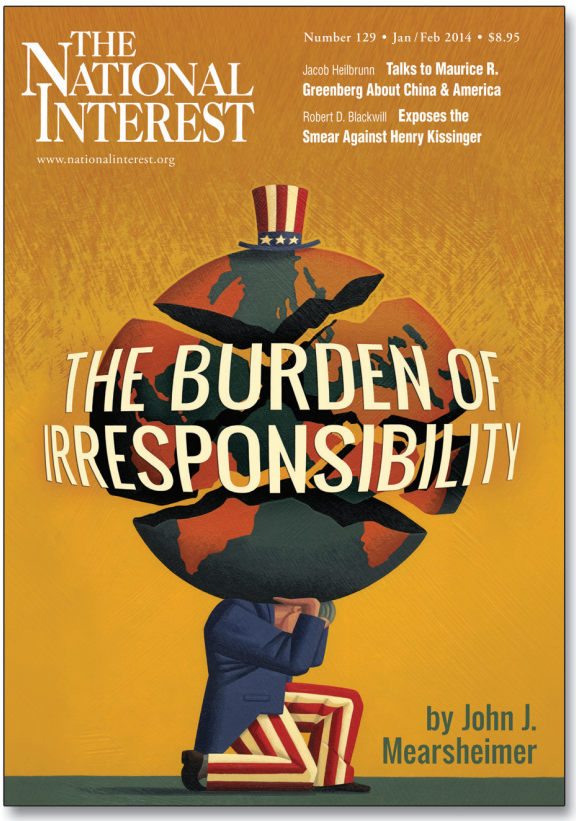
THE NATIONAL INTEREST

Number 129 • Jan / Feb 2014



Editor *Jacob Heilbrunn*

The National Interest • 1025 Connecticut Avenue, N.W. • Suite 1200 • Washington, D.C. 20036
Phone (202) 467-4884 • Fax (202) 887-5222 • editor@nationalinterest.org

The contents of *The National Interest* are copyrighted. ©2014 The National Interest, Inc.
All rights reserved. Reproduction and distribution of this material is permitted only
with the express written consent of *The National Interest*.

Tinker, Tailor, Leaker, Spy

By David V. Gioe

Between the trial of Chelsea (formerly known as Bradley) Manning and the revelations of Edward Snowden, the debate regarding the leakers and their information has focused primarily on the balance between liberty and security, or between government transparency and secrecy. This is a necessary, even overdue, discussion. But it is also important to reflect upon the lasting damage these unauthorized disclosures will have on future U.S. intelligence collection.

Both Manning and Snowden betrayed the public trust and disclosed national-security information that they had sworn to protect. Both seriously impeded America's future ability to recruit foreign sources that provide human intelligence (HUMINT). And both harmed America's ability to enter into cooperative relationships regarding signals intelligence (SIGINT) with foreign partner intelligence agencies—termed "liaison services" in the business.

The degree of access with which Manning was entrusted—hundreds of thousands of diplomatic cables, in addition to the so-called war logs of Afghanistan and Iraq—can be traced to the U.S. intelligence-community reforms suggested by the 9/11 Commission after the terrorist attacks on September 11, 2001. The 9/11 Commission criticized the U.S. intelligence and law-enforcement communities for not connecting the dots and for hoarding information, thus leaving America vulnerable on 9/11. In the reckoning during the post-9/11 intelligence reforms, the enduring counterintelligence principle of "need to know" was transformed into "need to share," a new paradigm that mandated that intelligence agencies share information broadly across bureaucratic lines and prepare analysis for the widest possible dissemination in order to prevent intelligence stovepiping.

This expansive conception of information sharing enabled a young army intelligence analyst to access diplomatic cables from around the world that had nothing to do with her core duties as a military-intelligence analyst serving in the Middle East. This access illustrates the distance that the intelligence-community pendulum has swung in the direction of almost-blind information sharing. If an event of the magnitude of 9/11 forced the pendulum in the direction of increased sharing, more recent events such as the Manning and Snowden leaks could reverse the trend back toward greater compartmentalization, especially involving more stringent information-technology protection.

