Entangling Alliances: NATO’s Security of Information Policy and the Entrenchment of State Secrecy

Alasdair Roberts

Follow this and additional works at: http://scholarship.law.cornell.edu/cilj
Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.cornell.edu/cilj/vol36/iss2/4

This Article is brought to you for free and open access by Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell International Law Journal by an authorized administrator of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.
Entangling Alliances:
NATO's Security of Information Policy
and the Entrenchment of State Secrecy

Alasdair Roberts†

Introduction

The past decade has been heralded as one in which the movement for
greater governmental transparency has made substantial progress. In this
period, twenty-six nations have enacted legislation giving their citizens a
right of access to government information.2 Supranational institutions are
said to have experienced their own “transparency revolution,”3 making
unprecedented commitments to disclose information.

The countries of Central and Eastern Europe (CEE) have been at the
forefront of this movement. Within a decade, at least ten nations in this
region have adopted national right-to-information laws, and several have
affirmed a right to information in their constitutions. In doing this, the
societies of Central and Eastern Europe have signaled their desire to repu-
diate a legacy of authoritarian government and emulate the democratic
practices of their Western European neighbors. Formal processes of Euro-
pean integration, such as the expansion of the European Union to include
many states in Central and Eastern Europe, may have encouraged efforts to
adopt westernized institutional arrangements, including right-to-informa-

† Associate professor of public administration in the Maxwell School of
Citizenship and Public Affairs, Syracuse University; Director of the Campbell Public
Affairs Institute; JD, University of Toronto; Master of public policy and doctoral degree,
Harvard University. Email: asrobert@maxwell.syr.edu.

1. This paper could not have been completed without assistance provided by Ulf
Oberg, David Banisar, Toby Mendel, Maurice Frankel, and Will Ferroggiaro. I am also
grateful for help provided by Bethany Walawender and Kelley Coleman of the Campbell
Public Affairs Institute, and my research assistants: Lillian Foo, Kevin Lo, and Sarah
Holsen. This research was supported by a fellowship provided by the Open Society
Institute.

2. Thomas Blanton, The World's Right to Know, FOREIGN POL'Y 50 (July/August
2002).

3. Stanley Fischer, Farewell to the IMF Board (International Monetary Fund
2001).

The process of European integration is also being expedited through the expansion of the North Atlantic Treaty Organization (NATO), a collective security arrangement established in 1949 by western European states, the United States and Canada. In March 1999, three CEE countries—Poland, Hungary and the Czech Republic—became signatories to the North Atlantic Treaty. Eight other CEE countries—Albania, Bulgaria, Estonia, Latvia, Lithuania, Macedonia, Slovakia and Slovenia—were accepted as candidates for NATO membership in November 2002. These eight candidates argue that integration into NATO will help to consolidate “the values of the Euro-Atlantic community” throughout the region.

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>NATO STATUS</th>
<th>ACCESS TO INFORMATION LAW</th>
<th>STATE SECRETS LAW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Albania</td>
<td>Candidate</td>
<td>Law on the Right to Information for Official Documents, 1999</td>
<td>Law on Creation and Control of Classified Information, 1999</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Candidate</td>
<td>Access to Public Information Act, 2000</td>
<td>Classified Information Protection Act, 2002</td>
</tr>
<tr>
<td>Estonia</td>
<td>Candidate</td>
<td>Public Information Act, 2000</td>
<td>State Secrets Act, 1999; amended, 2001</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Candidate</td>
<td>Law on Provision of Information to the Public, 2000</td>
<td>Law on State Secrets, 1995</td>
</tr>
<tr>
<td>Macedonia</td>
<td>Candidate</td>
<td>None</td>
<td>Not available</td>
</tr>
<tr>
<td>Poland</td>
<td>1999</td>
<td>Act on Access to Information, 2001</td>
<td>Classified Information Protection Act, 1999</td>
</tr>
<tr>
<td>Romania</td>
<td>Candidate</td>
<td>Law Regarding Free Access to Information of Public Interest, 2001</td>
<td>Law on Protecting Classified Information, 2002</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Candidate</td>
<td>None</td>
<td>Classified Information Act, 2001</td>
</tr>
</tbody>
</table>

4. Alex Grigorescu provides a more skeptical view about the influence of institutions such as the European Union and the Council of Europe on the diffusion of transparency norms. Alex Grigorescu, European institutions and unsuccessful norm transmission: The case of transparency, 39.4 INTERNATIONAL POLITICS 467-89 (2002).


Although integration into NATO promises larger benefits, it has also presented proponents of democratization with unexpected challenges. NATO has made clear that admission depends on the ability of nations to establish "sufficient safeguards and procedures to ensure the security of the most sensitive information as laid down in NATO security policy."\(^7\) One result has been the rapid diffusion of state secrecy laws throughout the region (Table One). The eleven countries that have recently joined NATO, or wish to join, have been candid in explaining that these laws have been adopted to satisfy NATO requirements.\(^8\) New state secrecy laws have been accompanied by less obvious changes in internal policies and practices intended to regulate the flow of sensitive information.

These initiatives have provoked anxiety and vigorous protest in several CEE countries.\(^9\) The establishment of new national security authorities and rigorous personnel clearance procedures sits uneasily within societies that have only recently dismantled state security agencies and the informant networks upon which they relied. Broad definitions of state secrets, and the threat of penalties for unauthorized disclosure of state secrets, seem to undermine the effort at building more open government, and clash

---


with constitutional or statutory guarantees on transparency. Debate has been soured by some CEE governments' insistence on quick action to meet NATO deadlines, and by NATO's own refusal to publish the requirements that it expects candidate nations to fulfill.

Concerns about the impact of NATO's security of information (SOI) requirements are justified. Although NATO's policy remains inaccessible, its broad outlines can be deduced. It is a conservative policy, largely crafted at a time when the western powers were faced with overwhelming military threats and non-state actors played a much smaller role in the process of governance. Archival records show that the original signatories went through a similar process of policy rationalization and articulated concerns comparable to those being expressed by critics today. In fact, NATO's SOI policy continues to play an important role in frustrating the work of transparency advocates in Western Europe and North America, some of who may be unaware of the role that is played by NATO and other similar SOI agreements.

European nations are caught in an increasingly dense web of multilateral commitments on the handling of information, based largely on the conservative policy crafted by the North Atlantic Treaty countries in the early years of the Cold War. There is good reason to think that the same may be said of countries in other parts of the globe. This may give us reason to be cautious in assuming that global integration is favorable to increased transparency. Advocates of transparency will also find that domestic policy on matters of state secrecy is increasingly constrained by this thickening web of agreements on security of information.

I. What Does NATO Require?

Governments throughout Central and Eastern Europe have said that their legislation is tailored to suit NATO requirements. 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 SOI policy is itself unduly tilted against transparency. These are reasonable questions, but NATO has done little to provide answers. Its SOI policy is not publicly accessible. However, available evi-

10. A Romanian newspaper reported in April 2002: "On Wednesday [April 3] a certain Colonel Constantin Raicu of the SRI [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 16 April, 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.'" NATO Used as Scarecrow to Pass Law on Secrets, BUCHAREST ZIUA, INTERNET EDITION, April 8, 2002, at http://www.ziua.net/.

