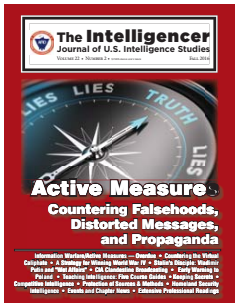

From AFIO's **The Intelligencer**
Journal of U.S. Intelligence Studies
Volume 22 • Number 2 • $15 single copy price **Fall 2016**

Association of Former Intelligence Officers
7700 Leesburg Pike Ste 324, Falls Church, VA 22043.
Web: www.afio.com. Email: afio@afio.com

Keeping U.S. National Security Secrets

Why Is This So Hard?

James B. Bruce, Ph.D.

If someone wants to protect a personal secret, he or she only needs to exercise restraint and tell no one. If no one else is told, the secret is safe. If the US Government wants to protect a national security secret, restraint is not enough. The government is huge, so keeping secrets requires rules, regulations, and laws; added safeguards, such as classifying information; physical, personnel, information, and operational security for the secure use, dissemination, storage, and retrieval of protected information; and a counterintelligence capability to thwart spies.

Despite an elaborate edifice of protection, the government is not good at keeping secrets.[1] As a consequence, foreign governments and terrorist groups exploit disclosed secrets: They thus expand their abilities to neutralize, defeat, or deceive US intelligence. Diminished intelligence results in diminished military and diplomatic capabilities. The net result of poor secret-keeping is the diminution of American power.

There are many threats to government secrets. Leakers and spies represent the greatest threats. What leakers have demonstrated over time—and dramatically of late—is that for all its power and resources, the US Government is unable to stop the leaking. The most notable recent disclosures are those of Edward Snowden, a contractor for the National Security Agency.[2] In mid-2013, he stole 1.5 million files of classified information—nearly all of it highly classified. Possibly 200,000 of these documents have been leaked to the press so far; and all those taken are presumed to be now in the possession of Russia and China.

The staggering scale of Snowden's theft is unprecedented. But the means of doing this, i.e., massive electronic downloading to thumb drives and small portable media, had only one precedent—Army Private First Class Bradley (now Chelsea) Manning. Manning provided roughly 750,000 classified documents to WikiLeaks, run by fugitive Julian Assange whose avowed mission is the large-scale exposure of classified information.[3] Today, Manning is serving a 35-year sentence in a federal prison. Snowden defected to Russia. And as of July 2016, Assange has been holed up more than four years in the Ecuadorian Embassy in London where he took refuge in 2012 to evade criminal charges in Sweden, Britain, Australia, and the United States.

Yet much of the publicity surrounding mega-leakers Snowden and Manning, and WikiLeaks founder Assange, portrays them as heroes and whistleblowers, press-freedom fighters combating governments' excessive secrecy practices to reveal alleged wrongdoing. Their declared aim is to expose US intelligence, military, and diplomatic secrets.

The favorable press coverage afforded these leakers demonstrates the power of the one-sided argument. While the government has, for the most part, taken a low profile and constrained its public commentary, supporters of Snowden in particular, and those of Manning and Assange, have succeeded in controlling the public narrative. And their polemic plays well to sympathetic press elements that tout unrestrained First Amendment freedoms and often encourage leakers to circumvent government rules.[4] For example, the *Washington Post* editorial board explains: "As a newspaper, *The Post* thrives on revelatory journalism and often benefits from leaks, sometimes inspired by dissent and other times by spin."[5] Bill Keller of the

1. James B. Bruce and W. George Jameson, *Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures* (Santa Monica: The RAND Corporation, 2013), 11-16.

