Commentary

The Death of Secrecy: Need to Know...with Whom to Share

Bowman H. Miller, PhD

The US envoys expelled from Mexico City and Quito for remarks made in cables to Washington were among the first victims of WikiLeaks, but there will be more. The only "crime" these ambassadors committed was reporting candidly in accordance with the best traditions and expectations of the US Foreign Service. While there will doubtless be many more casualties of such global disclosure manias, the real victims may encompass other entities and processes that will suffer the second-order effects of these disclosures. Analysts as well as policy- and decisionmakers should be concerned, for these effects are likely to endure and to prove very damaging. What is truly endangered now is the ability to keep anything secret, along with the ability to write for or brief policy- and decision makers with as much candid, relevant information as possible. Wary of having sensitive information revealed on the Internet, foreign interlocutors will clam up, and reports officers in diplomatic posts abroad will err on the side of extreme caution in telling Washington what they have learned.

All-source analysts, whose insights and judgments have long relied in part upon the candid, often sensitive observations and reporting from our diplomatic missions around the world, will see their perspectives and interpretations suffer. To the extent foreign affairs analysts are forced to rely on classified, clandestinely acquired intelligence—from that much smaller pool of recruited or co-opted foreign sources, whose identities are never fully disclosed in intelligence reporting—the confidence level of their assessments may also decline. The rolling disclosures from the 2010–11 WikiLeaks scandal—an aberrant manifestation of transparency advocacy—are having a chilling effect on the reporting that policy makers and analysts rely upon for interpretive perspective, cogent assessment, and informed policy formulation and implementation.[1]

One need not be paranoid to wonder if this tourniquet on US reporting concerning foreign states and leaders does not also serve a more deleterious purpose. It is one thing to see part of one's source information shrivel up and die based on the hacker world's credo of "information wants to be free." This blatant disclosure can partially blind US analysts and decisionmakers to foreign developments and intentions by forcing the United States to rely more heavily on clandestine intelligence, a sparser, more difficult, and more costly enterprise—as well as to depend upon often dubious, open-source information. However, the WikiLeaks episode can also serve America's adversaries the world over, from pariah regimes and ideological foes to a host of hackers and fabrica-

[1] A key difference between intelligence and diplomatic reporting has long been in the area of source protection, where diplomatic traffic generally has named its sources but then noted "(please protect)" in the text. Clandestine human source reporting, already classified much higher than diplomatic reporting and more restricted in its dissemination, never actually identifies any source beyond a generic description of the human source's access and record of reporting credibility.
The debate over the WikiLeaks phenomenon continues to rage among politicians and legal minds concerning issues of transparency vs. secrecy, a realignment of First Amendment interpretive thinking, definitions of journalism vs. a kind of information voyeurism, and the like. What has escaped us thus far is a reasonable, defensible balance between freedom of expression and irresponsible license in the context of preserving protected communications impacting US national security.

tors, since the whole notion of operational security and protection of sensitive sources has been turned on its head. The alleged WikiLeaks leaker, a certain Private Manning, was either stupid or disingenuous in claiming that he could have acted more maliciously by giving the leaked reports "to China or Russia." In making them available globally via WikiLeaks, he did all of that and much more.[2]

Need to Share—Overshooting the Target

The US national security information environment has gone from being overly protective and constricted to becoming unmanageably complex and dispersed. The problem now is less one of vertical stovepipes and more one of uncontrolled, anonymous cyberspace—an "irrational exuberance" of sharing. The United States needs to refocus its efforts on finding the "happy medium," a sensible and sustainable middle course that can shield sensitive information from inordinately wide, unauthorized dissemination and "data-basing" but also enable fulfillment of the critical obligation to get key information to those who actually need it and can use it appropriately and responsibly.[3] While some worry about how to bring to justice culprit insider leakers who hold security clearances and have sensitive information access, others try to right the disrupted balance between responsible and minimally restricted information sharing. A credible damage assessment must address the effects that these and similar unauthorized, mammoth disclosures have on the US government's ability to talk with and report candidly on foreign counterparts.

This costly outcome for US interests already takes on at least two forms. Foreign interlocutors are markedly reticent to share sensitive information and internal perspectives with American diplomats for fear of seeing their comments portrayed, out of context but with attribution, in the public sphere. Secondly, desire to preserve others' security, safety, and continued candor is causing US diplomatic reporters to pull their punches in reporting fully what they see and hear abroad.

