UNCLASSIFIED

Previous Next Contents

Laws and Leaks of Classified Intelligence

The Consequences of Permissive Neglect

James B. Bruce

> *It is "obvious and inarguable" that no governmental interest is more compelling than the security of the Nation.*
>
> US Supreme Court in Haig v. Agee (1981)

Intelligence requires secrets. And secrecy is under assault. The future of US intelligence effectiveness depends to a very significant degree on keeping its secrets about collection sources and methods and analytical techniques. When secrecy is breached, foreign targets of US intelligence—such as adversary countries and terrorists—learn about, and then often develop countermeasures to, US intelligence techniques and operations. As a result, the effectiveness of intelligence declines, to the detriment of the national security policymakers and warfighters, and the citizenry that it is meant to serve.

The US press is an open vault of classified information on US intelligence collection sources and methods. This has been true for years. But the problem is worse now than ever before, given the scope and seriousness of leaks coupled with the power of electronic dissemination and search engines. The principal sources of intelligence information for US newspapers, magazines, television, books, and the Internet are unauthorized disclosures of classified information. Press leaks reveal, individually and cumulatively, much about how secret intelligence works. And, by implication, how to defeat it.

This significant issue—the unauthorized disclosure of classified intelligence—has been extraordinarily resistant to correctives. It will never be solved without a frontal assault on many levels, and an essential one is US law. This article addresses key legal issues in gaining better control over unauthorized disclosures that appear in the press. It advocates a range of legal solutions that have not been tried before, some of which are controversial. The views expressed here are my own.[1]

Importantly, I would not hold these views had I not come to them from the vantage point of 20 years in the intelligence business, and particularly my last seven with the Foreign Denial and Deception Committee. This committee represents an inter-agency effort to understand how foreign adversaries learn about, then try to defeat, our secret intelligence collection activities. I have come to appreciate that unauthorized disclosures of classified intelligence pose a serious, seemingly intractable, problem for US national security. The Director of Central Intelligence, George Tenet, made the point during an interview, that unauthorized disclosures "have become one

of the biggest threats to the survival of US Intelligence."[2] A skeptical public can rightly question whether the DCI might not be exaggerating the seriousness of the problem. Unfortunately, he is not, and no intelligence specialist who is knowledgeable about the damage caused by leaks would disagree.

This presents an important anomaly in public discourse: Nearly all of the compelling evidence in support of the argument that leaks are causing serious damage is available only in the classified domain. It thus seems daunting to make a persuasive public case for legal correctives to address unauthorized disclosures when so little of the evidence for it can be discussed publicly. Proponents for better laws—it will soon become clear why I am one of these— sometimes feel that this is not a fair fight. Freedom-of-the-press advocates and professional journalists exert disproportionate influence on this debate, at least when compared to advocates of criminal penalties for the leaking and publishing of sensitive classified intelligence. But I have come to believe that First Amendment objections to criminal penalties for disclosing classified *intelligence* now demand a more critical reconsideration than we have given them to date.[3] Once we get over this hurdle, it will be more of a fair fight, a more reasoned debate.

The Seriousness of Unauthorized Disclosures

> *Any sources and methods of intelligence will remain guarded in secret. My administration will not talk about how we gather intelligence, if we gather intelligence, and what the intelligence says. That's for the protection of the American people.*
>
> President George W. Bush, following the 11 September 2001 terrorist attacks on the World Trade Center and the Pentagon.[4]

It is a myth, too commonly held outside the Intelligence Community (IC), that leaks really do not do much harm. The genealogy of this erroneous view traces to the publication of *The Pentagon Papers* in 1971. After much government carping about all the damage that those Top Secret revelations in the press would do to US national security, few today would claim that any damage was done at all. And I am unaware of any that was done to intelligence. *The Pentagon Papers* flap took us off the scent. The view that leaks are harmless is further nourished by other popular myths that the government over-classifies everything —including intelligence—and classifies way too much. This seduction has become a creed among uncleared, anti-secrecy proponents. But this, too, at least in regard to intelligence, I would argue, is wrong.

