NATO, Secrecy, and the Right to Information

Alasdair Roberts

In December 2001, the international movement for open government marked a small victory: Romania's new right-to-information statute, the Law Regarding Free Access to Information of Public Interest, came into force. Unfortunately, the victory was short-lived. In April 2002, Romania adopted a new state-secrets law creating a broad authority to withhold information that has been classified as sensitive by government officials.

Nongovernmental organizations complained about both the haste with which the state-secrets law was adopted, as well as its drafting. The first version of the law was struck down on procedural grounds by Romania's Constitutional Court in April 2001. A second version, although revised in response to criticisms, still proved objectionable. The International Helsinki Federation stated that the law "failed to strike a proper balance" between secrecy and the public's right to know, and Article 19, a freedom-of-expression advocacy group, said that the "incredibly broad" restrictions in the law could "substantially undermine" the new right-to-information statute.[1]

Romania is not an unusual case. Ten countries in Central and Eastern Europe have adopted right-to-information laws in the last decade—but eleven have also adopted laws to restrict access to information classified as sensitive (table one). Complaints about undue haste and poor drafting have arisen in several of these countries. The Hungarian Helsinki Committee complained that Hungary's state-secrets law, first adopted in 1995, became problematic, in December 1999, after the addition of "extremely vague wording" about the classification of information.[2] In Slovakia, protests from nongovernmental organizations compelled the cabinet to withdraw a proposed secrecy law in February 2001.[3] Article 19 also complained about "absurdly broad" restrictions in Bulgaria's proposed secrecy law. Other critics suggested that the law, eventually adopted in April 2002, might weaken the accountability of the state-security service.[4] In May 2002, a cross-party coalition of legislators launched a court challenge, claiming that the law contradicted Bulgaria's constitutional guarantee of a right to information.[5]

The spread of state-secrets laws has also led to strict policies on security clearances. In 1999, Poland's ombudsman questioned the constitutionality of rules in the country's new Classified Information Act that determined which public officials would receive access to sensitive information.[6] Poland's judges also complained about intrusive investigations to determine whether their lifestyles could make them "susceptible to . . . pressure," and Slovakia's new security agency will review political and religious affiliations, as well as lifestyles—including extramarital affairs—that are thought to create a danger of blackmail.[7] The Associated Press reported that Romania intends to deny clearances to security staff with "anti-western attitudes."[8]

There is a simple explanation for this wave of legislative activity. In 1999, NATO stated that those countries that wanted to join the alliance would need to establish "sufficient safeguards and procedures to ensure the security of the most sensitive information as laid down in NATO security policy."[9] Central and Eastern European countries rushed to put such legislation in place before NATO's meeting in Prague in

Table 1: Right-to-Information and State-Secrets Laws in Central and Eastern Europe

Country	NATO Status*	Access-to-Information Law	State-Secrets Law
Albania	candidate	Law on the Right to Information for Official Documents, 1999	Law on Creation and Control of Classified Information, 1999
Bulgaria	candidate	Access to Public Information Act, 2000	Classified Information Protection Act, 2002
Czech Republic	1999	Law on Free Access to Information, 1999	Protection of Classified Information Act, 1998
Estonia	candidate	Public Information Act, 2000	State Secrets Act, 1999; amended, 2001
Hungary	1999	Act on the Protection of Personal Data and Disclosure of Data of Public Interest, 1992	Act on State and Official Secrets, 1995; amended 1999
Latvia	candidate	Law on Freedom of Information, 1998	Law on State Secrets, 1997
Lithuania	candidate	Law on Provision of Information to the Public, 2000	Law on State Secrets, 1995
Macedonia	candidate	none	Not available
Poland	1999	Act on Access to Information, 2001	Classified Information Protection Act, 1999
Romania	candidate	Law Regarding Free Access to Information of Public Interest, 2001	Law on Protecting Classified Information, 2002
Slovakia	candidate	Act on Free Access to Information, 2000	Law on Protection of Classified Information, 2001
Slovenia	candidate	none	Classified Information Act, 2001

