PRELIMINARY DRAFT

DO NOT CITE

REVISION / February 28, 2005

TRANSPARENCY IN THE SECURITY SECTOR

Alasdair Roberts

A DECADE OF REVELATIONS

The 1990s were a decade of horrible revelation. Around the world, walls of secrecy that had been built in the name of national security collapsed, giving proof of the terrible abuses done by military, intelligence and police forces in the decades of the Cold War.

In 1992, a dissident KGB archivist, Vasili Mitrokhin, seized the opportunity created by the collapse of the Soviet Union to smuggle thousands of documents that revealed how Soviet leaders had wielded power over seven decades. The "Mitrokin Archive" provided evidence of Moscow's attempt to liquidate "enemies of the people", its disinformation campaigns against western leaders and its own dissidents, and infiltration of western governments, political parties, and media (Andrew and Mitrokhin 1999).

The collapse of military regimes throughout South America also unveiled evidence of systematic terror. In Paraguay, activists discovered tons of documents -- dubbed an "Archive of Terror" -- that traced the torture and execution of dissidents. Proof of collaboration among national intelligence agencies in "disappearances" was found in a court archive in Buenos Aires (Dinges 2004 233-241). In Chile and Argentina, truth and reconciliation commissions provided more evidence of human rights abuses by military and police forces.

In the Soviet Bloc, the end of the Cold War lead to the opening of the archives of the state security services. One million Germans applied within five years to read surveillance files of the Stasi, the East German secret police -- sometimes discovering that friends or co-workers had betrayed them as Stasi informers (Garton Ash 1998). The collapse of other authoritarian regimes led to further revelation of secrets once hidden in

the name of public security. South Africa's apartheid regime had relied on emergency laws that prevented the distribution of information about activity of the police and defense forces; the post-apartheid regime established a Truth and Reconciliation Commission that laid bare the cruelties of apartheid and adopted a new constitution that guaranteed a right to government information (de Giorgi 1999). In June 2002, Mexican President Vicente Fox Quesada released sixty thousand files that documented the government's long "dirty war" against its left-wing proponents, and signed the country's first right to information (RTI) law (Doyle 2003).

The United States itself tore down walls of secrecy throughout the decade, revealing many cases of governmental misconduct. Special projects were undertaken to declassify documents that revealed the government's complicity in the Chilean coup of 1973, and its knowledge of human rights abuses by Chilean and other South American security forces (Kornbluh 2003; Dinges 2004). Other declassification efforts uncovered the support given by U.S. officials to former Nazi officials in the earliest years of the Cold War (Breitman, Goda et al. 2004), as well as radiation experiments undertaken by government scientists on unwitting American citizens (Advisory Committee on Human Radiation Experiments 1995; Schwartz 1998).

These exercises in disclosure might have taught us something about the perils of allowing state actors to insist on absolute secrecy in the name of national security. Unfortunately, the lesson was not taken to heart. Even as right to information laws spread around the globe, the national security establishments within most governments remained enclaves in which the presumption of secrecy held fast. In fact, there is evidence that for a combination of reasons the problem of undue secrecy is becoming

more severe. Such secrecy is indefensible in principle, because it undermines political participation rights and other basic human rights. Excessive secrecy may also be imprudent as well: as we shall see, secrecy actually corrodes the capacity of government agencies to perform their mission of promoting better security. A sound policy is one that allows for open deliberation about the boundaries of secrecy, and effective independent review of government decisions to deny access to information.

THE SECURITY SECTOR AS A PROTECTED ENCLAVE

Throughout the Cold War, the security sector of government -- comprising agencies that are responsible for defense, intelligence and internal security[i] -- was regarded as a special enclave of secrecy, even in countries that professed a general commitment to open government. Security imperatives seemed to overwhelm any possible case for transparency in this sector. But the first decade of the post-Cold War period provided grounds for challenging the wisdom of this policy. Secrecy, justified in the name of national security, had provided cover for serious abuses of power. The rapid diffusion of right to information laws -- throughout Central and Eastern Europe, South America and South Africa -- seemed to suggest that in many places the old practice of blanket secrecy would no longer be followed.

Unfortunately, secrecy did not retreat so readily. For a combination of reasons, the security sector of government remained a protected enclave in which transparency norms held little or no sway. In many countries -- Russia, China, and Indonesia, to name a few major cases -- there was little success in establishing a statutory right to

government information at all. Elsewhere, the right to information was carefully bounded to preserve secrecy norms.

One difficulty was the limited scope of the many new RTI laws. The United Kingdom's Freedom of Information Act, adopted in 2000, explicitly acknowledged that a portion of the country's security sector would continue as a protected enclave. Some security agencies -- such as the intelligence service (MI6) and counterintelligence service (MI5) -- are not subject to the law at all (Wadham and Modi 2003). There is also a strict prohibition on disclosure of information sent by security agencies to other government departments, or which relates to security agencies. India's new Freedom of Information Act, adopted in 2002, takes a similar approach: the law does not apply to sixteen of the country's security and intelligence organizations. South Africa's National Intelligence Agency has lobbied for a similar exclusion from the South African law (Terreblanche 2003).

Other techniques were also used to protect an enclave of secrecy. In the United States, four intelligence agencies have successfully lobbied to have their "operational files" completely excluded from the country's Freedom of Information Act.[ii] Several countries give elected officials the right to issue "conclusive certificates" that can block any attempt to apply an RTI law to national security information. [iii]

Elsewhere, more liberal RTI laws have been confounded by the judiciary's unwillingness to challenge official claims that disclosure of information would compromise national security. In the United States, the United States Supreme Court said in a 1974 decision that the national RTI law gave it "no means to question any Executive decision to stamp a document 'secret,' however cynical, myopic, or even

corrupt that decision might have been."[iv] The U.S. Congress amended the law to expand the court's power, but judges still proved reluctant to challenge executive claims that disclosure of information would jeopardize national security.[v]

In the United States, and in many other countries, the field of national security is still one that is protected by a distinctive aura of impenetrability. Its influence is evident in the tendency of officials to deny categorically that there is a right to information relating to the work of institutions in the security sector. "The right to classified information is not a human right," the head of Slovakia's security bureau said in 2002 (SITA 2002). The Latvian Supreme Court reached the same conclusion in 2003.[vi]

