social media platforms, enriching social network analysis, sociographic mapping, and behavior and sentiment trend analysis. Most importantly, FID clouds spread trust in a creative and super-empowered way that helps to establish long-lasting influence with allies, coalitions, and other partners.

Counternetwork COIN

Counternetwork COIN (CNCOIN) is a simple concept aimed at leveraging, harnessing, and exploiting social media networks.[44] Designed to break an adversary's asymmetric information advantage, CNCOIN employs nontechnical attacks against people to manipulate their perceptions, behaviors, and actions. It puts a military twist on many of the ill-defined yet ubiquitous anti–social networking tactics practiced across cyberspace. Although these tactics are not clearly defined, this article characterizes them as actions that obscure a perpetrator's true identity while he manipulates social media for reasons other than what is stated. Although social media pose a wide array of opportunities for any anti–social network, ranging from criminally exploitative to benignly misrepresentative, from a military perspective, social media present a rich array of information on ways to influence psychological vulnerabilities and an ideal attack platform from which to do it.

There are three broad functional categories for classifying CNCOIN: operations, intelligence, and IO. There are also several techniques within each functional category that help highlight its practice rather than define it outright. These techniques are by no means all encompassing or without overlap.

The first CNCOIN category is operations. It includes but is not limited to cyber-pseudo and cyber-herding operations. A *cyber-pseudo operation* is a classic COIN strategy "in which government forces and guerrilla defectors portray themselves as insurgent units" to infiltrate enemy networks and apply advanced tradecraft inside the network to destroy it.[45] A *cyber-herding operation*, on the other hand, "is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm."[46] The beauty of both techniques is that they drive invisible wedges between insurgents and their command and control by exploiting the inherent weaknesses of communication and communication platforms within every network. Cyber-pseudo and cyber-herding operations prey on an enemy network's natural need to maintain a low signature to survive. Both techniques target intermittent and decentralized insurgent leader communications, manipulating or replacing them, which synergistically leads to growing opportunities for the cyber counterinsurgent.[47] The virtual world simply amplifies the environmental factors because personalities are harder to authenticate as real or fictitious.[48] The lack of command and control authentication, communication frequency, and platform availability are key cyber-pseudo and cyber-herding pressure points to manipulate, misinform, or drive targets toward desired outcomes.

The second CNCOIN category is intelligence, which includes but is not limited to crowdsourcing and social networking analysis (SNA) exploitation techniques. *Crowdsourcing* is a practice that taps into large pools of diverse knowledge willingly provided by participants to solve problems with new ideas, services, or observations and quickly broaden the organizer's perspective.[49] *SNA* visually depicts and measures relationships, their density, and the centrality of social links in order to illuminate social network structures.[50] The social network visualizations, or sociograms, provide a unique window to assess, map, and even predict the intensity of relationship events over temporal, geospatial, and relational horizons.[51]

During the September 2013 Zamboanga City crisis in the Philippines, rogue Moro National Liberation Front (MNLF) forces, dissatisfied with the state of national reconciliation, mobilized a force that seized over 200 civilian hostages, raided businesses, and burned buildings throughout the city.[52] During the crisis, both crowdsourcing and SNA exploitation were successful techniques. Although inadvertently at first, Philippine security forces (PSF) used crowdsourcing techniques to encourage Zamboanga residents to spot and report information on rogue MNLF locations throughout the city. The PSF fused crowdsourced information with intelligence analysis, informing both security and humanitarian operations. The PSF used SNA exploitation to assess populace support for rogue MNLF, as well as to counter and discredit rogue MNLF statements on social media by taking down propaganda Web sites that violated social media user agreements. The PSF also used crowdsourced information to cordon pockets of rogue MNLF forces and raid ad hoc command posts. Although less sophisticated than Iran's cyber-enabled COIN, the PSF thwarted rogue MNLF asymmetric advantage by using social media to target key information and leadership nodes, following up with physical force to defeat them.

The third CNCOIN category is IO and includes but is not limited to cyber aggression, sock-puppeting, and astro-turfing techniques. All three techniques exploit social media anonymously to misrepresent, misinform, and manipulate behavior, sentiment, and actions. Advanced by Diane Felmlee, *cyber aggression* "refers to electronic or online behavior intended to harm another person psychologically or damage his or her reputation" by using "email, instant messaging, cell phones, digital messages, chat rooms, as well as social media, video, and gaming Web sites" and is wider in scope than common cyber bullying.[53] Its anonymous application could cause substantial psychological harm and negative consequences as messages are repeatedly viewed by the target or forwarded across social media sites.[54] Its value to CNCOIN is in exploiting sensitive digital information that could shame, demoralize, or traumatize targets into taking psychologically impaired actions. These deliberate cyber aggression operations could undermine the target's credibility, influence, and power to the point of triggering the target to neutralize himself or other insurgents.