2. See Peter C. Oleson, "Assessing Edward Snowden—Whistleblower, Traitor, or Spy?" *The Intelligencer 21* (2), Spring/Summer, 2015, 15-24; David V. Gioe, "Tinker, Tailor, Leaker, Spy: The Future Costs of Mass Leaks," *The National Interest*, Jan-Feb 2014; Edward Jay Epstein, "Was Snowden's Heist a Foreign Espionage Operation?" *Wall Street Journal*, May 9, 2014. Views sympathetic to Snowden are in James Bamford, "The Most Wanted Man in the World," *Wired Magazine*, Sep 2014, 78-85; and Glenn Greenwald, *No Place to Hide: Edward Snowden, The NSA, and the US Surveillance State* (New York: Holt & Co., 2014). Official views in the Intelligence Community are in Office of the Director of National Intelligence, IC [Intelligence Community] on the Record, at *http://icontherecord.tumblr.com/tagged/statement; and http://icontherecord.tumblr.com*.

3. For Manning and WikiLeaks coverage, see Steve Fishman, "Bradley Manning's Army of One," *New York Magazine*, July 31, 2011; and articles by Nakashima, Tate, and Londono in the *Washington Post*, May 4, 2011 and July 30, 2013.

4. See Paul Pillar, "Leaks and an Irresponsible Press," *The National Interest*, December 26, 2013.

5. Washington Post Editorial Board, "Not Every Leak Is Tantamount to

New York Times has written frequently of the *Times's* putative right to publish leaked classified information. And *Washington Times* writer Bill Gertz often publicly trolls his readers for classified leaks as grist for his articles and books. Quite apart from the supportive public narrative, their successes highlight numerous vulnerabilities in the US Government framework for information protection. When seen against the long history of successful leaking of secrets, these vulnerabilities reveal a fundamentally flawed system of preserving secrets, suggesting the need for a new paradigm for secrecy protection, or at least a significantly more effective one.

Why Is Secrecy Important?

In general, the US Government classifies information it wishes to protect from disclosure at three levels: Confidential, Secret, and Top Secret. These ascending levels of classification assign relative importance and increased protection to discrete pieces of information. Executive Order (EO) 12356 states that compromised Confidential information would cause *damage* to US national security; if information is Secret, its compromise would cause *serious damage*; if Top Secret, *exceptionally grave damage*.[6] Additionally, some information of great sensitivity may be further categorized as "sensitive compartmented information" (SCI—usually identified by a codeword), and afforded greater protection from disclosure than other classification levels.

The secrets that the government wishes to protect can involve the following organizations and topics:

Department of Defense:

- Military plans, weapons capabilities, and operations;
- Military intentions and capabilities, including tactics, techniques, and procedures (TTPs) for special operations forces as well as those for strategic and conventional conflict;
- US security and military weaknesses and vulnerabilities; and
- Sensitive military technologies.

Intelligence Community (IC):

- Collection sources and methods, including identities of intelligence officers; recruited agents; and technical characteristics of collection sensors, platforms, systems, and architectures; and
- Operational activities such as covert action.

Department of State:

- Diplomatic discussions and protected communications; and
- Foreign policy deliberations and initiatives.

Department of Energy:

- The safeguarding of nuclear materials, facilities and sensitive technologies; and
- Weapons design data.

Other departments and agencies:

- This includes many governmental organizations who must protect sensitive information related to homeland security, law enforcement investigations, proprietary intellectual property, individual's private data, or other information that is restricted by law.

The rationale for such secrets is not to keep the American public in the dark or to hide official wrongdoing. It is rather to deny sensitive information to foreign enemies and adversaries and, in cases of privacy data, protect individual citizen's rights.

Threats to Secrecy and Why That Matters

Disclosures of classified information can be authorized or unauthorized.[7] *Authorized* disclosures entail foreign intelligence sharing; use of sensitive intelligence to support a diplomatic *démarche* that asks a foreign government to do or stop doing something (such as to stop underground nuclear testing); the major government declassification program in support of greater transparency;[8] and official release of classified information through the Freedom of Information Act (FOIA) process. Disclosures from these authorized procedures, while fully legal, can still be potentially damaging.

Unauthorized disclosures can be diverse, but the two most serious — foreign espionage and leaks of classified information — are considered here.[9] Both

Treason," *Washington Post*, August 1, 2013.

