February 2011

Policy Outlook
GEORGE C. Marshall INSTITUTE

Wikileaks and Cyberspace Cultures in Conflict

Eric Sterner,
Fellow, The George C. Marshall Institute

INTRODUCTION

Every few months, Wikileaks and its founder, Julian Assange, make headlines for publicizing yet more titillating information passing through the U.S. government's classified systems. Each round of publication does real damage to U.S. national interests, compromising relations with other countries and revealing to current and potential adversaries the internal thought processes of the U.S. government. Policymakers tend to approach these problems episodically -- they view Wikileaks as a specific challenge. It may be that, but it also symbolizes a burgeoning conflict between two differing views of cyberspace and how it relates to society. One perspective generally holds that cyberspace must be managed in such a way that conforms it to society's existing institutions, particularly in matters related to national security. Another philosophy holds that cyberspace is fundamentally reordering society and that, in doing so, it will unleash new possibilities in the story of human liberty. That conflict will run for decades, with consequences not just for U.S. national security, but for the very future of cyberspace.

WIKILEAKS

In December 2010, Wikileaks released some 250,000 classified diplomatic cables that embarrassed policymakers around the world, exposed classified government activities, and provided ammunition to one side or the other, in any number of public policy debates—debates not limited to the United States.[1] More dire, the most recent release included information that identified critical infrastructure vulnerabilities. Earlier mass releases of classified information and unfiltered military reports from Iraq and Afghanistan placed the lives of U.S. allies and pro-democracy forces at risk by, among other things, giving terrorist groups a "hit list."[2] In short, Wikileaks is successfully waging a concerted disclosure campaign that, intentionally or not, damages U.S. national security and interests via cyberspace. The group's founder, Julian Assange, for example, has primarily described his purpose as enhancing public insight into the operations of large institutions. According to Assange, Wikileaks' goal is to create "a world where companies and government must keep the public, or their employees, or both, happy with their plans and behavior."[3] To that end, he seems to

1601 North Kent Street, Suite 802 • Arlington, VA 22209
Phone (571) 970-3180 • Fax (571) 970-3192 • Email: info@marshall.org • Website: www.marshall.org

believe that secrecy of any kind (and, perhaps by extension, privacy) cannot be justified: "The more secretive or unjust an organization is, the more leaks induce fear and paranoia in its leadership and planning coterie. Since unjust systems, by their nature induce opponents, and in many places barely have the upper hand, mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance."[4] Yet Assange ignored repeated warnings from the U.S. government that he was placing lives at risk and quickly adopted the language of warfare, tweeting, "The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops," and threatening to unleash the information equivalent of a "thermonuclear device" if he was arrested on pending sex crime charges.[5] Setting aside Assange's motivations, Wikileaks' success at compromising classified information over time represents a kind of 21st century cyber siege.

Unsurprisingly, the Obama administration initially attempted to control the political damage, both at home and abroad, by downplaying the importance of the latest leaks publicly while apologizing to foreign leaders for insulting them in official government documents or compromising their interaction with the United States. Defense Secretary Robert Gates told reporters, "I've heard the impact of these releases on our foreign policy described as a meltdown, as a game-changer and so on…I think those descriptions are fairly significantly overwrought. . . . Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest."[6] Summing the results of a trip through the Middle East, Secretary of State Clinton concluded, "A lot of people were reassured…They got their questions answered and joke about it and realize we're going to keep doing business, and nothing was going to slow down our outreach and our diplomacy."[7]

> … Assange and Wikileaks have demonstrated that a very small group of individuals can now use cyberspace to do massive damage to U.S. national security. In so many ways, Wikileaks only represents the practical manifestation of a threat long feared.

Nevertheless, even as international leaders publicly reassure one another that all is well and shift blame for the damage on to Assange or ungracious diplomatic reporting by low-level officials, the damage will be long-lasting, leading officials around the world to speak less candidly with one another, both to domestic and foreign interlocutors. Instead, we are likely to see greater posturing, less constructive interaction, and less trust. Assange's mission may have been to undermine the United States as an "unjust system," but he has also done real damage to the very gears that enable diplomacy to take place. If Churchill's aphorism, "To jaw-jaw is better than to war-war," has any truth to it, Wikileaks has made the former more difficult.

