Cybermilitias and Political Hackers

Use of Irregular Forces in Cyberwarfare

Recent cyberattacks have grayed the line between political hacker and legitimate combatant. This article explores the possible benefits and drawbacks of cyberconflict and the ramifications of cybermilitias.

Scott D. Applegate
US Army

Politically motivated cyberattacks have increased in recent years, but in almost all cases, they've generally been attributed to unidentified political hackers, or *hacktivists*. These attacks have ranged from mere annoyances, such as the defacement of websites in Japan, to full-scale digital blockades of the target country, such as the 2008 cyberattacks against Estonia. In cases such as Estonia or Georgia, a heated debate continues as to whether the attacks were instituted by a nation-state or if they were merely the work of patriotic hackers defending their country's honor in the digital world. Even if evidence supported these claims, no legal definition of cyberwarfare or agreement on what constitutes an act of war in cyberspace currently exists, and it's unlikely that either will be forthcoming in the near future.

Unlike other domains associated with warfare, cyberspace provides a high level of anonymity; attackers can carry out actions in this domain with little or no attribution. Consequently, nations have little incentive to embrace a definition of cyberwarfare or to formally claim credit for cyberattacks. These types of attacks can be carried out inexpensively, with little or no political ramifications to the nation-state, and give the attacker a distinct asymmetric advantage. If a nation-state can covertly initiate, fund, or guide such attacks, relying on hacktivists to act as a kind of cybermilitia in their stead, they can potentially achieve their political objectives without the burden of attribution or the need to adhere to the Law of Armed Conflict. (For the purposes of this article, I define *cybermilitia* as a loose confederation of hackers conducting cyberattacks under the overt or covert direction of a nation-state against another nation-state to further the strategic, political, or military objective of the initiating state.) This alone implies a benefit to maintaining the status quo of ambiguity, especially for smaller nations that can't compete on a kinetic battlefield.

Recent Examples of Political Hacking

Although the anonymity offered by the Internet makes proving whether nations are engaging in cyberwarfare difficult, many patriotic hackers are suspected of performing several recent high-profile cyberattacks that were backed at least in part by nation-states. The list of nations engaging in political hacking includes Iran, Turkey, Israel, and North and South Korea. I focus here primarily on the People's Republic of China and the Russian Federation as two examples of nations performing these types of attacks, and the ambiguity surrounding them. Russia and China are aggressively building cyberwarfare programs, and China has developed a large body of doctrine and professional publications supporting this new concept.

Russia

Russia has been implicated in several recent, high-profile cyberattacks, including those against Kyrgyzstan, Lithuania, Chechnya, Estonia, and Georgia. In most cases, no definitive evidence tied the Russian government to these attacks; patriotic hackers taking

 1540-7993/11/$26.00 © 2011 IEEE

up the Russian cause of their own accord purportedly performed them. In 2009, a Russian State Duma deputy, Sergei Markov, announced that his assistant, later identified as Konstantin Goloskokov, had carried out the cyberattacks against Estonia. However, rather than clarify responsibility for these attacks, this admission further muddied the waters because Goloskokov has stated that he conducted these attacks on his own—without government support or direction—as "an act of civil disobedience."[1] Many observers and researchers remained unconvinced in spite of Goloskokov's and Markov's claims, noting that it's "unlikely that Goloskokov's scheme, if true, could have been carried out without at least tacit support from the Kremlin. Many point to the fact that Goloskokov has spoken freely about the incident, with no apparent fear of prosecution, as indicating the attack was backed by higher forces."[1]

Many researchers consider the cyberattacks in Georgia particularly suspicious given that they directly preceded military actions on the ground. "Just hours before bombs started falling on certain towns… local Web sites were hit with denial of service (DoS) attacks, in which site servers shut down after receiving a flood of requests. Many targeted sites had high military value, including those run by law enforcement and by media outlets."[2] However, tensions had been rising in this region for several months before the conflict started, and some previous cyberattacks against Georgia occurred in the weeks prior to the start of hostilities.[3]