6. Whether these distinctions remain useful or are merely archaic is beyond the scope of this article but might be worth examining in a research project or classroom exercise given today's Information Age.

7. See discussion in the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States, March 31, 2005* (Washington, DC: US Government Printing Office, 2005), 380-384.

8. DNI Clapper's recent initiative on implementing transparency, *Principles of Intelligence Transparency for the Intelligence Community,* is described in ODNI Press Release Number 22-15, October 27, 2015, and can be downloaded from *http://www.dni.gov*.

9. Other examples of unauthorized disclosures can include verbal comments involving classified information with persons who do not

can be seriously damaging and diminish American power.

Espionage

The United States has long been a high priority target of foreign intelligence services. And too many Americans have either volunteered or have been recruited to help them spy against their country. Since the end of World War II, as many as 217 Americans have been identified and prosecuted for committing espionage. Three-fourths have been volunteers, reaching out on their own initiative to offer their services to foreign intelligence.[10]

American spies have provided, or tried to provide, US classified information to 26 foreign countries and to Al–Qa'ida. Russia has enjoyed the greatest success with roughly 86 penetrations from 1947 to 2007. Counting the former Warsaw Pact countries (East Germany, Hungary, Czechoslovakia, and Poland) having run another 29 American spies, China 13, and Cuba 9 more, the loss of US classified information to Cold War adversaries from their combined 137 penetrations can be described as a hemorrhage. As many as 10 friendly or allied countries can also claim espionage successes against the United States, and several have run more than one American spy (Philippines, 5; Israel, 4; and Taiwan, 2).[11] America stands tall as the target of choice, and a lucrative one to adversaries who have defeated underperforming US counterintelligence.

Understanding these penetrations would be better appreciated when the full damage is assessed. But it never has been. Although damage assessments have been conducted of most individual cases, a comprehensive damage assessment compiling the results and implications of multiple spy cases — even across the major ones — has never been done. Lacking that, assessing overall espionage losses is impossible.

Military Spies. In the tradition of the Soviet atomic spies who penetrated the Manhattan Project (Klaus Fuchs and the Rosenbergs are the most well known), some Cold War spies, such as the Navy's John Walker and the Army's Clyde Lee Conrad, provided the Soviets with significant military secrets. According to the Defense Personnel Security Research Center (PERSEREC) 2009 study, *Espionage and Other Compromises of National Security*,[12] the Walker spy ring compromised key cards used for enciphering messages, information about encryption devices themselves, and at least a million classified messages of the US military and intelligence. This study notes that a defector said that the KGB considered the Walker operation as the most important in its history. Some believe that the third leg of the US strategic triad, the submarine force that carries long-range nuclear missiles, could have been rendered impotent in a nuclear war as a result of Walker's treachery.

The Conrad spy ring compromised secrets regarding the planned use of tactical nuclear weapons, manuals on military communications, and documents concerning NATO's war plans against the Warsaw Pact. These included detailed descriptions of nuclear weapons and plans for the movement of troops, tanks and aircraft.[13]

Intelligence Community Spies. For all the espionage damage to US military capabilities during the Cold War, the damage to intelligence was almost certainly worse. It entailed many more spies, and their reach into classified repositories was stunning. The two showstopper cases — it is arguable which was worse — were the CIA's Aldrich Ames and the FBI's Robert Hanssen. But there were many others.

Undetected for nine years, Ames provided Moscow the identities of perhaps a dozen clandestine US penetrations (of whom 10 were executed); the identities of other US double agents run against the Russians; tradecraft of agent operations and communications; identities of CIA officers under cover and other US intelligence personnel; ongoing technical collection operations, sensitive analytic techniques; and hundreds of intelligence reports including National Intelligence Estimates, arms control studies – some analyzing scenarios of how the Russians could cheat on treaties – and the cable traffic of several federal departments.[14]

Hanssen was almost as prolific, though perhaps more damaging because of his special compartmented accesses, well beyond Ames'. Hanssen's espionage went undetected for 22 years, more than twice as long as Ames. Highlights of his compromises include over

have clearances or a need-to-know, or inadvertently leaving classified materials on a bus.