Other forces have also compromised recently adopted RTI laws. One of these has been the diffusion of new state secrecy laws, which set rules for the handling of information that has been classified as secret by government officials. The trend was most obvious in Central and Eastern Europe, (CEE) where the spread of RTI laws in the early 1990s was followed, a few years later, by the spread of new state secrecy laws. These statutes affected access to information in two ways. Some state secrecy laws -- such as those as Belgium and Spain -- simply deny any right to information that has been classified as secret by officials (Banisar 2004). The grounds on which information can be classified may be very broad. In addition, these laws may impose severe penalties for the unauthorized disclosure of classified information by officials, or its subsequent publication by journalists.[vii]

The diffusion of state secrecy laws was one result of the reconstruction of political and military alliances in the post-Cold War era. In the early 1990s, CEE countries abandoned secrecy rules that had been imposed to preserve security within the

Soviet Bloc. By the end of the decade, however, many countries in the region were striving to join the North Atlantic Treaty Organization (NATO) -- and NATO expected that its members would adopt laws that ensured the security of information shared within the alliance. Precisely what NATO required in the way of new secrecy laws has never been made clear: NATO itself has refused to publish its standards. Nevertheless, many CEE countries said that their new state secrecy laws were tailored to meet NATO requirements. The European Union also tightened its secrecy rules as it began collaborating more closely with NATO. In several countries, the new laws prompted protests or constitutional challenges from civil liberties groups (Roberts 2003).

The decade also saw a growth in intergovernmental agreements on defense and intelligence cooperation that restricted the capacity of governments to respond to citizens' pressure for increased openness. In 2003, for example, the United States and the United Kingdom negotiated an agreement on the sharing of information relating to British participation in the development of the United States' controversial ballistic missile defense (BMD) system. The agreement prevents the United Kingdom from releasing any information received from the United States without its permission. The agreement itself, although unclassified, has been withheld by the British government, which relied on the national security exemption in its code on access to government document (BASIC 2003).

Secrecy within the security sector has also been bolstered by the increased reliance on private contractors within the sector. As Peter Singer has shown, private firms have taken on a growing role in defense, policing and intelligence work, often fulfilling functions that were once thought to be the exclusive responsibility of

government employees (Singer 2003). Although the security work undertaken by private firms can have a profound effect on human rights -- as controversies over the role of contractors in Iraq, Kosovo and Colombia have recently shown -- contractors are rarely required to comply with RTI laws (Roberts 2001). "Company contracts are protected under propriety law," says Singer, "often making their activities completely deniable" (Singer 2003 x).

The terror attacks of September 2001 also led to a consolidation of the rule of secrecy within the security sector, particularly in the United States. Government agencies withdrew much published information about vulnerable facilities and systems. Federal agencies also developed new policies for the sharing of unclassified information which threatened to undermine federal and state RTI laws. The Bush administration resisted demands for disclosure of information about individuals detained by the immigration service, about combatants or civilians held within a chain of secret prisons run by the Department of Defense, and about its motivation and plans for the invasion of Iraq. Other countries also restricted transparency following September 2001. Canada amended its RTI law to restrict access to national security information, and adopted special review procedures for information requests that appeared to have security implications (Roberts 2005).

CONSEQUENCES OF EXCESSIVE SECRECY

The case for greater openness in the security sector does not rest on a challenge to the importance of public security itself. As Thomas Powers has recently argued, public order is is a prerequisite for the construction of a viable liberal democracy. A society

cannot honor the civil and political rights of its citizens if it has not already obtained a reasonable level of security (Powers 2003). A widespread sense of insecurity can also compromise the legitimacy of a democratic state (Perez 2004 642). And a certain level of secrecy is essential for public order to be maintained. Complete openness would compromise efforts to collect intelligence about looming threats, and undermine efforts to plan for national defense or investigate criminal behavior.

There is a need for secrecy within the sector sector. But this does not imply that the security sector should be a protected enclave, in which a national security claims always trump for demands for openness. Officials often argue that national security claims *should* be a trump, and that officials themselves can be trusted to exercise power responsibly behind that wall of complete secrecy. However, experience has shown that a policy of total secrecy can create an environment within the security sector in which power is abused, and civil and political rights undermined.

In the early years of the United States' Freedom of Information Act, public officials made a determined effort to preserve the absolute secrecy of the security sector, arguing that any increased transparency would jeopardize vital national interests. Responding to President Johnson's concern about greater openness in the sector, the U.S. Congress included a broad exclusion for national security information in the first Freedom of Information Act, adopted in 1966. The 1966 law, a Supreme Court justice later said, "ordained unquestioning deference to the Executive's use of the 'secret' stamp."[viii] In the Pentagon Papers case (1971), the Nixon administration again warned about the dangers of interfering in "difficult and complex judgements" about the disclosure of national security information.[ix] In 1974, President Ford made an

unsuccessful attempt to block statutory changes that improved access to national security and law enforcement information, arguing that the proposals would would endanger vital interests of the United States.[x]

Throughout the 1970s, a succession of leaks and special investigations revealed how the United States' police, intelligence and defense forces had wielded power behind this wall of complete secrecy. The Pentagon Papers revealed how several administrations had escalated U.S. involvement in the Vietnam War, while publicly exaggerating the threat to the United States and the effectiveness of the American intervention (Ellsberg 2002). The Federal Bureau of Investigation had twisted legitimate counterintelligence efforts into a program aimed at monitoring and crushing legitimate political dissent. The Central Intelligence Agency had engaged in domestic spying, sponsored experiments with LSD on unwitting patients, and plotted efforts to assassinate foreign leaders and overthrow unfriendly governments (Olmsted 1996 97-108).

The same cycle -- demands for deference, followed by revelations of abuse -- has been repeated more recently. Senior officials in the Bush administration have criticized legislative controls such as the Freedom of Information Act as "unwise compromises" that "undermine the ability of the President to do his job" (Milbank 2002). As the administration's the "global war on terrorism" has expanded, officials have become more forceful in asserting the need for greater deference to executive branch judgements about the balance to be struck between security concerns and civil liberties. In January 2004, White House counsel Alberto Gonzales deployed this argument to rebuff calls for greater scrutiny of the administration's handling of detainees. Congress and the public, Gonzales

said, needed to rely on the administration's assurance that it was doing its best to reconcile security needs with detainees' rights (Gonzales 2004).

Unfortunately, revelations of abuse within American prisons and interrogation centers have provided new proof of the foolhardiness of a policy of blind trust. The U.S. government resisted scrutiny of its detention systems through the Freedom of Information Act, by the courts, or by non-governmental organizations such as the International Committee of the Red Cross. It did this in the name of national security. But its practice of complete secrecy created an environment that resulted in unjustified detention and torture, and ultimately in a collapse in the legitimacy and effectiveness of U.S. security forces.