A recent classified study of media leaks has convincingly shown that leaks *do* cause a great deal of harm to intelligence effectiveness against priority national security issues, including terrorism. This is principally because the press has become a major source for sensitive information for our adversaries about US intelligence—what it knows, what it does, and how it does it. Unfortunately, serious leaks of US intelligence cumulatively provide substantial information to foreign adversaries. At CIA alone, since 1995 there have been hundreds of investigations of potential media leaks of Agency information, and a significant number of these have been referred to the Department of Justice for follow-up action. Leaks that have damaged the National Security Agency's (NSA) signals intelligence sources and methods also number in the hundreds in recent years; dozens of these cases have also been referred to Justice. The National Imagery and Mapping Agency (NIMA) has experienced roughly a hundred leaks just since 2000 that have damaged US imagery collection effectiveness. Many dozens of leaks on the activities and programs of the National Reconnaissance Office (NRO) have also helped foreign adversaries develop countermeasures to spaceborne collection operations. DIA and the military services, too, have suffered collection losses as a result of media leaks.

It is impossible to measure the damage done to US intelligence through these leaks, but knowledgeable specialists assess the cumulative impact as truly significant. Some losses are permanent and irreversible; others can be recovered, though sometimes only partially, and with the expenditure of substantial resources that could

well be spent elsewhere.

While leaks of classified information are often intended to influence or inform US audiences, foreign intelligence services and terrorists are close and voracious readers of the US press. They are keenly alert to revelations of US classified information. For example, a former Russian military intelligence officer wrote:

> *I was amazed—and Moscow was very appreciative—at how many times I found very sensitive information in American newspapers. In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier.*[5]

I call this the *Lunev Axiom*: Classified intelligence disclosed in the press is the effective equivalent of intelligence gathered through foreign espionage. Importantly, more than just Russian intelligence officers understand this. Key adversaries of the United States, such as China and al-Qaida, derive a significant amount of their information on the United States and US intelligence from the media, including the Internet. What we need to understand are the legal implications of this key principle.

Reported Examples of Intelligence Losses due to Press Leaks

Soviet ICBM testing, 1958. *A New York Times* story on 31 January 1958 reported that the United States was able to monitor the eight-hour countdown broadcasts for Soviet missile launches from Tyuratam (now Baykonur), Kazakhstan, which provided enough lead time to dispatch US aircraft to observe the splashdowns and, thus, collect data used to estimate the accuracy of the intercontinental ballistic missiles. Following publication of the article, Moscow cut the countdown broadcasts to four hours, too little time for US aircraft to reach the landing area. Occurring in the midst of the missile-gap controversy, the publication of the press item left President Eisenhower livid, according to Wayne Jackson in *Allen Welsh Dulles, Director of Central Intelligence* (July 1973, declassified history, Volume IV, pp. 29-31, in Record Group 263, National Archives). According to the same source, some intelligence was lost forever, and, to recoup the remainder, the US Air Force had to rebuild an Alaskan airfield at a cost of millions of dollars.

Politburo conversations, 1971. In a 16 September 1971 column in *The Washington Post*, Jack Anderson wrote that US intelligence was successfully intercepting telephone conversations from limousines used by members of the Soviet Politburo in Moscow. In his book, *For the President's Eyes Only* (New York, NY: Harper Perennial, 1966, p. 359), British historian Christopher Andrew says that this US collection program producing highly sensitive information ended abruptly after Anderson's revelations.

Soviet submarine, 1975. *The Los Angeles Times* published a story on 7 February 1975 that the CIA had mounted an operation to recover a sunken Soviet submarine from the Pacific Ocean floor. *The New York Times* ran with its own version the next day. After this story broke, Jack Anderson further publicized the secret operation on national television on 18 March. In his memoir, *Honorable Men: My Life in the CIA* (London: Hutchinson, 1978, pp. 413-418), 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."

How Leaks Hurt

The Intelligence Community faces improved foreign countermeasures as adversaries use leaks to expand their understanding of US intelligence. In the mid-1990s, for example, dozens of press articles covered the issue of whether Chinese M-11 missiles had been covertly transferred to Pakistan. If 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 mandates sanctions against proven MTCR violators.

