Democracy, Human Rights, and Intelligence Sharing

ELIZABETH SEPPER*

ABSTRACT

In this Article, the author explores the networks used by intelligence agencies to share intelligence and conduct joint operations with foreign counterparts worldwide. Understanding how these intelligence networks operate, the author argues, is imperative both for effective intelligence gathering and for a democratic society. Characterized by secrecy, flexibility, and informality, intelligence sharing networks are constrained almost exclusively by a shared professional ethos, rather than law. According to the author, such an ethos can exert some degree of accountability to professional norms, but has been strained by the inclusion of less professional and often ruthless intelligence services in the network. Nonetheless, all such networks pose serious threat to the preservation of liberal democracies in that they essentially govern themselves. The very concept of democracy demands that an intelligence agency be held accountable to a democratic body or officials outside of the agency itself. Yet, as this Article shows, few democratically elected officials are aware of intelligence sharing; and virtually no mechanism, other than self-regulation, provides oversight or accountability for any intelligence agency’s transnational activities. As a result, through their network ties, intelligence agencies that are expected to serve democratic interests have undermined foreign policy and circumvented safeguards established by domestic law and international treaties. The author argues that this serious gap in the rule of law must be filled and posits ways to render intelligence agencies more accountable to the democracies they purport to serve.

SUMMARY

INTRODUCTION ............................................................................................................... 153

I. CHARACTERISTICS OF TRANSNATIONAL INTELLIGENCE SHARING NETWORKS........................................................................................................... 154

* Fellow, Columbia Law School and the Center for Reproductive Rights; LL.M. in International Legal Studies, New York University School of Law; J.D., New York University School of Law; B.A., 2002, Boston University. Special thanks to Stephen Holmes, who supervised my LL.M thesis upon which this Article is based. Many thanks to Benedict Kingsbury, Simon Chesterman, Philip Alston, Samuel Rascoff, and the participants of the Institute for International Law and Justice Scholars Workshop, particularly Emily Berman and Jared Schott, for their comments and suggestions. My profound thanks to the editors of the Texas International Law Journal for all their hard work.
A. Secret and Flexible Arrangements ................................. 156
B. Adherence to Professional Network Norms .................. 159
C. Reputational Sanctioning to Ensure Compliance with Professional Norms ......................................................... 163

II. CHALLENGES OF TRANSNATIONAL INTELLIGENCE COOPERATION FOR DEMOCRACY AND HUMAN RIGHTS ................................................................. 166
A. Deficit of Democratic Accountability and Control................ 167
   1. Lack of Transparency ......................................................... 168
   2. Absence of Democratic Oversight ....................................... 169
B. Collusion to Avoid Democratically Determined Policies and Statutes ... 172
C. Undermining Foreign Policy and Human Rights through Connections to Illiberal Agencies ..................................................... 174
   1. Quid Pro Quo: Intelligence at What Price? ......................... 175
   2. Silencing Criticism and Bolstering Authoritarian Regimes ....... 176
   3. Complicity of Liberal Democracies in Rights Violations........... 178

III. A PROPOSAL FOR MORE PROFESSIONAL, DEMOCRATIC INTELLIGENCE EXCHANGE .......................................................................................................... 182
A. Acculturation of Intelligence Agencies to Ethical Professional Norms ................................. 183
   1. New Rules for Intelligence Cooperation ................................. 183
      a. Ethical Standards in Compliance with International Human Rights Law ............................................................... 184
      b. Caveats as a Requirement ................................................ 185
      c. Restrictions on the Use of Shared Information .................. 187
   2. Professionalization of Illiberal Agencies ................................. 189
   3. Limits on Quid Pro Quo ....................................................... 192
B. Establishing Democratic Oversight and Accountability .......... 193
   1. Improve Transparency through Declassification ................. 194
      a. Declassification and Legislative Approval of Intelligence Sharing Agreements ....................................................... 194
      b. Presumption in Favor of Declassification of Shared Information ................................................................. 195
   2. Establish Democratic Control and Oversight ...................... 197
      a. Set Clear Statutory Authority and Limitations on Intelligence Cooperation ....................................................... 197
      b. Develop Budgetary Control ............................................. 200
C. Rely on and Bolster Law Enforcement Intelligence .................. 201
   1. Improve Law Enforcement Sharing Networks ..................... 202
   2. Benefits of Law Enforcement Intelligence and the Involvement of Courts ................................................................. 203