In general, the power to obtain information held by government is important as a tool for protecting a range of basic human rights.[xi] Obviously there may be circumstances in which basic rights may have to be weighed against more fundamental security needs. But the danger, now demonstrated by much experience, is that governments that are able to operate within a enclave of secrecy will give little or no weight to basic rights. The Abu Ghraib prison scandal has showed how easily highly trained military and intelligence forces, operating with no expectation of public accountability, could descend to grievous abuses, including violations of the right to protection against arbitrary detention (Article 9 of the Universal Declaration of Human Rights), and the right to protection against torture or cruel, human or degrading treatment (Article 5 of the Declaration). Of course, the decade of revelations that followed the end of the Cold War revealed more widespread abuses of these rights by governments operating under the mantle of secrecy.

Political participation rights. A policy of strict secrecy can also undermine the right to participate effectively in political affairs. The Universal Declaration of Human Rights says that individuals have the right to take part in the government of their country, and that government should exercise its authority on the basis of the will of the people (Article 21 of the Declaration). Political participation is obviously compromised if citizens lack access to the information that is needed to make informed decisions about national policy. Secrecy compels the public to defer to the judgement of a narrow elite (Alterman 1998).

This has been illustrated by the debate over the process by which the American and British governments took the decision to invade Iraq. A decision to go to war is arguably one of the most important choices that a nation can be expected to make, because it involves an explicit gamble with human lives. Citizens are entitled to expect that they will be given an opportunity to make an informed judgment about the need for war. In the case of preventative rather than defensive war, this expectation cannot be dismissed on the grounds of urgency.

There is good evidence that citizens in the United States did not make an informed judgement about the Bush administration's proposed war with Iraq. In the months before the start of the war, opinion polling showed that a large majority of Americans believed that the Iraqi regime had weapons of mass destruction, and that it had played an important role in the September 2001 terrorist attacks. On the eve of war, almost half of Americans believed that Saddam Hussein had been "personally involved" in the attacks, and that some or most of the attackers had been Iraqis (Feldmann 2003; Kull, Ramsay et al. 2004 572).

In fact, the evidence available to U.S. government agencies did not establish that there was an immediate threat that the Iraqi regime would develop or use weapons of mass destruction. Nor was there good evidence that the regime had involvement with the September 2001 attacks (Bamford 2004). Nevertheless, senior policymakers in the Bush administration succeeded in contorting the available evidence to bolster the case for war with Iraq. National security concerns were invoked to justify the suppression of dissenting views held by officials within the intelligence community (Prados 2004 33 and 113). In the United Kingdom, the Blair government made similar efforts to bend the available evidence to make the strongest case for war -- a project that was also made easier by the secrecy which habitually coveres the British intelligence community, and which hid internal disagreements about the meaning that should be put on the evidence at hand (Rogers 2004 358).

Citizens of the United States and the United Kingdom had a right to participate in the decision to go to war that was undercut by overreaching secrecy. Much of the information that was withheld did not relate to pieces of intelligence, or sources of intelligence, which if released would compromise security. Instead, much of the withheld information related to the conflicting interpretations put on available intelligence by specialists within each government. The widespread disclosure of information in both countries as a result of inquiries following the war now show the extent to which the withholding of information was driven by political and not security concerns.

Transparency during emergencies. Many well-established democratic states, facing uncertain but potentially fundamental threats to their security, resort to the use of

emergency powers. Security agencies insist on a loosening of rules that restrict search and surveillance, arrest, detention and deportation. Policymakers insist that extraordinary circumstances demand immediate action, and that the usual processes for lawmaking must be circumvented. In moments of crisis, it is difficult for citizens to resist these calls for stronger state powers. Nevertheless, the resort to extraordinary powers is perilous. Under conditions of uncertainty, it is unclear how far the state should go, and there is the risk that it will overreact.

There is an understandable tendency for governments to insist on greater secrecy during emergencies. However, this is the moment at which openness actually plays an especially important role. Openness allows citizens to understand precisely what a grant of emergency authority means in practice -- how it is used, and how far it appears to compromise basic rights. It helps electorates to debate policy and correct over-reactions. Openness can also maintain the accountability of entire electorates, by subjecting them to scrutiny of citizens in neighboring democracies. And openness also limits the capacity of security agencies to abuse new powers.[xii]

In sum, openness is a critical safeguard against abuse or over-extension of emergency powers. This point has been affirmed in the United States since the terror attacks of September 11. The existence of a free press and unrestricted rights to free expression have allowed journalists and civil liberties groups to protest government policies of on the detention of aliens who are alleged to pose a national security risk. (The new policies allow detention of aliens based on minor violations of immigration law, or detention without charges "in times of emergency.") Such scrutiny -- and the risk

of embarrassment in world opinion -- have probably discouraged more dramatic steps against suspect aliens.

On the other hand, the capacity of civil liberties groups to monitor government has also been compromised by excesses of secrecy regarding these detention programs. As David Cole has observed, many of the details about the Bush administration's preventative detention program have been "shrouded in mystery" (Cole 2003 25). The U.S. Justice Department has refused to disclose the names of detainees or the place of their detention. In November 2001 the department also stopped providing a weekly statement on the number of detainees, already over one thousand, and subsequently refused requests for information about the detainees made under the Freedom of Information Act.[xiii]

By May 2002, over six hundred of these detainees had been subjected to deportation hearings that were closed to family members, journalists, and any other member of the public. The Justice Department did not rely routinely on classified information in these hearings, or impose nondisclosure requirements on the detainees or their lawyers -- actions that might explain or reflect a serious worry over national security. "The real concern," says Cole, "may not have been that Al Qaeda would find out what was going on, but that the American public would find out" (Cole 2003 27-30).

The secrecy which surrounds the 660 foreign nationals who are held at the U.S. military base at Guantánamo Bay, Cuba is more profound. The government has not identified all of the detainees or acknowledged their right of habeas corpus, which would compel the presentation of reasons for their detention. Although the International Committee of the Red Cross is permitted to visit the prisoners, it attempts to preserve its

neutrality by providing opinions in confidence to U.S. officials. Remoteness and military restrictions have limited media coverage. The government says that the Guanatanamo detainees may be tried in secret proceedings, using secret evidence, and with proscriptions imposed on defense lawyers against consultation with outside experts or public disclosure of information about the trials (Lawyers Committee 2003 56-58).

