THE HOMELAND SECURITY SECRETARY'S MORNING CLIPS

WEDNESDAY, JUNE 1, 2011 5:00 AM EDT

[redacted]

[redacted]

[redacted]

[redacted]

Lessons Of Wikileaks And U.S. Cyberspace Counterinsurgency Strategy (HERF)

Heritage Foundation, June 1, 2011

Abstract: Over the past 10 years, the United States has devoted significant resources to the development of a counterinsurgency strategy for fighting non-traditional enemies on the ground. As the global scandal caused by the unauthorized publication of classified government material on the infamous WikiLeaks Web site has demonstrated, it is time for a counterinsurgency strategy in cyberspace as well. While the U.S. government has authored a number of cybersecurity strategies, they all focus too much on technology and not enough on a comprehensive approach to battling cyber insurgency. This Heritage Foundation Backgrounder explains what the U.S. should do if it wants to win the escalating cyber battle.

The tale of WikiLeaks and its founder Julian Assange demonstrates how the U.S. should fight bad actors in cyberspace. WikiLeaks has become a brand name for the disclosure of government secrets. But the more interesting (and less widely remarked upon) part of the story concerns the reaction to Assange's arrest in Great Britain and the decision of many companies (including PayPal, MasterCard, and Amazon.com) to sever financial relationships with his Web site. Their response turned the WikiLeaks fiasco into a kind of cyber war involving a non-state group of commercial actors. The important decisions, however, had nothing do with technology. They were tough calls made by corporate boards reacting responsibly to an irresponsible act. Undermining WikiLeaks's finances likely played a larger role in hindering access to the Web site than any other effort.[1]

The best way to address cyber conflict is to resist the temptation to view it as a one-dimensional contest of "our electrons" versus "their electrons." Like with any conflict, the best strategy is to examine all factors, seeking to exploit one's own strengths and the enemy's weaknesses. This is the same bitter lesson the U.S. learned in Iraq in 2005. During that conflict, the U.S. military faced a small but dedicated group of stateless actors (in that case al-Qaeda operatives and their sympathizers) who used asymmetric means of warfare to harass American troops and to create chaos for the Iraqi government. The U.S. military, in turn, had no doctrine for dealing with countering the influence of these insurgents. Recognizing that gap in doctrinal training, the Army conducted an extended examination of the problem, led by then-Lieutenant Generals David Petraeus and James Amos. The result was a new field manual on counterinsurgency (COIN).[2] The manual advanced the thesis of coordinated military–civilian measures against insurgents—a thesis that now forms the intellectual framework of all U.S. activities in Iraq and Afghanistan. In Iraq, weaning local leaders off support for al-Qaeda arguably had a greater impact in weakening the insurgency than tracking down and killing insurgents.

The approach to warfare that turned back al-Qaeda in Iraq, and the Taliban in Afghanistan, is the right doctrinal solution for winning in cyberspace. The real lesson of the WikiLeaks war is that malfeasant cyber actors behave, in many respects, like insurgents in a kinetic conflict. The methods for confronting these cyber insurgents will be different from those used to confront armed insurgents in the real world, but the principle should be the same. Since 2000, the U.S. government has authored a number of cybersecurity strategies. They all fall short. They have no real doctrinal foundation. They focus too much on technology and not enough on a comprehensive approach to battling cyber insurgency. The U.S. should develop a cyber-insurgency doctrine first—then a strategy to implement it.

The WikiLeaks War

With the disclosure of classified information, WikiLeaks appeared to be launching an assault on state authority (and more particularly, that of the United States, though other governments were also identified). Confronted with WikiLeaks's anti-sovereignty slant, the institutions of traditional commerce soon responded. None of the affected governments ordered any actions, but the combination of governmental displeasure and clear public disdain for Assange soon led a number of major Western corporations to withhold services from WikiLeaks. Amazon.com reclaimed rented server space that WikiLeaks had used, and PayPal and MasterCard stopped processing donations made to WikiLeaks.[3]

What soon 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" (naturally), began a series of distributed denial-of-service (DDoS) attacks on the Web sites of major corporations that had taken an anti-WikiLeaks stand.[4] (A DDoS attack uses many computers to flood an opponent's server with incoming communications, preventing legitimate efforts to connect to the server by sucking up bandwidth.) The Web site 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 Facebook and Twitter.[5]

Meanwhile, other supporters created hundreds of mirror sites, replicating WikiLeaks content, so that it could not be effectively shut down.[6] The hackers even adopted a military-style nomenclature, dubbing their efforts “Operation Payback.”