Against this backdrop, policymakers face ambiguity about how to prevent repeat episodes. Some tools are case-specific. Swedish sex crime allegations against Assange resurfaced, leading to his arrest in Great Britain. (As of this writing, Assange has been released on bail.) Companies that had enabled Wikileaks to function, ranging from server farms to bill collectors, severed their relationships, making it difficult for Wikileaks to maintain its online capabilities. The Justice Department is investigating and some have called for Assange's prosecution under the Espionage Act of 1917. Others have further argued that the United States should wage a cyber "war" against Wikileaks much as Wikileaks is doing against the United States.

Wikileaks supporters respond by defending the principles of government transparency, accountability, and free speech rights and by launching anonymous cyber attacks on those companies that severed relationships with Wikileaks and individuals who criticized Assange or the website.[8] So much for principles of transparency, accountability, and free speech. Much of this response appears loosely coordinated, at best.

Ultimately, the specific matters of Assange and Wikileaks liability in the damage to U.S. national security and any deaths that result from their acquisition and publication of classified material will be decided in the courts, both of justice and public opinion. Meanwhile, internal investigations and prosecutions of leakers will proceed apace, along with corrective actions to minimize the prospect of repeating such massive data losses.

As long discussed in policy circles concerned with the national security implications of cyberspace, Assange and Wikileaks have demonstrated that a very small group of individuals can now use cyberspace to do massive damage to U.S. national security. In so many ways, Wikileaks only represents the practical manifestation of a threat long feared.

CYBER CULTURES IN CONFLICT

A larger question looms. Wikileaks represents a growing trend that will undermine the long-term utility of the internet for commerce and governance. It's customary to think of cyber conflict in terms of actions between cyber actors. Indeed, that may be the best framework for developing public policy, which must ultimately deal with the specifics of the conflict. Analytically, however, it may be fruitful to view cyber conflicts through the lens of culture, because that conflict may have longer term implications for the future of cyberspace than the end result of any specific interaction.

Wikileaks and Assange represent a mindset as much as a specific security threat to the United States. The mindset raises long-term challenges for U.S. national security. Even should the United States successfully deny Wikileaks access to cyberspace and punish it in some fashion for harming U.S. national security, other individuals and organizations will spring up and perform the same function. Indeed, multiple mirror websites sprung up with archived Wikileaks data when the latter's web presence declined. Former Wikileaks associates have already started a new entity under the moniker "OpenSecrets.Org." Writing in *The Washington Post*, Tim Hwang calls them expansionists, "who hold that the Web should remake the rest of the world in its own image. They believe that decentralized, transparent and radically open networks should be the organizing principle for all things in society, big and small."[9] One often finds a belief that cyberspace also liberates the individual, that it empowers people to rise above the artificial constraints that social institutions place upon them. Thus, for expansionists, it becomes essential to the spread of human liberty. Expansionists subscribe to a certain worldview and often ascribe to themselves some higher responsibility to a principle that should exempt them from state authority.[10] Thus, some give little thought to "hacktivism" against

entities that do not share their worldview, ranging from corporations to governments. In other words, Wikileaks only represents a surge in the tide of an expansionist worldview. Of course, it is not possible to define a group that calls itself "expansionist" and subscribes to a specific doctrine. Rather, expansionism as used here reflects a strain of loosely consistent thought when it comes to discussions of cyberspace and its relation to society.

> Instead, the "attack" was on a fundamental trust in cyberspace as a means of executing a national security function, i.e., distributing classified information to people who need it and have been vetted to see it while maintaining its classified nature. This may or may not have been the intent of the leaker or Wikileaks, but that will likely be one consequence of their actions.