To calculate or quantify the amount of damage that a document might cause if improperly disclosed, the U.S. government looks to the sliding scale of its classification system; logically, the more sensitive

David V. Gioe is a former CIA operations officer and a PhD candidate at the University of Cambridge.

a document, the higher the classification. According to Executive Order 12356, revelation of a "Confidential" document causes "damage" to U.S. national security, exposure of a "Secret" document causes "serious damage" and a "Top Secret" document's contents would cause "exceptionally grave damage" if improperly disclosed. This system makes sense for characterizing damage to U.S. national security at a fixed point in time, but it is woefully inadequate to assess the future impact of such disclosures. It may not be possible to charge a leaker under the law on the basis of what might have been obtained had it not been for their negligent public disclosures, but despite the lack of legal recourse, it is worth at least discussing the intelligence ramifications past the time and date stamp on the document itself. It is true that time horizons factor into damage assessments because many classified documents contain automatic declassification dates that usually range from ten to thirty years in the future. However, most documents dealing with HUMINT sources and SIGINT methods usually fall under several exemption codes and are not automatically declassified at any point in time.

It remains hotly debated whether Manning's revelations actually led to the deaths of either U.S. soldiers or foreign sources. For instance, in 2010 Admiral Mike Mullen, then chairman of the Joint Chiefs of Staff, suggested that "the blood of some young soldier or that of an Afghan family" might be on Manning's hands. Indeed, it is easy to see why this could be the case judging by the sheer volume, and the classification levels, of material that was released. Others have disputed this claim based on the recent courtroom testimony by the Pentagon's damage-assessment team in the Manning trial. Mullen may not have been referring exclusively to American military deaths that may have been caused because the locations, timing or movements of soldiers were divulged, but rather in terms of revenge attacks whose seeds may have germinated in the outrage over American military mistakes caught on film, such as the widely known case of the helicopter pilot accidentally engaging a media crew or other tragic incidents involving civilians (described by the misnomer "collateral damage").

Nevertheless, the scope of this debate so far has been about water under the bridge. It would be appropriate to consider the water that will now not pass under said bridge to fill American intelligence aquifers. Thus far the debate about the damage wrought by Manning and Snowden has only dealt with what has been revealed about U.S. intelligence and diplomacy; surprisingly, there has been little public discourse regarding the future implications for U.S. intelligence of their wanton actions. Perhaps the popular choice of terms is to blame

for this narrow discourse. The term "leak" suggests a drip that, over time, might result in a problem but in the short term is more of a nuisance than an emergency. The opposite of a deluge, of course, is a drought. If intelligence agencies must perform all-source analysis in order to connect the proverbial dots, what happens if a single important dot never materializes?

Of course, a hypothetical argument is difficult to prove and might not be considered as evidence in a court of law, but the prosecution team in the Manning case did not even attempt to make the argument about future intelligence losses and collection efforts that will be stillborn because of the leaks. During the sentencing phase the prosecution did solicit testimony about the leaks' impact on American diplomacy, but consideration of future effects stopped there. This is surprising because future loss of earnings (if intelligence gained is the profit derived from the investment of national-security resources) is often considered in legal cases. Granted, the Manning trial is a criminal case under the Uniform Code of Military Justice, not a civil suit, but there is a logical parallel between what income is to an injured person and what intelligence is to a nation: the latter both require the former to thrive.

What would future losses to American intelligence actually look like? Recruiting human-intelligence sources is already a difficult task, made harder by Manning's treachery in particular. A representative of a hostile government or a member of a terrorist network may wish to cooperate with American intelligence for any number of reasons, provided his safety can be reasonably assured. If he is considering cooperation, he will look for an American official who is a discreet professional to provide his information. He may study the Americans for a long time in order to make up his mind about such a potentially life-changing decision. Indeed, any slipup on the part of the recruiting officer, such as indiscretion or sloppy agent tradecraft, could very well cost the foreign agent his life and potentially even jeopardize the well-being of his family in his home country. This is serious business, and a potential foreign agent will weigh carefully the risks and benefits of a clandestine relationship with the U.S. government. The potential agent must be satisfied that the Americans can assure his safety, and, of course, these assurances must be credible.