Reports in the Washington press claimed that US intelligence had indeed found missiles in Pakistan, but that the information, apparently, was not solid enough to trigger sanctions. Based on numerous leaks, readers of both *The Washington Times* and *The Washington Post* learned that intelligence had failed to convince the Department of State of the missiles' existence. "Spy satellites," the press announced, were unable to "confirm" the presence of such missiles. The message from the press coverage was, in effect, that any nation—such as Pakistan or other signatories to the MTCR who sought to circumvent its terms— 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 specific countermeasures that other potential violators could take to prevent US intelligence from satisfying the standards needed for sanctions.

US imaging capabilities are a favorite press topic. An example is leaked intelligence about India's nuclear program in the mid-1990s. Unauthorized disclosures about issues such as this have revealed to our adversaries, directly and indirectly, unique elements that underpin our analytic tradecraft. Thoughtful manipulation by adversaries, as well as friends, of such knowledge exposed in the press impairs our ability to provide policymakers with timely intelligence before they are taken by surprise—as happened when the Intelligence Community failed to warn of the Indian nuclear tests in May 1998.6

In addition, effective intelligence depends on cooperative relationships with friendly governments and individuals who trust the United States to protect their confidences. Press disclosures can—and sometimes do—undermine these relationships, making both governments and individuals reluctant to share information, thereby inhibiting intelligence support crucial to informed policymaking, counterterrorist efforts, and, when necessary, military operations.

In 1998, for example, newspaper reports provided lengthy coverage of UNSCOM, the UN Special Commission charged with inspecting Iraq's weapons of mass destruction (WMD) facilities following the Gulf war. These reports were widely cited in subsequent worldwide media coverage. Although the articles contained many inaccuracies, information in them interfered with the US government's ability to aggressively pursue its policy on Iraqi weapons inspections. Other serious leaks clearly have degraded Washington's ability to obtain intelligence on Iraq. Damaging press disclosures based on imagery-derived intelligence on Iraq have included the movement of missile systems, the construction of a new command and control network, and the dispersal of WMD equipment following the 11 September 2001 terrorist attacks in New York and Washington.

Terrorists feed on leaks. Through their investigations into whether the 9/11 attacks resulted from intelligence failure, Congress and the special Commission will learn that important intelligence collection capabilities against Osama bin Laden and al-Qaida were lost in the several years preceding September 2001. With the concurrence of NSA, the White House officially released just one of these. As press spokesman Ari Fleischer explained:

> *And let me give you a specific example why, in our democracy and in our open system, it is vital that certain information remain secret. 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. 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.[7]

What the public cannot easily know, because the overwhelming bulk of this intelligence must necessarily remain classified, is that the bin Laden example cited here is just *the tip of the iceberg.* In recent years, all intelligence agencies—CIA, NSA, NIMA, NRO, and the Defense Intelligence Agency, to cite just the larger ones—have lost important collection capabilities, including against high-value terrorist targets. These losses have impaired human operations, signals intelligence, and imagery collection. And they have deprived analysts and policymakers of critical information, unavailable elsewhere, that they should have had.

Weak Enforcement

The seriousness of the [unauthorized disclosures] issue has outpaced the capacity of extant administrative and law enforcement mechanisms to address the problem effectively.

Attorney General John Ashcroft[8]

Logic and facts reveal a highly inverse correlation between law enforcement and leaks: the less the enforcement, the greater the leaks of classified information—and probably the other way around as well. A statistical approach is impossible, however, because there has been only a single example of any prosecution for an intelligence leak—Navy analyst Samuel Loring Morison in 1985. The glaring absence of criminal penalties for leaking and publishing classified intelligence establishes a law enforcement climate of utter indifference—actually permissive neglect. The unofficial message seems to be: Leak all you want, and no matter how much, or how serious, nothing will happen to you.

Perversely, for perpetrators there seem to be only *benefits* to leaking, rather than penalties. Anonymous government officials seek to skew public debate in their favor by selectively leaking intelligence that supports their favored policy positions. Journalists and book publishers can gain policy influence, brandishing relevant intelligence that their opponents may not have seen and cannot easily refute—at least not in the press, without more leaks. But also, over time, journalists and writers can gain public renown and recognition—better newspaper, magazine, and book sales—as well as bigger incomes and profits, merely by exploiting the classified materials that law-breaking government officials provide to them. This unholy alliance works exceedingly well as long as the legal climate remains indifferent to it.