CONCLUSION ................................................................................................................... 206
INTRODUCTION

Although the global community—and the United States in particular—had long discussed improving information sharing to combat transnational crime, the events of September 11, 2001 brought networks for information sharing center-stage. Coalition forces in Afghanistan formed networks to exchange information about military operations; financial regulators established formal links to enforce sanctions; and law enforcement agents institutionalized more frequent contact with other services. Pride of place was reserved, however, for the intelligence agencies and their networks.

The post-9/11 counterterrorism strategy was intelligence-driven, and intelligence agencies and their networks would be at the helm. These agencies, which had long networked with foreign counterparts, thus broadened and deepened their connections. They incorporated new, and sometimes surprising, partners for the exchange of information. Network exchanges became frequent and widespread with ever more information shared with an increasing number of actors.

Almost ten years later, the role of intelligence agencies has not diminished. If anything, their prominence has grown. Barely a week goes by without a government touting its intelligence cooperation. Media reports hinting at the degree and regularity of cooperation and intelligence sharing have become commonplace.

Yet, the specifics remain secret. For those outside the intelligence profession, little is clear about how intelligence agencies cooperate with each other, which partners are most involved, and how sharing mechanisms function in practice.

This Article argues that it is imperative that we understand these little known intelligence networks, given their central role in global counterterrorism strategy and their serious risk to democracy and accountability. Characterized by secrecy, flexibility, and informality, the intelligence sharing networks are constrained almost exclusively by a shared professional ethos, rather than law. Such an ethos can exert some degree of accountability to professional norms, but has been strained by the inclusion of less professional and often ruthless intelligence services in the network. These networks, which essentially regulate themselves, pose an increasingly serious threat to the preservation of liberal democracies. Intelligence agencies in a liberal democracy are expected to act professionally, to inform foreign policy, and to serve democratic interests. The very concept of democracy demands that an intelligence agency be watched and held accountable by a democratic body or officials, outside of the agency itself. Yet, as this Article shows, virtually no other mechanism provides oversight or accountability for an intelligence agency’s transnational activities. Democratically elected officials, whether legislative or executive, often are entirely ignorant of intelligence cooperation. With little oversight or regulation of their network ties, agencies can circumvent domestic and international legal restraints and collude with one another to the detriment of their respective states. These networks thus strain our conceptions of the role of intelligence agencies, the effectiveness of national control, and the democratic state itself. Recognizing that intelligence cooperation and democratic principles will likely always be in tension, this Article proposes several solutions to tip the balance from self-regulation to democratic oversight and accountability.

Part I begins with an examination of currently known network arrangements and their common characteristics. It explains that intelligence sharing networks
trade information on shared threats, function in secrecy, and operate with a high level of informality. Most importantly, intelligence professionals identify with one another—especially their trusted partners. Within their network arrangements, agencies develop standards of professional behavior and enforce some degree of compliance with them by sanctioning violations of professional standards.

Part II argues that in addition to the benefits they offer for the rapid exchange of information, transnational intelligence network arrangements exact significant costs for democracy and human rights. Without vigilant oversight, intelligence networks have significant ability to undermine foreign policy and circumvent safeguards established by domestic statutes and international treaties. The human rights abuses committed by intelligence services in recent years are not isolated examples but rather symptoms of a more systemic problem inherent in allowing intelligence services to escape scrutiny of their transgovernmental ties. As Part II will show, intelligence agencies through their network contacts have been able to countermand policies made in democratic fora. Together, agencies have undermined human rights protections, strengthened authoritarian governments, and outsourced torture and abuse.

Accepting that intelligence networks can and should counter transnational threats, Part III proposes several improvements to make intelligence sharing more effective. It recommends two reinforcing methods to secure better, more democratic and human rights-compliant intelligence exchange. First, agencies from liberal democracies should establish more robust professional standards and use their networks to acculturate less reputable agencies to more ethical and accurate behavior. Second, democratic representatives and the global public should devote greater time and attention to the problems that persist in transnational intelligence networks. The transnational activities of agencies should be monitored and regulated. Ultimately, intelligence agencies should be rendered accountable to the democracies they purport to serve.