Recruitment of a foreign source may take many forms. For instance, a potential source may be sought out due to his placement and access, approached by a CIA case officer or FBI special agent. He might walk into a U.S. embassy or consulate abroad and volunteer his services. Or he may seek out an American representative at a diplomatic function, although it will not be obvious for him to know who is an intelligence officer. Perhaps he will need some convincing that the risk is worth the reward and, in any case, the risks will be minimized by clandestine interactions with well-trained professionals.

But how can the U.S. government continue to attract these sorts of people whose information our policy makers and defense planners urgently need? Human-intelligence sources have a nuanced risk calculus and are motivated to provide secrets for a range of reasons, including money, ideology, ego, revenge or some combination of these. But in all cases potential sources must be reassured that hushed words stated in confidence won't endanger them in the next tranche of leaked information. The consequences for diplomats, military officers or security personnel of hostile regimes or terrorist networks would be swift and severe. Given this guaranteed punishment, it is wholly understandable that a potential

Mass disclosure of classified information was never part of the risk calculus of a potential human-intelligence source. Surely, it is now.

foreign agent may decide against walking into a U.S. embassy, seeking out a U.S. representative or accepting a follow-up meeting with an American. In fact, those who would face the harshest retribution if exposed have the information most desired by U.S. policy makers.

American diplomats might also have additional trouble in the future engaging foreign interlocutors, and one can envision why. Diplomats may meet privately with each other and may say some typically undiplomatic things in order to get past public posturing and move an issue forward. The American diplomat will honestly relate the information provided by his interlocutor to Washington and will naturally include the name and position of his interlocutor along with his interlocutor's unvarnished remarks. In the era of Manning, foreign government officials will think twice about sharing frank thoughts with their U.S. counterparts if they think what they say will be online tomorrow. For instance, German Free Democratic Party (FDP) member Helmut Metzner was identified in a WikiLeaks cable as providing candid information to the U.S. embassy in Berlin about German government coalition negotiations in 2009. Metzner was fired from his position as chief of staff to the FDP chairman in light of his forward-leaning approach to keeping U.S. officials apprised of German political developments. Perhaps with the Metzner case in mind, Patrick Kennedy, the under secretary of state for management, characterized Manning's disclosures as having a "chilling effect" on foreign officials. If the practice of diplomacy requires trust and discretion, how much more difficult is the task for intelligence officers?

The real question of the Manning case, beyond the damage of what information he has revealed, is the potential value to American policy makers of the intelligence that won't be collected. It is the discreet conversation with a potential cooperative source that will not happen that is the intelligence price to be paid. To be sure, Manning did not have access to CIA operational cable traffic (the internal communications of the National Clandestine Service), but we can be reasonably confident that if he had it, he would have provided it to WikiLeaks, and the cost in human lives would have been dramatically higher.

The CIA takes the protection of source identities extremely seriously, and even in a "need to share" culture, Manning did not have access to this sort of information. But does a potential future human-intelligence source know exactly the types of cable traffic to which a low-level army analyst may or may not have access? Or, rather, might he assess that people like Manning could know his identity? What might he calculate the chances to be that his name could be buried somewhere within hundreds of thousands of U.S. government cables? A dedicated counterintelligence service would surely invest the time and energy to comb through tens of thousands of cables to find—and connect—dots that would lead to the exposure of sources, as was vividly illustrated by the Iranian revolutionary students who painstakingly reconstructed shredded cables

from the U.S. embassy in Tehran in 1979.

Former defense secretary Robert Gates concluded:

> I spent most of my life in the intelligence business, where the sacrosanct principle is protecting your sources. It seems to me that, as a result of this massive breach of security, we have considerable repair work to do in terms of reassuring people and rebuilding trust, because they clearly—people are going to feel at risk.