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, Bulgarian Parliament Starts Vote on Classified Information Protection Law, RADIO FREE EUROPE/RADIO LIBERTY NEWSLINE, April 18, 2002.
dence does suggest that the policy, crafted in the early years of the Cold War, is excessively tilted toward secrecy.

For most of NATO’s history, its SOI policy was contained in a document known as C-M(55)15(Final), 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 at the third meeting of the North Atlantic Council in January 1950, as one of the basic components of NATO’s “master Defense Plan.” This became Enclosure “A” of C-M(55)15(Final). A second component, first adopted in 1950 but substantially revised over the next five years, outlined detailed security procedures for the protection of NATO classified information. This became Enclosure “C” of C-M(55)15(Final). A third component, 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 produced by NATO or not. This became Enclosure “B” of C-M(55)15(Final) (See Table 2).

| TABLE TWO: COMPONENTS OF NATO’S SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION |
|---|---|
| Enclosure “A” | Security Agreement |
| Enclosure “B” | Basic Principles and Minimum Standards of Security |
| Enclosure “C” | Security Procedures for Protection of NATO classified information |
| Enclosure “D” | Industrial Security |
| Enclosure “E” | Protection Measures against Terrorist Threats†† |
| Enclosure “F” | INFOSEC††† |

† Titles for Enclosures “A” to “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.

A document which compiled these three components was approved by the North Atlantic Council in March 1955, and given the designation C-M(55)15(Final). The SOI policy was substantially revised in later years, although it retained this designation. Enclosure “D,” providing guidance on information given to defense contractors, was added in 1958. A Confi-
idential Supplement was added in 1961 that provided additional guidance on methods of personnel screening. Enclosure "E," which addressed anti-terrorism efforts, was added in the early 1980s, and apparently revised in early 2002.

The strictness of NATO's SOI policy may be illustrated by its treatment of the policy itself. The fact that NATO had adopted a SOI agreement was not acknowledged in the final communique of the January 1950 meeting of the Council. Although C-M(55)15(Final) was for many years an unclassified document, NATO refused for decades 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 some NATO member states. Versions of C-M(55)15(Final) adopted before 1964 have also been made available in the NATO Archives.

Nevertheless, the complete and current version of C-M(55)15(Final) always remained inaccessible. The policy reminded national governments that documents such as C-M(55)15(Final) are the property of NATO, and may not be given to any other individual or organization without NATO's consent. As a consequence, several governments recently refused requests made under national right to information laws for copies of the policy. NATO's Security Office, responding to one of these requests, explained in February 2002 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 . . . NATO information marked in this manner is subject to release via agreement from its originators and subject to recognized storage procedures for its protection.

NATO began an overhaul of C-M(55)15(Final) in the late 1990s. The review, guided by an Ad-Hoc Working Group for the Fundamental Review for NATO Security Policy, was completed in early 2002. A revised SOI policy, now known as C-M(2002)49, was adopted by NATO on June 17, 2002.

14. The document was originally classified as RESTRICTED. It was declassified sometime after 1964. However, NATO does not consider that all unclassified documents should necessarily be accessible to the public. See NATO, Publication Policy. AC/323-D/22, March 2001, Annex VIF.
16. The author made a request for C-M(55)15(Final) to the Canadian Department of National Defence in September 2001, which was declined. Comparable requests were made by the National Security Archive to the U.S. Department of Defense; and by the Campaign for Freedom of Information to the U.K. Ministry of Defence. Mr. Ulf Öberg, Faculty of Law, Stockholm University, made the same request to the Swedish Ministry of Defence.
17. Letter from Wayne Rychak, Director, NATO Office of Security, to Jacob Visscher, General Secretariat of the Council of the European Union. February 6, 2002. Available from the General Secretariat of the Council of the European Union. Emphasis in original. This letter was written in response to a request for C-M(55)15(Final) made to the Council of the European Union by Mr. Ulf Öberg.
The Working Group completed its work in secrecy, and the new policy remains inaccessible to the public\textsuperscript{18}, although its broad outlines may be reconstructed from other sources (Table 2).

NATO's reticence means that an assessment of its SOI policy must be largely speculative. Nevertheless it is possible to describe the policy in broad terms, drawing on NATO's archival documents\textsuperscript{19} and other sources, such as the language of the CEE's new state secrecy laws.

Another of these sources is the SOI policy of a related collective security pact, the Western European Union (WEU). Established by the Brussels Treaty of March 1948, the WEU actually served as the foundation for the broader alliance established by the North Atlantic Treaty in April 1949.\textsuperscript{20} There is good reason to believe that the two pacts maintained comparable security policies. Policymakers within NATO acknowledged that the first drafts of its security policy were based on the WEU's policy.\textsuperscript{21} All ten of the nations that are currently members of WEU are also members of NATO; in addition, there is a NATO-WEU SOI agreement, signed in 1992. An early version of NATO policy recognized that NATO and WEU materials might be "co-mingled" in the same administrative processes.\textsuperscript{22}

Fortunately, the WEU's security policy is publicly accessible. The government of Sweden signed the WEU security agreement, and became responsible for complying with its security regulations, as a precondition for entering into cooperation on certain issues with the WEU in 1992. The Swedish government released the WEU security agreement and the 1996 version of the WEU security regulations in February 2002 in response to a request under Sweden's Freedom of the Press Act.\textsuperscript{23}

Another view of NATO policy may be provided by bilateral agreements that are publicly accessible. The Council of the European Union recently released correspondence in 2001 between its Secretary General, Javier Solana, and NATO Secretary General Lord Robertson, which outlined an interim security agreement that serves as a foundation for closer cooperation between the two organizations.\textsuperscript{24} The Council of the European Union subsequently adopted security regulations that must be presumed to con-

\begin{itemize}
  \item \textsuperscript{18} 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.
  \item \textsuperscript{19} The policy on access to archival materials can be found at http://www.nato.int/archives/policy.htm.
  \item \textsuperscript{20} Until 1954, the Western European Union was known as the Western Union.
  \item \textsuperscript{21} NATO Standing Group, Record of Meeting of the Standing Group of the North Atlantic Military Committee. Brussels: NATO Archives. November 18, 1949. SG 7.
  \item \textsuperscript{23} These documents were released in response to a request to the Swedish government made by Mr. Ulf Öberg. Western European Union, Security Regulations. January 1996. RS 100: §§ II.8, II.9.
  \item \textsuperscript{24} These documents were also released by the Secretariat General of the Council of the European Union in response to a request by Mr. Ulf Öberg.
\end{itemize}
form to NATO requirements.\textsuperscript{25}

From all this, what can be said about NATO's SOI policy? That it has five basic features, each of which has been adopted with the aim of ensuring a high level of security for information. The cumulative effect of the rules is to put an extraordinary emphasis on control of information.