The methodology of recruiting and enlisting hacktivists for this attack is very similar to that of the attacks against Estonia a year earlier. Detailed instructions, tools, and target lists were posted on Russian-language hacker forums.[4] Who actually posted these instructions, kept track of the targets, and changed them as Georgian websites were overwhelmed remains a mystery, but mounting evidence suggests the Russian government's partial involvement. Security researcher Jeff Carr noted that "the available evidence supports a strong likelihood of GRU/FSB planning and direction at a high level while relying on [Russian political hacker] intermediaries and the phenomenon of crowdsourcing to obfuscate their involvement and implement their strategy."[5]

Russian professional military literature on information warfare is not as readily available as Chinese publications, but many recent articles discuss these topics in the context of Russian military theory. In a 2003 *Russian Naval Journal* article, R. Bikkenin "noted that information conflict has become a kind of military art wherein offensive and defensive actions are used to influence the intellect of civilians and servicemen."[6] Of more interest, Bikkenin defined the concept of an *information weapon* as "a means of eliminating, distorting or stealing information for the purpose of obtaining necessary data after penetrating the security system; blocking of access to information by its legitimate users; and in final account, disorganization of all means of society's life support including the enemy military infrastructure."[6] This definition comes surprisingly close to the actions associated with both the Georgia and Estonia attacks that occurred several years after this article's publication.

China

Chinese hackers have been accused of mounting numerous cyberattacks against both civilian and military targets. Most have focused on espionage, such as the Titan Rain and GhostNet attacks. In the GhostNet attack, a group of Chinese hackers compromised more than 1,200 hosts in 103 countries. According to the Munk Centre for International Studies, "up to 30 percent of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media and NGOs [nongovernmental organizations]."[7] Although researchers investigating the GhostNet attacks have been unable to tie them directly to China or any other state, evidence suggests that these attacks were state sponsored at some level. The Munk Centre also notes that "the list of computers controlled by the GhostNet is significant, and certainly atypical for a cybercrime network. The size of the network is small, and the concentration of high-value systems is significant."[7]

Chinese hackers are known for mobilizing and attacking very quickly during any political crisis. In the week following the accidental bombing of the Chinese Embassy in Yugoslavia, hacktivists attacked numerous US government websites.[8] Shortly after the collision between a US Navy surveillance plane and a Chinese fighter on 1 April 2001, a virtual war erupted in cyberspace between politically motivated hackers in both countries.[9] Although this unofficial cyberwar was clearly the work of hacktivists on both sides of the Pacific, it's an example of how quickly politically motivated hackers can mobilize. This fits in very well with Chinese information warfare theories about the use of cybermilitias and cyberreservists to defend the country against attacks. Xu Xiaoyan, while discussing Chinese information warfare theory, stated that "information mobilization actions include strengthening the mobilization awareness of citizens since even nonmilitary personnel can use a computer as an operational platform" for information warfare.[10]

The *Science of Strategy*, published in China, notes that the concept of the People's War "corresponds not only to low-tech wars but also to high-tech ones. Arm-

ing the masses is to be carried out by organizing established units and deploying militia or reserve units."[10] Chinese information warfare theory has embraced the use of reserve and militia forces in conjunction with traditional forces to defend China's digital frontier. As early as 2005, China had already organized both civilian cybermilitia reserve forces and conventional cyberbrigades in its military,[6] and China doesn't limit its use of cyberwarfare solely to times of war. According to Timothy Thomas, "information attacks in peacetime can cause social disorder and achieve the art of 'winning without fighting.'"[10] Many assume that China is already covertly using cybermilitias to carry out limited engagements in cyberspace, and some of the official cables recently released on WikiLeaks lend support to this assumption.[11]

Legal and Political Considerations

Cyberwarfare has posed some very distinct challenges to the legal frameworks that currently govern warfare between states. Does cyberwarfare meet the criteria of an act of war or, more specifically, an act of aggression as described by the United Nations charter? Do cyberattackers—whether state supported or acting of their own accord—enjoy the legal status of combatant? How can a state conducting a cyberattack differentiate between civilian and military targets? How can a cyberattacker ensure proportionality? In many cases, the use of cyberattacks would violate at least the spirit if not the direct tenets of the Law of Armed Conflict, assuming such laws are applicable to cyberwarfare. Because of this, it might be in many nation-states' best interest to ensure that such laws aren't applicable because it would be virtually impossible to conduct many types of cyberattacks and remain within this legal framework. Such states could also skirt these laws by covertly utilizing political hackers as cybermilitias to conduct attacks for them. In either case, the current level of ambiguity favors the attacker and leaves little recourse to cyberattack victims under international law.

