The Reality of Cyber Conflict: Warfare in the Modern Age

Paul Rosenzweig

Consider a fairly typical incident from 2014. In March of that year, *The New York Times* reported a persistent cyber threat, known by the code name "Snake," that had infiltrated the cyber systems operated by the Ukrainian government. The program gave its operators full remote access to the compromised systems, which allowed the attackers to steal information as well as insert additional malware to create further harm. Citing confidential U.S. government sources, the newspaper attributed Snake to Russian actors and connected the deployment of the Snake virus to Russian intelligence collection and disruption of Ukrainian command-and-control systems.[1]

At the same time, of course, Russian troops were on the ground in Crimea, and the potential for kinetic conflict between Ukrainian and Russian military forces loomed. Russia formally annexed Crimea just a few weeks later and since then has rather brazenly supported "separatists" in the Eastern Ukraine.

That single episode captures the new reality of military operations in the cyber domain in many ways. At a minimum, cyber conflict will be part of combined operations against physical opponents. Cyber tools will partake of the character of both espionage activities and traditional military activities. At times, the effect of cyber tools may be equivalent to kinetic weapons; at other times, they will be used in a more limited manner to degrade, disrupt, or destroy data and information. In some cases, the origin and source of the tools used in a cyber conflict will be difficult, if not impossible, to discern, rendering attribution of responsibility for an attack problematic; in others, the origins are likely to be crystal clear but the long-term effects of the tool obscured. And all of this will occur at a time when legal norms about appropriate conduct in cyberspace are in a state of flux, without settled definition.

Perhaps even more confusingly, the nature of the conflict in the cyber domain may diverge from settled patterns of military conflict. We will, of course, likely see conflict between nation-states, but we will also see nation-states in conflict with non-state actors and, oddest of all, can also anticipate conflicts in the cyber domain between two non-state parties. How these conflicts will manifest themselves and the nature of the American military response to them will vary significantly in each context.

State vs. State

In a state-vs.-state conflict, we are likely to see cyber activity coupled with conventional operations. For example, since 2014, the cyber-enabled nature of the Russian–Ukrainian conflict has morphed even further. A partial list of cyber activities associated in open-source media with the conflict between Russia and Ukraine over Crimea and Eastern Ukraine would include:

- Russian pre-attack cyber espionage and network mapping of Ukrainian systems;
- Degradation of Ukrainian telecommunications links to Crimea during the Russian invasion, followed by the severing of cross-border telecommunications connections;
- Russian social network sites blocking sites and pages with pro-Ukrainian messages;
- Russia Today (the Russian English-language website) being hacked with the word "Nazi" prominently inserted into headlines to describe Russian actors;
- An IP-telephonic attack on the mobile phones of Ukrainian parliamentarians;
- Russian forces jamming cell phones, severing Internet connections with Ukraine, and seizing telecommunications facilities in Crimea;
- Multiple hacking operations under the #OpRussia and #OpUkraine hashtags including recruitment operations among local cyber-capable actors;
- A large-scale DDoS attack on Russian websites including the Kremlin and the Russian central bank;
- Similar DDoS attacks on Ukrainian news sites, most noticeably during the Crimean "independence" vote, using the DirtJumper botnet; and
- Noticeable activity by hackers of Turkish, Tunisian, Albanian, and Palestinian origin, more commonly attacking Russian sites in support of Ukraine.

One aspect of the conflict worthy of commentary is the evident restraint by both parties. It appears, for example, that no efforts have been made to have a kinetic, destructive effect on critical infrastructure on either side of the border.