Laws on Leaks

Is leaking classified intelligence against the law? Probably—but you would not know it from the prosecution's data: Morison, as noted, has been the only person convicted, and he was pardoned as President Clinton was leaving office. President Clinton also vetoed the "Shelby Amendment," an anti-leaks law written into the FY2001 Intelligence Authorization Act.

It is precisely the legal ambiguity of leaking that is the heart of this problem. Certainly there are laws against it—chiefly the 1917 espionage law (Title 18 US Code §§ 793 (d)-(e) and 798) and the narrower Intelligence Identities Protection Act (Title 50 USC § 421). One could devote a whole legal seminar to what is wrong with these laws— and I urge legal experts to address this. But suffice it here to offer a non-lawyer's view that a law that is almost never enforced is either unneeded or useless. I contend that effective anti-leaks laws are urgently needed—but since the present ones are not enforced and virtually unenforceable, they are useless. Worse, consistent conspicuous failure to enforce these laws actually *encourages* the very crimes that they proscribe.

This problem is not new. The "Willard Report" (after its chairman Richard K. Willard, then Deputy Assistant

Attorney General) drew an unsettling conclusion two decades ago:

> *In summary, past experience with leak investigations has been largely unsuccessful and uniformly frustrating for all concerned .... This whole system has been so ineffectual as to perpetuate the notion that the government can do nothing to stop the leaks.*[9]

Legal correctives proposed in the Willard Report resulted in draft legislation in 1984. Although supported by the Office of Management and Budget and the Reagan Administration, the Intelligence Community later withdrew the legislation due to a perceived lack of support.

Twelve years later, responding to a request from the Assistant to the President for National Security Affairs, the National Counterintelligence Policy Board (NACIPB) completed another study and reported no discernible change in the government's ability to control leaks. The 1996 report explained the continuing failure as a result of two key factors:

- A lack of political will to deal firmly and consistently with unauthorized executive branch and Congressional leakers.

- The use of unauthorized disclosures as a vehicle to influence policy.[10]

Given the palpable history of failure to protect classified intelligence information from press disclosures—and given the epidemic proportions of leaks and the deleterious consequences they wreak in countermeasures that reduce the effectiveness of US collection—it is fair to question why past failed approaches should be expected to work today. They will not.

There has never been a general criminal penalty for unauthorized disclosures of classified intelligence. Although intelligence leaks technically can be prosecuted under the espionage statutes (18 USC §§ 793 and 798), only the single case, *US v. Morison,* ever has been. Given that literally *thousands* of press leaks have occurred in recent years—many serious and virtually all without legal penalty— it is clear that current laws do not provide an effective deterrent to leakers or to the journalists and their media outlets that knowingly publish classified intelligence.

Federal law enforcement officers would probably agree that bad laws are hard to enforce. A penetrating critique of what passes for anti-leak laws is provided in a comprehensive Note in the June 1985 *Virginia Law Review* by Eric Ballou and Kyle McSlarrow. Although written before the Morison prosecution, the chief points remain as valid today as when written. A key passage highlights the responsibility of Congress:

> *The disjointed array of statutes shows that Congress does not have a comprehensive scheme to deal with the problem of leaks. The existing statutes either prohibit those disclosures with a specific intent to harm the United States or to advantage a foreign nation, or they apply only to a few narrowly defined categories of disclosures. The specific intent statutes do not apply to information leaks because of their high culpability standard. Those statutes are more appropriate to the problem of classic espionage. As a result, persons who leak [classified] information to further public debate may do so with impunity, as long as the information they disclose is not protected by one of the more narrowly directed statutes. A second infirmity of the specific intent statutes is that they only protect information relating to the national defense. These statutes do not cover diplomatic secrets, nonmilitary technology, and other nonmilitary secrets that affect the country's security. The more narrowly directed statutes, although protecting some of this information, nonetheless constitute an incomplete solution to the problem of leaks. Congress has*