This latter concern will no doubt prompt a move to reporting in channels often beyond the reach of most analysts, and to hedging on disclosing sources in diplomatic reports. socio-political insights in these reports, so valuable to the analyst, are based on candid, closed-door discourse with foreign actors on a broad range of issues and trends as they affect US entities, personnel, interests, and foreign and security policy objectives. In the future these areas will more often be reported through highly restricted reporting channels, e.g., via secure telephone and in "addressee only" e-mails or via compartmented dissemination pathways. Even e-mail transmission is not sacrosanct, however, and many shy away from that channel. Few, if any, of these reports will reach most analysts, become part of a searchable data base, or become a part of the researchable historical record. This diminution will continue an already observable trend toward compartmentalizing both raw and finished reporting and analysis, erecting more and more computer firewalls, and layering additional access restrictions.

The Information Spectrum's Mid-range Reporting and Ground Truth in Jeopardy

One of the most valuable kinds of information for all political analysts comes from those with a true sense of the pulse of a country. These can be scholars and journalists steeped in a country's history, society, culture, and trajectory; they also be observant, schooled diplomats, whose personal radars are attuned to everything going on—publicly and behind the scenes—in the country to which they are

[2] See Ellen Nakashima, "Who is Bradley Manning?" *Washington Post Magazine*, 8 May 2011: 18.
[3] One account estimates that the total cost of keeping the nation's secrets approximated $10.2 billion for fiscal year 2010 (Oct 2009–Sep 2010), a quadrupling since 1995. See Sean Reilly, "The Steep Price of Secrets," *Federal Times*, 9 May 2011: 3.

posted. Unlike instant global news accounts and the accompanying paid "talking heads" dialed up for "instant analysis," US diplomats can provide validated on-scene accounts, continuing coverage between news cycles, and interpretive reflections on the significance, impact, and implications of foreign events and decisions. Diplomatic reporting is not just airing others' dirty laundry; it is not relaying to Washington the galloping gossip in foreign capitals; nor is it solely reminding Washington policymakers and analysts how US policies and pronouncements are being received, interpreted, and affecting events abroad. While it does include all of these at times, most important is each US foreign mission's work in informing and analyzing for Washington what is going on in the thinking and behaviors of foreign actors, most especially as they affect those matters about which the United States cares most.

All of these critical areas of coverage will now suffer from a decline of regular, especially candid, reporting. Several senior Foreign Service Officers have asserted they will no longer put anything sensitive in their reporting to Washington, an indication of how sparse "ground truth" perspectives threaten to become.[4] And this loss of highly relevant current information and insights will exacerbate a steady diminution of US Foreign Service analytic reporting per se, a negative trend already visible over the past two decades at the least. Embassies never have written primarily for the use and benefit of Washington analysts. Indeed, the idea of doing so is an abomination to many diplomats, especially those in the senior ranks. However, as more and more requirements have been placed on already over-stretched and understaffed US missions, political reporting increasingly has found itself on the chopping block, sacrificed to time pressures and operational priorities. Instant news reporting has edged out quality analytic reporting from US diplomatic missions in many respects, but this does not include those unique, sensitive conversations with senior foreign interlocutors—and their plans and perspectives shared in intimate, often one-on-one, settings. It is in these arenas that the WikiLeaks intrusion will prove most costly and destructive. Moreover, the threat of a continuing spiral of revelations from the WikiLeaks treasure trove of sensitive State Department reporting will keep both diplomats and analysts on tenterhooks for years to come.

A Leak is a Leak is a Leak?

What makes WikiLeaks different from leaks to other media outlets? The short answer is twofold: first, bona fide journalists operate cognizant of an ethical code which, despite their calling to hold government to account, helps to govern their actions and underline their responsibility in dealing with national security issues and information; secondly, those journalists write for a public, large or small, and have a purpose and are selective in their reporting. On the other hand, WikiLeaks' actions have no stated purpose beyond disclosing, without restraint, what it illicitly has received from unnamed sources. Contrary to some claims, the leaker of the vast amounts of Department of State and other reporting was not and is not a whistle-blower. That name only deserves to be used for those revealing embarrassing, illegal, unethical, or negligent behavior by those enjoying the public's trust and confidence. The WikiLeaks leaker defies this definition. For its part, limited dissemination diplomatic reporting protects information that serves a specific set of consumers and legitimate purposes for the benefit of America's foreign and security policy aims, just as the trade secrets of a company enjoy the benefits of proprietary or intellectual property protections under the law.

[4] These statements were made to the author by two senior US Foreign Service Officers, who confided their attitudes in confidence. No change in reporting doctrine or guidance, however, has been issued by the Department of State per se, according to a third senior official there with access to such policy decisions.