But that does not mean that the critical infrastructure is immune. To the contrary, Russia has been strongly implicated in an attack that took six Ukrainian power companies offline. The power outage was caused by a sophisticated attack using destructive malware known as BlackEnergy, which wrecked computers and wiped out sensitive control systems for parts of the Ukrainian power grid. The attack was so severe that it knocked out internal systems intended to help the power companies restore power. While the power generation systems themselves were not attacked, controlling computers were destroyed, and even the call centers used to report outages were knocked out.[2]

State vs. Non-State

Sometimes a state may be confronted by actions by a non-state actor (or perhaps a putative non-state actor whose activity cannot be convincingly attributed to a nation). Consider the recent late 2014 intrusion at Sony, which provides an instructive case both for testing the limits of our understanding of the legal definition of war and for demonstrating that the laws of armed conflict are not the only means of addressing cyber intrusions.[3]

The intrusion, conducted by a group identified as the "Guardians of Peace," exfiltrated terabytes of data from Sony. Some of the data involved unreleased films; other data included embarrassing internal e-mails and proprietary information. Additionally, the hackers demanded that Sony withhold from release *The Interview*, a movie depicting the assassination of North Korean leader Kim Jong-Un. After delaying the release for several days, Sony eventually made the movie available through several alternate outlets. The FBI (relying in part on information provided by the National Security Agency) attributed the intrusion to North Korean government agents.[4] Sony is not saying how great the damage to its financial interests is, but estimates range upward of $50 million.

Here we have a state actor, North Korea, or its non-state affiliates using cyber means to degrade the economic interests of the citizens of another nation, the U.S. How shall we characterize this action? It had no kinetic effects, nor did it significantly affect the American economy. No matter how we view it, Sony is not "critical infrastructure" of the United States (though, oddly enough, the Department of Homeland Security does characterize it as such), so this is not an "armed attack" triggering the laws of armed conflict. Nor is it even an act of espionage. But calling this a state-sponsored criminal act seems to trivialize its geopolitical context.

In the end, the Sony intrusion and Russia's disruption of the Ukrainian power grid seem to reflect a new category of conflict: a quasi-instrumental action by a nation-state or its surrogates that has significant but non-kinetic effects on a target nation. Such "attacks" are not a "use of force" or an "armed attack," but they are likely to generate reciprocal responses from the target state that involve a wide array of state powers. The United States, for example, has publicly announced financial sanctions against North Korea[5] and may very well have taken other, non-public actions in response.

Individual vs. State

Then we have the case of a well-placed or technically proficient individual "attacking" a state, often from inside an organization in much the same way a mole would operate to conduct espionage for a foreign intelligence service. In many ways, this insider threat is the most challenging for a nation because it takes advantage of asymmetric attack capabilities that are especially pronounced in the cyber domain.

Consider the following question: What or who has been the most significant cause of damage to the national security of the U.S. through cyber means in recent years? By any absolute measure, the most likely answer is Edward Snowden—a single individual who, through his own activities or perhaps with a small cadre of a few fellow travelers, caused immense damage to American national security interests. The consequences of Snowden's actions in 2013 include:

- Major damage to formal diplomatic relations between the U.S. and numerous countries identified as targets of U.S. surveillance or "cyber snooping";
- Popular outrage among U.S. allies and friends in Europe over what they perceive as egregious American spying against their own national security interests (even though people generally accept that spying occurs even among friends, it becomes a different matter when it is revealed so publicly); and
- Opportunities for countries like China and Russia to create a perception of false equivalence between the nature of what they are doing (rampant economic espionage) and what the United States has been doing (more traditional national security intelligence activities).

Even worse, Snowden disclosed intelligence sources and methods to the detriment of the United States. As a result, terrorist groups and other governments have changed their communication activities so that the U.S. cannot as readily intercept their communications and understand their plans. China, for example, was alerted to a particularly significant penetration of one of their cyber systems—a penetration that, presumably, has since been terminated.

The scope of the damage caused by Snowden is nearly incalculable, and he did it as an independent actor rather than as an agent of a foreign government, which in past times would have been critical to his ability to operate at this level. Advances in the cyber domain have made it possible for individuals or small groups operating unaffiliated with any nation-state to cause profound, national-level damage that would have been unthinkable in

previous eras. And as non-state entities, they have no sovereign interest that might be leveraged as would be the case in a conflict between states.