> *ignored large categories of information that should not be disclosed with impunity. In summary, Congress has not constructed a principled and consistent scheme of criminal sanctions to punish the disclosure of vital government secrets. Moreover, persons who leak government secrets are but one side of the problem; the government must also pursue remedies against those who publish secrets. Like the disclosure provisions, however, the statutes relevant to the publication of government secrets are vaguely drafted and incomplete.*[11]

A Call for New Laws

Given the intractable nature of controlling leaks, we need to try remedies that have not been tried before. I defer to the drafting skills of competent attorneys to translate any promising ideas here into workable legislation. My suggestions are grouped into three categories: Write new laws. Amend old ones. And enforce them all—new and old.

Given the fact that many thousands of leaks of classified intelligence in recent years have seriously damaged intelligence effectiveness, thereby jeopardizing the nation's security—and that existing penalties provide no effective deterrent to leaking—we urgently need a comprehensive anti-leaks statute to empower law enforcement and investigators to better protect intelligence. A new law should:

- Unambiguously criminalize unauthorized disclosures of classified intelligence.
- Hold government leakers accountable for providing classified intelligence to persons who do not have authorized access to that information, irrespective of intent; *and* hold unauthorized recipients accountable for publishing information that they know to be classified.
- Distinctly define "intelligence information"—including substantive content, activities, operations, and sources and methods—as distinguished from "defense information," creating a discrete protected category for intelligence that does not require proof that it is related to military defense.
- Provide better protection to especially sensitive and highly classified intelligence information in trials and other judicial proceedings than is presently afforded through the Classified Information Procedures Act.

Congress can ensure that such legislation is drafted in a manner that is consistent with constitutional requirements.

In addition, a separate new law should be crafted to provide the same protection to technical sensors deployed on any platform (space, air, land, sea) that is now afforded to human operations. Such a law would constitute a technical counterpart to the Intelligence Identities Protection Act (50 USC § 421).

Accountability

Should journalists have legal accountability? Absolutely, in my view. Few would dispute that the first line of enforcement must be drawn to include government officials who unlawfully steal and disclose classified intelligence. Like citizens everywhere, government officers have different opinions on the propriety of holding journalists legally accountable for what they publish. Still, I believe that to be fully effective, a worthy law should also hold uncleared publicists—i.e., journalists, writers, publishing companies, media networks, and Web sites that traffic in classified information—accountable for intelligence disclosures. Specifically, media representatives should be held responsible for publicizing intelligence information—thus, making it available to terrorists and other US adversaries—that they know to be classified. Whether journalists understand it or not—

and many probably do not—the public exposure of significant intelligence often damages intelligence effectiveness by compromising valuable US sources and methods. Journalists should also be held responsible under present criminal statutes for unlawful possession of classified documents when they have them.

Legal accountability for journalists is necessary because declassification authority is assigned *by law* exclusively to government officials, elected and appointed, through lawful procedures. Journalists who publish classified intelligence arrogate to themselves an authority legally vested in government that they do not by right possess. In publishing classified intelligence, no journalist can convincingly claim the constitutional right to do so. Any journalist's First Amendment right to publish information does not appear to—and should not— extend to disclosing lawfully classified intelligence information. In any case, a constitutional claim of right-to-publish classified intelligence remains to be established.

A close reading of Title 18 USC § 798 (sometimes referred to as the SIGINT statute) and 50 USC § 421 (the Intelligence Identities Protection Act) shows that journalists are *already* legally accountable for publishing leaked classified intelligence. But since no one has ever been prosecuted under these statutes, they remain unenforced and yet to be tested in the courts.

Like government officials, journalists also exercise a public trust. But they exercise it without any apparent legal accountability for violating the public trust when they reveal the nation's secrets. This is wrong. Legal accountability for journalists is especially needed in the absence of an enforceable code of ethics for journalist conduct.