10. Discussion here draws from the PERSEREC study, *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008* (Monterey, CA: Defense Personnel Security Research Center, 2009); and from David Major and Peter C. Oleson, "Espionage in America," *The Intelligencer*, in printed version of *The Guide to the Study of Intelligence* [Falls Church, VA: AFIO, 2016] and also online at *http://www.afio.com/40_guide.htm*, who cite the 217 prosecutions.

11. Data presented for the period 1947 to 2007 are based on conservative, open source information in the PERSEREC study of documented cases of passing classified information to a foreign intelligence service. Espionage can also be more broadly defined, and data supporting a more expansive definition are in the Major and Oleson study, which also notes a spike in cases since 2002.

12. PERSEREC, *Espionage*, 58-59.

13. PERSEREC, *Espionage*, 10.

14. See Pete Early, *Confessions of a Spy: The Real Story of Aldrich Ames* (New York: Putnam, 1997); and PERSEREC, *Espionage*, 2-3.

6,000 pages of classified documents, the identities of seven US penetrations (three were executed), details on many US counterintelligence operations, information on some of the most sensitive and highly *compartmented* projects in the US Intelligence Community, and even details on otherwise well-protected and sensitive US nuclear war defenses.[15]

The voluminous materials provided by these two spies will serve as playbooks for Russia to neutralize US intelligence effectiveness in many important areas, and provide the basis for future deception operations to hoodwink American leaders. As exemplars of damaging cases, the measure of harm Hanssen and Ames wrought to US security may be incalculable, but must also be assessed in the context of other serious foreign penetrations of US intelligence.

Foreign knowledge of US intelligence is the bedrock foundation of foreign denial and deception. It begins with an understanding of how the major collection disciplines work. Since intelligence capabilities are best defeated—that is, denied, deceived, or otherwise neutralized—by attacking individual collection disciplines, we can array the major spy cases against them. Spies damage classified collection capabilities by exposing secrets to adversaries about how classified collection techniques work. Sometimes referred to as intelligence "sources and methods," the better that adversaries understand them, the better they can counter them.

Table 1. Major Spies Who Damaged US Collection Disciplines

SPY	HUMINT	SIGINT	IMINT/ GEOINT	MASINT
Aldrich Ames, CIA	X	X	X	X
Robert Hanssen, FBI	X	X	X	X
Ana Montes, DIA	X	X	X	X
David Barnett, CIA	X			
Edward Howard, CIA	X			
Harold Nicholson, CIA	X			
Earl Pitts, FBI	X			
Richard Miller, FBI	X			
Jonathan Pollard, Navy		X	X	
James Hall III, Army		X	X	
David Boone, Army		X	X	
Christopher Boyce, Contractor		X		
Ronald Pelton, NSA		X		
Jeffrey Carney, Air Force		X		
Ronald Kampiles, CIA			X	
Glenn Souther, Navy			X	

The spies in Table 1 represent the most damaging from a long list. The worst of these – Hanssen, Ames, and Ana Montes (a Defense Intelligence Agency all-source analyst who spied for Cuba for 16 years) — passed highly damaging information pertaining to multiple disciplines. Much of what these spies passed was in the form of analytical reports descriptive of classified collection capabilities and limitations. Others, such as Pollard, Hall, Boone, and Boyce, caused significant damage to technical collection capabilities. Some spies only damaged a single discipline, such as Nicholson for human intelligence (HUMINT), Pelton for signals intelligence (SIGINT), and Kampiles for imagery intelligence (IMINT), but the sensitive information they provided was highly detailed and especially destructive.

Intelligence is sometimes described as collecting secret information by secret means. When classified collection capabilities are compromised, adversaries can develop countermeasures, including *denial*—hiding the targets of collection. Commonly used denial techniques include better-informed counterintelligence against HUMINT, encryption against SIGINT, and camouflage and concealment against IMINT. Adversaries are also better able to conduct *deception* against US collection by manipulating information that they allow to be collected or that they make available (including disinformation) through compromised channels. Unless such collected information is recognized as deceptive, it can influence analytical judgments provided to policymakers. "Collected" information of this kind—i.e., deceptive information—serves the purposes of the deceiving country, and damages the unwitting country.