I. CHARACTERISTICS OF TRANSNATIONAL INTELLIGENCE SHARING NETWORKS

Often presumed nationalistic and averse to cooperation, intelligence agencies in fact have long networked with one another, sharing information and coordinating operations to address mutual problems. Some contemporary intelligence networks date back to the Cold War.1 Many others materialized after the fall of the Soviet Union, when agencies found that, in a globalized world, they were increasingly called upon to combat problems spanning borders, such as drug and human trafficking, organized crime, and terrorism.2 After the attacks of 9/11, these networks were

1. See Richard Aldrich, The Hidden Hand: Britain, America and Cold War Secret Intelligence 8–9 (2001) (discussing the development of the Western intelligence community after World War II). These intelligence exchange networks took on one of three forms: the client-server network of the Union of Soviet Socialist Republics; Western, or Western-allied, agencies exchanging information through NATO and more commonly bilateral arrangements; and former (or then) colonial powers continuing ties with intelligence services in former colonies. Id. at 8–9, 408; Chris Clough, Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation, 17 INT’L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 601, 603–04 (2004) (discussing the Soviet client-server network).

2. Richard J. Aldrich, Dangerous Liaisons: Post-September 11 Intelligence Alliances, HARV. INT’L REV., Fall 2002, at 50, 54 (“[T]here is something to be said for viewing clandestine agencies and their
further expanded to include some unlikely and otherwise hostile intelligence partners and, in some cases, deepened to allow more regular information exchange.

Although intelligence networks are often described as a one-on-one relationship or as a “hub and spokes” configuration, they are best conceptualized as a spider web with a multiplicity of connections expanding in every direction. The complexity of connections cannot be overstated. A single intelligence agency may have hundreds of ties and relationships to counterpart agencies worldwide. The Canadian Security Intelligence Service (CSIS), for example, which has relatively little independent ability to collect intelligence globally, has more than 250 information sharing arrangements with foreign security and intelligence organizations. Unlike the CSIS, the U.S. Central Intelligence Agency (CIA) has global reach, including connections to more than 400 agencies.

These networks supply reach and competence far beyond that permitted by the budgets and resources of each individual agency, giving members access to fiscal and technological intelligence resources and global intelligence product. Through contacts with foreign intelligence agencies, an intelligence official receives information she otherwise might not have because of her agency’s limited technical, geographical, human, or linguistic resources. Even the United States—which has by far the highest intelligence budget in the world, exceeding capability in technical
areas, and world-wide reach—depends on foreign intelligence agencies with comparative advantage in other specialized areas.  

This Part provides a brief background of the defining characteristics of transgovernmental intelligence networks. Such networks are transgovernmental in that the relevant actors are not heads of state or foreign ministers, but rather specialized government agencies. “Intelligence” networks thus connect intelligence agencies to their counterparts in other countries for the purpose of exchanging information. The primary characteristics of these networks, as Section A describes, are absolute secrecy and flexibility in the form, style, and mechanisms of sharing. Section B explains that networks give rise to a professional community that sets its own standards and norms. Within this community, the extent to which an intelligence agency receives valuable information is decided by its reputation (the degree to which it can be trusted and add value). Therefore, as Section C argues, reputation is sacrosanct. As a result, in the absence of control by more democratic organs, networks can exert some compliance with professional norms through sanctioning.

A. Secret and Flexible Arrangements

Although transgovernmental networks generally lack transparency as compared to other institutions, intelligence sharing networks operate with the highest levels of secrecy. The very structures through which agencies share information are among the intelligence community’s top secrets even where the existence of such

---

7. See, e.g., SHLOMO SHPIRO, THE COMMUNICATION OF MUTUAL SECURITY: FRAMEWORKS FOR EUROPEAN-MEDITERRANEAN INTELLIGENCE SHARING 6 (2001), available at www.nato.int/acad/fellow/99-01/shpiro.pdf (noting that most intelligence services of Mediterranean countries do not have global coverage but “possess the capabilities to train and operate agents throughout the region in a better way than the US intelligence community or many of their European counterparts”).