The other techniques, *sock-puppeting* and *astro-turfing*, are defined as fictitious online propaganda tools that disseminate contrived views to fabricate a broader illusion of support or nonsupport.[55] Astro-turfing is the same concept as sock-puppeting, but it is more sophisticated and organized and is undertaken on a larger scale than sock-puppeting.[56] Both astro-turfing and sock-puppeting use virtual personas and "bots" to pump false information across cyberspace to incite reaction or mobilize mass action. As witnessed with Russia's army of trolls, botnets, and hired hackers in Ukraine, astro-turfing networks are awash with an arsenal of propaganda, pictures, and videos stoking conflict and obscuring actions on the ground. Counternetwork IO becomes even more effective when combined with deliberate and misleading cyber-targeting activities, such as IRGC activities during the 2009 Green Movement.

Cyber UW Pilot Teams

The third way to advance U.S. cyber-enabled special warfare is the Cyber UW Pilot Team, a capability meant to harness social media networks to shape a physical environment, establish regional mechanisms, and stitch together area complexes prior to executing UW operations. Cyber UW Pilot Teams are purpose-built around the nucleus of a Special Forces Operational Detachment Alpha, augmented with interagency and technical support, whose mission is to digitally prepare an area for UW operations.[57] The teams undertake the same traditional pilot team tasks that previously were accomplished upon infiltration in the physical domain, but do it through virtual means before they ever put boots on the ground in sensitive, hostile, or denied areas.[58] By operating virtually, Cyber UW Pilot Teams could decrease the time, risk, exposure, and attribution to the U.S. and partnered resistance forces because most of their activities would have been digitally accomplished prior to physical infiltration.[59]

Conceptually, Cyber UW Pilot Teams build human, physical, intelligence, and information infrastructures on social media platforms with cyber tools and advanced techniques. The teams could sharpen their localized language and cultural skills while deepening their understanding of the local human terrain. They could also identify resistance leaders, assess motivations, evaluate resistance capabilities, and assess overall support for U.S. Government objectives while simultaneously evaluating informal hierarchies, psychology, and behavior. In addition, the teams could blend into the white noise of the Internet by tapping into social media networks to "improve U.S. contextual understanding of potential partners and the situation on the ground before the United States commits to a course of action."[60]

Every Cyber UW Pilot Team would have tailored execution authorities and acceptable levels of UW infrastructure development. Once those levels are reached and authorities given, the same team that established the infrastructure virtually would ideally execute its own plan on the ground with the area complex and resistance forces they nurtured online. Cloaked in dual-purpose technology, indigenous equipment, and mobilized networks, these teams would digitally initiate and then physically execute their assigned UW operations from beginning to end.

While there has long been recognition of the strategic role of cyber operations in U.S. national security, this awareness has not fully translated into the development of clear strategic-level thinking and operational capacity. For example, the *Department of Defense Strategy for Operating in Cyberspace* offers few solutions or specifics, but rather reiterates earlier cyber themes in a five-point outline.[61] The lack of well-defined ideas creates a vacuum in cyber strategy that puts the United States in danger of ceding its superior cyber-technological advantage to potential adversaries.[62] In contrast, the asymmetric innovations demonstrated by Iran and Russia present a template for other aspiring regional and global powers to imitate as an irregular pathway to circumventing U.S. military dominance and securing their strategic interests.[63] Moreover, the diffusion of inexpensive yet sophisticated technology increases this potential every year. Iran and Russia have made the American lack of specificity in strategic-level cyberspace documents irrelevant, as the country does not need simply to write about strategy, but must now catch up.