Therefore, when we look at cyber conflict and threats to national security, we should not focus exclusively on other national opponents. Rather, our cyber conflict strategy needs to account for the "democratization" of conflict in and extending through the cyber domain, by which we mean simply that the tools and weapons of attack are now widely available and that the use of force—and in the context of modern societies, information is very much a tool of force—is no longer the exclusive province of nation-states.

Non-State vs. Non-State

In this light, the U.S. is in the midst of what scientist-philosopher Thomas Kuhn would call a paradigm shift.[6] It is a shift that is empowering individuals to act with force in ways that were beyond our conception a few short years ago. To see one example of how that paradigm shift operates in practice, reflect on what we might call the "WikiLeaks War" from 2010—a conflict exclusively between non-state actors—and what role (if any) a national government might have in such a conflict.

With the disclosure of classified information from American sources like Chelsea (née Bradley) Manning, WikiLeaks appeared to be launching an assault on state authority and, more particularly, that of the United States, though other governments were also identified. Interestingly, the most aggressive and decisive response came not from government, but from the institutions of traditional commerce. There is no evidence that any of the governments ordered any actions, but the combination of governmental displeasure and clear public disdain for WikiLeaks Editor-in-Chief Julian Assange soon led a number of major Western corporations (MasterCard, PayPal, and Amazon, to name three) to withhold services from WikiLeaks. Amazon reclaimed rented server space that WikiLeaks had used, and the two financial institutions stopped processing donations made to WikiLeaks.

What followed might well be described as the first cyber battle between non-state actors. Supporters of WikiLeaks, loosely organized in a group under the name Anonymous, began a series of distributed denial-of-service (DDoS) attacks on the websites of the major corporations that they thought had taken an anti-WikiLeaks stand, flooding the websites with "hits" to prevent legitimate access to them. The website of the Swedish prosecuting authority, who is seeking Assange's extradition to Sweden to face criminal charges, was also hacked.

Some of the coordination for the DDoS attacks was done through social media, such as Facebook or Twitter. Meanwhile, other supporters created hundreds of mirror sites, replicating WikiLeaks content, so that WikiLeaks could not be effectively shut down. The hackers even adopted a military-style nomenclature, dubbing their efforts "Operation Payback."

When Anonymous attacked, the other side fought back. The major sites used defensive cyber protocols to oppose Anonymous, rendering attacks relatively unsuccessful. The announced attack on Amazon, for example, was abandoned shortly after it began because the assault was ineffective. Perhaps even more tellingly, someone (no group has publicly claimed credit) began an offensive cyber operation against Anonymous itself. Anonymous ran its operations through a website, AnonOps.net, and that website was subject to DDoS counterattacks that took it offline for a number of hours.

In short, a conflict readily recognizable as a battle between competing forces took place in cyberspace, waged almost exclusively between non-state actors.

Anonymous's failure to target corporate websites effectively and its relative vulnerability to counterattack are likely only temporary circumstances. Anonymous and its opponents will learn from this battle and approach the next one with a greater degree of skill and

a better perspective on how to achieve their ends. Many of their more recent attacks, such as the effort to shut down the Vatican's website, have already shown a great deal more sophistication and effectiveness.

Moreover, Anonymous has demonstrated that even with its limited capacity, it can inflict significant damage on individuals and companies. When Aaron Barr, corporate head of the security firm HB Gary, announced that his firm was investigating the identity of Anonymous participants, Anonymous retaliated by hacking the HB Gary network (itself a significantly embarrassing development for a cybersecurity company) and taking possession of internal e-mails that suggested that HB Gary was engaged in some questionable business practices. As a result, Barr was forced to resign his post.