\textit{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 rules that a member state adopts regarding security of information should govern all kinds of sensitive information, in all parts of government. It eschews narrower approaches, perhaps limited to information received through NATO, or information held within military or intelligence institutions. Laws adopted by several CEE countries have this comprehensive quality. 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 \ldots to the secrets in which all have a common interest."\textsuperscript{26}

\textit{Depth}. The next principle underpinning NATO policy is that of depth of coverage, although again the rule 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 an SOI policy. This is evident in the NATO classification policy, whose lowest category, RESTRICTED, applies to information whose relevance to security is negligible. Information may be classified at this level if its disclosure would be "undesirable to the interest of NATO."\textsuperscript{27} Several CEE 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;\textsuperscript{28} in Slovenia, information is RESTRICTED if disclosure could harm the activity or performance of tasks of an agency.\textsuperscript{29}

\textit{Centralization}. A third principle of NATO policy is that of centralization. This has a national and intergovernmental aspect. At the national level, centralization of responsibility and strong coordination are regarded as "the foundations of sound national security."\textsuperscript{30} Member states are

\begin{itemize}
\item \textsuperscript{28} Protection of Classified Information Act, 1998, section 5(5).
\item \textsuperscript{29} Classified Information Act, article 13.
\end{itemize}
expected to establish a "national security organization" (NSO) that is responsible for the security of NATO information and screening of personnel; for "the collection and recording of intelligence regarding espionage, sabotage and subversion"; and for advice to government on threats to security and appropriate responses. Presumably the NSO is also responsible for leading the "high-level" system of inter-departmental coordination that is required to ensure tight integration of departmental policies and procedures. The NSO 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.

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 Bureau, now renamed as the NATO Office of Security, 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. National authorities have an obligation to report possible breaches of security to the NATO office, which in turn must "coordinate with national authorities" in investigations.

Controlled distribution. The NATO security policy invokes two rules that are intended to strictly control 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, and access should never be authorized "merely because a person occupies a particular position, however senior." 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 docu-


34. 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.

ment, or by one of the addressees identified by the originator.\textsuperscript{37}

The second rule that restricts the distribution of information might 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. The principle was central to the agreement signed by NATO members in January 1950, which stipulated that:

The parties to the North Atlantic Treaty . . . will make every effort to ensure that they will maintain the security classifications established by any party with respect to the information of that party's origin; will safeguard accordingly such information; . . . and will not disclose such information to another nation without the consent of the originator.\textsuperscript{38}

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. Nor may a document be downgraded or declassified without the consent of its originator.\textsuperscript{39} The principle is even stricter with regard to distribution of documents outside the community of NATO governments. In this case, distribution is absolutely prohibited without consent, even if the information is graded as UNCLASSIFIED. In these circumstances, the information is regarded as "the property of the originator," which retains absolute control over its distribution.\textsuperscript{40}

**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 were still withheld in late 2002.41

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.42 NATO’s early policy made clear that decisions could be based on assessments of character and lifestyle, and that the evidentiary threshold 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.”43

Evidence that these rigorous standards are still applied can be found in CEE countries. Slovakia’s new security agency recently stated that it will review political and religious affiliations, as well as lifestyles—including extramarital affairs—that are thought to create a danger of blackmail.44 The Associated Press reported that Romania intends to deny clearances to security staff with “anti-western attitudes.”45 A constitutional challenge to Poland’s Classified Information Act by Polish judges was also motivated by their concern about intrusive investigations to determine whether their lifestyles could make them “susceptible to . . . pressure.”46

Other controls are imposed to control personnel after a clearance has been provided. The 1964 edition of C-M(55)15(Final) stipulated that supervisors had a 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.47 Finally, there was an expectation that “disciplinary action” would be taken against individuals who are responsible for the unauthorized disclosure of information.48 Additionally, as demonstrated later in this article, there appeared to be an expectation that member states would establish clear criminal penalties for unauthorized disclosure.

41. These were contained in a Confidential Supplement that was added to C-M(55)15(Final) in January, 1961. Clearance criteria for the WEU do not appear to be contained in its security regulations.
45. NATO Officials Want Romania to Exclude Some Former Communists From Intelligence Positions, ASSOCIATED PRESS NEWSWIRE, March 20, 2002.
II. Echoes of Earlier Debates

Observers in the CEE countries are probably right in seeing a clash between NATO security requirements and national policies on the right to information. There is a fundamental conflict with the principle undergirding transparency laws: that information held by government should be generally accessible, subject to a few narrowly defined exceptions. More concretely, there are several ways in which NATO policy appears to clash with the Johannesburg Principles, a set of rules regarding the balance to be struck between national security and transparency developed by a group of experts convened by ARTICLE 19, a freedom of expression advocacy organization, in 1995.49

In fact, contemporary debate in CEE countries echoes earlier disagreements among the first signatories to the North Atlantic Treaty. Archival records show that the early evolution of the policy was marked by clear divergences among governments about the balance to be struck between security and transparency. In the end, the balance was tipped toward security—the understandable result of a policy process dominated by military leaders, undertaken in secrecy, and in the context of immense threats to collective security.

Military influence over security policy. In NATO’s first three years, a body known as the Standing Group held sole responsibility for security policy. The Standing Group crafted the first NATO security policy, DC 2/1, approved by the North Atlantic Council in January 1950, and conducted the first field inspections of security practices of each member state to ensure compliance with NATO policy.

Formally, the Standing Group was a subcommittee of the Military Committee, which consisted of the Chiefs-of-Staff of all member countries and was “the supreme military authority” within NATO.50 The Standing Group had only three members, representing the Chiefs-of-Staff of the United States, the United Kingdom, and France. In practice, however, the Standing Group dominated the Military Committee. A chairman of the Military Committee observed: “The Standing Group... did not in practice ‘assist’ the Military Committee as discharge its functions almost entirely. All of the day-to-day business was done and all the day-to-day decisions were taken by this Group.”51 There were inequalities within the Standing Group as well. British and American officers believed that the French

49. The Johannesburg Principles are provided in SANDRA COIVER ET AL., SECRECY AND LIBERTY: NATIONAL SECURITY, FREEDOM OF EXPRESSION AND ACCESS TO INFORMATION 1-10 (1999). NATO policy appears to permit the categorical denial of public access to information, regardless of importance, in violation of Principle 12; and punishment for unauthorized disclosure of information, without regard to harm or benefit from disclosure, in violation of Principle 15. It may also encourage the denial of employment based on opinion or beliefs, or denial of due process in removal, in violation of Principles 5 and 20.


armed services was riddled with Communist sympathizers\textsuperscript{52} and often discussed security matters on a bilateral basis.