Expansionists exist against a backdrop of a young generation that lives an "expansionist" lifestyle, happily sharing information about themselves, each other, life, politics, and business for all to see on the internet—information that earlier generations wouldn't have thought about sharing with their neighbors. For many of them, large institutions and organizations, such as governments, are not entitled to privacy or secrecy. Institutional attempts at such "un-expansionist" behavior signify evasion, an attempt to escape accountability to a larger society, simple technological conservatism, or an outdated worldview. If the boomer generation encouraged itself not to trust anyone over 30, the internet generation seems inclined not to trust anyone who's not completely plugged in.

This may partly explain the confluence of events that allegedly led 23-year old Bradley Manning, reportedly disenchanted with the Army and U.S. foreign policy, to determine unilaterally that the classified information to which he had access belonged in the public domain. Manning, a low-level Army intelligence analyst in Iraq, reportedly worked with classified networks that gave him access to tens, even hundreds, of thousands of classified documents, which he first offered to well-known hacker Adrian Lamo, with an eye toward publication. Lamo turned him in to authorities over concerns that Manning was placing lives at risk. While the Army continues investigating, there are parallels between the information Manning offered Lamo and the information that appeared on Wikileaks. Manning's personal history is somewhat unique and his motives diverse, but he appears to have found a home in the hacker culture that embraces an expansionist view of cyberspace and its relationship to society.[11] The Manning case highlights the challenges that a generation accustomed to an expansionist experience of cyberspace creates for institutions with other expectations for cyberspace.

That other perspective tends to hold the view that cyberspace exists as a tool of society and that it should conform to established relationships, values, and laws. While such instrumentalists accept that cyberspace will lead to broad social and economic change—one cannot help but notice that Amazon.com is replacing the corner bookstore and Google the library—they still view it as accountable to society's institutions. That generally leads them to try to torque it into existing legal and secrecy practices and procedures. While expansionists embrace the mantra that "information wants to be free" in the belief that content should be permitted to flow across networks without restriction, instrumentalists see value in it and the infrastructure that created it. They often generally find it necessary to secure that value for

those that invest the time and effort to create information and the infrastructure over which it flows. Thus, content providers place content behind "pay-to-look" firewalls while service providers seek to charge more for greater use of their bandwidth.

When it comes to national security and cyberspace, the government has largely approached the issue from an instrumentalist perspective. It is naturally, and rightly, concerned with how cyberspace might be used as an instrument of power by those who wish to harm the United States, its allies, and their interests.

Wikileaks, its imitators, Bradley Manning, and the similarly-minded, represent something altogether different. They did not attack the United States by using cyberspace to attack America's power grid or other critical infrastructures. Instead, they compromised an instrumentalist use of cyberspace. That is, they recognized that the government's growing use of cyberspace created an unprecedented opportunity to reveal information that was not intended for distribution outside certain vetted channels. That opportunity only existed because the government sought to use cyberspace to improve government functions. Manning would not have had access to so many files or found them so easy to allegedly duplicate and move out of secure systems without the government's adoption of cyberspace as a tool of collecting, sorting, and disseminating classified information internally. Cyberspace enabled the leaker to act on an unprecedented scale. Imagine attempting to physically copy over 250,000 classified documents, many of which no doubt ran to multiple pages, and sneak them out of a war zone multiple times. Nothing tangible, such as a power grid or command and control system was destroyed, or even hampered. Instead, the "attack" was on a fundamental trust in cyberspace as a means of executing a national security function, i.e., distributing classified information to people who need it and have been vetted to see it while maintaining its classified nature. This may or may not have been the intent of the leaker or Wikileaks, but that will likely be one consequence of their actions.

The clash of these two cultures has intensified with cyberspace's penetration of mass society. More often than not, it plays out in courtrooms and legislatures in debates over such things as intellectual property rights, copyright laws, and net neutrality. Government's role in this space has been that of neutral arbiter trying to develop solutions that best serve the public interest. (That may be a charitable view, but one does find government officials on both sides of public policy debates reflecting a conflict between expansionist and instrumentalist perspectives.)