More to the point, Anonymous has made quite clear that it intends to continue to prosecute its cyber war against the United States, among others. "It's a guerrilla cyberwar—that's what I call it," says Barrett Brown, 29, a self-described senior strategist and "propagandist" for Anonymous. "It's sort of an unconventional asymmetrical act of warfare that we're involved in, and we didn't necessarily start it. I mean, this fire has been burning."[7]

Or consider the manifesto posted by Anonymous, declaring cyberspace independence from world governments: "I declare the global social space we are building together to be naturally independent of the tyrannies and injustices you seek to impose on us. You have no moral right to rule us nor do you possess any real methods of enforcement we have true reason to fear."[8] In February 2012, Anonymous went further by formally declaring "war" against the United States and calling on its citizens to rise and revolt.

In many ways, Anonymous conducts itself much as an opposing military organization might conduct itself. In February 2012, for example, it was disclosed that Anonymous had hacked into a telephone conversation between the FBI and Scotland Yard, the subject of which was the development of a prosecution case against Anonymous. That sort of tactic—intercepting the enemy's communications—is exactly the type of tactic any government or insurgent force might use, and by disclosing the capability, Anonymous successfully created uncertainty about how much else it might be intercepting.

In advancing their agenda, the members of Anonymous look somewhat like the anarchists who led movements in the late 19th and early 20th centuries, albeit anarchists with a vastly greater network and far more ability to advance their nihilistic agenda through individual action. And like the anarchists of old, they have their own internal disputes, thus making comprehensive or singular analysis of objectives, methods, and potential points of leverage quite difficult. In 2011, for example, another group called Black Hat effectively declared war on Anonymous because it disagreed with the Anonymous agenda.

Even more important, however, Anonymous and its imitators look like the non-state insurgencies that the U.S. has faced in Iraq and Afghanistan: small groups of non-state actors using asymmetric means of warfare to destabilize and disrupt existing political authority.

A Strategy for Cyber Warfare

What are the implications of this paradigm shift for cyber/military strategy? They appear to be profound.

From Russia and China, we can expect some form of rationality in action. We can understand their motivations. We know why the Chinese are stealing intellectual properties to jumpstart their economy. We can make some judgments about what would and would not annoy them. In the end, they are rational actors just as the Russians were during the Cold War.

In the cyber domain, by contrast, the motivations of the actors are as diverse as the number of people who are there, and the closer you look, the more unclear things become. There are indeed many actors with many different motivations. They are often characterized as irrational chaotic actors. Perhaps it is a little

unfair to call them chaotic, but what seems to unify them is disrespect for authority, for hierarchy, for structure, a dislike of it and an effort to work outside of it. In this structure, they look much more like insurgents than national military forces.

Given this evolving shift from primary state actors to the n-player world of cyber warfare, a compelling case can be made for a new strategy that is relevant to the changed security environment.[9] There are three factors that should guide thinking about a new cyber strategy—factors that are remarkably similar to those that shape counterinsurgency strategies.

- Cyber warfare favors asymmetries. Non-state actors with power nearly equal to the power of governmental actors are going to be the rule, not the exception. They can serve as proxies for state actors, as the Russian "patriotic hackers" do, but they are not nation-states themselves and thus exploit extraordinary flexibility in adapting to evolving conflicts.

- The capabilities of non-state actors are currently rather limited. They cannot take down the electric grid in the United States, for example, but that will change. We have five or perhaps even 10 years at the outside before the capabilities of non-state actors become almost equivalent to those of nation-state actors. Thus, the window of opportunity to get our strategy right is limited, and the U.S. must take advantage of the time while it can.

- The hardest part of the game is attribution. Knowing who the other side is and what their motivations are is the most difficult challenge of all. How does the U.S. deal with that? Who are these people? What are their true motivations? That is not something that can be fixed technologically. In the end, the U.S. must get better at it, but it is not something for which the same confidence in identifying the enemy can be obtained that is often found in the kinetic world.