The Group's preeminence was at first understandable, given the military weakness of the other allies and the extraordinary threats that confronted the Alliance in its first years.\textsuperscript{53} Nonetheless, its power was "if not mildly resented, then certainly a cause for muttering."\textsuperscript{54}

Complaints about the Standing Group had two distinct dimensions. The first related to the disproportionate influence of the "Anglo-Saxons" and the exclusion of the nine other signatories of the North Atlantic Treaty.\textsuperscript{55} Based in the Pentagon, the Standing Group refused to distribute the agendas or minutes of its meetings to the representatives of the other nine governments.\textsuperscript{56} The Standing Group's attitude toward these other states was illustrated by its approach to field inspections of national security practices. All of the excluded states were inspected first, while the Standing Group's member states were inspected last.\textsuperscript{57} The British Security Service, MI5, conducted these inspections on behalf of the Standing Group.\textsuperscript{58}

A second concern was the dominant role played by the military in setting security policy. It soon became clear that NATO would serve as a vehicle for the coordination of political and economic questions, as well as military affairs.\textsuperscript{59} This implied a growing volume of communications between foreign and finance ministries, all undertaken under restrictive rules set by military staff. Non-military staff within the NATO secretariat itself also complained about the rigid rules that the Standing Group had imposed regarding the dissemination of information, about its unwilling-

\textsuperscript{52} RICHARD ALDRICH, THE HIDDEN HAND: BRITAIN, AMERICA AND COLD WAR SECRET INTELLIGENCE 145 (2002).


\textsuperscript{54} SIR PETER HILL-NORTON, NO SOFT OPTIONS: THE POLITICO-MILITARY REALITIES OF NATO 7 (1978).

\textsuperscript{55} PETER DUIGNAN, NATO: ITS PAST, PRESENT AND FUTURE 11 (2000). There were eleven other signatories after the accession of Greece and Turkey in October 1951.


\textsuperscript{57} With one exception: Canada was also one of the last countries to be inspected. The order of inspections is provided in NATO Security Coordinating Committee, Report by the Security Coordinating Committee to the Standing Group on the proposed examination of the functioning of the NATO security system in the United States, Canada United Kingdom and France. Brussels: NATO Archives. July 27, 1951. SG 7/42.


\textsuperscript{59} The importance of NATO's work in non-military fields was later emphasized by the 1956 Report on Non-Military Cooperation in NATO. See, SIR PETER HILL-NORTON, NO SOFT OPTIONS: THE POLITICO-MILITARY REALITIES OF NATO 9 (1978).
ness to acknowledge the authority of civilian officials within NATO, and about its secretiveness. “Never in all the positions I have held,” said Lord Ismay, who as Secretary General served as the head of NATO’s non-military staff, “have I felt so much in the dark.”

Complaints about the Standing Group’s role increased when it began an overhaul of DC 2/1 in early 1951. Its draft of a new security policy seemed to affirm—and perhaps strengthen—the Standing Group’s powers. In response, the Canadian government submitted a proposal to include military representatives from all twelve countries on the Security Coordinating Committee, which had been established by the Standing Group in January 1950 to specialize in security matters. The Belgian government went further. It was unacceptable, said Belgium, that SOI policy should be set by a body representing three nations, and “exclusively military in character”:

It is therefore necessary to find a way of . . . restoring to the civilian side its proper share in Security matters. . . . It is out of the question that [the North Atlantic Council] should be subject, in this connexion, to the decisions of the Standing Group, especially in view of the fact . . . that the secrets which have to be kept are not only military, but also political and economic secrets.

The solution, Belgium suggested, was the creation of a new security committee that would include civilian as well as military representatives, and be responsible directly to the Council, rather than NATO’s Military Committee.

The Standing Group dismissed the Canadian and Belgian proposals as unnecessary and impractical. This reflected a more general concern on the part of the Standing Group that reforms aimed at enlarging the influence of other countries would undermine its efficiency. Nevertheless, one of its members recognized that complete obduracy was unlikely to be effective in preserving the Standing Group’s influence.

62. On the effect that the proposed new policy would have on the authority of the Standing Group, see the brief submitted by the Belgian government in June 1951: Belgium, Memorandum by the Belgian Government to the Working Group on NATO Security. Brussels: NATO Archives. July 1951. AC/6-D/3.
The United Kingdom therefore put forward a compromise proposal. The Standing Group's Security Coordinating Committee would establish a subcommittee of civilian and military representatives from other European states that could advise on problems referred to it by the Security Coordinating Committee. The proposed European Security Committee would operate "on an equal level" with the Security Coordinating Committee on non-military matters, and the Council would arbitrate if the Standing Group's Security Coordinating Committee could not accept its recommendations.

This proved unacceptable to the United States. As a consequence, the next revision of the British proposal reduced the proposed European Security Committee to an arm of the Security Coordinating Committee, which would retain all authority on security matters. Meanwhile, France offered an even more modest concession: two representatives of NATO's civilian agencies would be permitted to join the Security Coordinating Committee whenever a revision of security policy was contemplated or inspections of civilian agencies were undertaken.

A deadlock among NATO governments persisted for a year. A Standing Group official wrote in March 1952 that

[T]here is still a diversity of views on this matter. All are apparently agreed that Security is indivisible, but the first divergence comes from those who consider it indivisibly a civil responsibility and those who consider it indivisibly military. There is a further minor divergence produced by members who, though willing to admit that Security may be a military responsibility in certain countries, are loath to see a top-level security body... containing any military representatives..... There is also the feeling that the highest technical body responsible for security should be more representative than the [Security Coordinating Committee] and should include at least some civil representation.

The official warned the Standing Group to ensure that "that the Military view received due consideration" in the final resolution of the debate.

The impasse appeared to be broken in May 1952. A Working Group on NATO Security finally proposed the establishment of a new Security Committee consisting of civilian or military representatives of all member countries, and supported by a new Security Bureau. The Standing Group's role would be reduced to the implementation of security policy within the

---

military sphere, although it would retain the right to send recommendations for changes in security policy directly to the Council.\footnote{72} The Standing Group, although still dubious about the merits of the proposal, nevertheless yielded, and the Council adopted the new structure in August 1952.\footnote{73}

**Controversy over breadth of NATO policy.** Within months, however, the Standing Group demonstrated that it still held a dominant role in the formulation of SOI policy. Between 1953 and 1955, it was the principal advocate for a policy overhaul that significantly expanded the breadth of NATO's influence over the practices of member states—but not without objection by some governments.

Concern about the breadth of NATO's SOI rules had been expressed since the adoption of the organization's first policy, DC 2/1, in January 1950. One of the main innovations of DC 2/1 was the establishment of the COSMIC security system. Documents flowing through the NATO apparatus were to be given a COSMIC marking, in addition to a security grading.\footnote{74} The distribution of COSMIC documents was to be carefully managed. They were to be sent only by cipher machines or in accompanied bags, and sealed in double envelopes to prevent unauthorized inspection. Each government was to establish a central registry to manage the flow of COSMIC documents, as well as sub-registries in each department. Receipts were to be issued whenever documents changed hands so that the registry could trace distribution. Only personnel with COSMIC authorization were permitted to view COSMIC documents.\footnote{75}

Within months of its adoption, the COSMIC system proved unworkable. The problem, said NATO's Secretary General, was "that too many papers were being called COSMIC and the result was that nobody could take any papers to study them anywhere, and it was thought to be too


\footnote{73} North Atlantic Council, Summary record of meeting of the Council on August 20, 1952. Brussels: NATO Archives. C-R(52)18. As late as April 1952, the Standing Group continued to insist that it should have sole responsibility for security policy. NATO Standing Group, Report by the Security Coordinating Committee to the Standing Group on establishment of a European Security Committee. Brussels: NATO Archives. April 9, 1952. SG 7/50: 2. Nevertheless, it recognized the probability that a larger, all-nations committee would be formed. Fears about the workability of this larger committee led the Standing Group to suggest that the new Security Bureau should report to the Secretary General rather than this new committee. The Working Group accepted this proposal, but the Council rejected it, and made the Security Bureau responsible to the new NATO Security Committee. A British official said privately that "this was palpably a further effort on the part of the Americans to build up the Secretariat at the expense of the committees on which national Delegations were represented." Foreign Office, Memorandum on Meeting of Working Group on NATO Security. May 23, 1952. United Kingdom Public Records Office. FO 371/102548, Jacket WU 1692/56.