In the "WikiLeaks" era, diplomatic reporting (as noted, already thinner and sparser than in years past) is likely to find analysts tapping into dry wells for information in many instances. This will put added pressure on analysts to build mutually advantageous relationships with reporting officers and outside experts. While the mythology persists that analysis should drive intelligence collection, and perhaps elements of diplomatic reporting as well, the fact is that most analysts have little, if any, contact or relationship with those diplomats and "collectors" reporting this kind of information. This is all the more true as the generational change in the US analytic workforce continues to bring in more and more untested, less experienced analysts. Thus, while desirable, encouraging more give-and-take—perhaps via "secure" internet connections—with those stationed abroad as Washington's "eyes and ears" will continue to be sporadic and often personality-dependent.

Moreover, because the emphasis on getting diplomats into the field as "transformation agents" (under the aegis of former Secretary of State Condoleezza Rice) has further drained on reporting out of embassies and consulates, it has become that much more critical to broaden analysts' networks of "informants," e.g., in the academic, think tank, and journalistic worlds even as the bulk of the US Intelligence Community (IC) remains captive to a hidebound, inflexible security regimen that stresses strict avoidance of contact with the uninitiated interlocutor, be he an American or foreign citizen. That culture is the polar opposite of the diplomatic approach, which seeks to maximize information acquisition, but not through recruitment and direction of paid informants committing espionage for the United States. Both types of information gathering depend on trust, and while the data that WikiLeaks obtained was not intelligence, it did include a host of diplomatic telegrams in which there has been much less focus heretofore on masking the identities of foreign information sources. Denying access to what were becoming IC-wide data-base assets will no doubt be another by-product of this damage.

Death of the "Need to Know" Sacred Cow

The 9/11 Commission found great fault with the stovepiping and bureaucratic hoarding of national security information, some of which (in proper hands and at the right time) might have aborted or altered the devastating terrorist assaults in New York, Washington, and in the skies over Pennsylvania in September 2001.[5] The recipe for correction, however, was an overstated, virtually unqualified call for greater sharing of information—an implicit overturning of the prevailing "need to know" culture, one admittedly in need of revision. However, in this age of rapid and ready access to electronic information in a variety of locations, the newly enshrined emphasis on "need to share" has swung the pendulum much too far in the opposite direction. In essence, any tin pot hacker or information junkie can probe data access portals and data-base entry points (both private and government-owned) to intrude on all manner of information holdings—some classified, many others merely sensitive. The hackers' motives may be adversarial, but they may also simply be to prove they can succeed.

For all of its untold advances and advantages, the Internet has proved itself also to be the bane of national security. The more we rely on computerized networks, the more juicy they become for our adversaries to target, interdict, and damage, whether those adversaries are in the ranks of hostile governments, hackers, or foreign actors. Their motivations run the gamut: from proving a system is vulnerable and insecure, to embarrassing a government or

[5] "The biggest impediment to all-source analysis…is the human or systemic resistance to sharing information…. [The 'need to know'] system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate." *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (WW Norton: New York, 2002), 416–17.

official, to inflicting major damage to a critical piece of information infrastructure. Thus, the government is increasingly focused on cyber security, both for its own systems and for the larger public infrastructure, upon which rests the functioning of our economy and the information society writ large.

Need to Know ... With Whom to Share

Transparency advocates in the extreme ask: Why is anything classified? Shouldn't the American public be entitled to know what its government knows and is doing?[6] Such naïve questions are reminiscent of the now-ridiculed credo of nearly a century ago, i.e., that "gentlemen do not read each other's mail."[7] The fact is that—after the Cold War and a half century in which deterrence could only succeed if the adversary knew some but not all of one's capabilities and intentions—in today's world, the explosion of information sources of varying value and validity still requires that some kinds of information be kept secret. Given the expansion and variety of threats to the nation's security and interests, a number of things deserve to be kept to a limited audience with, yes, a "need to know"—in the best interests of the American public. Some examples are: how to make nuclear and biological weapons; how to access nuclear and other sensitive facilities (physically and electronically); US plans and capabilities, given different contingencies and demands, both at home and abroad (e.g., war plans); and who is providing us insights into the plans and actions of foreign entities and terrorist and criminal enterprises.