The wisdom of this emphasis on secrecy with regard to the United States' detainees could be questioned on purely tactical grounds. The government's treatment of aliens within the United States following September 11 had the effect of discouraging cooperation within immigrant communities, thereby undermining security efforts in the long run (Cole 2003 189). Its excesses have also stoked popular protests in allied nations and soured diplomatic relations with countries that should be partners in the war on terror.

More importantly, this secrecy also undermines the capacity of citizens to determine whether the new balance of security concerns and basic rights is appropriately struck. Secrecy denies citizens the ability to understand the real impact of new policies -- such as the accuracy of the government's suspicions about detainees, or the psychological effect of prolonged and indeterminate detention. Secrecy makes it easier to forget the individuals who have borne the burden of extraordinary measures, and in this way abets the process of normalizing emergency measures.

HOW OPENNESS PROMOTES SECURITY

Secrecy has been justified in the name of national security for so long that we naturally assume that the two ideas are perfect correlates, and that any limitation on

secrecy necessarily implies some weakening of security. In many respects this is incorrect. For at least three reasons, improved openness may actually improve the capacity of societies to preserve security.

Better policy decisions. In April 1968, Professor James C. Thomson Jr. wrote a widely acclaimed article in *The Atlantic* magazine that attempted to explain the weaknesses in the United States government's policy toward Vietnam. Thomson, who had served in the Kennedy and Johnson administrations, predicted that historians would look back at the Vietnam years and wonder how "men of superior ability, sound training, and high ideals" could have made decision that were "regularly and repeatedly wrong." The answer, thought Thomson, could be found largely in process of decision-making itself. The concentration of responsibility at the top lead to executive fatigue, and an inability to respond to new and dissonant information. This was compounded by a lack of expertise within key agencies and "closed politics" of policy-making on sensitive issues (Thomson Jr. 1968).

Defense Secretary Robert McNamara understood the weaknesses of the process by which decisions on Vietnam were being made. Unknown to Thomson, McNamara had taken the unusual step a few months earlier of commissioning a large study of American decisionmaking on Vietnam. Unfortunately the Pentagon Papers -- as they were eventually known -- did little to improve the quality of government policy. Classified as TOP SECRET, the papers were largely inaccessible inside government until leaked by Ellsberg in 1971.

The problems identified by Thomson were not unique to the Vietnam controversy. On the contrary, they are typical of large public bureaucracies. The concentration of

authority at the top of the bureaucratic pyramid means that leaders and their advisors are overwhelmed with information, juggling problems that are often be outside their area of expertise. Fatigue, confusion, and ignorance about key facts are commonplace, and the damage that can be done by flawed decision-making can be substantial. The price that America paid for the series of missteps on Vietnam was incalculable. A intervention begun with the aim of promoting the United States' own security turned into a "calamity", Thomson concluded -- a brutal, unwinnable and immoral war.

Increased openness can help to solve problems such as these. By granting access to internal documents, governments give non-governmental organizations the capacity to spot bad analysis or contribute data not already collected by public agencies. Non-governmental organizations can also share the burden of synthesizing analysis and reaching conclusions about policy. The public sphere is a more powerful analytic engine than even the largest public bureaucracy, but it cannot be harnessed to serve the decision-making needs of government leaders without transparency. Of course, this policy may require the disclosure of information that would otherwise be protected in the name of national security. But the important point is that disclosure improves security in the long run -- by avoiding the tremendous costs that can be associated with poor bureaucratic decision-making.

Openness certainly would have improved the U.S. government's policy on the administration of post-war Iraq. There are strong similarities between the Bush administration's approach to post-war planning and the problems observed by Thomson thirty years earlier. The Bush administration carefully avoided a public presentation of its estimate of the cost of post-war reconstruction in Iraq and likely troop requirements

(Slevin 2003; Tyler 2003), as well as other elements of its occupation plan. This precluded effective public scrutiny and allowed decision-makers to act on assumptions about the nation's long-run obligations in Iraq which have since proved to be grossly inaccurate.

Moreover it stretched the administration's internal resources to the limit. James Fallows, writing in *The Atlantic* magazine in 2004, provides a description of post-occupation planning that is similar to Thomson's summary of thirty years earlier. "Everyone had that 'Stalingrad stare'," a senior administrator told Fallows, "People had been doing stuff under pressure for too long and hadn't had enough sleep" (Fallows 2004).

Improved agency coordination. Citizens outside government may not recognize that their complaints about lack of access to government information are often shared by officials who work inside public agencies. Rules designed to protect sensitive information can also impede the flow of information within government agencies, sometimes with disastrous consequences for national security. The United States' Congressional Joint Inquiry into September 11 concluded that such impediments contributed to country's inability to prevent the terror attacks in New York and Washington (Congressional Joint Inquiry 2002).

This problem is not unique to the United States. In the southern Chinese province of Guangdong, a similar obsession with secrecy in the name of national security also imposed a terrible cost. In the early weeks of 2003, the province's health department received a warning from a government health committee about the emergence of a dangerous new pneumonia-like illness -- later identified as severe acute respiratory

syndrome, or SARS. Unfortunately, the warning came in a document classified TOP SECRET, and for several days there was no employee in the health department with the security clearance to read it.

Guangdong's health officials, fearful of criminal penalties for disclosure of state secrets, later failed to share the information with colleagues who had begun to encounter the mysterious new disease in Hong Kong (Pomfret 2003). At the same time, China's government-controlled media were restrained from publishing information about the epidemic (Congressional-Executive Commission on China 2003 36-38). This chokehold on information produced the disruption which secrecy had been intended to avoid: needless deaths; broad damage to the Chinese economy; and further corrosion of the credibility of government officials.

The weaknesses of conventional approaches to information security are now widely recognized, even within government. The rules on management of classified information that were designed in the early years of the Cold War are now seen to encourage the over-production of "classified information" and impose excessively strict limitations on the circulation of classified information to other officials (Berkowitz 2001). As a consequence, this is an area in which internal pressure for reform of information controls coincides with external pressure for reform. For government agencies to do a better job of protecting national security, they will need to reduce the incentives for over-production of classified information and liberalize rules on the distribution of classified information within government. Incidentally, this will make it easier for non-governmental organizations to argue that the benefits of public disclosure of information outweigh the potential harm to national security.