The military often talks about "whole of government" approaches to winning wars when "winning" is more than just the battlefield victory over an enemy's military force. When it comes to cyber warfare, "whole of government" is the only approach that will work against the array of potential adversaries that are exploiting the cyber domain to accomplish their objectives. Integrating military and civilian activities, collecting intelligence, and building a host nation's security capabilities are all critical elements when combating both state and non-state entities. The full suite of military, intelligence, diplomatic, law enforcement, information, financial, and economic tools will come into play in the new age of cyber warfare.

Organizing for Cyber Warfare

A strategy implies proper organizations and capabilities for fighting a war, but the current manifestations of both are in need of substantial review and investment. During the past several years, many cyber analysts—this author among them[10]—thought the best approach for the U.S. government in dealing with growing cyber threats was to maximize federal government control. What was needed, so the argument went, was a strong cyber czar who had budgetary and directive authority over as much of the government's cyber capabilities and responsibilities as possible in order to centralize planning for and response to cyber attacks.

Unfortunately, this was precisely the wrong approach to take in dealing with cyber warfare as it has evolved over time. Cyberspace is the world's most distributive dynamic domain. More than 3.5 billion people and more than a trillion things are connected to the network across the globe. It changes on a daily, even hourly, basis. The advanced, persistent threats that are intruding on Department of Defense (DOD) .mil computers today did not exist six months ago. They are newly

and purposefully built for that enterprise. A centralized hierarchy seems a poor fit for conflict with a diverse, multifaceted, morphing opponent in a battle space that changes every day.

The "big military" complex does a lot of things well, but one of the things it does *not* do well is turn quickly. The military's conceptual turning radius is like that of an aircraft carrier, not a Corvette. The military's major component in dealing with the cyber threat is U.S. Cyber Command (CYBERCOM), a sub-unified command that reports to U.S. Strategic Command. Though it was established only seven years ago in 2009, proposals are already being made to turn it into an independent command.

Given a lengthy pattern of behavior within the Pentagon, it is reasonable to expect that in spite of best efforts to the contrary, CYBERCOM is likely to feature many of the defining characteristics of very large military organizations: lots of rules; lengthy, hierarchical reporting chains; stifling acquisition rules; and a battalion of staff judge advocates (lawyers) who will oversee cyber activities down to the lowest levels of the organization. In this conflict space, however, a model based on "big military" design is the wrong model to pick. Rather, the cyber force needs to be much more akin to special operations: lean, quick to react, and flexible, with a flat administrative structure and possessing the tactical equivalent of a small operational detachment that has top-tier skills and broad authorities to conduct "special mission operations."[11]

Consider the cyber aspects of some of the recent conflicts America has faced. President Obama continues to consider physical action in Syria or Iraq to confront ISIS. What will ISIS's cyber response be? What might Syria's be? The Syrian Electronic Army has already told us that it is going to counterattack if American troops ever go to Syria, and ISIS has threatened to disrupt the American economy. The complexities of conflict are compounded by tactical interdependences and a lack of actionable intelligence.

- What do we know about their capabilities? On the public record, very little—though, to be fair, this may reflect less a gap in our understanding than the existence of capabilities that have not been publicly disclosed. As far as can be seen from the public sources, we do not have anybody on the inside of many of these non-hierarchical organizations.

- What are their likely targets? We may not know, because we do not have any sense of what their capabilities are or any intelligence on their targeting methodologies or what they think are our soft points.

- Do we have targeted weapons that can find the ISIS or Syrian Electronic Army command-and-control servers and take them out without taking offline the entire Syrian and Iraqi electric grids? I suspect that whatever such weapons we have are limited.

- Do we want to take down the entire Syrian and Iraqi electric grid? No, because that is both what the anti-ISIS militia and the Iraqi government are using for their command and control and what the civilians are using to ameliorate the horrible effects of the warfare they are undergoing.

When it comes to the zeroes and ones of DOD efforts to wage cyber warfare, DOD's organization for battle in cyberspace is typical: offense, defense, functionally focused teams, specified and rigidly envisioned command authorities. DOD speaks of its awareness that "talent" is critical to acquire but hard to find, yet it operates largely within the conventional military model—recruit, train, assign, rotate, and promote—rather than finding and leveraging raw "organic" talent that is optimally suited for this sort of warfare but is very likely not to be found in a conventional military mold.