* Status as of November 15, 2002. The main source for this table is David Banisar, *Freedom of Information and Access to Government Records Around the World* (London: Privacy International, 2002)

November 2002, where the decisions on expansion were made. The sense of urgency was conveyed in a Romanian news report on the legislative debate in April 2002:

> [On April 3] a certain Colonel Constantin Raicu [of the Romanian Intelligence Service], who is in charge of the protection of state secrets, came down like a storm on the members of the Senate Juridical Commission, telling them: "This morning we have received signals from Brussels indicating that if the bill on classified information is not passed before April 16, they cannot exclude adopting a critical attitude regarding Romania. We agree with any form—the colonel added—but please, pass it as soon as possible, or we will be facing huge problems." The senators . . . grasped the situation very quickly, and they approved the draft bill in the form passed by the Chamber of Deputies.[10]

What is NATO's policy?

East European governments claim that their legislation is tailored to suit NATO requirements.[11] However, observers have asked whether governments in the region are using the process of NATO expansion as a pretext for adopting unnecessarily broad laws—or whether NATO's requirements are unduly biased against transparency. These are reasonable questions, but NATO has done little to provide answers; its security-of-information policy is not publicly accessible. However, the available evidence does suggest that the policy—crafted in the early years of the Cold War—is indeed tilted toward secrecy, to an unwarranted degree.

Throughout most of NATO's history, its secrecy policy was contained in a document referred to as C-M(55)15(Final), also known as *Security within the North Atlantic Treaty Organization*. This document had three components. The first and oldest component was a security agreement adopted by parties to the North Atlantic Treaty in January 1950, which became enclosure "A." The second component, which became enclosure "C," was first adopted in 1950 but substantially revised over the next five years and outlined detailed security procedures for the protection of NATO classified information. The third component, enclosure "B," adopted for the first time in 1955, had a

broader reach. It outlined "basic principles and minimum standards" that were to govern the overall design of national-security systems. This affected the handling of all sensitive information, whether provided by NATO or not.

The strictness of NATO's secrecy policy may be illustrated by its treatment of the policy itself. Although this document was unclassified, for decades NATO refused to make it publicly available. A narrow glimpse of NATO policy may have been provided in 1998, when a revised version of the "Security Agreement"—which apparently still constitutes enclosure "A" of the policy—was made publicly available by NATO member states.[12] Versions of C-M(55)15(Final) adopted before 1964 have also been made available in the NATO Archives.

Table 2: Components of NATO's Security Documents

	C-M(55)15(Final)*	C-M(2002)49(June 2002)
Enclosure "A"	"Security Agreement"	"Security Agreement"
Enclosure "B"	"Basic Principles and Minimum Standards of Security"	"Basic Principles"
Enclosure "C"	"Security Procedures for Protection of NATO Classified Information"	"Personal Security"
Enclosure "D"	"Industrial Security"	"Physical Security"
Enclosure "E"	"Protection Measures against Terrorist Threats"**	"Security of Information"
Enclosure "F"		INFOSEC***

* Titles for enclosures "A" through "D" are based on the version of C-M(55)15(Final) issued in July 1964.
** This title is based on information in Canadian government documents released in response to an Access to Information Act request. Apparently revised in March 2002.
*** INFOSEC relates to the identification and application of security measures to protect information processed, stored, or transmitted in communication, information, and other electronic systems.

Nevertheless, the complete and current version of C-M(55)15(Final) has remained inaccessible. In February 2002, NATO's Office of Security refused access to the document, explaining that "NATO unclassified information . . . can only be used *for official purposes*. Only individuals, bodies, or organizations that require it for official NATO purposes may have access to it."[13] NATO also instructed member countries to withhold their copies of C-M(55)15(Final). As a result, requests for the policy made under several national right-to-information laws have been refused.

NATO began an overhaul of C-M(55)15(Final) in the late 1990s. The review, guided by the Ad Hoc Working Group for the Fundamental Review for NATO Security Policy, was completed in early 2002. A revised security policy, now referred to as C-M(2002)49, was adopted by NATO on June 17, 2002. The Ad Hoc Working Group completed its task in secrecy, and the new policy remains inaccessible to the public, although its outlines can be reconstructed from other sources (table 2).[14]

NATO's reticence means that an assessment of its secrecy policy must be largely speculative. Nevertheless, it is possible, from archival and other sources, to describe the policy in broad terms. It has five basic features, each designed to ensure a high level of information security.