UNDERMINING TRUST

Unfortunately for both cultural mindsets, the success of their perspectives depends on maintaining trust in cyberspace, which the very existence of their conflict undermines. Cyberspace and its tools enable one to create, collect, organize, and analyze data ranging from individual web browsing, spending patterns, physical movements and entertainment preferences to mass financial and traffic flows. This is an unprecedented amount of power, the control and consequences of which society has not mastered.

Expansionists are understandably concerned that such tools can be used to invade privacy and manipulate groups. They tend not to trust such tools in the hands of large, impersonal organizations, such as governments or companies. While the appropriateness, efficacy, and legitimacy of such conscious intrusions into an individual's behavior in cyberspace can be debated, the power that the ability to conduct such intrusions represents cannot. Legitimate concerns have been raised about the use of various electronic intelligence tools in the United States as a response to the attacks of 9/11.[12]

Setting aside concerns about authorized intrusiveness, the prospect for abuse also exists. Indeed, a federal judge ruled last year that a warrantless wiretapping program established to combat terrorism violated the law.[13] The Electronic Frontier Foundation, an organization that holds technology is "empowering us as speakers, citizens, creators, and consumers," has programs dedicated to documenting and countering what it believes to be government abuse of cyberspace, most notably in privacy rights and security.[14] The Foundation recently released a report based on information obtained under the Freedom of Information Act that predicted 40,000 potential violations of law, executive orders, or other regulations governing intelligence investigations.[15] The Foundation's estimate represents an analytical leap that may be highly suspect, but even a fraction of that number of potential abuses should raise serious concerns.

Indeed, cyberspace creates many such opportunities that were unthinkable a generation ago. Some cyberspace mechanisms may be particularly vulnerable to certain kinds of abuses. For example, one type of router may fail to create password traps for frequent use of the wrong password or maintain logs on attempts to enter a cyber account, making it nearly impossible to confirm whether an account has been, or has not been, "tapped" by government authorities or internet service provider insiders.[16] In other words, an intrusion in and of itself would leave no evidence that could be used to hold an intruder accountable to whatever higher authority exists.

Whereas government's authorized use of cyberspace to conduct investigations and abuses of that authority may undermine expansionist trust of large institutional users of cyberspace, involuntary or negligent behavior may also undermine trust in cyberspace—among instrumentalists—as a useful mechanism for some substantive activities. For example, poor security on the part of instrumental data aggregators has contributed to instances of massive numbers of individuals seeing their privacy violated by cyber criminals. Criminals routinely break into cyber systems and steal massive amounts of personal and financial data. (The sin of omission here is a failure to provide adequate security; it should be noted that someone still had to launch a successful attack.) Thefts of personal account information hit millions of users annually. Just recently, the Justice Department indicted a Malaysian for hacking the U.S. Federal Reserve system and possessing 400,000 stolen credit and debit card numbers.[17] A hacker illicitly entered the Virginia Department of Health Professionals and compromised 8 million patient records.[18] The consulting firm, Deloitte, identified over 100 million credit card accounts at risk due to the existence of malware on systems used by an online payment facilitator.[19] In short, cyberspace changes the scale of well-established problems, such as the

need to ensure privacy while conducting legitimate investigative activities, the need to prevent abuses of investigative authorities, and the harm done to individuals by criminals.

Thus, Wikileaks can claim some sympathetic ears when it argues that its decision to air massive amounts of internal information publicly is merely holding organizations such as states, banks, and multinational corporations accountable to the public.[20] As the latest Wikileaks episode reveals, the organization is not alone in such sentiments. Indeed, it allied itself with several multinational media organizations that assert a similar responsibility.[21] Nevertheless, expansionist-motivated attacks on the instrumental use of cyberspace, such as Wikileaks itself and pro-Wikileaks hacktivism, undermine fundamental trust in cyberspace as an institutional means of conducting activities. Already, the phrase "Don't put it in an e-mail if you don't want to see it on the evening news," is commonplace. Similarly, the government is likely to step back from the kind of extensive reliance on cyber distribution of intelligence information as a result of the Wikileaks releases. It is easy forget that much of the increased sharing in intelligence information was undertaken in response to the 9/11 Commission's conclusion that stove-piping intelligence channels was a contributing factor to the successful attack. Restricting access to data will, inevitably, mean that an individual with a legitimate need does not have access to certain kinds of information. The benefits of such restrictions may well exceed the costs, but that does not mean the costs are zero. Ironically, if large social, political, and economic institutions step back from the use of cyberspace because they lose trust in cyberspace, its propensity to re-order society productively, as expansionists envision, will likely diminish.