CYBERCOM has to work trans-domain and trans-COCOM (combatant command), accounting for the nature of the weapons

being used, the diversity and character of actors involved, and the combination of actor interactions. Yet CYBERCOM does not control most of the resources and lacks the authority to dictate to the broad range of largely non-government, private-sector entities that are of critical importance to cyber warfare.

A Separate Command for a Distinct Domain?

One final note: U.S. cyber organization reflects a relatively controversial decision to characterize cyber as a distinct domain. Often, cyber conflict is thought of as a component of information operations (using the cyber domain and related tools to shape perceptions and understanding) or as a subset of electromagnetic warfare (leveraging the same to cause effects on an opponent's physical ability to conduct operations).[12] Both characterizations are plausible, the first looking at the target area of a conflict (particularly the people in the battle zone) and the latter looking at the cognate physical domain (the assets the people are using to wage war). For this reason, many think that cyber weapons, as a tool of warfare, should be no different from other tools that are incorporated directly into the operational planning of geographic combatant commanders.

The counterargument is that it is useful to characterize the cyber domain as a separate domain, if only because its characteristics are sufficiently different in degree from those of warfare in the kinetic realm that they tend over time to become differences in kind. Under this construct, CYBERCOM is seen as akin to SOCOM (Special Operations Command), managing and employing a unique, highly valued capability that is not defined by region and can be used both for strategic effect and to support conventional military operations of the geographic COCOMs.

Whatever the merits of the debate, the U.S. government has chosen its course. For better or worse, we have characterized the domain based principally on the type of tool (or weapon, if you will) that is used.

But that characterization as a separate command resonates with even greater adverse consequences than a mere category mistake. It seems on reflection to be emblematic of a fundamental misperception of the nature of cyber conflict. To be sure, senior officials often speak of the newness of cyber warfare and acknowledge that new ways of thinking are required, but seven years on, most of the military response to cyber vulnerability reflects, to this author, an inability to reconceptualize military organization and response in light of the domain's unique characteristics. For example:

- The principal tenet of U.S. legal policy in the domain was a successful effort to adopt existing laws of armed conflict for cyberspace.

- Each of the military services has created within the service a cyber-focused military organization modelled on the fleet/air force model that governs the organization of kinetic military platforms.

- Similarly, CYBERCOM has organized itself along traditional lines with 13 teams, known as Cyber National Mission Teams, responsible for responding to an attack on U.S. critical infrastructure, accompanied by Cyber Combat Mission Teams. To address a lack of training, CYBERCOM has instituted a training system to create "common and strict operating standards" for U.S. cyber operators.[13]

Perhaps this is the right course. To be fair, the Mission Team approach does look somewhat like a special operations approach of the sort this author has advocated. Looking back 10 years from now, we may conclude that these more or less traditional military approaches to conflict in the cyber domain were the right ones.

Nevertheless, one may be skeptical. Considering how cyber capabilities are morphing into a hybrid form of conflict, some of this

seems misguided. Traditional military law, training, procurement, and organization are insufficiently nimble to be responsive to the democratization of conflict in cyberspace. We are seeing a sea-change in the capability of non-state actors, ad hoc groups, and even individuals that allows them to compete on an almost level playing field with nation-states and do significant damage to our national security interests. If we do not reconceptualize how we are thinking about cyber security, cyber policy, and cyber conflict, we are going to miss the boat.

Conclusion

We are facing a new world that is replete with new challenges and rapidly evolving requirements for new ways to respond to those challenges. Anonymous and its ilk are a harbinger: Power and force are being democratized, and we are not ready for it. We are in the midst of a Kuhnian paradigm shift from a time when nation-states had a monopoly on the use of significant force to a time when destructive potential in cyberspace is increasingly available to anyone with the technical skills to employ it anywhere in the world from anywhere in the world irrespective of borders, authorities, or affiliations.