\footnote{74} A document could be designated COSMIC TOP SECRET, COSMIC SECRET, and so on.

cumbrous."  

Acknowledging the difficulty, the Standing Group proposed an amendment "in order that the operations on non-military bodies . . . shall not be needlessly restricted."  

Approved in May 1950, the amendment narrowed the definition of COSMIC documents. The COSMIC marking would not apply to documents that did not refer to military defense planning, or which "by their nature of their content . . . require wide distribution for necessary action within Government ministries and departments." Instead, these documents would be given a new NATO marking, in addition to a security grading.

This amendment made the COSMIC system more manageable, but created a new problem: the SOI policy provided no guidance on the handling of NATO-marked material. In 1951, the Standing Group suggested that civilian arms of NATO might each develop their own security regulations, but this proposal was not pursued. An overhauled SOI policy adopted in March 1952 provided more detailed guidance on COSMIC procedures but said little about documents with the NATO marking. NATO documents, the policy said, should "receive the same care and handling as laid down for national classified material in each nation's own security regulations."

This proved unsatisfactory to the Standing Group. By July 1953, following discussions with military staff in the member states, it had decided that further reform of the SOI policy was essential. Although the Council had by now established a larger and more representative Security Committee, the Standing Group took the initiative to draft the proposed new policy. Delivered to the Security Committee in August 1954, the draft outlined the rationale for further changes:

---

The expansion of NATO now requires the wide dissemination of a vast amount of classified information, the bulk of which does not merit... the special protection of the COSMIC system. It is desirable, however, that this lower graded information should be given standardized protection according to its degree of secrecy, so that each member nation may be assured that any information which it contributes is being given the protection which security requires.\textsuperscript{82}

The draft proposed to limit the COSMIC system to TOP SECRET information, while introducing new requirements for handling all remaining NATO information. However, the draft went further, suggesting the need to assure adequate security for any sensitive information held by member states, even if it had not been distributed through the NATO apparatus:

In addition, it is desirable that all NATO nations should agree to conform to basic principles and standards for the protection of all information, both national and international, the unauthorized disclosure of which would endanger the security of present NATO planning.\textsuperscript{83}

The Standing Group withdrew its draft policy in September 1954, after "military sources" expressed a desire for further modifications.\textsuperscript{84} The Standing Group produced a second draft in December 1954,\textsuperscript{85} but within weeks military representatives made further recommendations for strengthening the policy.\textsuperscript{86}

The NATO Security Committee began a five-day review of the proposed policy in January 1955. By this time, there was significant pressure to adopt a revised policy quickly. In August 1954, the U.S. Congress had loosened statutory restrictions on the dissemination of information about nuclear weapons programs.\textsuperscript{87} Soon after, the U.S. government told its allies that it was prepared to sign an agreement on the sharing of atomic information at the NATO ministerial meeting planned for March 1955—but only on the condition that the revised SOI policy was adopted by the Council at the same meeting.\textsuperscript{88}


\textsuperscript{84} NATO Security Committee, Note by the Secretary of the NATO Security Committee. Brussels: NATO Archives. September 6, 1954. AC/35-N/5.


\textsuperscript{87} The Atomic Energy Act of 1946 overturned wartime agreements between the U.S. and major allies by blocking the transfer of information about nuclear weapons development to other nations. The Atomic Energy Act of 1954 loosened some of these restrictions.

As a result, there was little room to explore the implications of the new policy. At the Security Committee’s January meeting, several countries expressed concern about the breadth of the new policy:

The DANISH REPRESENTATIVE stated that his Government experienced some hesitation in approving Enclosure “B” as it stood since some provisions seemed to go further than laying down basic principles and minimum standards of security. . . . Enclosure “B” might be interpreted as applying to national as well as NATO information. There still existed a wide field of classified national information the security of which was a national responsibility. . . .

The CANADIAN REPRESENTATIVE supported the view expressed by the Danish Representative, stating that . . . Enclosure “B” should be regarded as a set of guiding principles rather than regulations which were binding on all governments.

The ITALIAN REPRESENTATIVE sympathised with this view and envisaged difficulties of a constitutional nature if some margin of latitude was not provided.89

The Committee responded with a minor amendment to the section’s preface that conceded that the basic principles and standards could be applied “in an appropriate manner” by national governments. Otherwise the scope and content of the section was not significantly changed.

Controversy over centralization. The mandate of the Security Bureau was also questioned during the 1954-55 overhaul of NATO’s SOI policy. The Standing Group’s August 1954 draft provided that the Security Bureau would be responsible for “periodic inspection of security arrangements for the protection of North Atlantic Treaty defense information within international and national civil organizations.”90 This affirmed existing practice. However, the Standing Group’s December redraft was more ambitious. The reference to NATO information was removed, and the Security Bureau was given a broad mandate to undertake “periodical examinations of the security system in national and international civil agencies.”91 This proved too expansive, and the final revision struck a middle ground. The Bureau could carry out “periodic examinations of the security arrangements for the protection of NATO classified information and material in national and NATO civil agencies.”92

The Canadian government continued to express concern about the degree of centralization implied in the proposal, and asked for assurance that the policy was not intended to give the NATO Security Bureau “any

executive or other authority within national systems." The assurance was provided. However, the British government countered with a proposal that the Security Bureau should have a mandate to give advice on the application of the basic principles and minimum standards of security. The Council approved this mandate and quickly invoked it. In August 1955, NATO appointed an advisor to the West German government, whose accession to NATO had recently been approved, to provide guidance "in setting up an overall security system" that would safeguard national information as well as NATO documents.

Controversy over depth of NATO policy. Concerns about the depth of the new policy—that is, the extent to which captured less sensitive information within classification rules—were also aired but defeated. Two governments, Norway and Denmark, joined in a proposal to simplify the classification system by eliminating the RESTRICTED grading. The Norwegian government "felt that this grading was superfluous, and that its definition as well as the rules governing the safeguarding of document so graded were so vague that they might lead to confusion instead of contributing to overall NATO security." Most other nations disagreed, and "for the sake of unity," Norway withdrew its proposal.

The concerns expressed by Norway and Denmark echoed those made by American journalists five years earlier. The RESTRICTED grading had been an element of U.S. classification policy since the first executive order on classification in 1940. In 1950, it became the subject of controversy, when President Truman issued a new executive order giving civilian agencies the authority to classify documents for the first time. The vagueness of the RESTRICTED grading reinforced fears that the order would give officials "vast discretion" over the release of information. Despite a year of protests by editors and journalists, the order went into effect in October 1951. However, in November 1953, the Eisenhower administration reversed course and eliminated the RESTRICTED grading in U.S. policy.