Cyber-enabled special warfare is a strategic-level offensive capability gap that must be filled. Clearly, the United States must aggressively pursue a form of special warfare that integrates cyber operations into tactical-level irregular operations. A recent RAND report on special warfare concluded that "the United States needs to employ a more sophisticated form of *special warfare* to secure its interests . . . and given recent trends in security threats to the United States and its interests, special warfare may often be the most appropriate way of doing so."[64] Cyber-enabled special warfare is the answer in an increasingly interconnected global environment in which physical infrastructure is rapidly being assigned Internet Protocol addresses for assimilation into an "Internet of things." By the year 2020, over 50 billion machine-to-machine devices (compared to 13 billion today) will connect to cyberspace through "the embedding of computers, sensors, and Internet capabilities."[65] Cyber-enabled special warfare bridges the gap between the virtual and the physical by harnessing modern-day information networks and melding them with old-fashioned, face-to-face SOF partner engagement.

Today's global environment impels the United States to adopt cyber-enabled special warfare as a strategic tool of national military strategy. The devastating examples of integrating offensive cyber capabilities into irregular tactics as demonstrated by Iran and Russia pave the way for other U.S. adversaries to soon follow. This article offers the Nation three new options for aligning emerging technology to special warfare missions: cloud-powered FID, counternetwork COIN, and Cyber UW Pilot Team operations. Developing these three concepts to their fullest transcends simply maintaining a U.S. cyber-technology edge; their development projects revolutionary influence across the globe to build critical partnerships and shape issues across the spectrum of conflict. If successfully developed, cyber-enabled special warfare will become a powerful new strategic option for the Nation. JFQ

Notes

[1] General Joseph L. Votel, USA, commander of U.S. Special Operations Command, email correspondence with author, December 18, 2014.

[2] Maren Leed, *Offensive Cyber Capabilities at the Operational Level: The Way Ahead* (Washington, DC: Center for Strategic and International Studies and Georgia Tech Research Institute, 2013), 12, available at <http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf>.

[3] John Arquilla and David Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 2, available at <www.prgs.edu/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf>.

[4] Tom Gjelten, "First Strike: U.S. Cyber Warriors Seize the Offensive," *World Affairs* (January–February 2013), 1–2, available at <www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive>.

[5] Votel.

[6] Dan Madden et al., *Special Warfare: The Missing Middle in U.S. Coercive Options* (Santa Monica, CA: RAND, 2014), 1–4.

[7] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Courier*, February 27–March 5, 2013.

[8] *Towards the Next Defense and Security Review: Part Two—NATO*, HC 358 (London: House of Commons Defense Committee, August 5, 2014), 13.

[9] U.S. Army doctrine defines *unconventional warfare* as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with

an underground, auxiliary, and guerrilla force in a denied area." See Army Doctrine Reference Publication 3-05, *Special Operations* (Washington, DC: Headquarters Department of the Army, August 31, 2012), 1-5.

[10] Michael Gordon, "Russia Displays a New Military Prowess in Ukraine's East," *New York Times*, April 24, 2014, 2.

[11] Tom Fox-Brewster, "Russian Malware Used by 'Privateer' Hackers Against Ukrainian Government," *The Guardian* (London), September 25, 2014, 1–2.

[12] Misha Japaridze, "Inside Russia's Disinformation Campaign," *DefenseOne.com*, August 12, 2014, available at <www.defenseone.com/technology/2014/08/inside-russias-disinformation-campaign/91286/>.

[13] Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," *DefenseOne.com*, September 9, 2014, available at <www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/>.

[14] John Vandiver, "SACEUR: Allies Must Prepare for Russia 'Hybrid War,'" *Stars and Stripes*, September 6, 2014, available at <www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464>.

[15] Ibid.

[16] "Cyber Security Pro: Finland Under Hybrid Warfare Attack," *Yle.fi*, September 13, 2014, available at <http://yle.fi/uutiset/cyber_security_pro_finland_under_hybrid_warfare_attack/7470050>.

[17] Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *World Post*, September 2, 2014, available at <www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html>.

[18] Ibid.

[19] Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society* 9, no. 1 (May 2011), 50.

[20] Mark Dubowitz and Matthew Levitt, *Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development*, Statements, House of Commons Chambre Des Communes Canada, 41st Parliament, 1st sess., May 30, 2013, available at <www.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&DocId=6191680&Language=E>.

[21] Golkar, 62.

[22] Ibid., 63.

[23] Dubowitz and Levitt, 2.

[24] Farnaz Fassihi, Jay Solomon, and Sam Dagher, "Iranians Dial Up Presence in Syria," *Wall Street Journal*, September 16, 2013.

[25] Ephraim Kam, "The Axis of Evil in Action: Iranian Support for Syria," Institute for National Security Studies Insight No. 372 (October 10, 2012), 3, available at <www.inss.org.il/index.aspx?id=4538&articleid=5207>.