Breadth. The first of these elements might be called the principle of breadth, although this term is not used in NATO documents. It implies that the policies a member state adopts regarding security of information should govern all kinds of sensitive information, in all parts of government. It eschews narrower approaches that would be limited, for example, to information received through NATO, or information held within military or intelligence institutions. The principle is expressed in the 1964 edition of C-M(55)15(Final), which articulates standards for information security that apply to all sectors of government, on the grounds that member states must be assured that each country gives "a common standard of protection . . . to the secrets in which all have a common interest."[15]

Depth. The next principle underpinning NATO policy is that of depth of coverage, although, again, the principle is not expressed in this way in NATO documents. The policy errs on the side of caution when determining what information should be covered by secrecy rules. This is evident in the NATO classification policy, whose lowest category—"restricted"—applies to information whose relevance to security is negligible. The next highest category—"confidential"—relates to information "the unauthorized disclosure of which would be prejudicial to the interests of NATO"; restricted information does not need to meet even this

test.[16] (Several East European countries have adopted equally broad classifications for the whole of government. Under Czech law, for example, information is classified as restricted if disclosure would be unfavorable to the Republic; in Slovenia, information is restricted if disclosure could harm the activity or performance of tasks of an agency.)[17]

Centralization. A third principle of NATO policy is that of centralization. This has both a national and an intergovernmental aspect. At the national level, centralization of responsibility and strong coordination are regarded as "the foundations of sound national security."[18] Member states are expected to establish a "national security organization" with multiple responsibilities—for the security of NATO information and the screening of personnel; for "the collection and recording of intelligence regarding espionage, sabotage, and subversion"; and for providing advice to governments on threats to security and the appropriate responses.[19] Each country's organization must also have the authority needed to conduct inspections of security arrangements for the protection of NATO information within other departments and agencies, and to investigate and respond to breaches of security.[20]

This structure is roughly replicated at the intergovernmental level. In 1955 the North Atlantic Council gave its Security Bureau the responsibility for "overall coordination" of security in NATO. The Security Office, as it is now known, advises national authorities on the application of principles and standards and carries out surveillance of national systems to ensure that NATO information is adequately protected. NATO documents refer to periodic inspections of national systems. ("Surveillance" is the term used to describe comparable oversight arrangements in other multilateral agreements, such as the Article IV consultations undertaken by the International Monetary Fund, and the trade policy reviews undertaken by the World Trade Organization.) National authorities have an obligation to report possible breaches of security to the NATO office.[21]

Controlled distribution. The NATO security policy also invokes two rules that are intended to control strictly the distribution of information. The first of these is "*the need to know* principle": that individuals should have access to classified information only when they need the information for their work, not "merely because a person occupies a particular position, however senior."[22] This is regarded as a "fundamental principle" of security. Judgments about whether an individual has a "need to know" are made by the originator of the document, or by one of the addressees identified by the originator.[23]

The second rule that restricts the distribution of information may be called the principle of originator control. The principle acknowledges the right of member states, and NATO itself, to set firm limits on the distribution of information that is circulated among member states. Such information may not have its classification reduced, or be declassified, without the consent of the government from which the information originated.[24] As a consequence, the principle of originator control trumps the need-to-know principle, since originators may impose a high level of classification that restricts the number of individuals to whom the document might be referred by an addressee.

The principle of controlled distribution is even stricter with regard to the availability of documents outside the community of NATO governments. In this case, distribution is absolutely prohibited without the originator's consent, even if the information is unclassified. In these circumstances, the information is regarded as "the property of the originator," which retains absolute control over its distribution.[25]

Personnel controls. The fifth and final element of the NATO security policy comprises strict rules regarding the selection of individuals who are entitled to view classified information. The precise requirements for personnel screening are not easy to discern. Some of the exact criteria adopted during the Cold War are probably no longer applicable; and some of the criteria used in NATO's early years continue to be withheld. (These appear to be contained in a confidential supplement that was added to C-M[55]15[Final] in January 1961.) Archival copies of the supplement are not accessible, but a sense of its content can be obtained from the index to C-M(55)15(Final).