It would be wrong to conclude that massive leaks might only affect strategic-level HUMINT. Operational- and even tactical-level HUMINT are also potentially compromised. For instance, the Taliban claimed to have reviewed the WikiLeaks war logs looking for names of people who had cooperated with the Americans in Afghanistan. The Taliban, thanking WikiLeaks for revealing "spies," further claimed to have executed tribal elder Khalifa Abdullah of Kandahar, who was unmasked by the documents. Others have argued that Abdullah was not actually named in any leaked document. However, belatedly scouring WikiLeaks for Abdullah's name misses the point: regardless of whether the Taliban positively identified Abdullah in a cable and then targeted him for execution, perception is the reality that matters in the world of intelligence. An Afghan who heard the Taliban's lethal claim, true or false, may decide to believe retired general Robert Carr, chief of the Manning "Information Review Task Force," when he testified that the Taliban's claim to have executed an American source was false, but the consequences of believing Carr cannot compete with taking the Taliban's threat seriously and steering clear of Americans. Carr is probably correct given his former position, but the Taliban's credible threat is also worth considering, especially if more massive disclosures come in the near term.

Under cross-examination by Manning's defense team, Carr acknowledged that Arabic (and presumably Pashto, Dari, etc.) names were not rendered in their original language in U.S. cables, but rather were transliterated into English. Manning's defense team pressed Carr by asking if Iraq or Afghanistan shared an alphabet with the United States. Carr truthfully replied, "No," and then conceded that Afghans are less "plugged in" than Westerners. Even if Manning's defense team was able to demonstrate that Afghans aren't as glued to their smartphones as Westerners are, they exhibited a fundamental misunderstanding of the nature of Al Qaeda and the Taliban.

Manning's defense team made the willfully ignorant suggestion that their client's disclosures did not have a great impact on the safety of deployed soldiers because the areas in which U.S. troops are deployed are not English-speaking countries. This canard is insidious because

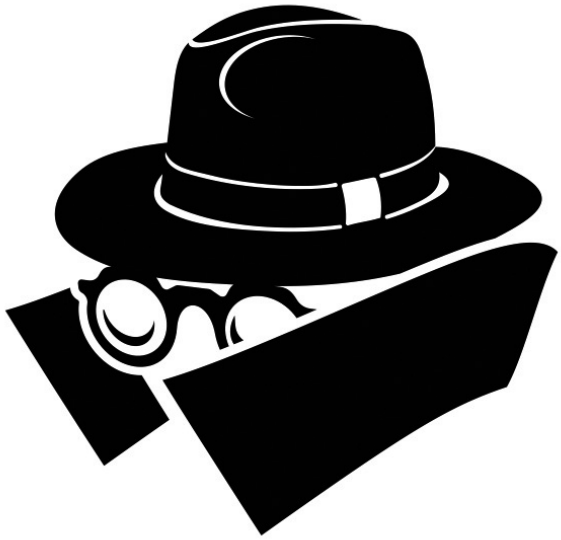
one can be certain that the Taliban, Al Qaeda, and other extremist or insurgent groups have plenty of members who speak passable or even native English. In fact, in the era of online linguistic and translation tools such as Google Translate, America's enemies do not need to speak English. Yet they often do—and some are even native-born American citizens or former U.S. residents. For instance, the architect of the Japanese surprise attack on Pearl Harbor in 1941, Admiral Isoroku Yamamoto, attended Harvard University and later was a naval attaché at the Japanese embassy in Washington, DC. He was not only a fluent English speaker, but also a true student of his American adversaries. The former leader of Al Qaeda in the Arabian Peninsula, Anwar al-Awlaki, a U.S. citizen, held various advanced degrees from American universities. "American Taliban" John Walker Lindh and Al Qaeda spokesman Adam Yahiye Gadahn (born Adam Pearlman in Oregon) are two further American citizens who switched allegiances and could review WikiLeaks documents just as easily as any literate American with an Internet connection.

In addition to American HUMINT, American SIGINT has also paid a steep price in potential but nonactualized intelligence recently with the Edward Snowden affair. Appearing before Congress in June 2013, FBI director Robert Mueller testified that Snowden's leaks had caused "significant harm to our nation and to our safety." Mueller could have reasonably gone even further to assert that Snowden's actions made intelligence "liaison" (clandestine diplomacy between intelligence services) more difficult as well. In the same way that potential human sources may now be wary of working with American intelligence officers, potential SIGINT partners may wish to distance themselves from mutually beneficial cooperative partnerships (called "liaison agreements") with the U.S. government.