In information dissemination terms, there is no longer any such entity as "the American public." In the contemporary environment, any public, regardless of how small or seemingly remote, can instantly morph into a global audience. Examples are plentiful. Recall the demise of a politician who spouted an ethnic slur, suffered a slip of the tongue, made an untoward remark on a microphone wrongly assumed to be inoperative, committed a glaring error in judgment or timing, or said virtually anything controversial, even to a "closed," hometown Rotary Club gathering. If it can be made newsworthy, it will be, particularly in our world of ubiquitous cell phone filming, recording, blogging, and tweeting. Given the present-day technological reality, one cannot simply insist on a sunshine policy to govern the actions and information disclosure decisions of the US or any government. Indeed, many foreign governments—in particular their intelligence, security and law enforcement components—are increasingly leery of providing the United States with sensitive information that could end up in the wrong hands, appear in the news or on the Internet or in a courtroom, and thereby be compromised, along with its originator.

It will be a lot harder in the future to get foreign sources to provide under-the-table insights into their governments' leaders, inner workings, policy plans and disputes, and more. It should go without saying that this information has never been easy to acquire. And this elicitation is not espionage but rather the work of socio-cultural cultivation best accomplished by diplomats who can (or could, in the past) display behaviors worthy of another's trust and confidence. Just as diplomacy seeks to build and then steer relationships,[8] the damage of a WikiLeaks exposure sows mistrust and undercuts those relationships in whatever phase they find themselves. In the world of spotting, assessing, recruiting, and handling human intelligence assets, trust is the ultimate coin of the realm: we must be able to trust in the credibility of information from a source (lest he be a plant, swindler or fabricator); and, in turn, the

[6] See Nakaskima, 10f.

[7] A contemporary bumper sticker reflects this zealotry in the words "Secrecy Promotes Tyranny." Those of this view clearly have no appreciation for the vulnerability of some aspects of national security, were it not for the ability to avoid publicizing them to our adversaries.

[8] One definition of diplomacy is "the art of letting the other guy have *your* way." (Originator unknown)

source must have a basic trust in this handler that the source's identity, reporting, and personal security will be fully protected. These principles also hold in the world of diplomacy.

WikiLeaks Copycats

As potentially harmful as the exposure of sensitive, US government communications and reporting has been and most likely will continue to be, the technology of a globalizing world makes it more than likely that we will continue to witness exposures akin to that of the contemporary WikiLeaks case. Indeed, leaving WikiLeaks aside, concerns over privacy and information retention already explain Europeans' reluctance to provide "[airline] passenger name recognition" data to the United States for security purposes, absent binding agreements as to who will have access to it and for which purposes, and how long it can be retained in US computer holdings.[9] Skeptical European partners have already witnessed such data of theirs appearing in US airline industry hands, when it was supposed to be fenced off solely for US government databases and access.

Keeping anything secret in today's world, outside of an effective police state that chooses isolation and persecution as its tools, will become increasingly difficult. That, after all, is also the thrust of part of America's concerned focus on cyber security, both for information integrity and for shielding information technology from "denial of service" and virus attacks. While one can hope that future "transparency crusaders" might exercise some caution and consideration by sifting out the most devastating information from blanket Internet exposure, the likelihood remains that many will grab and broadcast sensitive reporting simply to prove their capabilities or to embarrass authorities. Leakers with a security conscience seem to be the ultimate oxymoron. The same holds for hackers, who joyride into others' data bases and e-mail troves to plant worms and viruses, and to extract or destroy data.

A strange irony in all of this may even find government users of WikiLeaks revelations in a catch-22: if they use WikiLeaks-disclosed secondhand data in any unclassified product, oral or written, they may fall prey to violating secrecy stipulations that forbid publishing or broadcasting information that the government still considers classified, whether leaked or not. This situation already prevails concerning the news media milieu, i.e., government personnel, especially intelligence officials, are on notice never to corroborate leaked information by lending it the aura of legitimacy when it appears, unauthorized, in unclassified form.[10]

The challenge for the IC is to right the balance between finding the appropriate safeguards and compartmentation of information on the one hand, while on the other sustaining candid, analytical reporting from across the world to the benefit of the president, his cabinet, military planners and decisionmakers, Congress, and, only when appropriate, the US (and thus global) public. Expecting the Internet or the likes of a WikiLeaks enterprise to police itself is a vain hope. In safeguarding the nation's critical secrets, officials have encountered one more major hurdle and dangerous adversary.

❖ ❖ ❖

[9] This reluctance, particularly among some representatives in the European Parliament, prompted a rescission of the original PNR agreement and its renegotiation with added safeguards. See also: Kristin Archik, "U.S.-EU Cooperation against Terrorism," *CRS Report for Congress* (RS22030), US Congressional Research Service, July 9, 2010.

[10] I am indebted to Dr. Cathryn Thurston, Director of Strategic Intelligence Research, National Intelligence University, for this insight.