Unfortunately, it was impossible for U.S. editors and journalists to mount a similar protest against the broad classification standards in the NATO policy, which was itself a RESTRICTED document at that time, and therefore inaccessible. In October 1957, the Danish government again proposed a simplification of the grading system, which it believed encouraged over-classification.101 Again, a majority of 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.102

**Personnel controls.** The Standing Group's 1954 draft of a new SOI policy also proposed tougher rules for personnel handling sensitive information. For the first time, NATO policy would affirm the need for "positive vetting," a practice of active background investigations intended to uncover evidence of disloyalty or improper affiliations, or character defects that might make an individual susceptible to improper influences.103 Positive vetting was central to the "loyalty program" for American government employees introduced by the Truman administration in 1947, and strengthened by the Eisenhower administration in November 1953.104

For several years the British government had resisted the American system of positive vetting. Many British policymakers found American methods "repugnant"105 and doubted their effectiveness.106 In 1948, the British government had adopted a more restrained system of "negative vetting," consisting only of a check against security service files for evidence of inappropriate political affiliations.

Positive vetting was not included in early versions of NATO SOI policy due to this disagreement between the U.S. and the United Kingdom. The January 1950 version of the SOI policy, DC 2/1, suggested only that "positive inquiries" might be necessary for some of the most sensitive positions in government.107 Its March 1952 successor, DC 2/7, did not discuss per-

---


102. 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 on the control of the volume of classified documents in NATO agencies had earlier reported that a majority of its members opposed the Danish proposal. See Note by Chairman of the Working Group on the control of classified documents in NATO agencies. Brussels: NATO Archives. January 13, 1958. AC/35-WP/13.


However, the British did not protest the incorporation of positive vetting requirements in C-M(55)15(Final). The Truman and Eisenhower administrations, pressured by powerful isolationist elements in Congress, made clear that they could not reestablish the practice of sharing of atomic information unless the British adopted the positive vetting system. Also pressured by its own military leaders, the British Cabinet relented and adopted the American procedures. The Eisenhower administration reciprocated by proposing reforms to the Atomic Energy Act in February 1954 to facilitate the sharing of atomic information.

In late 1955, the British government publicly affirmed its new commitment to the practice of positive vetting. It conceded that the new measures were "alien to our traditional practices" but insisted on the necessity of "tilting the balance in favour of offering greater protection to the security of the State rather than in the direction of safeguarding the rights of the individual."

Penalties for unauthorized disclosure. The security policy adopted by the Council in March 1955 made clear that "disciplinary action" was to be taken "against any individual who is responsible for the compromise of NATO classified information." No comparable provision was included in earlier policies. However, a series of substantial leaks in 1952 and 1953 demonstrated the need for firmer rules, and resulted in increased pressure on member states to adopt criminal penalties for unauthorized release of NATO information.

109. On the evolution of British policy, and American pressure to adopt positive vetting, see MARGARET GOWING, INDEPENDENCE AND DETERRENCE: BRITAIN AND ATOMIC ENERGY, 1945-1952 (1974); RICHARD ALDRICH, THE HIDDEN HAND: BRITAIN, AMERICA AND COLD WAR SECRET INTELLIGENCE (2001). An advisor to Prime Minister Attlee observed: "We want the American Atomic secrets and we won't get them unless they modify the McMahon Act. Officials have already offered the procedure now proposed [positive vetting] and nothing short of that offer and the direct question to the candidate about Communist association is from the Americans' point of view a sine qua non - will secure their cooperation": RICHARD ALDRICH, THE HIDDEN HAND: BRITAIN, AMERICA AND COLD WAR SECRET INTELLIGENCE 425 (2001).
111. White Paper on Security Precautions in the British Civil Service. 35 PUB. ADMIN. 297, 297-304 (Autumn 1957); DAVID VINCENT, THE CULTURE OF SECRECY IN BRITAIN, 1832-1998 at 203 (1998). The Canadian government, which also participated in a collaborative atomic program with the UK and US during the war, was in a similar predicament and adopted the positive vetting system before 1950.
Frustration with leaks peaked after a meeting of the Council in April 1953.\textsuperscript{114} The main aim of the meeting was the resolution of the sensitive issue of how much each nation would contribute toward a £250 million defense infrastructure program. The \textit{New York Times} published details of the proposed plan two weeks before the meeting.\textsuperscript{115} A week later, the \textit{Times}, London’s \textit{Daily Telegraph}, and the Associated Press simultaneously published details of NATO’s plans for production of fighter aircraft. Matters deteriorated during the meeting when \textit{Le Monde} reproduced the agenda and provided a running summary of the talks, while the \textit{Times} summarized American and British background reports on relations with the Soviet Union.\textsuperscript{116} Major press services transmitted the final communiqué hours before the NATO secretariat formally released it. Later, the \textit{Times} excerpted a secret paper on Soviet-Chinese relations discussed at the meeting.\textsuperscript{117}

In May 1953, Secretary General Ismay told the Council that leaks such as these posed a “grave threat” to NATO’s effectiveness. The NATO Council directed the Security Committee to study “the extent to which each member government could take legal action in respect of leakages of NATO classified information . . . [and] report to the Council as soon as possible with regard to any practical steps that could be taken to ensure that leakages of NATO classified information would not occur in future.”\textsuperscript{118}

The Security Committee made a ten-month study of state secrets laws and reported to Council in March 1954. Only three countries—France, Italy, and Turkey—had clear criminal penalties for the unauthorized disclosure of NATO classified information. (In fact, France recently had modified its law to address this issue, perhaps in response to the leaks controversy.\textsuperscript{119}) Many countries were found to have state secrets laws that were deficient or ambiguously worded. Two of these countries, Belgium and the Netherlands, reported that they were contemplating amendments to address problems with their state secrets laws. The Security Committee recommended that governments consider “suitable supplementary legisla-

\textsuperscript{114} This summary of leaks relating to the meeting is drawn from North Atlantic Council, Summary record of meeting of the North Atlantic Council. Brussels: NATO Archives. May 6, 1953. C-R(53)25: 9. The final communiqué for the April 1953 meeting can be found at LORD ISMAY, NATO: THE FIRST FIVE YEARS 195-97 (1955). A former chairman of the NATO Military Committee observed that negotiations over infrastructure programs were “a highly contentious and time-consuming process.” SIR PETER HILL-NORTON, NO SOFT OPTIONS: THE POLITICO-MILITARY REALITIES OF NATO 114 (1978).
\textsuperscript{115} See Benjamin Welles, NATO Experts Urge 3-Year Joint Plan on Defense Costs, N.Y. \textsc{Times}, April 15, 1953, at 1.
\textsuperscript{116} See C.L. Sulzberger, NATO Council Opens Vital Session Today, N.Y. \textsc{Times}, April 23, 1953, at 1.
\textsuperscript{117} See C.L. Sulzberger, China-Soviet Ties Scanned by NATO, N.Y. \textsc{Times}, April 27, 1953, at 7.
\textsuperscript{119} \textsc{Decret} 52-813 of July 11, 1952 amended French law to criminalize the unauthorized disclosure of NATO information. Similar provisions were incorporated into the French Penal Code in 1960, through \textit{Ordonnance} 60-529 of June 4, 1960. Correspondence from Mr. Hervé Halimi, University of Paris (November 28, 2002).
tion” to ensure that there would be criminal sanctions for leaking NATO information.\footnote{120} The Council endorsed the recommendation.\footnote{121}

In August 1954, the Standing Group considered the problem of leaks. Its draft overhaul of the NATO security policy included a new section dedicated to the problem of “leakages of information to the press.”\footnote{122} It proposed that national security authorities should have the duty to immediately investigate leaks and take “disciplinary action” against leakers. The Standing Group later added another proposal, giving the NATO Security Bureau the authority to coordinate with national authorities on leak investigations.\footnote{123} Comparable rules are found in the final version of the policy adopted by the Council in March 1955.