Ironically, if large social, political, and economic institutions step back from the use of cyberspace because they lose trust in cyberspace, its propensity to re-order society productively, as expansionists envision, will likely diminish.

QUESTIONS FOR THE FUTURE

It is not entirely clear how a conflict between two different cultural views of cyberspace will unfold. The conflict will play out for decades, as most cultural conflicts do, with different strains rising and falling in their dominance at varying times. As it has thus far, this contest will unfold throughout society's existing institutions, changing them along the way, destroying some, and creating new ones.

The culture clash will present the United States with important national security questions:

- How will/should cyberspace change government's structure and capabilities its existing security missions? How much dependence on institutions it does not control can the United States government accept in the performance of its constitutional responsibilities? Do the criteria used for determining whether something should be classified need to change in the light of 21st cyber technologies? How can the government adjust to new generations of personnel in its national security institutions who may not share the assumptions that underlie the creation, organization, and operations of those institutions? How

will it detect the rise of cyberspace threats that do not originate with a traditional nation-state, or even well-defined international actors? How will it respond to such threats?

- Must the United States government more assertively extend the concepts of sovereignty into cyberspace in order to protect American use of it? If so, how would such an extension affect cyberspace?

- How will the U.S. government act as a neutral arbiter among society's competing interests in light of its own interests in the outcome of some debates, particularly as they relate to its fundamental responsibility to provide for the country's security? (As important, how will it recognize its role?) Can it reconcile institutional interests in privacy/security with expansionist expectations for cyberspace's transforming capabilities?

- How will the U.S. government enable the entrepreneurial spirit of innovation to continue creating new technologies, businesses, and applications without creating new vulnerabilities for the nation as a whole? How will it avoid regulatory capture that compromises the public interests while still partnering with information technology firms to promote security and productivity? How should it treat private owners and operators of cyberspace infrastructure in light of its responsibility to protect the United States and its interests? What responsibilities and liabilities should those infrastructure providers be subjected to in light of U.S. dependence on them for its access to and use of cyberspace?

In debating each issue, parties will bring a variety of perspectives to the table. In understanding their positions, it will be helpful to know whether they view cyberspace as the horse or the cart.

ENDNOTES

[1] Anne Flaherty, "US: WikiLeaks has hurt US foreign relations," *The Washington Post*, December 7, 2010.

[2] Robert Winnett, "Wikileaks Afghanistan: Taliban 'hunting down informants," *The Telegraph* (UK), July 30, 2010.

[3] Ryan Singel, "Immune to Critics, Secret-Spilling Wikileaks Plans to Save Journalis…and the World," *Wired*, July 3, 2008.

[4] Christopher Torchia, "Intellectual Life of Wikileaks Chief," *The Washington Post*, December 14, 2010. In this case, Assange seems not to accept any legitimate public interest in secrecy.

[5] Marc Thiessen, "You're either with us, or you're with WikiLeaks" *The Washington Post*, December 7, 2010.

[6] Craig Whitlock, "Gates: Warnings of Wikileaks fallout overblown," *The Washington Post: Checkpoint Washington blog*, November 30, 2010.

[7] Robert Burns, "Clinton tour showed limits of WikiLeaks damage," *The Washington Post*, December 4, 2010.

[8] Peter Svensson "WikiLeaks cyberbrawl is battle of amateurs," *The Washington Post*, December 13, 2010; Raphael G. Satter and Jill Lawless, "Protests, cyber-skirmishes rage over WikiLeaks," *The Washington Post*, December 10, 2010; Ian Shapira and Joby Warrick, "WikiLeaks' advocates are wreaking 'hactivism'," *The Washington Post*, December 12, 2010; Associated Press, "Hackers Strike Back to Support Wikileaks," *Wall Street Journal.com*, December 8, 2010.