The overwhelming majority of journalists do not publish classified information, and some recognize the ethical implications of compromising sensitive intelligence sources and methods.12 But a few egregious offenders traffic heavily in classified intelligence. In one example, Steven Aftergood, director of the Federation of the American Scientists' anti-secrecy project, has written that: "Over the past couple of years, Mr. Gertz [of the *Washington Times*] has written more stories based on classified government documents than you can shake a stick at, infuriating Clinton Administration officials and making a mockery of official classification policy." Aftergood also repeats a quote from Gertz that ran in the conservative *Weekly Standard*: "We believe in stories that make you say 'holy shit' when you read them," the columnist boasted.13 The complete lack of accountability of such journalists for costly compromises of information that jeopardize the nation's security must change under the force of law.

First Amendment Issues

Constitutional experts will address First Amendment implications of any proposed laws that may be interpreted to constrain freedom of the press. Importantly, the Supreme Court has not recognized an absolute right of publication. But neither has it made clear its conception of acceptable restrictions. Still, I believe that holding publishers of classified intelligence legally accountable under carefully drawn legislation would not be proscribed by the First Amendment.

Constitutional arguments will have to address First Amendment issues from a variety of angles:

- The government's exclusive authority to classify—and de-classify—government information is firmly established in law.

- Congress's willingness to regulate publications disclosing intelligence where the potential for serious harm exists is already established in the Intelligence Identities Protection Act (IIPA, 50 USC § 421), and in the SIGINT statute (18 USC § 798) as well.14

- One leaker (a government employee, not a journalist) has been convicted of providing classified information to the press, and this decision was upheld on appeal.15

- Publishing classified intelligence has not been established as a constitutionally protected right.

- A compelling argument can be made for extending the *harm principle* (see below) to protecting classified intelligence from press exposure when the nation's security is jeopardized as a consequence. For example, the media's assistance (unwitting, to be sure) to the terrorists who planned and conducted the attacks in New York and Washington on 11 September 2001 provides a vivid example of harm to intelligence that deserved better protection than we now afford it.16

Of course, the inherent tension between First Amendment rights and the government's interest in protecting national security is dynamic, and may never be solved "once and for all." But the current balance so favors First Amendment rights that compelling constitutional interests involving national security can be superseded. Here we should entertain redressing a potential constitutional imbalance by reconsidering a time-tested democratic principle first developed by the preeminent philosopher of liberty, John Stuart Mill:

> *. . . the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others.17*

Under the "harm principle"—for example, yelling "FIRE!" in a crowded theater when there is no fire—a variety of exceptions to free speech are well established in American law, such as obscenity, defamation, breach of peace, and "fighting words." To this list we should add: "the compromise of US intelligence required in the service of the nation's security."

Improving Existing Laws

Referring to the conclusion of the 1996 report of the National Counterintelligence Policy Board, if we lack the political will to write a new law—and I am convinced that lack of will is our chief obstacle here—then I urge that we amend our present, defective laws to help us curtail the loss of present and future US intelligence capabilities.

First, we should amend the 1917 espionage statute (18 USC § 793) to establish a distinct legal identity for intelligence information, activities, operations, and sources and methods—apart from national defense. Since a considerable number of intelligence activities can be argued as unconnected to national defense, stricter definition would remove the need to satisfy an additional prosecutorial burden. We should also ease the burden of intent or "willfulness" standards, requiring only that the government show that classified intelligence information was publicly disclosed. I would restrict any "intent" burden only to establishing a leaker's intent to knowingly *disclose* classified intelligence instead of the higher culpability bar of establishing intended *damage* to the nation.

Second, we should amend the Intelligence Identities Protection Act (50 USC § 421) to remove the burden of establishing "patterns" of disclosures, since some singular disclosures are so serious, perhaps resulting in loss of life, that legal penalties for exposing sensitive agents who risk their lives to help the United States and its allies must be clearly established. The intent standard should also be relaxed because agent identities can be revealed to discerning readers (such as foreign intelligence services or terrorist organizations) through merely descriptive information even when actual names are withheld. And, unless we craft a new law to accomplish this, I would broaden the scope of this narrow statute that now covers only human operations to also apply to technical collection activity, including from spaceborne sensors.

Third, we should amend 18 USC § 794 to include non-state actors such as terrorist organizations, along with "foreign governments or agents thereof" as is currently written, and soften the intent burden analogous to the amended § 793 above.