The policy relies on a system of "positive vetting," in which individuals who handle sensitive information are subjected to active background investigation before receiving clearance.[26] NATO's early policy made clear that decisions could be based on assessments of character and lifestyle, and that the evidentiary burden for denying clearances was low. Individuals were expected

to demonstrate "unquestioned loyalty [and] such character, habits, associates and discretion as to cast no doubt upon their trustworthiness."[27]

Other controls are imposed to monitor personnel after a security clearance has been provided. In C-M(55)15(Final) it is stipulated that supervisors have the duty "of recording and reporting any incidents, associations or habits likely to have a bearing on security." Evidence that created a "reasonable doubt" about loyalty or trustworthiness required the removal of a security clearance. There is also an expectation that "disciplinary action" will be taken against individuals who are responsible for the unauthorized disclosure of information, and that there will be clear criminal penalties for unauthorized disclosure.[28]

Constraints on national policies

Of course, it is not surprising that NATO—as an organization whose mission is the promotion of collective security—should seek to establish strict rules on the handling of sensitive information within the governments of its member states. But there are also special historical reasons that may explain the strictness of NATO's secrecy-of-information policy.

The policy was codified between 1953 and 1955, in the early and most difficult years of the Cold War. American military planners played the leading role in defining the policy, sometimes overriding civilian policy makers in other governments who considered that military secrecy standards were excessive.[29]

The policy was also shaped by domestic politics within the United States.[30] The anticommunist crusade in America reached its zenith in 1954, with Senator Joseph McCarthy's hearings into alleged communist subversion in the US Army, as well as the hearings that led to the revocation of the security clearance of J. Robert Oppenheimer, former director of the Manhattan Project, because of "fundamental defects in his 'character.'"[31] The Eisenhower administration was determined to avoid the kind of criticism over internal security that had undermined President Truman's 1952 election campaign, and it boasted in January 1954 that new loyalty rules had already resulted in the dismissal of over 2,000 federal employees. This preoccupation with internal security was reflected in the American government's approach to the adoption of NATO policy in 1954–55.

The difficulties created by the exportation of these demanding secrecy rules were evident to other NATO governments. For several years following the establishment of NATO in 1948, the British government resisted American pressure to adopt positive vetting procedures like those contained in the domestic "loyalty program" introduced by the Truman administration in 1947. Many British policy makers found American methods severe and distasteful and doubted their effectiveness. They preferred a less comprehensive system—"negative vetting"—combined with stricter criminal sanctions for unauthorized disclosure of information. The disagreement meant that rules on positive vetting were not included in early versions of NATO's secrecy policy.

However, the British government capitulated in 1952. Its position had been undermined by the Anthony Burgess and Donald McLean defections, and the American government had made clear that positive vetting was essential if the British government expected to receive information on the development and deployment of nuclear weapons. The British government affirmed its commitment to a screening process that searched for evidence of character defects or "loose living" that might make individuals susceptible to pressure. It conceded that the new policy was "alien to our traditional practices" but argued that individual rights had to be subordinated to the need for state security.[32]

NATO's archival records show that other concerns were expressed as C-M(55)15(Final) was prepared for adoption. The Canadian government feared that the new policy might give the NATO Security Bureau an inappropriate role in shaping national-security policies.[33] The Danish government expressed its concern about the breadth of the new regime, suggesting it overreached by attempting to set rules on the handling of non-NATO information. The Italian government suggested that the policy's breadth might create "difficulties of a constitutional nature."[34] Nevertheless, the scope of the policy was not changed.