Public disclosure of information can also be an effective way of circumventing information blockages within large bureaucracies. Frontline officials in government agencies do not rely exclusively on internal sources for information on how to do their jobs effectively: they rely on public sources -- the print and electronic media -- as well. The sheath of publicly accessible information that surrounds every government organization plays an important but unacknowledged part in maintaining the organization's effectiveness. As Tom Blanton points out, it was publicly accessible information, and not internal communications, that provided a US Customs official with the clues needed to detain a suspicious visitor to the United States -- and thereby thwart a terror attack apparently planned for Los Angeles or Seattle on the eve of the millenium (Blanton 2003 65-66). Improved transparency enriches the informational environment in which frontline officials do their work.

Fighting bureaucratic inertia. National security is a function that stretches the capacities of public organizations to their limits. It requires that intelligence and defense bureaucracies stay on alert for events that rarely occur. Unfortunately, we know that bureaucracies find it hard to maintain vigiliance and readiness at a high level for prolonged periods of time. Human and organizational factors can conspire to make security agencies inattentive and sluggish.

Oversight by political leaders and legislators is one way of ensuring that security agencies maintain their vigilance and readiness. But this kind of oversight has its own limitations. Top decision-makers have limited time and are distracted by multiple problems, many of which can seem more urgent than the hypothetical dangers posed by inadequate readiness.

Oversight by non-governmental organizations -- made possible by access to information held by security agencies -- can compensate for inadequate supervision within the political process. However, the ability of non-governmental organization to exercise oversight is often constrained precisely because access to information is denied on the grounds of national security. This is, of course, another irony: long-term risks to security created by weak oversight are allowed to fester because of a short-term concern with risks posed by openness.

This has become a common problem since the September 2001 terrorist attacks. For instance, Canada's transport ministry stopped releasing the results of its routine airport security screening tests, previously made available through its RTI law. Government officials justify the decision by arguing that the data would provide a road-map to terrorists looking for vulnerable points in the Canadian airport system. But the Canadian government could have released summary data for the entire system that would have showed whether efforts to improve security were making headway. A legislative committee later complained about "unreasonable secrecy" surrounding the test results. The committee's chair argued that secrecy "hides incompetence [and] inefficiencies" and warned that the refusal to release information could endanger lives (Bronskill 2003).

Secretiveness has also compromised efforts to monitor progress in securing ports. In June 2004, a spokesman for the International Maritime Organization complained that the agency had little information about national efforts to comply with new security requirements, because of governments' reluctance to alert terrorists to vulnerabilities (Shipping Times 2004). The United States Department of Homeland Security has denied Freedom of Information Act requests for information about inspection practices at U.S.

seaports, as well as information about grants given to seaport operators for security improvements, on similar grounds.[xiv]

New rules developed by the Department of Homeland Security to protect "critical infrastructure information" that are contained in the U.S. Homeland Security Act of 2002 create similar difficulties of accountability. The rules impose an absolute prohibition on the public disclosure of information about the vulnerabilities of privately-owned infrastructure, such as communication or water systems. Obviously this sort of information needs some protection. But critics have complained that the complete ban on disclosure will actually increase the danger to security in the long-run, by reducing the capacity of citizens to exert pressure for improvements (Steinzor 2003 664).[xv] As Joseph Jacobson says, efforts to restrict information about vulnerabilities in critical infrastructure will easily be overcome by determined terrorists -- so that restrictions will do no good, and serve only to compromise public monitoring of government efforts to fix vulnerabilities (Jacobson 2002).

DEFINING THE LIMITS TO SECRECY

There have been at least two efforts by non-governmental bodies to draft general principles about openness and national security. In 1995, a group of leading experts on freedom of expression and transparency met in Johannesburg, and prepared a declaration -- the Johannesburg Principles -- that sought to define the limits to secrecy in the security sector (Mendel 2003). The declaration included four key propositions:

- That the public's right to information held by the security sector must be recognized;

- That agencies within the security sector should permitted to withhold only "specific and narrow" categories of information, enumerated in law, to protect national security;
- That these justifications for withholding information must be put aside if some larger public interest would be better served by disclosure; and
- That there should be independent review of a government decision to deny access to information on the grounds of national security.[xvi]

In 2001, the freedom of expression group ARTICLE 19 proposed a model RTI law that would allow government agencies to withhold information if disclosure would be likely to cause "serious prejudice to defence or national security," unless there is a broader public interest in disclosure, and subject to the requirement of review by an independent tribunal.[xvii]

There is an important distinction between the Johannesburg Principles and ARTICLE 19's Model Law. The two documents share an interest in keeping the bar for non-disclosure high. But the 1995 Principles attempt to achieve this goal by enumerating the "specific and narrow" categories of information that could be withheld for national security reasons, while the 2001 Model Law proposes a rigorous but general test of serious prejudice to national security. Which of these two approaches is more appropriate? This question has often provoked spirited debate -- as it has recently during the revision of the Czech Republic's Classified Information Protection Act (Svatosova 2003).

The rationale for insisting on a precise enumeration of the categories of information that might be protected on national security grounds is clear enough. The

expectation is that this will impose a check on the temptation of governments to invoke national security considerations indiscriminately, thereby withholding information that properly belongs in the public domain. However, the effectiveness of this check should not be overestimated. American law defines six circumstances in which information can be withheld on national security grounds[xviii], but complaints about the indiscriminate withholding of information in the name of national security have persisted in any case (Leonard 2004).

There are, in addition, potential dangers associated with a too-detailed enumeration of the categories of information that can be withheld for national security reasons. Any such enumeration may be inflexible, and incapable of adapting to shifts in perceptions about threats to national security and the degree of secrecy that is needed to counter those threats. It is arguable, for example, that rules of thumb about secrecy and openness that were developed in the Cold War era are no longer suited to a world in which security threats are posed by loose networks of non-state actors. The practice of withholding information about intelligence agency budgets may have had some justification in a world dominated by superpower rivalries, but seems to have little justification today. By contrast, our calculus about the risk of disclosing information about private chemical facilities -- which during the Cold War would have faced a low risk of sabotage from other governments outside a state of war -- has clearly changed. As we noted earlier, a shift in threats might also lead to greater openness, by prodding a reassessment of the practice of holding information about homeland security threats closely within a small group of senior decision-makers.[xix]

There are two truly critical elements in a policy within the security sector. The first is an insistence that the standard for withholding information should be rigorous. A law that requires a mere apprehension of possible harm is likely to be abused, resulting in the denial of access to information that properly ought to be in the public domain. (In Vietnam, the ordinance on state secrets is so broadly drawn that economic data that is routinely published elsewhere is classified, its disclosure punishable by death (Kazmin 2003).) It ought to be necesssary for officials to substantiate that disclosure of information would pose a serious threat to public security.