If this is the case, then our current military strategy for operations in cyberspace is focused on the wrong enemy at the wrong time, using the wrong tools and with the wrong hierarchy. This almost certainly means that we are setting ourselves up for catastrophic failure that will lead to nearly unimaginable consequences. Crafting a relevant and effective set of capabilities and response options is therefore a matter of increasing urgency.

The U.S. must get its cyber act together soon: Time is running out.

Endnotes:

1. David E. Sanger and Steven Erlanger, "Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government," *The New York Times*, March 8, 2014, http://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html?_r=1 (accessed May 18, 2016).
2. Evan Perez, "First on CNN: U.S. Investigators Find Proof of Cyberattack on Ukraine Power Grid," CNN Politics, February 3, 2016, http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/ (accessed May 18, 2016).
3. For a useful timeline of events related to the Sony hack, see Trend Micro, "The Hack of Sony Pictures: What We Know and What You Need to Know," December 8, 2014, http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-hack-of-sony-pictures-what-you-need-to-know (accessed May 18, 2016).
4. Michael S. Schmidt, Nicole Perlroth, and Matthew Goldstein, "F.B.I. Says Little Doubt North Korea Hit Sony," *The New York Times*, January 7, 2015, http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?_r=1 (accessed May 18, 2016).
5. Everett Rosenfeld, "US Sanctions North Korea for Sony Hacks," CNBC, January 2, 2015, http://www.cnbc.com/2015/01/02/us-sanctions-north-korea-for-sony-hacks.html (accessed May 18, 2016).
6. Thomas S. Kuhn, *The Structure of Scientific Revolutions: Third Edition*, (Chicago: University of Chicago Press, 1996).
7. Michael Isikoff, "Hacker Group Vows 'Cyberwar' on US Government, Business," NBC News, updated March 8, 2011, http://www.nbcnews.com/id/41972190/ns/technology_and_science-security/t/hacker-group-vows-cyberwar-us-government-business/#.Vz8S3PkrJpg (accessed May 20, 2016).
8. See "Anonymous to the Governments of the World—Web Censorship," YouTube, uploaded April 25, 2010, https://www.youtube.com/watch?v=gbqC8BnvVHQ (accessed May 20, 2016).
9. I first wrote about this in a paper for The Heritage Foundation. See Paul Rosenzweig, "Lessons of WikiLeaks: The U.S. Needs a Counterinsurgency Strategy for Cyberspace," Heritage Foundation *Backgrounder* No. 2560, May 31, 2011, http://www.heritage.org/research/reports/2011/05/lessons-of-wikileaks-the-us-needs-a-counterinsurgency-strategy-for-cyberspace.
10. Paul Rosenzweig, "The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence," in National Research Council, Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, Policy and Global Affairs Division, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington: National Academies Press, 2010), pp. 245–270, http://www.nap.edu/read/12997/chapter/18#270 (accessed May 20, 2016).
11. For a solid discussion of this approach, see Frank Cilluffo and Sharon L. Cardash, "A Cyber JSOC Could Help the US Strike Harder and Faster," *Defense One*, April 25, 2016, http://www.defenseone.com/ideas/2016/04/cyber-jsoc-network-attacks/127778 (accessed May 20, 2016).
12. See, for example, U.S. Department of the Air Force, "Cornerstones of Information Warfare," 1995, http://www.csse.monash.edu.au/courseware/cse468/2006/cornerstones-iw.html (accessed July 1, 2016), and U.S. Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities*, February 2014, https://blog.cyberwar.nl/2014/02/fird-edition-of-us-army-fm-3-38-cyber-electromagnetic-activities/ (accessed July 1, 2016).
13. See, for example, "Statement of General Keith B. Alexander, Commander, United States Cyber Command, Before the Senate Committee on Armed Services," March 12, 2013, p. 7, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf (accessed July 1, 2016).