Similarly, complaints about the depth of the new arrangements were aired but defeated. In January 1955, the Norwegian government proposed that the classification system should be simplified by eliminating the lowest security grading for information ("restricted").[35] It argued that the definition of the restricted category and the rules governing the use of restricted information

"were so vague that they might lead to confusion instead of contributing to overall NATO security." A majority of other nations disagreed, and "for the sake of unity" Norway withdrew its proposal.[36] In October 1957, the Danish government once again proposed a simplification of the grading system, which it said encouraged overclassification.[37] Again, a majority of the other countries vetoed the proposal. The record of the July 1958 meeting of the Security Committee at which the Danish proposal was rejected is still withheld by NATO.[38]

Because of NATO's unwillingness to release internal documents produced after 1964, it is impossible to know how the debate regarding information security continued in later years. But it seems certain that there must have been further contention. One reason would be the diffusion of right-to-information laws among NATO member states. Before 1966, no NATO state had such a law; by 2001, sixteen of the nineteen states had adopted right-to-information statutes. (The first law was adopted by the United States in 1966. Today, the three exceptions are Germany, Luxembourg, and Turkey.) These laws are typically founded on principles that are completely at odds with the restrictive rules on the dissemination of information contained in NATO policy.

The tension between international obligations and domestic expectations is sometimes evident in debates over national right-to-information laws. For example, the British government was careful to accommodate the principle of originator control, a basic feature of NATO policy, within its proposed Freedom of Information Act of 1999. (The originator rule is preserved in section 27.3 of the Freedom of Information Act of 2000.) The nongovernmental organization Campaign for Freedom of Information criticized this as one of several "indiscriminate" provisions that would allow the withholding of "harmless information," but the government opposed attempts to remove the provision.[39] Similar complaints were lodged against the comparable provision in the proposed Scottish freedom-of-information bill; however, the Scottish executive was also explicitly constrained—by the agreement governing the delegation of power to Scotland from the United Kingdom—to respect the terms of C-M(55)15(Final), and thus the provision remained intact.[40]

The Canadian government has also resisted efforts to weaken the originator-control rule contained in its 1982 Access to Information Act. In 2002, it argued that any weakening of this provision would "set Canada apart from its key allies."[41] Indeed, the government recently amended the 1982 law so that it would be allowed to eliminate a right of appeal against its decisions to withhold information received from allies. (The new restrictions were contained in the Anti-Terrorism Act adopted in December 2001. The minister responsible justified the restrictions by telling parliament that "our allies . . . will not provide us with information . . . unless we can provide them with a guarantee of confidentiality.")[42] Internal memoranda suggest that the highly contentious amendment was the product of bureaucratic frustration with requests for information were affected by rules such as those in NATO's secrecy-of-information policy.

Similarly, NATO procedures have had a controversial impact on the European Union's policy concerning access to information. The EU adopted its first code on access to documents in December 1993. However, the code was substantially revised in August 2000, and a large number of classified documents were wholly excluded from possible access. Moreover, the EU Council's discretion to withhold other documents relating to security matters was also broadened. At the same time, the council hardened its policy on the control of classified information.[43]

Many observers were shocked by these changes, protesting that the council had executed a "summertime coup" against transparency. However, the council's decisions proved to be prerequisites for a cooperation agreement with NATO signed in July 2000, in which the council agreed to comply with the requirements of C-M(55)15(Final). (The EU's letter of agreement with NATO was released in February 2002 in response to a right-to-information request—with the specific reference to NATO's security policy carefully excised. The secretary-general of the EU, Javier Solana, is also a former secretary-general of NATO.)

The spirit of the August 2000 amendments was carried forward into a new regulation, adopted in May 2001, governing access to information held by EU institutions. Under the new regulation, national governments and institutions such as NATO retain the right to veto the disclosure of classified information relating to public security or defense that they have provided to the EU. The classification policy of the

authoring institution, rather than that of the EU, will determine whether documents are subject to the rule of originator control.[44] These arrangements were unpopular among advocates of transparency but clearly consistent with NATO requirements.

The impact of EU-NATO cooperation expanded in March 2001, when new security regulations governing EU classified information were approved by the council. The regulations replicate NATO security-of-information rules. The reach of these regulations is not limited to EU institutions: member states also have an obligation to adopt "appropriate national measures" to ensure that the council's rules on the handling of classified information are respected within their governments.[45] This imposes another constraint on the transparency policies of the fifteen EU member states—and on the policies of those Eastern European states that were invited to join the European Union at its December 2002 summit.