The second critical element is that decisions to withhold information on security grounds should be subject to effective review by an independent office. Independent review accomplishes several goals. In general, the threat of independent review encourages officials to make their initial decisions about disclosure more carefully. It also provides a remedy in cases where agencies have attempted to use national security as a pretext for avoiding embarrassment or accountability for misconduct. Finally, the process of independent review encourages public discussion about where the line should be drawn between secrecy and openness.

The extent to which government agencies may abuse the discretion given to them by the absence of effective independent review has been illustrated in two high profile cases in Europe and the United States.

The first case arose in 1979 after a Swedish carpenter, Torsten Leander, was denied work at the Swedish Naval Museum, following an unfavorable decision in the security vetting process. Leander suspected that he had been denied a security clearance because of his earlier and lawful involvement with radical organizations -- an outcome

that was explicitly barred by Swedish law. Leander asked to see the information that had been used to reach the decision, and was denied on national security grounds. The case was appealed to the European Court of Human Rights, which decided in 1987 that the Swedish government was justified in denying access to the information. Although the Court did not itself inspect the information, it was satisfied with the safeguards imposed on the security clearance system, such as the statutory restriction on collection or use of information about lawful activities and the oversight role played by the Minister of Justice, legislators, and special officers such as the Swedish Chancellor of Justice.[xx] The *Leander* decision became a leading case in European human rights jurisprudence.

A decade later, after the end of the Cold War, Leander finally received his file, which showed that the Swedish government had lied to the European Court of Human Rights. Leander had in fact been denied work because of his political affilations. Other documents showed a spectacular corruption of the security clearance system. The Swedish Security Police, operating under secret instructions that flatly contradicted national law, had routinely collected information about the lawful political activities of Swedish citizens. A succession of government ministers had sanctioned the practice. Legislators and other overseers had either neglected to monitor the Security Police or quietly approved of their work. In 1990, the Chancellor of Justice had issued a public report clearing the government of wrongdoing -- and at the same time prepared a secret report to the government that documented systematic abuses of national law. In 1987, Leander received a public apology from the Swedish government, while the Security Police -- in the understated words of his lawyer -- "suffered certain legitimacy problems" (Tollborg 2003).

A comparable controversy has recently arisen in the United States. In 1952 the United States Supreme Court heard arguments in a case that arose following the death of three civilians in the crash of an Air Force B-29 Superfortress. The widows of the three men had asked for the Air Force's investigation report, and the Air Force refused, arguing that release of the information would seriously hamper national security by revealing details about the test of highly secret electronic equipment. The U.S. Supreme Court, without inspecting the report itself, acceded to the Air Force's position and ruled that the report need not be released to the widows. Relying in part on the *Reynolds* decision, the federal government made comparable arguments against disclosure in a growing number of cases in succeeding years (Weaver and Pallitto Forthcoming).

In 2000, a daughter of one of the three victims finally obtained the investigation report, which became publicly available as part of routine declassification effort a few years earlier. The report contained no information about experiments with secret electronic equipment. On the contrary, it showed that the B-29 had crashed because of the Air Force's repeated failure to deal with mechanical problems that ultimately caused the plane's engines to catch fire. The Secretary of the Air Force and other senior officials had misled the Supreme Court when they said in 1952 that the threat to national security was so dire that even the Court could not see the documents. "In other words," as Tom Blanton says, "the *Reynolds* precedent -- cited in more than 600 subsequent cases . . . rose directly from government fraud and lies" (Blanton 2003 45-46).

Most of the devices used to preserve the security sector as an enclave of secrecy -- such as the wholesale exclusion of security organizations or security files, a demand for unqualified deference to classification decisions, or ministerial certificates that trump

access laws -- are designed to thwart effective independent review of government judgements about the weighing of security and transparency claims. They are problematic precisely because they deny an opportunity for independent review. Experience has showed that discretion that is given to government officials is easily misused to prevent accountability for abuses of authority and block public participation in critical decisions about government policy.

Governments sometimes resist the principle of third party review because of concern that this may lead to unauthorized disclosure of sensitive information. However, steps can be taken to minimize this risk. Ombudsmen or commissioners and their staff can be subjected to the same security clearance procedures that are applied to other public officials, and equally strong rules on the physical protection of sensitive information that has been delivered for review can also be maintained. The office of the Canadian Information Commissioner has operated under such rules for two decades without any instance of unauthorized disclosure of sensitive information sent to the office for review (Information Commissioner of Canada 2002 16).

THE BROADER CONTEXT

Despite important advances in the last decade, the security sectors of many governments remain enclaves of secrecy, largely unaffected by transparency norms. In fact, a combination of factors -- deeper networking among security agencies, privatization of security functions, and new concerns about security against terrorist attacks -- may actually be deepening the commitment to secrecy within the security sector.

For several reasons, excessive secrecy within the security sector is troubling. Experience has showed that secrecy corrodes accountability and increases the likelihood that basic rights will be abused. During periods of emergency, secrecy also compromises the ability of citizens to monitor and control the use of extraordinary powers. Secrecy can also compromise security, by restricting the ability of non-governmental actors to sort out complex questions of national policy and monitor bureaucratic performance in preparing for threats.

The principles that should govern transparency in the security sector are essentially the same as those that operate in any other sector of government. Agencies in the sector should be subject to a justiciable right of access to information. National security claims can be invoked to defend decisions to withhold information, but the bar for withholding information should be high. The possibility that reasons for withholding information might be outweighed by broader public interest considerations should be anticipated. The decision to withhold information should be subject to independent review, and not left in the hands of government officials.

These rules, codified in an RTI law. are a necessary condition for greater openness in the security sector. However, an RTI law alone may not be enough. In many countries, other laws may also play an important role in discouraging the outflow of information. In some Commonwealth countries, the ability to obtain government information is compromised by Official Secrets Acts that impose severe sanctions on public servants for the unauthorized disclosure of information. These laws are often said to perpetuate a culture of secrecy that undermines the influence of new RTI laws.