[26] Dexter Filkins, "The Shadow Commander," *The New Yorker*, September, 20, 2013, 3.

[27] Fassihi, Solomon, and Dagher.

[28] Filkins, 30.

[29] Dubowitz and Levitt, 6.

[30] "Iran Confirms Sending Troops to Syria, Says Bloodshed Otherwise Would Be Worse," *Al Arabiya*, May 28, 2012.

[31] Madden et al., 2.

[32] Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare, 2013–2014," Institute for National Security Studies Insight No. 536 (April 3, 2014), 1, available at <www.inss.org.il/index.aspx?id=4538&articleid=6809>.

[33] Max Fisher and Jared Keller, "Syria Digital Counter-Revolutionaries," *The Atlantic*, August 31, 2011, available at <www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>.

[34] Ibid.

[35] Gabi Siboni and Sami Kronenfeld, "Iran's Cyber Warfare," Institute for National Security Studies Insight No. 375 (October 15, 2012), 3, available at <www.inss.org.il/index.aspx?id=4538&articleid=5203>.

[36] Dubowitz and Levitt, 6.

[37] Leed, 12.

[38] Coalson, 3.

[39] Madden et al., 1–4.

[40] Ibid., 9.

[41] Department of Defense (DOD) Chief Information Officer, *Cloud Computing Strategy* (Washington, DC: DOD, July 2012), 41, available at <www.defense.gov/news/dodcloudcomputingstrategy.pdf>.

[42] Ibid., 3.

[43] Ibid., 4.

[44] Joint Publication 3-24, *Counterinsurgency* (Washington, DC: The Joint Staff, November 22, 2013), I-2, defines *counterinsurgency* as "comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances."

[45] Lawrence E. Cline, *Pseudo Operations and Counterinsurgency Lessons from Other Countries* (Carlisle, PA: U.S. Army War College, June 2005), 5, available at <www.strategicstudiesinstitute.army.mil/pdffiles/pub607.pdf>.

[46] David B. Moon, "Cyber-Herding: Exploiting Islamic Extremists," in *2007 JSOU and NDIA SO/LIC Division Essays*, Joint Special Operations University Report 007-5 (Hurlburt Field, FL: JSOU, April 2007), 4, available at <www.dtic.mil/get-tr-doc/pdf?AD=ADA495377>.

[47] Cline, 5.

[48] Moon, 15.

[49] Dragos Negoitescu and Mark Blaydes, "Crowdsourcing: Is NATO Ready?" *Three Swords Magazine*, no. 26 (2014), 2, available at <www.jwc.nato.int/images/stories/threeswords/crowdsourcing.pdf>.

[50] Seth Lucente and Greg Wilson, "Red Line: Social Media and Social Network Analysis for Unconventional Campaign Planning," *Special Warfare* 26, no. 3 (July–September 2013), 21–23, available at <www.dvidshub.net/publication/issues/12346>.

[51] Ibid.

[52] Al Jacinto, "Zambo Propaganda, Drama Plays On," *The Manila Times*, September 28, 2013, available at <www.manilatimes.net/zambo-propaganda-drama-plays-on/40435/>.

[53] Diane Felmlee and Robert Faris, "Toxic Ties: Networks of Friendship, Dating and Cyber Victimization," paper presented at the American Sociological Association Annual Meeting, Hilton, NY, August 9, 2013.

[54] Ibid.

[55] Alex Comninos, "Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond," *Academia.edu*, June 2011, 4, available at <http://academia.edu/633706/Twitter_revolutions_and_cyber_crackdowns_User-generated_content_and_socialnetworking_in_the_Arab_spring_and_beyond>.

[56] Ibid., 14.

[57] Patrick Duggan, "UW in Cyberspace: The Cyber UW Pilot Team Concept," *Special Warfare* 27, no. 1 (January–March 2014), 69, available at <http://static.dvidshub.net/media/pubs/pdf_14790.pdf>.

[58] Ibid.

[59] Ibid.

[60] Madden et al., 1–4.

[61] Thomas M. Chen, *An Assessment of the Department of Defense Strategy for Operating in Cyberspace* (Carlisle, PA: U.S. Army War College, 2013), 30.

[62] Ibid., 36–37.

[63] Madden et al., 1–4.

[64] Ibid., 4.

[65] Patrick Tucker, "The CIA Fears the Internet of Things," *DefenseOne.com*, July 24, 2014, available at <www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/>.