Given that no comprehensive effort has yet been made to synthesize and aggregate assessed damage done by multiple spies compromising separate collection disciplines, it is probably fair to say that the

15. David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House, 2003); PERSEREC, *Espionage*, 19-20; and Victor Cherkashin with Gregory Feifer, *Spy Handler: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames* (New York: Basic Books, 2004), 246-147.

US IC lacks a good understanding of the effects of foreign espionage on the performance of its various collection capabilities. Lacking such understanding, impairments in current collection are difficult to overcome, analysts are unable to assess the effects of these breaches on their analyses, research and development may build on compromised concepts and technologies, and users of intelligence may never receive critical intelligence because our collection capabilities can no longer produce high-value intelligence where espionage did the most damage to them.

Press Leaks

As damaging as espionage has been, leaks to the press are arguably as bad or even worse. As former Director of Central Intelligence (DCI) George Tenet explained to the House intelligence oversight committee:

> I'm appalled by the sheer number of leaks and the number of government officials who apparently have no concern whatsoever for the harm their disclosures cause, nor any feeling that they may get caught. It is indefensible, inexcusable, and highly damaging. *The damage caused by leakers can be every bit as great as damage caused by espionage*... It is impossible to measure the total damage done to U.S. intelligence through these leaks, but knowledgeable specialists assess the cumulative impact as truly significant.[16]

He later added in an interview that press leaks "have become one of the biggest threats to the survival of US Intelligence."[17] The volume and seriousness of leaks have not let up since these gloomy characterizations. Rather with the massive Manning and Snowden disclosures, Tenet's alarming view has become an understatement.

The government cannot publicly present evidence to substantiate Tenet's argument because such evidence is necessarily classified. Government is hamstrung, unable to make a detailed public case as further publicity can only cause further harm. Thus, markedly different understandings emerge of the damage that press leaks cause between the government on one side, and journalistic and general public opinion on the other that cannot grasp why leaks are so damaging to intelligence. This is not a level playing field.

A few cases have been made public—the tip of a huge iceberg—that illustrate the harm that press leaks can cause: [18]

- **HUMINT: A CIA asset killed through press exposure.**[19] Although his body has never been found, a CIA terrorist source was certainly killed when a front-page article by Tim Weiner in the *New York Times* on August 21, 1995—despite strenuous efforts by the Agency to prevent it — revealed enough identifying details that he disappeared shortly after he was exposed. The press leak occurred within 24 hours of briefing Congress about the agent, a so-called "unsavory asset" who had earlier participated in a terrorist attack that injured Americans, but whose subsequent intelligence reporting on terrorism was judged to be of incalculable value.
- **HUMINT: Liaison Relationships.** Effective intelligence depends on cooperative relationships with friendly governments and individuals who trust the United States to protect their confidences, sources, and sensitive intelligence. Liaison relationships are conducted through HUMINT cooperation. Press disclosures can—and sometimes do—undermine these relationships, making both governments and individuals reluctant to share information, thereby inhibiting intelligence sharing. Foreign countries are increasingly reluctant to trust the United States to protect their human and technical sources. The Snowden and Manning disclosures elevated this problem to a new level, exacerbating diplomatic relationships with close allies and intelligence partners on whom we depend for shared intelligence especially in counterterrorism, and with partners in industry as well.[20]
- **SIGINT: Al–Qa'ida and Osama bin Laden.** After the 9/11 attacks, US intelligence was criticized about why it did not have better warning intelligence on Al–Qa'ida. White House Press Secretary Ari Fleisher provided part of the answer in a press conference: "In 1998, for example, as a result of an inappropriate leak of NSA information, it was revealed about NSA being able to listen to Osama bin Laden on his satellite phone. As a result of the disclosure, he stopped using it.