Law of Armed Conflict Considerations

The UN defines aggression as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[12] The first problem with this definition and its application to cyberwarfare is the term *armed force*. While many militaries now treat the computer as a weapon system, no international agreement or legal statute defines it as such. It's highly debatable whether simply using a computer system, or even large numbers of computer systems, to attack a country can be deemed to be the use of armed force under current international agreements. In addition, although cyberattacks can undoubtedly cause serious financial damages, and might under the right circumstances cause physical damage, injury, or death, such attacks are unlikely to damage the territorial integrity or political independence of the target nation. Moreover, no such concept as territorial integrity exists in cyberspace, and the very nature of cyberspace as a boundless, borderless, open domain contradicts the 1648 premise of the nation-state. Consequently, this definition in its current form won't likely be applied to the concept of cyberwarfare. Cyberattacks might not even constitute an attack under current international law. The Geneva Convention defines an attack as an act of "violence against the adversary, whether in offense or in defense," but characterizing a computer attack as an act of violence is difficult.[13] Michael Schmitt and Thomas Wingfield of the George C. Marshall European Center for Security Studies have suggested that rather than trying to determine whether the cyberattack constitutes a use of force, evaluating the results of such an attack against a series of criteria to determine whether they rise to a level that resembles a direct use of force might be more useful.[14] But whereas this approach could provide a framework for evaluating cyberattacks, it requires some form of acknowledgment of computer system use as an act of violence or use of force as well as amendment of current international agreements.

Under the Law of Armed Conflict, armed forces must distinguish between military and civilian targets. Protocol I, the 1977 amendment to the Geneva Convention, states that "parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[13] Distinguishing such targets in cyberspace is sometimes difficult, as the vast majority of systems—both civilian and military—are only identifiable by their Internet protocol addresses and domain names. Not all systems are individually identifiable under domain names, and the widespread use of private IP addressing further complicates matters. Moreover, cyberattackers targeting a nation-state's information infrastructure would almost be forced to attack civilian systems by default to achieve their objectives, because in many countries, the majority of the information infrastructure utilizes civilian systems. Crippling a nation's military communications would probably require a direct attack on the civilian information infrastructure, but such an act would most likely be considered illegal. "A direct attack on a civilian infrastructure that caused damage, even loss of life of civilians, would, I think, be a war crime,"

noted Daniel Ryan, an instructor on cyberlaw at the National Defense University.[15] If such attacks can't be committed legally using conventional forces, nations have a strong incentive to covertly sponsor cybermilitias rather than overtly engaging in such activities and suffering the political and legal recriminations.

Other legal considerations under the Law of Armed Conflict that would have significant implications for cyberwarfare are the concept of proportionality and attackers' inability to maintain tight control on cyberweapons. "The Principle of Proportionality, codified in the Protocol I Additions to the Geneva Conventions, defines as disproportionate any attack in which the incidental damage to civilians is excessive in relation to the military advantage anticipated from the attack."[16] The very nature of cyberweapons makes them difficult to control, and the complexity of the systems they attack breeds unintended consequences, especially if such attacks are carried out by hacktivists and cybermilitias relying on crowdsourcing to escalate their attacks' effectiveness. The military uses numerous algorithms, technical studies, and previous experience to predict an attack's consequences; however, "those consequential analyses are much harder in cyberspace, and so it's hard to apply the proportionality test."[15] Comparing cyberweapons to conventional weapons is difficult, and therefore applying the same legal constructs will be equally difficult.

Combatant Status

What determines whether an individual conducting a cyberattack is legally a combatant, and is this distinction useful in cyberwarfare? The Geneva Convention defines two types of combatants—*privileged* and *unprivileged*. Privileged combatants are defined as forces or personnel participating in hostilities who[13]

- are commanded by a person responsible for subordinates;
- have a fixed, distinctive sign visible at a distance;
- carry arms openly; and
- conduct operations in accordance with the laws and customs of war.