9. A number of scholars and intelligence professionals define intelligence functionally, as information generated by intelligence agencies. See MICHAEL HERMAN, INTELLIGENCE POWER IN WAR AND PEACE 96 (1996) (stating that “[u]nprocessed single-source data is officially ‘information,’ and becomes intelligence only through ‘the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation’”); Roy Godson, INTELLIGENCE: AN AMERICAN VIEW, in BRITISH AND AMERICAN APPROACHES TO INTELLIGENCE 3 (K.G. Robertson ed., 1987) (noting that “[g]overnments and even intelligence services rarely define intelligence explicitly. Instead, they develop policies, programmes, and patterns of organization. These demonstrate the role the state visualizes for itself, and its concept—i.e. definition—of intelligence.”); Müller-Wille, supra note 2, at 7. For the purpose of this Article, intelligence is defined functionally as information generated by intelligence agencies. This Article will therefore use the terms intelligence and information interchangeably. The definition of intelligence used here excludes “open source” intelligence, which is publicly available, since it generally does not raise the human rights and accountability issues endemic to other forms of intelligence.

networks has been revealed, the essential elements—the participants, methods of operation, and agreements themselves—remain classified.\footnote{11}

In the rare case, these secret intelligence networks have been negotiated and agreed to by the heads of states, likely resulting in executive agreements between states.\footnote{12} Such is the case, for instance, with the most formalized and best-known intelligence network between the signals intelligence (SIGINT) services of the United Kingdom, Canada, Australia, New Zealand, and the United States.\footnote{13} The allied intelligence superpowers emerging from World War II negotiated the United Kingdom-United States Intelligence Agreement (“UKUSA Agreement”) in 1947 at a high level of government to achieve global SIGINT coverage, which neither could achieve alone.\footnote{12} Canada, Australia, and New Zealand rapidly signed on as second parties to the agreement. Unlike more informal arrangements, this agreement institutionalized and divided the collection and exchange of SIGINT between all five agencies—resulting in the most integrated known intelligence network.\footnote{15} These agencies were namely the U.S. National Security Agency (NSA), U.K. Government Communications Headquarters (GCHQ), Australian Defence Signals Directorate (DSD), Canadian Communications Security Establishment (CSE), and New Zealand Government Communications Security Bureau (GCSB).

While most academic studies have focused on the UKUSA Agreement, it represents an aberration both in its formality and its degree of integration. Other multilateral networks have developed more informally. Best known are the numerous, long-standing plurilateral “clubs” of European agencies focused on intelligence exchange against transnational threats.\footnote{16} TRIDENT, the cooperative

---

11. The UKUSA Agreement set the precedent for institutionalizing the requirement of absolute secrecy as to the agreement’s existence. Jeffrey T. Richelson, The U.S. Intelligence Community 294 (4th ed., 1999) (1985) (“Despite numerous references to the agreements in print, officials of some of the participating governments have refused to confirm not only the details of the agreement but even its existence.”). While recently there has been some public discussion of UKUSA’s existence, freedom of information requests to relevant governments generate no information. Kevin J. Lawner, Post-Sept. 11 International Surveillance Activity—A Failure of Intelligence: The ECHELON Interception System & the Fundamental Right to Privacy in Europe, 14 PACE INT’L L. REV. 435, 444–45 (2002).

12. Rudner, Hunters and Gatherers, supra note 10, at 195. The prime example involves the early SIGINT sharing agreements to which the Commonwealth countries are signatories. Jeffrey T. Richelson & Desmond Ball, The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries 4–7 (1985). See also Matthew M. Aid, The National Security Agency and the Cold War, in SECRETS OF SIGNALS INTELLIGENCE DURING THE COLD WAR AND BEYOND 27, 33 (Matthew M. Aid & Cees Wiebes, eds., 2001). Canada even permitted the United Kingdom to represent its interests in negotiations. Rudner, Hunters and Gatherers, supra note 10, at 196; Martin Rudner, Britain Between and Between: UK SIGINT Alliance Strategy’s Transatlantic and European Connections, 19 INTELLIGENCE & NAT’L SECURITY 571, 574 (2004) [hereinafter Rudner, Britain Between and Between] (“Later, countries like Denmark, Germany, and Turkey were reportedly included in a somewhat looser, more limited association as so-called ’Third Parties‘, usually by virtue of bilateral arrangements . . . .”).