Restrictions on free expression could also dampen the impact of RTI laws. In Israel, censorship laws allow the government to block the publication of information regarded as sensitive on national security grounds. Felipe González has documented the chilling effect of Latin America's *desacato* laws, which may be used to impose criminal penalties on writers whose work shows contempt for public figures (Gonzalez 2003). Governments may also resort to cruder measures -- such as the expulsion of individuals whose reports are critical of security agencies. in June 2004, the Indonesian government attempted to expel the Jakarta-based representative of the International Crisis Group. The decision was said to be dictated by security forces that had been stung by the Group's complaints on human rights abuses (Johnston 2004).

Finally -- and perhaps most critically -- the effectiveness of an RTI law hinges on the capacity of journalists and non-governmental organizations to exploit the potential created by the law. If media outlets cannot invest the resources needed for thorough investigative work, the value of an RTI law is less likely to be realized. Independent oversight groups such as the United States' National Security Archive, the South African History Archive, or the United Kingdom's LIBERTY, also play a critical role.

In short, transparency in the security sector requires a combination of steps that improve the right to information, eliminate barriers to free expression, and build up civil society's capacity to exercise these rights.

NOTES

[i] The term is defined in more detail by Ball, N., J. K. Fayemi, et al. (2003). Governance in the Security Sector. Beyond Structural Adjustment: The Institutional Context of African Development. N. van de Walle and N. Ball. New York, Palgrave Macmillan**:** 263-304..

[ii] The Central Intelligence Agency, National Reconnaissance Office, National Imagery and Mapping Agency, and National Security Agency.

[iii] Such as Australia, New Zealand, the United Kingdom and Ireland.

[iv] Statement of Mr. Justice Stewart in *EPA v. Mink*, 410 U.S. 73 (1973).

[v] . "The courts," a panel of federal judges later explained, "are unschooled in diplomacy and military affairs" Fisher, L. (2004). The Politics of Executive Privilege. Durham, NC, Carolina Academic Press..

[vi] A Latvian citizen, the court said, "has no right of requiring access to state secrets." Judgment of the Constitutional Court of the Republic of Latvia in Case 2002-20-0103, April 23, 2003.

[vii] As was the case with the Bulgarian government's proposed amendments to the Penal Code provisions on unauthorized disclosure of state secrets. This controversy has been reported on by the Bulgarian Access to Information Programme, http://www.aip-bg.org.

[viii] Statement of Mr. Justice Stewart in *EPA v. Mink*, 410 U.S. 73 (1973).

[ix] Brief for the United States in *New York Times v. United States*, June 197, pages 18 and 25.

[x] Veto Message from the President on the Freedom of Information Act, *Congressional Records,* November 18, 1974, page 36243.

[xi] This argument is developed at greater length in Roberts, A. (2001). "Structural pluralism and the right to information." University of Toronto Law Journal **51**(3): 243-271..

[xii] The critical importance of openness as a discipline on the use of emergency powers is emphasized by Michael Ignatieff Ignatieff, M. (2004). Lesser Evil: Political Ethics in an Age of Terror. Princeton, New Jersey, Princeton University Press.. A similar argument is made by Michael Freeman Freeman, J. (1999). Private Parties, Public Functions and the New Administrative Law.

Recrafting The Rule of Law. D. Dyzenhaus. Portland, Oregon, Hart Publishing**:** 331-369..

[xiii] The United States Court of Appeals for the D.C. Circuit upheld the Justice Department's refusal to provide the information. See *Center for National Security Studies v. Department of Justice*, D.C.C.A., June 17, 2003. Leave to appeal was denied by the United States Supreme Court.

[xiv] *Coastal Delivery Corp. v. United States Customs Serv.*, No. CV 02-3838 (C.D. Cal. Mar. 17, 2003). See also Lin, J. (2003). Big Grant to Oil Firm Shrouded in Secrecy. Philadelphia Inquirer. Philadelphia..

[xv] Some critics have already complained that the Department of Homeland Security lacks the authority and resources to monitor security precautions for critical infrastructure in the chemical industry, while the industry itself appears to have little new investment in security since September 11 Kriz, M. (2003). Bush Not Doing Enough to Protect Chemical Plants, Critics Contend. GovExec.com**:** http://www.govexec.com/dailyfed/0803/080703nj3.htm..

[xvi] Principles 11 to 14 of the Johannesburg Principles Coliver, S. (1999). Secrecy and Liberty: National Security, Freedom of Expression, and Access to Information. The Hague, M. Nijhoff Publishers..

[xvii] Sections 22, 30, 35 and 44(2) of the Article 19 Model Law. The Model Law is published at http://www.article19.org/docimages/1112.htm.

[xviii] See Section 1.4 of Executive Order 12958, as amended by Executive Order 13292.

[xix] There is also a risk of assuming that a similar list of legitimate national security concerns will be suited to different countries. Social and political differences may mean that information which seems harmless in one country could pose a serious threat to order if disclosed in another country.

[xx] *Leander v. Sweden*, European Court of Human Rights, Application No. 9248/81, Decision March 26, 1987.

SOURCES

Advisory Committee on Human Radiation Experiments (1995). Final Report. Washington, DC, Advisory Committee on Human Radiation Experiments.

Alterman, E. (1998). Who Speaks for America? Why Democracy Matters in Foreign Policy. Ithaca, NY, Cornell University Press.

Andrew, C. M. and V. Mitrokhin (1999). The Sword and The Shield. New York, Basic Books.

Ball, N., J. K. Fayemi, et al. (2003). Governance in the Security Sector. Beyond Structural Adjustment: The Institutional Context of African Development. N. van de Walle and N. Ball. New York, Palgrave Macmillan**:** 263-304.

Bamford, J. (2004). A pretext for war: 9/11, Iraq, and the abuse of America's intelligence agencies. New York, Doubleday.

Banisar, D. (2004). Freedom of Information and Access to Government Records Around the World. Washington, DC, freedominfo.org.

BASIC (2003). Press Release: BASIC Acquires "Confidential" Document on Missile Defence. London, BASIC.

Berkowitz, B. (2001). "Secrecy and security." Hoover Digest **2001**(1): Web. http://www-hoover.stanford.edu/publications/digest/011/berkowitz.html.

Blanton, T. (2003). Beyond the balancing test: National security and open government in the United States. National security and open government. Campbell Public Affairs Institute. Syracuse University, Campbell Public Affairs Institute.

Breitman, R., N. Goda, et al. (2004). U.S. Intelligence and the Nazis. Washington, DC, National Archives and Records Administration.

Bronskill, J. (2003). Transport won't release airport security results. Ottawa Citizen. Ottawa**:** A1.