The subject did not rest there. The chairman of the Security Committee, apparently dismayed by governments' response to the Committee's 1954 recommendation on reform of national laws, returned to the subject in a January 1956 meeting. "To make the position quite clear," the chairman said, governments were to answer five questions about their state secrets laws:

1. Is a NATO secret considered to be a “State secret”?
2. Can any person guilty of disclosing a “State secret” be prosecuted whether he be a member of the Government, an official or a private citizen?
3. Is the charge the same for a person who intentionally discloses a secret and for one who does so by negligence?
4. Can a person who discloses a “State secret” or a NATO secret be prosecuted in a country when the offence has been committed outside that country?
5. Can a country prosecute a foreigner who has disclosed a NATO secret on its territory?\footnote{124}

Most countries answered that their national legislation provided adequate protection. Denmark responded that its law had been modified in April 1955 to address these issues, while Belgium said that statutory changes had been introduced in April 1956. The Greek government also reported that “necessary steps to revise legislation to cover all possible cases” were being taken.\footnote{125}

Ironically, in the United States, sanctions for unauthorized disclosure of classified information remained weak. Congress refused to enact criminal penalties except in narrowly defined circumstances, such as the disclosure of atomic information or deliberate disclosure to foreign agents. The American representative to NATO conceded the inadequacy of these measures in his report to the Security Committee. In March 1955, the Department of Justice told Congress that it had broader penalties under "active consideration." A bipartisan commission on government security established in August 1955 recommended wider criminal sanctions, but Congress again failed to act.

III. Evidence of Continuing Influence

The tension between domestic policies on access to information and intergovernmental obligations continues to be evident among NATO's older member states. One critical conflict concerns the treatment of information received from other governments, or intergovernmental organizations such as NATO, under domestic access-to-information laws. Adopted after the establishment of the NATO security regime, these laws have been drafted to accommodate the principle of originator control that is entrenched in NATO SOI policy. Governments have resisted calls for loosening this rule in national access-to-information laws, but have rarely acknowledged that national policy is constrained by intergovernmental commitments. Consequently, many domestic policy actors continue under the misapprehension that the content of national policy can be decided in national fora.

Canada. Debate over Canada's Access to Information Act (ATIA) illustrates the problem. The law obliges the Canadian government to deny any request for access to information provided in confidence by other states or international organizations of states unless the originator consents to its release. In 1987, a parliamentary committee recommended that the law be amended to give the government discretion to release such information when disclosure seemed unlikely to cause harm.
Commissioner later gave qualified support to the proposal.  

The Canadian government has consistently resisted these proposals. In 1987, it argued that weakening the originator control rule would impair "[t]he willingness of other governments to continue to share their information." More recently, it has said that any reform would "set Canada apart from its key allies." This may be an indirect way of making clear the fundamental problem: that reform of this part of the ATIA would create a conflict between national law and Canada's obligations under the North Atlantic Treaty. Canada cannot explicitly acknowledge the potential conflict, because this would constitute a non-consensual disclosure of the substance of NATO's security policy. As a result, many Canadians continue to believe that reform is a matter that can be settled on the merits by domestic actors.

United Kingdom. The same misapprehension may prevail in other jurisdictions. In 1999, the British government was criticized for incorporating the originator control rule in its draft Freedom of Information Act. The Campaign for Freedom of Information, a non-governmental organization, described this as an "indiscriminate" exemption that would allow the withholding of "harmless information." Parliamentarians attempted to have the provision amended, but the government opposed these proposals on the grounds that they would violate a universally recognized norm of confidentiality. It failed to explain that the government was constrained by more than convention: such an amendment would create a conflict between statutory and intergovernmental obligations. Similar complaints were made against a comparable provision in the new Scottish Freedom of Information Act. However, the Scottish government was explicitly constrained by the agreement governing the delegation of power to Scotland from the United Kingdom, which required Scotland to respect the terms of C-M(55)15(Final).


135. The originator control rule is preserved in section 27(3) of the Freedom of Information Act 2000.


United States. In the United States, debate about the degree of protection to be given to information provided by foreign governments was stirred by the 1998 case of *Weatherhead v. United States*.\(^{140}\) At the center of that case was the question of whether the judiciary should be permitted to consider the reasonableness of the U.S. government's decision to withhold a communication from the British government. Advocates for transparency argued in favor of the court's power to intervene, saying that it was indefensible in an open society to support a policy of absolute secrecy for inter-governmental communications, and that foreign governments could not reasonably expect total secrecy.\(^{141}\)

The case did not involve NATO communications, however, the transparency advocates' case was probably overstated. As the NATO policy shows, there are clearly domains where other governments do have a reasonable expectation of complete secrecy, based on the existence of an SOI agreement. Furthermore, the capacity of the judiciary to intervene and impose the right balance on questions of disclosure is exaggerated. The effect of NATO's SOI policy is to deny domestic actors, including the courts, the opportunity to make their own decisions about the disclosure of information within a certain policy domain.\(^{142}\)

Sweden. Some governments have been more candid about the constraints that intergovernmental SOI agreements impose on national policy. Sweden has a long tradition of governmental openness that clashes sharply with the demands of the originator control rule. At the same time, Sweden wishes to engage with the international community, and thus must try to reconcile national practices with international norms.

The tension is evident in the SOI agreement between the WEU and Sweden signed in March 1997. A declaration by the Swedish government annexed to the agreement attempts to maintain the form of national policy while conforming to international norms. Sweden asserts the right to make its own decisions about disclosure of WEU documents, but observes that national law permits it to withhold information if disclosure would "disturb international relations." It then recognizes that any disclosure of WEU information without consent would "disturb relations" with the WEU.\(^{143}\) In effect, Sweden acknowledges its willingness to give the WEU a veto on disclosure, although the decision will be cloaked in the form of a calculation by national policymakers about the substantive harm likely to be caused by the release of WEU documents.

---

\(^{140}\) See *Weatherhead v. United States*, 157 F.3d 735 (9th Cir. 1998).