Web of secrets

The controversies over new state-secrets laws in Eastern Europe are not unusual. Rather, they may be part of a decades-long process through which the national policies of NATO member states, and allied institutions such as the European Union, have been reshaped to conform to NATO's security-of-information requirements.

This process of policy rationalization is deeply problematic. In many respects, NATO's policy does not appear to strike a reasonable balance between security concerns and other critical considerations, such as the need to ensure accountability through a right of access to government documents. In 1995, Article 19, the Global Campaign for Free Expression convened a group of experts to develop principles on the appropriate balance between national security and transparency. NATO's policy seems to violate several of the practices that are condemned by the so-called "Johannesburg Principles": the categorical denial of public access to information, regardless of importance; punishment for disclosure of information, without regard to harm or benefit from disclosure; denial of employment because of opinion or beliefs; or denial of due process in removal. NATO policy, by contrast, seems to perpetuate an approach forged in the hardest years of the Cold War, when citizens had more modest expectations regarding governmental transparency. Of course, this may be a mistaken view of NATO's current policy. It is difficult to be sure when the policy itself is inaccessible.

Two conclusions should be drawn from this discussion. The first is the need to be chary of claims about advances in government transparency over the past ten years. It is true that the number of right-to-information laws has increased substantially in the last decade. (Eighteen countries had national right-to-information laws in 1992; 49 countries had such laws in 2002.) Slow but significant reforms at major international institutions (such as the World Bank, the International Monetary Fund, and the World Trade Organization) might seem to suggest that intergovernmental organizations are also recognizing an obligation to conform to standards of transparency comparable to those imposed on national governments. These are important advances; however, we must weigh against them the impact of processes of defense and intelligence integration. The drive to promote collective security has produced a thickening web of intergovernmental commitments on the handling of sensitive information, and this network has entrenched norms hostile to the principle of governmental transparency.

The experience of East European countries with NATO policy also reminds us of a larger point: the need to ensure an appropriate balance between security concerns and democratic accountability. No one can dispute that the preservation of secrets is sometimes essential to national security. But at the same time, such secrecy compromises the capacity of citizens to monitor and control the actions of their governments. The best response to this dilemma, Dennis Thompson has argued, is to make certain that there is proper public discussion of the rules that determine when secrets shall be kept. "Secrecy is justifiable," Thompson says, "only if it is actually justified in a process that itself is not secret. First-order secrecy (in a process or about a policy) requires second-order publicity (about the decision to make the process or policy secret)."[46]

NATO's policy flouts this basic principle of accountability. The rights of citizens in NATO member states are clearly affected by NATO rules. NATO's requirements constrain their right to government documents and their ability to obtain security clearances and government employment. Nevertheless the policy—even though unclassified—

remains inaccessible to citizens. Nor are citizens able to participate in or observe the processes by which the content of this policy is determined. Indeed, they are not even informed when the policy is subject to revision, as it was during the last few years. This is an indefensible level of secretiveness. NATO's habit of secrecy should be broken, and the key elements of its security-of-information policy should be laid open for public review.

Alasdair Roberts is an associate professor of public administration in the Maxwell School, Syracuse University and director of its Campbell Public Affairs Institute.

NOTES

1. International Helsinki Federation, *Human Rights in the OSCE Region: Report 2002* (Vienna: International Helsinki Federation, 2002), p. 257; Article 19, *Memorandum on the Romanian Law for the Protection of Classified Information* (London: Article 19, 2002), pp. 2, 8.

2. International Helsinki Federation, *Human Rights in the OSCE Region: Report 2000* (Vienna: International Helsinki Federation, 2000), p. 185.

3. Alex Grigorescu, "European Institutions and Unsuccessful Norm Transmission: The Case of Transparency," *International Politics* 39, no. 4 (December 2002). A law was eventually adopted by Slovakia in May 2001.