Cole, D. (2003). Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism. New York, The New Press.

Coliver, S. (1999). Secrecy and Liberty: National Security, Freedom of Expression, and Access to Information. The Hague, M. Nijhoff Publishers.

Congressional Joint Inquiry (2002). Findings and Conclusions of the Congressional Joint Inquiry into September 11. Washington, DC, Government Printing Office.

Congressional-Executive Commission on China (2003). Annual Report. Washington, Government Printing Office.

de Giorgi, B. (1999). "The open democracy bill." Politeia **18**(2): Web edition.

Dinges, J. (2004). The Condor Years. New York, New Press.

Doyle, K. (2003). "Forgetting is not justice: Mexico bares its secret past." World Policy Journal **20**(2): 61-72.

Ellsberg, D. (2002). Secrets. New York, Penguin Group.

Fallows, J. (2004). Blind into Baghdad. The Atlantic Monthly. **293:** 53-74.

Feldmann, L. (2003). The Impact of Bush Linking 9/11 and Iraq. Christian Science Monitor.

Fisher, L. (2004). The Politics of Executive Privilege. Durham, NC, Carolina Academic Press.

Freeman, J. (1999). Private Parties, Public Functions and the New Administrative Law. Recrafting The Rule of Law. D. Dyzenhaus. Portland, Oregon, Hart Publishing**:** 331-369.

Garton Ash, T. (1998). The File: A Personal History. New York, Vintage Books.

Gonzales, A. (2004). Remarks to the ABA Standing Committee on Law and National Security. Washington, DC, Executive Office of the President.

Gonzalez, F. (2003). Access to Information and National Security in Chile. National Security and Open Government. Campbell Public Affairs Institute. Syracuse, New York, Campbell Public Affairs Institute, Syracuse University**:** 167-188.

Ignatieff, M. (2004). Lesser Evil: Political Ethics in an Age of Terror. Princeton, New Jersey, Princeton University Press.

Information Commissioner of Canada (2002). Annual Report 2001-2002. Ottawa, Office of the Information Commissioner.

Jacobson, J. (2002). Safeguarding National Security Through Public Release of Environmental Information. Washington, DC, George Washington University Law School.

Johnston, T. (2004). Indonesia Orders Crisis Group's Leader to Leave Over Work Permit. Financial Times. London**:** 7.

Kazmin, A. (2003). Hanoi's culture of secrecy thwarts IMF. Financial Times. London.

Kornbluh, P. (2003). The Pinochet File. New York, New Press.

Kriz, M. (2003). Bush Not Doing Enough to Protect Chemical Plants, Critics Contend. GovExec.com**:** http://www.govexec.com/dailyfed/0803/080703nj3.htm.

Kull, S., C. Ramsay, et al. (2004). "Misperceptions, the Media, and the Iraq War." Political Science Quarterly **118**(4): 569-598.

Lawyers Committee (2003). Assessing the New Normal: Liberty and Security for the Post-September 11 United States. Washington, DC, Lawyers Committee for Human Rights.

Leonard, J. W. (2004). Remarks to the National Classification Management Society's Annual Training Seminar. Washington, DC, Information Security Oversight Office.

Lin, J. (2003). Big Grant to Oil Firm Shrouded in Secrecy. Philadelphia Inquirer. Philadelphia.

Mendel, T. (2003). National security v. Openness: An Overview and Status Report on the Johannesburg Principles. National Security and Open Government: Striking the Right Balance. Campbell Public Affairs Institute. Syracuse, NY, Campbell Public Affairs Institute.

Milbank, D. (2002). Cheney Refuses Records' Release. Washington Post. Washington, DC**:** A1.

Olmsted, K. S. (1996). Challenging the Secret Government. Chapel Hill, University of North Carolina Press.

Perez, O. J. (2004). "Democratic Legitimacy and Public Insecurity." Political Science Quarterly **118**(4): 627-644.

Pomfret, J. (2003). China's Slow Reaction to Fast-Moving Illness. Washington Post. Washington, DC**:** A18.

Powers, T. (2003). "Can we be secure and free?" The Public Interest(151): 3-24.

Prados, J. (2004). Hoodwinked. New York, The New Press.

Roberts, A. (2001). "Structural pluralism and the right to information." University of Toronto Law Journal **51**(3): 243-271.

Roberts, A. (2003). "Entangling alliances: NATO's security policy and the entrenchment of state secrecy." Cornell International Law Journal **36**(2): 329-360.

Roberts, A. (2005). "Spin Control and Freedom of Information." Public Administration **83**(1).

Rogers, S., Ed. (2004). The Hutton Inquiry and Its Impact. London, Politico's Publishing.

Schwartz, S. I. (1998). Atomic Audit. Washington, D.C., Brookings Institution Press.

Shipping Times (2004). Ports Withholding Security Data Over Terrorism Fears. Shipping Times. Singapore.

Singer, P. W. (2003). Corporate Warriors. Ithaca, Cornell University Press.

SITA (2002). NBU Says Revision to Classified Information Law is Necessary. SITA Slovak News Agency. Bratislava, Slovakia.

Slevin, P. (2003). U.S. military lays out postwar Iraq plan. Washington Post. Washington, DC**:** A21.

Steinzor, R. (2003). ""Democracies Die Behind Closed Doors": The Homeland Security Act and Corporate Accountability." Kansas Journal of Law & Public Policy **12**(2): 641-670.

Svatosova, H. (2003). Analysis Of The Draft Bill On Classified Intelligence and Security Vetting. Prague, Transparency International Czech Republic.

Terreblanche, C. (2003). Intelligence Agency Wants Permanent Secrecy on Classified Documents. The Mercury. Johannesburg.

Thomson Jr., J. C. (1968). How Could Vietnam Happen? The Atlantic. **221:** 47-53.

Tollborg, D. (2003). Sweden. Transparency and Accountability of Police Forces, Security Services and Intelligence Agencies. D. Greenwood and S. Huisman. Geneva, Geneva Centre for the Democratic Control of Armed Forces**:** 117-138.

Tyler, P. (2003). Panel faults Bush on war costs and risks. New York Times. New York**:** A15.

Wadham, J. and K. Modi (2003). National Security and Open Government in the United Kingdom. National Security and Open Government: Striking The Right Balance. Campbell Public Affairs Institute. Syracuse, New York, Campbell Public Affairs Institute.

Weaver, W. G. and R. M. Pallitto (Forthcoming). "State Secrets and Executive Power." Political Science Quarterly.