Finally, we would need to amend the Classified Information Procedures Act to afford much greater protection during investigative and judicial proceedings for highly sensitive compartmented information, which, when leaked, may not even be investigated or officially reported for prosecution. This legal timidity results from an understandable government incentive to avoid calling further attention to a particularly sensitive activity or capability. The US government has shown a debilitating reluctance to pursue legal remedies for the most serious leaks partly because subsequent courtroom publicity of sensitive information subverts its first objective of protecting such information from further disclosures.

Strengthening Enforcement

> *Until those who, without authority, reveal classified information are deterred by the real prospect of productive investigations and strict application of appropriate penalties, they will have no reason to stop their harmful actions.*
>
> Attorney General John Ashcroft[18]

Better enforcement will also require real political will—surely more than we have seen since *US v. Morison.* Where to begin? First, acknowledge the Lunev Axiom: Recognize that government leakers and the journalists who publish the classified materials they provide do the equivalent work of spies. Even if their motives differ, the effects can be the same. Through press leaks, unauthorized disclosures can be every bit as damaging as espionage because of the focused exploitation of the US press by adversaries. If leakers and journalists were caught providing some of this classified information clandestinely to a foreign power, they could, and some probably would, be prosecuted for espionage. But if published in the press—where leaked sensitive information becomes available to *all* foreign governments and terrorists, not just one—leakers and journalists alike derive effective immunity from prosecution under a government that lacks the will to enforce its laws.

Let me state this categorically: Adversarial foreign countries and terrorists rely heavily on the US press to acquire sensitive information about intelligence in order to deploy countermeasures against it. Since such disclosures can have the same effect as espionage, we should treat government leakers and their collaborating journalists as subject to the same laws that apply to spies whose work is more clandestine, but sometimes no more damaging. While the espionage statutes are, for the most part, seriously flawed in their applicability to leaks, for the present they are all that we have. Also, to date, neither leaker nor publisher has been taken to account under laws specifically designed to protect against damaging disclosures of sensitive signals or human intelligence. We should thus begin by trying to enforce the three pertinent laws now on the books: 18 USC § 793 against leakers; 18 USC § 798 against leakers and publishers of classified SIGINT information; and 50 USC § 421 against leakers and publishers who expose HUMINT sources.

We should also enforce 18 USC § 794 against leakers and publishers of classified intelligence whose disclosures injure the United States and advantage foreign nations just as surely as any spies' disclosures that are provided clandestinely. Further, we should empanel grand juries to determine criminal offenses for serious unauthorized disclosures, and compel journalists under *Branzburg v. Hayes* (408 US 665, 1972) to identify their law-breaking government sources of classified intelligence. In addition, we should subpoena—in the course of legal proceedings to recover stolen government property—classified intelligence documents that we believe are in the possession of government leakers or journalists, and thus outside the normal physical protections that the US government provides to sensitive classified intelligence information. Government officials, journalists, and

publishers who are found to be in possession of documentary classified intelligence should also be prosecuted under 18 USC § 641 for possession of stolen government property.

We need to recognize that sensitive intelligence information is classified by this government for good reasons—precisely because its protection really *is* essential to the security of the nation. But the legal protections we afford it are woefully insufficient, and not nearly as good as those we provide to other government or government-protected information—such as banking, agricultural, and census data, and even crop estimates and insider trading for securities— whose acquisition by foreign adversaries and terrorists would not make any difference at all.

Consequences of Not Acting

> *"If the law supposed that," said Mr. Bumble, "the law is an ass."*
>
> Charles Dickens, *Oliver Twist*

The consequences of legal inaction are high—perhaps higher than we should ask the American citizen to bear. Years of inaction, indifference, and permissive neglect are taking an enormous toll on US intelligence capabilities. And the toll is higher still since 11 September 2001. Intelligence leaks do serious and often irreversible damage to our sensitive collection capabilities. By publicly unveiling unique and often fragile collection capabilities through leaks, the media actively *help* our adversaries to weaken US intelligence. These disclosures offer valuable insights—at no cost to our enemies—into possible errors in their assessments of how well or poorly US intelligence works against them, as well as useful feedback on how well they succeed or fail in countering US intelligence. This kind of feedback also increases the risk of foreign manipulation of our intelligence for deception operations.