16. George Tenet, Testimony to the House Select Committee on Intelligence on "The Impact of Unauthorized Disclosures on Intelligence," November 3, 1999; italics added.
17. *USA Today*, October 11, 2000, 15A.
18. Except for the first cited human source case (note 19 below), and the Snowden damage to counterterrorism (note 21), the remainder of the leaks cases cited here are discussed more fully in James B. Bruce, "Laws and Leaks of Classified Intelligence: The Consequences of Permissive Neglect," *Studies in Intelligence* 47 (1), March 2003, 40-43.
19. For elaboration of this tragic case, see the former CIA acting general counsel's account in John Rizzo, *Company Man: Thirty Years of Controversy and Crisis in the CIA* (New York: Scribner, 2014), 148-151.
20. Oleson, "Assessing Edward Snowden," 2015.

As a result of the public disclosure, the United States was denied the opportunity to monitor and gain information that could have been very valuable for protecting our country."[21] Uniquely valuable intelligence on the Al–Qa'ida leadership and operations was lost, much impairing the Intelligence Community's ability to warn of terrorism attacks.

- **SIGINT: Counterterrorism**. In 2014, former National Counterterrorism Center Director Matt Olsen described Snowden's damaging impact on US collection against terrorists:[22]
  - *We've lost ability to intercept the communications of the key terrorist operatives and leaders. Look, we know these groups monitor the press, we know they're suspicious of our ability to collect.... [It] is not news to them that the NSA and the United States Government Intelligence Agencies around the world are trying to collect their communications.*
  - *But [what] this information did was essentially confirmed in excruciating detail the scale and scope of our capabilities. And in many ways, it revealed information that had nothing to do with the privacy of civil liberties of Americans; it was purely information about the capabilities, the technical capabilities of US Intelligence agencies.*
  - *We have specific examples of terrorists who have adopted greater security measures in the last year including various types of encryption. They change Internet service providers. They drop their changed e-mail addresses and they had otherwise in some cases just ceased communicating in ways they had before and drop out of our ability to see what they were doing.*
- **SIGINT: Soviet Leaders' Conversations**. In the September 16, 1971 *Washington Post*, Jack Anderson disclosed that US intelligence was intercepting the radiotelephone conversations from the limousines of top Soviet leaders in Moscow. British historian Christopher Andrew explained that this extraordinary US collection program (codeword: Gamma Gupy), ended abruptly after Anderson's revelations.[23]
- **SIGINT and Imagery: Soviet ICBM Testing.** A January 31, 1958 *New York Times* story reported that the United States was able to monitor the eight-hour countdown broadcasts for Soviet missile launches from Kazakhstan, providing enough time for US aircraft to observe the splashdowns and collect data to estimate the intercontinental ballistic missiles' accuracy. Following publication, Moscow reduced the countdown broadcasts to four hours—too little time for US aircraft to react. Occurring in the midst of the missile-gap controversy, the press item left President Eisenhower livid. Reportedly, some intelligence was lost forever, and, to recoup the remainder, the US Air Force had to rebuild an Alaskan airfield at a cost of many millions of dollars.[24]
- **Imagery: Surprise Indian Nuclear Tests.** Both authorized and unauthorized disclosures about intelligence techniques can be damaging. In this case, classified imagery had been used to support a diplomatic *démarche* asking India to stand down from its plans to test nuclear weapons in 1995, and was also the topic of press coverage based on leaked intelligence. The 1995 intelligence and diplomatic success backfired in May 1998 when the Indians employed countermeasures learned from these earlier disclosures. They prevented satellite imagery from detecting the signatures of their nuclear test preparations, which caught the United States by surprise.[25]
- **Imagery—Missile Tests in Pakistan.** In the mid-1990s, dozens of press articles covered whether Chinese M-11 missiles had been covertly transferred to Pakistan. If such missiles had been acquired, Pakistan could be found in violation of the Missile Technology Control Regime (MTCR) to which it was a signatory. Under the National Defense Authorization Act, US law mandated sanctions against proven MTCR violators. Press reports claimed that US intelligence had found missiles in Pakistan but "spy satellites" were unable to "confirm" such missiles. Readers of both the *Washington Times* and the *Washington Post* learned that intelligence had failed to convince the Department of State of the missiles' presence in Pakistan. The message from the press coverage was, in effect, that any nation could avert US sanctions if they neutralized intelligence by shielding missiles from satellite observation. These articles not only suggested to Pakistan and China that some key denial measures were succeeding, but also spelled out