Political or patriotic hackers certainly don't fall within the constraints of this definition. If state sponsored, one could argue that they are being commanded by a person responsible for subordinates. However, they certainly don't wear a fixed, visible sign or carry weapons openly, and many of their actions could be construed as being contrary to the laws and customs of war. Military members conducting cyberattacks on behalf of their nation might also fail to meet this definition. Although members of the armed forces are afforded privileged combatant status, their actions in conducting a cyberattack could actually strip them of that status. Members of the armed forces conducting a cyberattack might be wearing a uniform, but victims won't be afforded the opportunity to see it. Attackers won't be carrying weapons openly—quite the contrary, as most cyberweapons are designed to be stealthy and provide attackers with anonymity. If their actions violate the laws of war, such as by intentionally targeting a civilian system, they automatically lose that privileged combatant status.[13] Unprivileged combatants are those who have violated the laws of war. The difference between these two statuses is that privileged combatants are entitled to treatment as a prisoner of war (POW), whereas unprivileged combatants might be subject to the capturing nation's domestic laws.

In his article "Combatant Status and Computer Network Attack," Sean Watts argues that these criteria might not apply to cyberwarfare and that state affiliation is a far more useful measure.[17] "As a threshold for combatant status in [computer network attacks], state affiliation enjoys solid textual support, appearing as a precondition in well over a century of positive law."[17] Given that cyberattack victims will likely never see their attacker, nation-state affiliation is a far more useful standard for determining combatant status in the context of cyberwarfare. By this logic, if attackers conduct cyberattacks on a nation-state, covertly or overtly, they should be considered a combatant.

Is this distinction useful? The US Department of Justice's Office of Legal Counsel has stated that these criteria "were an incentive to unconventional forces to comport and organize themselves in a manner consistent with the long-standing practices of regular armed forces" when they argued against granting Al Qaida and the Taliban combatant status.[17] The four criteria discussed above are designed to determine whether irregular forces should be granted POW status upon capture. However, in cyberwarfare, capture is very unlikely, so the need for attackers to adhere to these requirements to gain combatant status and POW privileges doesn't necessarily exist from the attacker's viewpoint. The protection that standoff distance and cyberweapon anonymity afford attackers is almost absolute given that most victims can't identify where the attack came from, much less whether the

The very nature of cyberweapons makes them difficult to control, and the complexity of the systems they attack breeds unintended consequences.

individual launching the attack was a legal combatant. This is somewhat different from other weapons that provide attackers enormous standoff distance, such as intercontinental ballistic missiles or predator drones, which leave obvious evidence of the attack's originating nation.

The nation-state covertly employing cybermilitias can achieve limited offensive objectives in cyberspace with little or no attribution and plausible deniability.

Benefits and Drawbacks of Using Cybermilitia

Although there are a number of potential drawbacks to using cybermilitias or hactivists, there are also some very decisive benefits. The strength of these benefits, coupled with the nonattribution afforded to a sponsoring nation-state, makes the employment of these types of forces very attractive, especially when such a state is focused on limited objectives.

Benefits

The attacks on Estonia and Georgia demonstrate several important points about cyberwarfare. In a cyberconflict,

- attackers have a clear and decisive advantage over defenders in virtually all aspects of cyberwarfare. Attackers immediately gain the initiative and most often conduct cyberattacks covertly, giving them the advantage of surprise as well as the benefit of plausible deniability. Initiating the attack forces defenders to respond—often in a manner that attackers can anticipate—and sets the initial conditions for the conflict.
- attackers conduct the attack at the exact time and place of their choosing, while defenders are forced to defend their entire network. Consequently, attackers have a financial advantage—potentially using a single computer to conduct an attack—whereas defending an entire network can be prohibitively expensive.
- attackers can determine the attack's scale and vary the attack mode to cause different desired effects. They can conduct the attacks themselves, or can enlist allies, often hacktivists, to conduct their attacks for them, magnifying both the attack's scale and the effects of plausible deniability.
- attackers, even if identified, are often shielded by the legal ambiguity generated by a lack of applicable international laws covering cyberwarfare.

We can easily infer the potential benefits of employing cybermilitias to conduct offensive operations in cyberspace if the assumption is made—right or wrong—that the Russians did sponsor the attacks on Estonia and Georgia. First, the nation-state covertly employing cybermilitias can achieve limited offensive objectives in cyberspace with little or no attribution and plausible deniability. Although employing hacktivists in this manner might raise suspicion in the international community about state participation, without direct and irrefutable evidence, the initiating nation is protected from political ramifications. If Russia launched a missile into Estonia, causing significantly less damage financially than the cyberattacks did, it would almost certainly receive broad international condemnation. This cyberattack resulted in little more than speculation and international debate.