[9] Tim Hwang, "WikiLeaks and the Internet's Long War," *The Washington Post*, December 12, 2010.

[10] Ryan Singel, "Immune to Critics, Secret-Spilling Wikileaks Plans to Save Journalism…and the World," *Wired.com*, July 3, 2008.

[11] Kevin Poulsen and Kim Zetter, "U.S. Intelligence Analyst Arrested in Wikileaks Video Probe," *Wired.Com*, June 6, 2010; Ellen Nakashima, "Messages from alleged leaker Bradley Manning portray him as despondent soldier," *The Washington Post*, June 10, 2010; Ginger Thompson, "Early Struggles of Soldier Charged in Leak Case," *The New York Times*, August 8, 2010.

[12] The author does not necessarily share those concerns, but neither should they be lightly dismissed.

[13] Charlie Savage and James Risen, "Federal Judge Finds N.S.A. Wiretaps Were Illegal," *New York Times.com*, March 31, 2010. Available at http://www.nytimes.com/2010/04/01/us/01nsa.html (Accessed January 12, 2011). The debate over warrantless wiretaps and similar tools touches on issues of law enforcement, intelligence collection, and the President's Constitutional authorities as Commander-in-Chief and his statutory authorities under laws passed in response to 9/11 that go well beyond the scope of this essay.

[14] See, https://www.eff.org/. Much of the foundation's work reflects an expansionist view of cyberspace. The American Civil Liberties Union also issued a report in 2009, *Reclaiming Patriotism: A Call to Reconsider the Patriot Act*, (New York: American Civil Liberties Union, 2009), which raises concerns about National Security Letters to obtain personal information, including cyber activities, without judicial review. Without commenting on the validity of the report, it reflects the kind of reporting that expansionists point to.

[15] Electronic Frontier Foundation, Patterns of Misconduct: FBI Intelligence Violations from 2001-2008, (Washington, DC: Electronic Frontier Foundation, 2011), available from the EFF. The 40,000 figure is an EFF estimate, extrapolating from self-reported violations to the Intelligence Oversight Board and an Inspector General Report covering the period 2003-2006.

[16] See, for example, Tim Greene, Legal wiretap mechanisms may be open to abuse within ISPs, *Newtork World*, July 30, 2010. Available at http://www.networkworld.com/news/2010/073010-black-hat-wiretapping.html. (Accessed January 12, 2011).

[17] U.S. Department of Justice, United States Attorney Eastern District of New York, "Press Release: Malaysian National Indicted for Hacking into Federal Reserve Bank," November 18, 2010.

[18] Robert Mueller, III, Director of the FBI, Address to the Commonwealth Club of California, October 7, 2009. Available at http://www.fbi.gov/news/speeches/cloak-and-dagger-in-the-virtual-world-the-fbi2019s-fight-against-cyber-threats. (Accessed on December 17, 2010.)

[19] Center for Security and Privacy Solutions, Deloitte, *Cyber crime: a clear and present danger, Combating the fastest growing cyber security threat*, 2010, p. 5.

[20] Julian Assange, "The truth will always win," *The Australian*, December 7, 2010. Assange also indicated that Wikileaks possessed information from a corporate executive's hard drive cache that he would use to "take down" a major bank. Nelson D. Schwartz, "Facing Threat from Wikileaks, Bank Plays Defense," *The New York Times*, January 2, 2011. Available at http://www.nytimes.com/2011/01/03/business/03wikileaks-bank.html?_r=1&sq=Wikileaks&st=cse&scp=2&pagewanted=all. (Accessed January 5, 2011).

[21] WikiLeaks has coordinated prior quasi-exclusive access to and publication of its materials with several traditional media outlets: *The Guardian* (UK), *El Pais* (Spain), *Der Spiegel* (Germany), and *The New York Times*, (US).