14. SHPIRO, supra note 7, at 12.

15. Richelson, supra note 11, at 293.

16. Rudner, Hunters and Gatherers, supra note 10, at 210 (“The Club of Berne, dating from 1971, is a forum for the heads of the security services of European Union (EU) member countries . . . . The Club has no statutory mandate; neither does it report to any authority within the EU framework.”). Established in the 1970s, the Kilowatt group now unites twenty-four states—including most EU members
arrangement between intelligence services of Israel, Turkey, and Ethiopia, is another example, although little is known about it.\textsuperscript{17} Informal regional arrangements, supplemented by bilateral ties, have been set up throughout the Asia-Pacific region as well.\textsuperscript{18}

The great majority of intelligence is shared, however, not through formal or multilateral agreements but rather through informal, typically bilateral network arrangements.\textsuperscript{19} Even among the five UKUSA countries, the UKUSA Agreement does not govern all intelligence exchange. Instead, hundreds of less formal ties connect the various agencies of the five countries.\textsuperscript{20}

Most commonly, national intelligence agencies (rather than governments) negotiate memoranda of understanding (MOUs), setting out modalities of intelligence exchange.\textsuperscript{21} In contrast to treaties, or even executive agreements, MOUs do not require approval by national legislators (or foreign policy ministers) and can be implemented by the agencies themselves.\textsuperscript{22} As non-binding, soft law agreements, MOUs regularize contacts and cooperation between individual intelligence services.\textsuperscript{23} Considered flexible and easy to establish, they “create a loose and adaptable framework in which to share information, ideas, and resources.”\textsuperscript{24} These written agreements establish both the degree and method of cooperation.\textsuperscript{25}

Less formal arrangements based on oral agreements or personal friendships are also widespread among intelligence agents. Generally speaking, they govern information exchanges in the absence of an MOU, supplant existing MOUs, and characterize ad hoc contacts during crises.\textsuperscript{26} Frequently operating below the level of

\begin{itemize}
  \item[17.] SHAPIRO, supra note 7, at 15.
  \item[18.] See, e.g., Simon S.C. Tay, \textit{Asia and the United States After 9/11: Primacy and Partnership in the Pacific}, 28 FLETCHER F. WORLD AFF. 113, 118 (2004) (“ASEAN signed an anti-terrorism pact that would commit members to cooperate in stemming the flow of funds to terrorist groups as well as sharing intelligence and increasing police cooperation in order to ‘prevent, disrupt and combat international terrorism.’”); ANDREW SCHEINESON, \textit{COUNCIL ON FOREIGN REL.}, PUB. NO. 10883, \textit{THE SHANGHAI COOPERATION ORGANIZATION} (Mar. 24, 2009), available at http://www.cfr.org/publication/10883/ (noting that under the Shanghai Cooperation Organization, the security services of Russia, China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan share intelligence and conduct joint counterterrorism drills).
  \item[19.] HERMAN, supra note 9, at 207.
  \item[20.] RICHELSON & BALL, supra note 12, at 141. To give an indication of the sheer number of agencies involved, the United States alone has fifteen intelligence agencies. Norman C. Bay, \textit{Executive Power and the War on Terror}, 83 DENV. U. L. REV. 335, 350 (2005).
  \item[21.] Lefebvre, supra note 4, at 533 (“Bilateral liaison arrangements are a defining characteristic of the intelligence world. Set up formally (i.e., with the signing of a Memorandum of Understanding) or informally (on the basis of an unwritten, gentlemanly agreement), they pay particular attention to the participants’ protection of their intelligence.”).
  \item[23.] Sol Picciotto, \textit{Networks in International Economic Integration: Fragmented States and the Dilemmas of Neo-Liberalism}, 17 NW. J. INT’L. L. & BUS. 1014, 1047 (1997); Raustalia, supra note 8, at 22.
  \item[24.] Raustalia, supra note 8, at 22. The relative level of formality or informality is not, however, determinative of the network’s efficiency. GILL, supra note 2, at 36.
  \item[25.] See SHAPIRO, supra note 7, at 13 (discussing three interrelated levels of cooperation—macro, micro, and meso—and what each level entails).
official control, informal cooperative arrangements also allow contact even when interaction with a certain intelligence agency (or state) is officially disfavored.  