As I discussed, conducting such an attack gives attackers a distinct asymmetric advantage over the defending nation, and because there's no attribution to the initiating state, there's little threat of a counterstrike. Recruiting actors from political message boards and hacker forums can allow for the rapid mobilization of a very large, ideologically motivated, and technologically sophisticated force and lets initiating nations leverage these individuals' skills and resources at little or no cost. Thus, the initiating state can dramatically increase a cyberattack's size and scale without having to directly employ the personnel or purchase the equipment necessary to conduct such an operation.

Drawbacks

Although attackers certainly benefit from these types of covert actions, there are also some potential drawbacks. The nation-state employing a cybermilitia would have no direct control over the attacks, and it would have difficulty stopping them, once initiated; for example, Estonia and Georgia were still receiving cyberattacks months after the initial assaults on their systems. This lack of control might also potentially prove very damaging as attacks could grow beyond the size and scope intended or target systems and services not initially included in the initiating state's original target set. Overly ambitious hackers who aren't subject to the formal restrictions that govern military organizations could attack sensitive targets, such as healthcare facilities or critical infrastructure, and create circumstances that, if linked back to the initiating state, could be politically devastating or even lead to a physical war. If these attacks were directed against civilian systems, as they most likely would be, the initiating state could be accused of committing war crimes. These types of actions could also lead to the initiating nation being branded as a state sponsor of terrorism if the connection between the hackers and the state is discovered.

Even if the attacks aren't linked to the initiating state's government, they could create the impression that this nation-state is harboring criminals or cyberterrorists. Such an impression could then lead to political or military recrimination. After the 11 September 2001 attacks, the US invaded Afghanistan on the premise that the country was harboring terrorists. Similar action against a country accused of harboring hackers isn't beyond the realm of possibility.

Analysis

Nation-states have little incentive to declare responsibility for cyberattacks. Doing so can potentially expose their armed forces to criminal prosecution if their actions are deemed to be against the laws and customs of war. Although some nation-states might prefer to codify the nature of cyberwarfare under international law, others might find it far more advantageous to maintain the status quo and ambiguity that currently surrounds cyberwarfare. Even if the international community was successful in creating a legal framework to define acts of aggression in cyberspace and implement limitations, this wouldn't likely prove effective. As Stewart Baker, former General Counsel for the National Security Agency, noted in a recent interview on cyberwarfare, "It is a near certainty that the United States will scrupulously obey whatever is written down, and it is almost as certain that no one else will."[15]

Cyberwarfare gives a tremendous asymmetric advantage to the attacker, especially if that attacker is anonymous. If a nation covertly employs hacktivists and cybermilitias to conduct attacks, it shields itself from recrimination while still achieving its strategic objectives. Unless an absolute and undeniable connection is established between the nation-state and the attacker, the attack is legally seen as criminal activity, not as an act of aggression. Even when a connection is established between hacktivists and the state, such a connection doesn't grant the participants combatant status. For example, in the Russia-Georgia cyberattacks, evidence has linked the StopGeorgia.ru forum, which was used to direct most of the attacks, to the Russian GRU/FSB intelligence services.[5] If this is the case, then the Russian government, in essence, used this forum to direct hacktivists as a cybermilitia to accomplish its objectives. However, these hacktivists aren't considered combatants under the law, and their actions have been characterized as criminal activity. The Russian government escaped recriminations that could have resulted from this action and demonstrated a usable model for conducting limited cyberattacks using informal cybermilitias recruited through patriotic messaging, anonymous provisioning, and directed target selection.

The attacks political hackers have conducted over the past decade present significant ramifications for present and future cyberspace conflicts. Politically motivated cyberattacks will likely escalate in both frequency and scale as the Internet becomes more pervasive and enables second- and third-world countries to attack their competitors. In addition, attribution for these types of attacks is likely to remain infeasible because of the anonymity the Internet provides. It's also unlikely that international agreements will be clarified in the near future because cyberattacks give many nations an attack mechanism that can be used with little or no recriminations under the current legal framework. However, this might change if a devastating cyberattack is conducted successfully against a nation-state. A digital 9/11 could quickly motivate the international community to create a legal framework to address this issue, where attacks such as Estonia and George have elicited only discussion and cooperative agreements among allied nations.