European Union. The position of the European Union also provides a clear demonstration of the influence of NATO policy. On July 26, 2000, the Council of the European Union approved substantial restrictions to its policy on public access to Council documents. The amendments eliminated the public's right of access to almost all classified information\(^{144}\) and permitted the release of other documents containing sensitive information about member states only with their consent. The Council's decision explained that the EU's expansion into the field of defense policy would require the exchange of "particularly sensitive" information, and that this could be accomplished "only if the originator of such information can be confident that no information put out by him will be disclosed against his will."\(^{145}\) Many observers were shocked by the decision. They did not know that on the same day the Secretary General of the Council had entered into an interim security agreement with NATO that incorporated the key elements of C-M(55)15(Final).\(^{146}\)

The spirit of the July 2000 amendments is continued in a new regulation governing access to information held by EU institutions adopted in May 2001. Under the new regulation, national governments and bodies like NATO retain the right to block the disclosure of classified information relating to public security or defense which they have provided to EU institutions. The classification policy of the originating institution, rather than that of the EU, will determine whether documents are subject to the rule of originator control.\(^{147}\) These arrangements proved highly unpopular among advocates of transparency but were 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 and WEU SOI rules. The span 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.\(^{148}\) This imposes another con-

---

\(^{144}\) RESTRICTED information was not included in this change.


\(^{146}\) The agreement was contained in an exchange of letters between Lord Robertson, Secretary General of NATO, and Javier Solana, Secretary General of the Council of the European Union. The identifying number of the NATO policy (that is, C-M(55)15(Final)) was redacted in the publicly accessible version of the correspondence. See Letter from Lord Robertson, Secretary General of NATO, to Javier Solana, Secretary General of the Council of the European Union on NATO-EU Interim Security Agreements. July 26, 2000. Available from the Secretariat of the Council of the European Union.


straint on the transparency policies of the fifteen EU member states, and will soon apply to the policies of the thirteen states that have applied for accession to the EU. The Council has also prepared a draft decision that would compel member states to adopt consistent criminal penalties for the unauthorized disclosure of EU classified information.\textsuperscript{149}

**Conclusion: A Thickening Web of Secrecy Rules**

The prevailing sentiment among advocates of transparency is that processes of globalization and intergovernmental collaboration help to promote greater governmental openness. "For nation-states," Ann Florini observed in 1998, "the shift is occurring between old ideas of sovereignty,

which allowed states to keep the world out of their domestic matters, and a new standard that they must explain their actions to the world."150 Thomas Blanton argued in 2002 that "more often than not, supranational organizations create a demand for greater access to information, both between and within countries."151

These assessments may underestimate the potential hazards of certain kinds of global integration. As Chart One shows, nations within Europe are subject to an increasingly dense web of intergovernmental arrangements that constrain the use and distribution of information by national governments. The United Kingdom, for example, is bound by SOI agreements with NATO and the WEU, and by the recent EU decision on classified information; these three intergovernmental organizations are themselves bound to one another by SOI agreements. This may facilitate the flow of information among states and intergovernmental organizations, but it does so at a price. It entrenches rules that strictly limit the flow of information to non-governmental parties, and even within the administrative arms of governments themselves. In this context, "old ideas of sovereignty"—at least insofar as control of information is concerned—have been strongly affirmed.

This web of SOI arrangements has dimensions which, although important, are not addressed in this paper. Governments have also negotiated innumerable bilateral SOI agreements that constrain national policies. In some instances, the content of these agreements is classified; in other cases, the very existence of the agreement is kept secret. Some bilateral agreements may explicitly adopt NATO standards to govern the handling of all sensitive information exchanged by the signatories. The United States acknowledges that it has negotiated at least fifty-three such agreements.152 Its agreement with Britain, signed in 1961 and only declassified in 2001, incorporates NATO standards, as does its agreement with Canada, signed in 1962 but only declassified in 2002.153 The influence of NATO rules is also extended by their explicit incorporation in SOI agreements between national and sub-national governments154 and between national governments, industry and the educational sector.155

---

150. See Ann Florini, The End of Secrecy, 111 FOREIGN POL’Y 50, 50-63 (Summer 1998).
151. See Thomas Blanton, The World’s Right to Know, FOREIGN POL’Y 50, 56 (July/August 2002).
152. The Office of the Secretary of Defense provided this information in September 2002, in response to a Freedom of Information Act request submitted by the author.
153. The US-UK General Security of Information Agreement was declassified and released by the UK Ministry of Defence in March 2001 following a parliamentary question by Mr. Robert Key, MP. The US-Canada Security of Information Agreement was declassified and released in November 2002 response to an Access to Information Act request by the author.
154. The agreement between the United Kingdom and Scotland, noted earlier, is an illustration. A comparable agreement was also made with the Government of Wales.
155. In fact, C-M(55)15(Final) says explicitly that standards for the protection of classified information entrusted to industry and universities should be consistent with the standards and principles which it prescribes. See NATO, Security within the North
This transnational web of SOI agreements diffuses values that conflict sharply with those promoted by advocates of transparency. The fact that these agreements exist and are increasingly interconnected with one another also makes the work of transparency advocates much more difficult. The problem is not just that reform of domestic policy may be constrained by a specific intergovernmental SOI agreement. The reform of one SOI agreement may also require modifications to other agreements that are linked and built on similar principles.\(^{155}\)

In fact, it is conceivable that the thickening web of SOI agreements could actually strengthen incentives for governments to tighten security practices. The connection of governmental networks means that the flow of information through any one government will be increased. It follows that the amount of information that could be improperly diverted at any point is also increased. To adapt a metaphor, the entire network becomes as porous as its weakest node. Bigger networks are necessarily more prone to compromise.

Internal documents recently prepared by Canadian security and intelligence officials highlight another difficulty. Since the end of the Cold War, Canada is said to have developed “more bilateral intelligence relationships, and arguably, a more complex set of sensitivities regarding the protection of information provided in confidence.” In some intelligence analyses, the officials note, it is now “impossible to distinguish information that may have originated from Allies.” The commingling of domestic and foreign-sourced information makes it harder to apply Canadian right-to-information law, which applies distinct disclosure rules to the two kinds of data. The proposed response was to rely exclusively on the more restrictive rule—that is, the rule for foreign-sourced information—in cases where commingling had occurred.\(^{157}\)

Of course, rules to preserve security of information are essential. However, these rules must be suited to the realities of the time, including the nature of the perceived security threat and the expectations of citizens about access to information. This fact has always been obvious to governments, who have debated the contours of SOI policy behind closed doors for decades. In a world in which security threats and citizen expectations have changed radically, it is no longer acceptable to conduct the debate

---


157. The proposed response was to eliminate the obligation to separate or “sever” information in cases where such commingling had occurred. The memoranda were prepared by the Security and Intelligence Secretariat of the Privy Council Office in April and May 2001, and released to the author in July 2002 in response to Access to Information Act request. The proposed response was included in a draft report of the government’s Access to Information Act Review Task Force, released in response to the same request.
over SOI rules in this way. It is time for the debate about SOI rules to be democratized. An appropriate first step would be for NATO, like other multilateral institutions, to recognize the need for greater transparency, and explain more fully what expectations it imposes on its member states.