When “Anonymous” attacked, the targets fought back. The major sites used defensive cyber protocols to oppose Anonymous. Most attacks were relatively unsuccessful—the announced attack on Amazon.com, for example, was abandoned shortly after it began because the assault did not succeed in preventing customers from accessing the Web site. Perhaps even more tellingly, someone (no group has, to this author’s knowledge, publicly claimed credit) began an offensive cyber operation against Anonymous itself. Anonymous ran its operations through the Web site AnonOps.net, which was subject to DDoS counterattacks that took it offline for a number of hours.[7] In short, a conflict readily recognizable as a battle between opposing forces was waged in cyberspace almost exclusively between non-state actors.[8]

The failure of Anonymous to effectively target corporate Web sites, and its relative vulnerability to counter-attack are likely only temporary circumstances. Both sides 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. Indeed, Anonymous has made quite clear that it intends to continue to prosecute the cyberwar against, among others, the United States.

“It’s a guerrilla cyberwar—that’s what I call it,” says Barrett Brown, 29, a self-described “propagandist” for Anonymous.[9] “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.” 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.”[10]

In advancing this agenda, the members of Anonymous look somewhat like the anarchists of the late 19th and early 20th centuries—albeit anarchists with a vastly greater network and far more ability to advance their agenda through individual action.[11] But even more, they look like the non-state insurgents 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.

Implications for Cyberspace Conflict

The question is: How will governments respond? Are U.S. policymaking systems nimble enough to come to grips with the asymmetric empowerment of the et? More profoundly, has the growth of cyberspace begun a challenge to the hegemony of nation-states that has been the foundation for international relations since the Peace of Westphalia? Policymakers ought to learn at least three lessons about the state of conflict in cyberspace:

Asymmetric warfare is here to stay. The Anonymous challenge to large corporations and to governments worldwide is, in the end, inherent in the structure of the Internet. That structure allows individuals and small groups to wield power in cyberspace that is disproportionate to their numbers. Similarly, states can use electrons to do their fighting for them rather than sending armies into battle. States can also use non-state actors as proxies or mimic the activities of cyber insurgents to hide a government hand behind malicious activities. (It is suspected that China and Russia do precisely that.)This description of the correlation of forces in cyberspace is, in many ways, congruent with similar analyses of the physical world. Terrorists enabled by asymmetric power (IEDs and box cutters) have likewise challenged traditional state authorities. And just as Americans must learn to deal with these kinetic insurgent challenges, so too must they respond to cyber insurgency.

Current capabilities of non-state actors are weak but improving. The current capabilities of organized non-state actors in cyberspace are relatively modest. While DDoS attacks can be a significant annoyance, they are not an existential threat. This state of affairs is unlikely to hold for long. As the recent Stuxnet computer virus demonstrates,[12] significant real-world effects can already be achieved by sophisticated cyber actors. It is only a matter of time until less sophisticated non-state actors achieve the same capability.

Attribution is always a challenge. Determining the origin of an attack can be problematic. Sending a message from a digital device to a provider is akin to mailing a letter. The service provider acts as an electronic carrier that sends the message through routers and servers which deliver the message to the targeted computer. The “attacking” computers may have been hijacked and be under the control of a server in another country. An attacker may disguise its locations by circuitous routing or masking the message’s source identification, similar to fudging a letter’s return address and postmark. A cyber insurgent may strike several countries, multiple Internet service providers, and various telecommunications linkages, all subject to varying legal requirements and reporting standards, which makes tracing the source extremely difficult.

Overcoming these difficulties by technical means alone is a vexing problem—and an unnecessary one. The U.S. government should use all techniques in its arsenal to exploit the weaknesses of America’s enemies.

Counterinsurgency v. Cyber Insurgency

The problem of dealing with non-state actors like Anonymous resembles, in structure, the problem of dealing with a non-state insurgency on the ground in Iraq or Afghanistan, or with a state-sponsored proxy like the Iranian-backed Shia groups in Iraq. There are, of course, significant differences between the two domains. In the "kinetic" world, the goal of an insurgency is often the overthrow of an existing government. As the U.S. Army's Counterinsurgency Field Manual puts it: "Joint doctrine defines an insurgency as an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict. An insurgency is an organized, protracted politico–military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control."[13] WikiLeaks-like insurgents seem to have a different aim—"independence" from government. That independence is premised on weakening political authority over the cyber domain. While the goals may be different, conceptually the challenges pose many of the same problems—how to isolate fringe actors from the general populace and deny them support and refuge and, most of all, the freedom to attack at the time and place of their choosing.

In the past 10 years, the United States has devoted significant resources to the development of a counterinsurgency strategy for combating non-traditional warfare opponents on the ground. COIN requires a complex mix of offensive, defensive, and sustainment operations. In the context of a land-based operation, U.S. doctrine has had to consider a range of issues, including integrating military and civilian activity; collecting intelligence; building up host nation security services; maintaining essential services in-country; strengthening local governance; conducting offensive military operations; and fostering economic development. Each counterinsurgency campaign is different and the building blocks will vary, but these and other aspects will all play a critical role.