This has moved beyond a mere possibility to actually impinging on current intelligence pacts. Consider the recent German decision to terminate a cooperative SIGINT treaty with the United States and the United Kingdom that dates from 1968. German foreign minister Guido Westerwelle justified the move by stating, "The cancellation of the administrative agreements, which we have pushed for in recent weeks, is a necessary and proper consequence of the recent debate about protecting personal privacy." Henning Riecke of the German Council on Foreign Relations downplayed the significance of this event, noting that it may have been done for domestic political consumption in advance of pending elections. Riecke suggested that this abrogation of the treaty would not affect the day-to-day sharing agreements between the United States and Germany. One hopes that Reicke's analysis is correct insofar as this treaty may have been a loose end and low-hanging political fruit for theater-driven politicians, but Anglo-American SIGINT officials may not wish to be thrown under the German electoral bus as their politicians wish to be perceived as "doing something" at the expense of their allies. The Germans would stand to lose more than the Americans, but the loss of German SIGINT might be particularly poignant to American audiences who may recall that Al Qaeda's Hamburg cell, led by hijacker Mohammed Atta, played a major role in the planning and execution of the 9/11 attacks. Obviously, any German-American intelligence-sharing agreement did not expose the Hamburg cell or stop the 9/11 attacks, but it is hard to see how even less cooperation could yield mutually beneficial results.

The German government, in this case, could have taken a page from the Obama

administration's playbook in trying to actually explain to its concerned electorate why SIGINT cooperation with allies benefits the security of both parties. Instead, it opted to take a politically expedient approach that only reinforced the conception that SIGINT cooperation is overly invasive. Sounding retreat in the face of misunderstood allegations about the Prism program likely will reinforce the pernicious suggestion that such programs are endeavors of which to be ashamed. In stark contrast to his German counterpart, British foreign secretary William Hague stood his ground, confidently stating, "The intelligence sharing relationship between the UK and the US is unique in the world, it's the strongest in the world and it contributes massively to the national security of both countries."



The question must now be asked: What is the intelligence legacy of Snowden's treachery? How many foreign governments will argue the case to their electorate like Hague? How many will cancel extant agreements like Westerwelle? And how many intelligence services will avoid future collaborative contact with the National Security Agency for fear of being painted with rhetorical brushes that evoke overwrought fears of an East German surveillance state while chiming the death knell of personal privacy?

Intelligence-liaison relationships are vital to the success of any intelligence or security service. As H. Bradford Westerfield asserted, liaison holds a "central place [in the] real world of intelligence" and is a "core feature" of American intelligence. No single service can track every malign actor, every rogue state, every weapons proliferator or terrorist. Intelligence services, all of which reside in the real world of resource limitations, rely on trusted cooperative services to act as force multipliers for their own efforts. It would be beyond the scope of this essay to include a raft of examples demonstrating the value of intelligence-liaison relationships, but, in brief, since World War II the "special" intelligence relationship between the United States and the United Kingdom, covering both HUMINT and SIGINT, has been a bedrock of foreign-policy and defense planning for both sides. As Hague counseled, the two countries' intelligence ties represented "a relationship we must never endanger because it has saved many lives over recent decades in countering terrorism and in contributing to the security of all our citizens."

To consider just one case that Hague may have been recalling, the joint handling of Colonel Oleg Penkovsky, a Soviet military-intelligence officer, by both the CIA and the United Kingdom's Secret Intelligence Service (SIS) may have "saved the world" during the tense days of the Cuban missile crisis in 1962, according to credible authors who have read the declassified files. Specifically, Penkovsky first volunteered to American intelligence in Moscow in 1961,

The issue isn't that American intelligence will become defanged or wither on the vine, but rather that it will not be as good as it could be, especially in an unstable global climate when it is most needed.