21. White House press statement, June 20, 2002.

22. Matt Olsen, Comments made at the American Political Science Association meeting, August 28, 2014.

23. Christopher Andrew, *For the President's Eyes Only* (New York: Harper Perennial, 1966), 359.

24. Wayne Jackson, *Allen Welch Dulles, Director of Central Intelligence* (July 1973, declassified history, National Archives, Volume 4, 29-31, record group 263).

25. For a fascinating Indian account of how India converted its newfound knowledge of US imagery collection to countermeasures to defeat it, see Raj Chengappa, *Weapons of Peace: The Secret Story of India's Quest To Be a Nuclear Power* (New Delhi: HarperCollinsIndia, 2000), 403, 413-414, 419-420, 425-428.

specific countermeasures that other potential violators could take to prevent US intelligence from satisfying the standards needed for sanctions under the MTCR.

- **Technical Recovery Operation: The Glomar Explorer.** *The Los Angeles Times* published a story on February 7, 1975 that the CIA had mounted an operation to recover a sunken Soviet submarine, its nuclear weapons and cryptographic equipment, from three miles deep on the Pacific Ocean floor. *The New York Times* ran its own version of the story the next day. Jack Anderson further publicized the secret operation on national television on March 18. In his memoir, former DCI William Colby wrote: "There was not a chance that we could send the Glomar [Explorer] out again on an intelligence project without risking the lives of our crew and inciting a major international incident.... The Glomar project stopped because it was exposed."[26]

Unlike spies, most of whom are eventually caught; leakers of classified information are infrequently identified. The dramatic cases of Snowden (who identified himself) and Manning are notable exceptions. Most leakers remain hidden, and only a handful have ever been prosecuted. The record is dismal. During the four-year period 2009-2013, intelligence agencies filed 153 crimes reports about classified leaks to the press with the Department of Justice. But only 24 were investigated; only half of these were identified, and not a single indictment was issued.[27] The scorecard reads: Leakers 153; Intelligence Community 0. In general, our legal system is ill equipped to deal with leakers.[28] And the culture that strongly supports First Amendment press freedoms often seems conflicted about whether leakers are really law-breakers and is skeptical that press leaks of intelligence actually do much damage. Perhaps the greatest damage to national security from press leaks, as with espionage, is opportunity costs: The intelligence that will never be collected or used for the nation's decision advantage because of the damage to or even the loss of classified collection sources and methods compromised by press leaks.

Conclusions

Importantly, American spies and government employees who leak classified information to the press have recently become a national priority for a concerted program to counter the threats they pose to national security. On November 21, 2012, the White House issued a Presidential Memorandum establishing a new Insider Threat Program. It aims to deter, detect, and mitigate such actions by government employees as espionage and unauthorized disclosures of classified information, including "vast amounts of classified data available on interconnected United States Government computer networks and systems."[29] While a notably important initiative, it falls dramatically short of the comprehensive steps really needed.

Until the United States makes game-changing improvements in the way it protects its sensitive and classified information, it cannot expect a fully performing intelligence community, military, or diplomatic corps. Poor performance in keeping secrets correlates directly with diminished capabilities of the major instruments of national power—and thus, a diminution of American power. The relationship is causal. A comprehensive, zero-based, review of how the nation keeps its secrets – and how to get better at it – is long overdue.