Elements of a Cyber Insurgency Strategy

The U.S. government has yet to develop an equivalent COIN strategy for cyberspace. The American strategy must be much more expansive than treating cyber threats as primarily a technical challenge. Concepts that might find their way into a cyber insurgency approach to battling bad actors online include:

Collecting Intelligence. Dealing with cyber insurgents requires human intelligence (HUMINT) on the operation of non-state actors in cyberspace. Rather than concentrating on technical intelligence, "human intelligence" focuses on information collected by human sources (such as through conversations and interrogations). HUMINT can provide all kinds of information on the cyber insurgents, not only the technical means of attack, but motivations, relationships, and finances—identifying weaknesses and vulnerabilities in their network that might not be available from merely deconstructing malicious software or looking through the files of an Internet service provider. Indeed, HUMINT and related intelligence tools may be the only means to positively attribute the source of an attack—one of the most critical tasks in combating cyber insurgents. Current U.S. strategies give short shrift to the critical role of a more comprehensive intelligence effort for cybersecurity. President Obama's National Security Strategy, for example, defines the mission of "securing cyberspace" exclusively in terms of designing "more secure technology" and investing in "cutting-edge research and development."[14] The strategy includes no discussion of the role of intelligence in cybersecurity.

Likewise, when Deputy Secretary of Defense William Lynn outlined the five pillars of the Department of Defense's cyber strategy, he emphasized the technical aspects of the threat and neglected to address the role of intelligence. Intelligence, however, could be crucial to identifying how to weaken the threat other than merely shutting down its servers. Good "ground" intelligence could be the precursor to other means at affecting the enemy (means that might range from a "naming and shaming" campaign to an assault on his financial assets to a direct attack).

Integrating Government and Civilian Action. As in the kinetic world, much of the U.S. effort will require coordination between military and civilian government assets. In cyberspace, the situation has the added layer of complexity posed by the need to coordinate with private-sector actors. President Obama's National Security Strategy rightly emphasizes the importance of public–private partnerships: "Neither government nor the private sector nor the individual citizen," the strategy notes, "can meet this challenge alone.[15]

When coordinated action is done well, it can have a demonstrative impact. In one recent case, the FBI worked with companies that had been identified as being infected with a "botnet" program called Coreflood, malicious software that infects Microsoft Windows-based computers and is designed to steal usernames, passwords, and financial information. According to a court affidavit filed in the case:

In one example, the chief information security officer of a hospital healthcare network reported that, after being notified of the Coreflood infection, a preliminary investigation revealed that approximately 2,000 of the hospital's 14,000 computers were infected by Coreflood. Because Coreflood had stopped running on the infected computers, the hospital was able to focus on investigating and repairing the damage, instead of undertaking emergency efforts to stop the loss of data from the infected computers.[16]

The Coreflood case and cooperative public–private activities, such as the U.S. Computer Emergency Readiness Team (US-CERT) program, demonstrate that despite the myriad legal, cultural, and bureaucratic obstacles, effective cooperation is possible.

For a cyber insurgency strategy to be effective, it is critical that the U.S. develop mechanisms for ensuring that "successes" and "best practices" are translated into a suitable doctrine and become part of the professional development of private-sector and public-sector leaders. Among other needs will be demands for education, training, and experience that qualify public and private actors to be real cyber leaders. A doctrine that addresses public–private cooperation must be a centerpiece of that strategy. No adequate effort to address this shortfall is currently underway.

Building Host Nation Cybersecurity. Strengthening the capacity of friends and allies for network security and resilience has to be an essential part of counter-cyberinsurgency. The more that nations with common purpose and values work together, the more that can be done to shrink the cyberspace available to cyber insurgents. In the case of the recent Coreflood investigation, for example, in response to a request by the U.S. for assistance from Estonia under the Mutual Legal Assistance Treaty between the two countries, law enforcement authorities there advised the FBI of the seizure of several additional computer servers believed to be "predecessors" to Coreflood command-and-control servers in the United States.[17] Estonia has undertaken some of the most innovative efforts to protect its nation's cyber-infrastructure and deal with cyber crimes and cyber attacks. Estonia counts as a first-class cyber ally. The U.S. could use many more such allies. Washington needs to encourage other nations to take similar steps to enhance their capabilities. This might be done through innovative assistance programs, such as the proposed Security for Freedom Fund (intended to assist other countries with their development of homeland security systems), or by cooperative agreements that model the U.S. SAFETY Act (which provides liability protection to companies that develop innovative new technologies).[18]

The foregoing is just a start—other questions of resilience and offensive operations will also need to be addressed. These kinds of initiatives reflect how all the nation's resources should be employed in the cyber war. To win the battle for cyberspace, cyber strategy must become much more multifaceted. The U.S. can, as it did in Iraq, wait until the need for such a strategy is brought home by failures on the ground. Or, the U.S. can, more wisely, see the WikiLeaks war as a wake-up call and begin the necessary doctrinal thinking now.

—Paul Rosenzweig is Visiting Fellow in the Center for Legal & Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.

[redacted]