Unless comprehensive measures *with teeth* are taken to identify and hold leakers and their publishing collaborators accountable for the significant, often irreversible, damage that they inflict on vital US intelligence capabilities, the damage will continue unabated. Conceivably, without some legally effective corrective action, the situation could even worsen, leading to intelligence on significant national security issues that is less accurate, complete, and timely than it would be without foreign countermeasures made possible by unauthorized disclosures. Warning of surprise attacks against the United States by terrorists or other hostile adversaries could be further degraded. Moreover, multi-billion-dollar collection programs could become less cost-effective than they would otherwise be if foreign adversaries were not learning, through unauthorized disclosures, how to neutralize such programs.

The alternative is *better* intelligence capabilities for the United States. This can result through *no added costs* by merely better protecting the sources and methods we now have and those that are in the pipeline. Stemming press leaks will afford significantly better protection. Better laws—and enforcement of these laws—will make this possible. If we continue to be encumbered by a failure of will, our present climate of permissive neglect will become one of pernicious neglect.

James B. Bruce is Vice Chairman of the DCI Foreign Denial and Deception Committee.

1. Although some may still disagree with portions of the arguments presented here, this article has benefited greatly from valuable suggestions provided by Valerie Bruce, John Norton Moore, George Jameson, George Clarke, Larry Gershwin, Mark Monahan, and Penny Martin.

2. *USA Today*, 11 October 2000, p. 15A.

3. The scope of my concern with classified information here extends only to *intelligence*, which encompasses intelligence *information, activities, operations, sources, and methods*. I exclude from my purview other kinds of classified information, such as military (e.g., war plans and weapons systems) and diplomatic secrets, not because they are unimportant, but because I believe that intelligence increasingly requires a distinct legal identity.

4. *New York Times*, 14 September 2001, p. 18.

5. *Stanislav Lunev, Through the Eyes of the Enemy* (Washington, DC: Regnery Publishing, Inc., 1998), p. 135.

6. In the case of India's nuclear program, damaging press leaks disclosed sources and methods beyond the data revealed to New Delhi in the official demarches delivered in 1995 and 1996.

7. *White House press statement, 20 June 2002.*

8. Letter to the Speaker of the House in compliance with Section 310 of the Intelligence Authorization Act for Fiscal Year 2002, 15 October 2002, p. 4.

9. Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information, 31 March 1982, prepared for the President.

10. NACIPB, *Report to the NSC on Unauthorized Media Leak Disclosures*, March 1996, p. D3.

11. *Eric E. Ballou and Kyle E. McSlarrow, "Plugging the Leak: A Case for Legislative Resolution of the Conflict between Demands of Secrecy and the Need for an Open Government," Virginia Law Review*, June 1985, p. 5. See also Michael Hurt, "Leaking National Security Secrets: Effects on Security and Measures to Mitigate," *National Security Studies Quarterly*, Volume VIII, Issue 4, Autumn 2001; and Harold Edgar and Benno C. Schmidt, "The Espionage Statutes and the Publication of Defense Information," *Columbia Law Review*, Vol. 73, No. 5 (May 1973), pp. 929-1087.

12. See David Ignatius, "When Does Blowing Secrets Cross the Line?" *The Washington Post*, 2 July, 2000; and Ed Offley, "We are Aiding Osama bin Laden," *Defense Watch*, 24 September, 2001.

13. Steven Aftergood, *Secrecy in Government Bulletin*, No. 64, January 1997, p. 1.

14. Ballou and McSlarrow, p. 7.

15. *US v. Morison*, 844 F. 2d 1057, 4th Circuit, cert denied, 488 US 908, 1988.

16. The compelling example identified by Ari Fleischer (see page 42) is far from an isolated case. Numerous others in the classified literature show damage to counterterrorist capabilities in all collection disciplines, particularly SIGINT and HUMINT.

17. *John Stuart Mill, On Liberty, 1859.*

18. Letter to the Speaker of the House in compliance with Section 310 of the Intelligence Authorization Act for Fiscal Year 2002, 15 October 2002, p. 5.

Previous Next Contents

UNCLASSIFIED