---

but the Americans were unable to act on his request for a cooperative relationship. The British SIS, hand in glove with the CIA, was able to secure personal meetings with Penkovsky both in Moscow as well as in London and Paris. Although unable to match the SIS's agent-handling resources in Moscow, the CIA provided two case officers, including the legendary George Kisevalter, as well as the primary reports and requirements officer to effectively handle Penkovsky and his enormous amount of intelligence.

Although Penkovsky was only active for a short period of time, he played a critical role. It is fair to say that the Cuban missile crisis may not have been so deftly handled by the Kennedy administration had it not been for Penkovsky's intelligence on Soviet missile systems and artillery-deployment philosophy. Even when the prospects of exfiltration dimmed, Penkovsky stayed the course until his arrest in 1962 and subsequent execution in 1963. One must wonder if the next Oleg Penkovsky to volunteer to the CIA will be even more courageous than the last one. He would have to be in an era where it appears questionable whether America can keep its secrets from the front pages of major media outlets and the Internet. In fact, the next Penkovsky may well wish to volunteer his services but may be reticent lest his identity (or information traceable back to him) be included in a possible deluge of American classified information. To retain its preeminence as well as its reputation for excellence, American intelligence must satisfy both its official liaison partners and its clandestine sources that it can continue to work in the shadows, not under a spotlight.

It could reasonably be asked if the impact of the Manning and Snowden disclosures might be worse than the results of a traditional penetration agent (commonly referred to as a "mole") working in the U.S. intelligence community. The combined treachery of former FBI agent Robert Hanssen and erstwhile CIA operations officer Aldrich Ames led to dozens of deaths of American human sources and nearly crippled U.S. intelligence operations aimed against the Soviet Union (and subsequently Russia after the end of the Cold War). There are several critical elements to this important question, including the nature of the intelligence business and the evolution of information technology in the practice of intelligence. On one hand, despite the Taliban's claims, no deaths have been conclusively linked to the Snowden or Manning revelations, in stark contrast to Ames and Hanssen. On the other hand, hostile penetrations of U.S. intelligence do not seem to have overly retarded offensive recruitment operations, even in the Soviet bloc. Moreover, an intelligence officer who switches allegiances is well aware that the adversary can penetrate his new intelligence service just as well as his original service. This has been an accepted part of spying since time immemorial. It's why even the most productive agents are eventually pulled out of a dangerous assignment before the risks outweigh the gains. Yet, Snowden and Manning represent a new dimension in espionage because mass disclosure of

classified information was never part of the risk calculus of a potential human-intelligence source. Surely, it is now.

American intelligence will survive, and possibly thrive, despite the increased challenges that massive unauthorized disclosures bring. As in the past, American intelligence officers will rise to modern challenges and continue to provide policy makers and analysts with timely and relevant intelligence, but the mountain has certainly become steeper and more treacherous. The issue isn't that American intelligence will become defanged or wither on the vine, but rather that it will not be as good as it could be, especially in an unstable global climate when it is most needed. As the Penkovsky case so aptly demonstrates, a single human source with the right placement and access, at the right juncture in time, can have a profound impact on policy and potentially even change the course of history. U.S. intelligence will not cease to recruit human sources or enter into important bilateral or multilateral SIGINT relationships, but one must recognize the chance that a skittish SIGINT liaison partner, a single prized HUMINT source, or even the next Penkovsky (although he could be Iranian, North Korean or Chinese, just to name a few) might prefer to play it safe rather than cooperate with American intelligence, at least until America gets its intelligence information locked back down to pre-Manning and -Snowden levels.

The future damage of the Manning and Snowden disclosures will wane over time, but this does not make them any less dangerous, especially now. In the short term, America has lost valuable diplomatic leverage as well as counterterrorist capabilities. In the medium term, America will have lost HUMINT from potential future sources as well as SIGINT from liaison partners that could provide an intelligence advantage over rival states, avert strategic surprise, and identify terrorists or proliferators of weapons of mass destruction. Only in the long term, once America has proven to both its allies and its adversaries that it can keep its secrets, will the country be able to benefit from HUMINT and SIGINT sources that will not be obtained in the short and medium term thanks to Manning and Snowden. This damage could take a generation to repair. □