Nations such as China and Russia will continue to aggressively develop their information warfare programs, and if current literature is an indicator, these programs will include the use of irregular forces such as hacktivists, militia, and cyberreserve forces. Second- and third-world nations will also explore these tactics given the low cost of entry, lack of attribution, and ability to prosecute attacks successfully. As long as nations can utilize these types of irregular forces to achieve their objectives with little or no recrimination, these methods will remain an attractive alternative to the use of conventional forces. In the hyperpolitical domain of cyberspace, hacktivists are here to stay, and there's a strong incentive for governments to leverage these political hackers as cybermilitias, especially if they can continue do so without the burden of legal or political restrictions. ☐

References

1. C. Arnold, "Russian Group's Claims Reopen Debate on Estonian Cyberattacks," Radio Free Europe Radio Liberty, 28 Feb. 2011; www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html.
2. J. Wagley, "Researcher Says Russian Government Involved in Georgia Cyber Attacks," *Security Management*, 22 Aug. 2008; www.securitymanagement.com/news/researcher-says-russian-government-involved-georgia-cyber-attacks-004509.
3. E. Morozov, "There Is No Need for Kremlin in This Hypothesis, or Why DDOS Is the New Poetry," *Foreign Policy*, 17 Aug. 2009; http://neteffect.foreignpolicy.com/posts/2009/08/17/there_is_no_need_for_kremlin_in_this_hypothesis.
4. M. Landler and J. Markoff, "Digital Fears Emerge after

Data Seige in Estonia," *The New York Times*, 29 May 2007; www.nytimes.com/2007/05/29/technology/29estonia.html?_r=1&pagewanted=2.
5. J. Carr, "Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare," Greylogic, 2009; www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report.
6. T.L. Thomas, "Cyber Silhouettes: Shadows over Information Operations, Foreign Military Studies Office," 2005.
7. Munk Centre for Int'l Studies, "Tracking GhostNet: Investigating a Cyber Espionage Network," 29 Mar. 2009; www.f-secure.com/weblog/archives/ghostnet.pdf.
8. L. Hoffman, "US Government Web Sites Attack by War Protesters," *The Topeka Capital-J.*, 12 May 1999; http://cjonline.com/stories/051299/new_webprotest.shtml.
9. R. Wallace, "It's an All-Out Cyber War as US Hacker Fight Back at China," 1 May 2001; www.foxnews.com/story/0,2933,19337,00.html.
10. T.L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice*, Foreign Military Studies Office, 2004.
11. J. Glanz and J. Markoff, "Vast Hacking by a China Fearful of the Web," *The New York Times*, 10 Mar. 2010; www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html?_r=1.
12. UN General Assembly, "Resolution 3314: Definition of Aggression. Resolutions Adopted by the General Assembly during Its Twenty-Ninth Session," 2010; www.un.org/documents/ga/res/29/ares29.htm.
13. Int'l Committee of the Red Cross, "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977," Int'l Humanitarian Law—Treaties and Documents, 2005; www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079.
14. D.E. Denning, "The Ethics of Cyber Conflict," *The Handbook of Information and Computer Ethics*, K.E. Himma and H.T. Tavani, eds., John Wiley and Sons, 2008.
15. T. Gjelten, "Extending the Law of War to Cyberspace," Nat'l Public Radio, 2010; www.npr.org/templates/story/story.php?storyId=130023318.
16. H.E. Shamash, "How Much Is Too Much? An Examination of the Principle of Jus in Bello Proportionality," *Israeli Defense Forces Law Rev.*, vol. 2, 2005–2006; http://papers.ssrn.com/sol3/papers.cfm?abstract_id=908369.
17. S. Watts, "Combatant Status and Computer Network Attack," *Virginia J. International Law*, vol. 5, no. 2, 2009; www.vjil.org/wp-content/uploads/2010/01/VJIL-50.2-Watts.pdf.

Scott D. Applegate *is a communications officer in the US Army. His research interests include security policy, information technology, cyberwarfare, and information assurance. Applegate has a masters of military studies (MMS) from the Marine Corps University and an MS in information technology with an emphasis in information assurance from the University of Maryland University College. He's currently pursuing a PhD in IT with an emphasis in information assurance at George Mason University. Contact him at Scott.Applegate@us.army.mil.*