4. Ulrich Buechsenschuetz, "Bulgaria's New Law on Classified Information." Radio Free Europe/Radio Liberty [RFE/RL], *Newsline*, Prague, April 30, 2002.

5. RFE/RL, "Opposition Appeals to Constitutional Court over Law on Classified Information, *Newsline*, Prague, May 30, 2002.

6. International Helsinki Federation, *Human Rights in the OSCE Region: Report 2000* (Vienna: International Helsinki Federation, 2000), p. 286; *Human Rights in the OSCE Region: Report 2001* (Vienna: International Helsinki Federation, 2001), p. 240.

7. Peter Sobcak, "New Security Office to Guard NATO Secrets," *Slovak Army Review* (Spring 2002).

8. The Associated Press (Bucharest, Romania), "NATO Officials Want Romania to Exclude Some Former Communists from Intelligence Positions," March 20, 2002.

9. NATO, *Membership Action Plan* (Brussels: NATO, April 24, 1999), Press Release NAC-S(99) 66.

10. "NATO Used as Scarecrow to Pass Law on Secrets," *Bucharest Ziua* (Bucharest), April 8, 2002, at www.ziua.ro.

11. It is reported that Bulgaria's foreign minister defended the country's proposed state secrets law by saying that NATO experts had described it as one of the best statutes of its type among all NATO applicant countries; see RFE/RL, "Bulgarian Parliament Starts to Vote on Classified Information Protection Law," *Newsline*, Prague, April 18, 2002.

12. The Canadian government published the revised agreement, "Agreement between the Parties to the North Atlantic Treaty for the Security of Information," as Canada Treaty Series, document 1998/56.

13. NATO Office of Security, *Letter from Mr. Wayne Rychak, Director, to Mr. Jacob Visscher, General Secretariat of the Council of the European Union* (Brussels: NATO Office of Security, February 6, 2002). Emphasis in original.

14. The existence of the Working Group was acknowledged in Canadian government documents released to the author in response to a request under Canada's Access to Information Act in September 2002. The first public acknowledgement of the existence of the new policy by NATO was made in September 2002: see www.shape.nato.int/BUDFIN.

15. NATO, *Security within the North Atlantic Treaty Organization* (Brussels: NATO Archives, reissued July 31, 1964), enc. "B," par. 1. This is the 1964 edition of C-M(55)15(Final) and will be referred to as NATO 1964. For the first edition of this document, see note 37 below.

16. NATO 1964, enc. "C," sec. II.

17. For the Czech Republic, see the Protection of Classified Information Act, 1988, sec. 5(5); for Slovenia, the Classified Information Act, art. 13.

18. NATO 1964, enc. "B," par. 3.

19. NATO 1964, enc. "B," par. 3, enc. "C," sec. I, par. 15.

20. NATO 1964, enc. "C," sec. I, par. 15(c), and sec. IX, pars. 3–5.

21. NATO 1964, enc. "C," sec. I, par. 3, and sec. IX, par. 4.

22. Security Committee, *A Short Guide to the Handling of Classified Information* (Brussels: NATO Archives, August 22, 1958), AC/35-WP/I4, p. 4. Emphasis in original.

23. NATO 1964, enc. "B," intro., par. 5(d); sec. VI, pars. 6–7; and sec. VIII, pars. 4–5.

24. NATO 1964, enc. "C," sec. V; see also NATO, *Agreement between the Parties to the North Atlantic Treaty for the Security of Information (with Annexes): In Force August 16, 1998,* Canada Treaty Series 1998/56, art. 1.

25. NATO 1964, enc. "C," intro.

26. The 1964 policy observes that the "fullest practicable use should be made of the technique of background investigation"; NATO 1964, enc. "B," par. 9.

27. NATO 1964, enc. "B," par. 9.

28. This point is discussed at greater length in Alasdair Roberts, "Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy." Forthcoming in *Cornell International Law Journal* 26, no. 2 (May 2003).

29. For security clearance removal, see NATO 1964, enc. "B," pars. 11, 15; for disciplinary action, ibid., enc. "C," sec. IX, par. 10. On the issue of improper disclosures and criminal penalties, see, for further discussion, Roberts, note 28.