There is compelling evidence that the classified information protection (or secrecy) paradigm, created in the mid-twentieth century long before the modern digital age was even imagined, is woefully outdated and does not meet present day national security demands. This broken paradigm requires disciplined scrutiny that will determine whether it is so broken that it must be replaced. If repairable, we should identify what needs to be fixed and fix it without further delay. If we determine that the secrecy paradigm is beyond repair, then we should work to develop a new one. Continued failure should not be an option, and doing little or nothing about severe impairments in keeping state secrets is a prescription for failure.

Readings for Instructors

Bowman, M. E. "Dysfunctional Information Restrictions," *The Intelligencer* 15 (2), Fall/Winter, 2006-2007, 29-37.

Bruce, James B. "Laws and Leaks of Classified Intelligence: The Consequences of Permissive Neglect," *Studies in*

26. William Colby, *Honorable Men: My Life in the CIA* (London: Hutchinson, 1978), 413-418.

27. Sharon LaFraniere, "Math Behind the Leak Crackdown: 153 Cases, 4 Years, 0 Indictments," *The New York Times*, July 20, 2013.

28. See Bruce, "Laws and Leaks of Classified Intelligence" in *Studies in Intelligence*, 43-48; and W. George Jameson, "Holding Leakers Accountable: Considering a Comprehensive Leaks Approach," in Paul Rosenzweig, Timothy J. McNulty, and Ellen Shearer (eds.), *Whistleblowers, Leaks, and the Media: The First Amendment and National Security* (Chicago: American Bar Association, 2014), 207-234.

29. *https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-standards-for-executive-branch-insider-threat-programs*.

Intelligence 47 (1), March, 2003, 39-49.

Bruce, James B. "The Impact on Foreign Denial and Deception of Increased Availability of Public Information about U.S. Intelligence," in Roy Godson and James J. Wirtz (eds.), *Strategic Denial and Deception: The Twenty-First Century Challenge* (New Brunswick, NJ: Transaction Pub. Co., 2001), 229–240.

Gioe, David V. "Tinker, Tailor, Leaker, Spy: The Future Costs of Mass Leaks," *The National Interest*, Jan-Feb 2014.

Kramer, Lisa A. and Richards J. Heuer, Jr. "America's Increased Vulnerability to Insider Espionage," *International Journal of Intelligence and Counterintelligence* 20 (1), 2007, 50-64.

Office of the Director of National Intelligence, IC on the Record, at *http://icontherecord.tumblr.com/tagged/statement.*

Rosenzweig, Paul S., Timothy J. McNulty, and Ellen Shearer (eds.). *Whistleblowers, Leaks and the Media: The First Amendment and National Security* (Washington, DC: American Bar Association, 2014).

Schoenfeld, Gabriel. *Necessary Secrets: National Security, the Media, and the Rule of Law* (New York: W. W. Norton, 2010).

Sulick, Michael. *American Spies: Espionage Against The United States from the Cold War to the Present* (Washington, DC: Georgetown University Press, 2013).

James B. Bruce, Ph.D., is a senior political scientist at the RAND Corporation. He retired from the CIA in 2005 as a senior executive officer after nearly 24 years. He held management positions in CIA's Directorates of Analysis and Operations, and served as deputy national intelligence officer for science and technology in the National Intelligence Council. His unclassified publications have appeared in *Studies in Intelligence*, *American Intelligence Journal*, *Journal of Strategic Security*, *Defense Intelligence Journal*, *World Politics*, and several anthologies. He co-edited, with Roger George, *Analyzing Intelligence: National Security Practitioners' Perspectives*, 2nd ed. (Georgetown University Press, 2014). He is an adjunct professor at Georgetown University and previously an adjunct at Columbia and American Universities. He is a member of the board of directors of the Association of Former Intelligence Officers.

The author thanks Peter Oleson for his keen editorial skills and uncommon patience in improving the clarity of the original draft and making it shorter at the same time.
This article has been reviewed by CIA's Publication Review Board to ensure it contains no classified information. The views expressed here are solely those of the author.

"We laugh at honor and are shocked to find traitors in our midst."

— C.S. Lewis,
The Abolition of Man, 1943.