30. Edward Shils, *The Torment of Secrecy* (Chicago: Ivan R. Dee, 1996), p. 214; see also Athan Theoharis, *Chasing Spies* (Chicago: Ivan R. Dee, 2002).

31. Richard Polenberg, *In the Matter of J. Robert Oppenheimer: The Security Clearance Hearing* (Ithaca: Cornell University Press, 2002), p. 380.

32. United Kingdom, "White paper on Security Precautions in the British Civil Service." *Public Administration* 35 (autumn 1957), pp. 297–304.

33. *Memorandum to Council from the Canadian Government on Proposed Security Regulations* (Brussels: NATO Archives, February 24, 1995, C-M(55)25; NATO, *Note by the Secretary-General and Vice-Chairman of the Council on Security Procedures for the Protection of NATO Classified Information* (Brussels: NATO Archives, March 8, 1955), C-M(55)15(Final).

34. Security Committee, *Summary Record of NATO Security Committee Meeting, January 24–28, 1955* (Brussels: NATO Archives, February 8, 1955), AC/35-R/11, p. 1

35. Ibid.

36. North Atlantic Council, *Summary Record of the Meeting of the Council on March 2, 1955* (Brussels: NATO Archives, March 2, 1955), C-R(55)8.

37. NATO, *Summary Record of the Meeting of the NATO Security Committee* (Brussels: NATO Archives, October 17–18, 1957), AC/35-R/22; for Denmark, see *Memorandum to the NATO Security Committee on Controlling and Reducing the Volume of Classified Information and Documents* (Brussels: NATO Archives, January 11, 1958), AC/35-D/226.

38. The withheld document is NATO AC/35-R/23, the summary record of the meeting of the NATO Security Committee held on July 16–17, 1958. A working group concerned with control of the volume of classified documents in NATO agencies had earlier reported that a majority of its members opposed the Danish proposal; see NATO, *Note by the Chairman of the Working Group on the Control of Classified Documents in NATO Agencies* (Brussels: NATO Archives, January 13, 1958), AC/35-WP/13.

39. Campaign for Freedom of Information, *Briefing for MPs for the Report Stage Debate on the Freedom of Information Bill* (London: Campaign for Freedom of Information); for the government's position, see United Kingdom, *Hansard Parliamentary Debates*, House of Lords (London: November 14, 2000), vol. 619, part 166.

40. Scottish Executive, *Concordat between the Scottish Ministers and the Secretary for Defence* (Edinburgh: Scottish Executive, July 2000).

41. Access to Information Review Task Force, *Access to Information: Making it Work for Canadians* (Ottawa: Treasury Board Secretariat, June 12, 2002), p. 51.

42. Hon. Anne McLellan, Minister of Justice, *Hansard Parliamentary Debates* (Ottawa: October 17, 2001), http://www.parl.gc.ca/37/1/parlbus/chambus/house/debates/096_2001-10-17/hand096_1420-E.htm.

43. For the withholding of documents for security reasons, see Council of the European Union, *Council Decision 2000/527/EC, Amending Decision 93/731/EC on Public Access to Council Documents* (Brussels: Council of the European Union, August 14, 2000); for the treatment of classified information, see Council of the European Union, *Decision of the Secretary-General of the Council/High Representative for Common Foreign and Security Policy on Measures for the Protection of Classified Information Applicable to the General Secretariat of the Council* (Brussels: Council of the European Union, July 27, 2000).

44. European Union, *Regulation (EC) 1049/2001 Regarding Public Access to European Parliament, Council, and Commission Documents* (Brussels: European Union, May 30, 2001), art. 9.

45. Council of the European Union, *Council Decision 2001/264/EC Adopting Council's Security Regulations* (Brussels: Council of the European Union, March 19, 2001). The European Parliament has challenged the security regulations before the European Court of Justice. The European Commission also adopted the same security regulations on November 29, 2001: Decision 2001/844/EC, ECSC, Euratom.

46. Dennis Thompson, "Democratic Secrecy," *Political Science Quarterly* 114, no. 2, p. 185.