Ultimately, these varied networks share numerous characteristics. We can expect them to form against common threats, to remain secret, and to operate with a high level of informality. Most importantly, intelligence professionals exhibit a high level of identity with one another—especially their trusted partners. This professional community and its potential for sanctioning violations of professional standards will be explored further in Section B.

B. Adherence to Professional Network Norms

Through their network ties, intelligence agencies form what Peter Haas terms “an epistemic community,” that is, a network of professionals who share a specialized expertise and knowledge in a particular field. Shared practices, normative principles, and evaluative criteria within their domain give agencies a sense of identity with their counterparts in other countries. These commonalities make it possible, indeed probable, that agencies network with one another.

Three principal attributes are common to all intelligence services. First among these is the requirement of secrecy in performing collection, analysis, counterintelligence, and covert operations. Second, security clearances and access to classified information generate “a deliberate culture of identification as a member of a unique, even elite club.” The secrecy of intelligence agencies magnifies this corporate cohesiveness—which all professions exhibit to some degree—generating a sense of superiority and an affinity for fellow intelligence professionals. Third, all intelligence agencies understand themselves to assist national-level decision-making and serve in the defense of the state. They consequently, at least among professionalized services, attempt to act in accordance with a professional ethos of objectivity and pursuit of truth so that decisions can be made on valid, reliable information.

---

27. Gill, supra note 2, at 36 (observing that with regard to law enforcement intelligence, “[s]ome of these contacts will be legitimated via official agreements while others will be officially frowned on”).
29. Id.
30. Id.
32. Id.
33. Id. See also Herman, supra note 9, at 327 (observing a “greater-than-usual sense of difference from other walks of life”).
34. Bruneau & Dombroski, supra note 31, at 166.
35. Loch K. Johnson, Bombs, Bugs, Drugs, and Thugs: America’s Quest for Security 100 (2000) (“The ethos—in theory at least and usually in practice—is objectivity, and the goal is to provide decision makers with accurate, timely, and relevant information and insight . . . .”); accord Herman, supra note 3, at 345.
Within this community of networked intelligence agencies, intelligence producers develop standards and norms—more or less formally articulated—to which members must adhere. The professional standards of the UKUSA network in particular are so well-developed that, according to James Bamford, an expert on the NSA, the UKUSA community constitutes “a unique supranational body, complete with its own laws, oaths, and language, all hidden from public view.” What then are the network standards with which intelligence agencies must comply, or stand accountable before their peers?

Information security and handling, as well as provision of reliable information, figure prominently in these standards. Because every exchanged secret risks disclosing sources and methods and thereby jeopardizing future information, sending agencies require the enforcement of tight rules for the handing and storage of shared intelligence. Communications, physical facilities, and personnel must be secure and able to protect sensitive information.

Two principal rules ensure that shared intelligence will be kept confidential and not further disseminated without the sending state’s consent. First, the “need to know” principle, typical of intelligence agencies worldwide, dictates that individuals only receive access to shared, classified information when they need it for their work. Within intelligence networks, a sending agency may stipulate that only it or the specific addressee of the intelligence may make the decision that an individual “needs to know.” In some cases, shared “intelligence may even be designated only for the specific agency with which it is shared; the latter being expected to restrict circulation even with its sister agencies.”

Second, information shared remains the property of the originator of the information. Known as originator or user control, this rule restricts subsequent dissemination of information. Before confidential information is released, a

---

36. See Simon Chesterman, The Spy Who Came in from the Cold War: Intelligence and International Law, 27 Mich. J. Of Int’l L. 1071, 1099 (2007) (arguing that intelligence agencies’ interactions have generated some agreed-upon normative guidelines and a professional ethic that suggests “a kind of community that generates, adapts, and internalizes rules”).

37. James Bamford, Body of Secrets: The Anatomy of the Ultra-Secret National Security Agency: From the Cold War Through the Dawn of a New Century 403–04 (2001); Richelson & Ball, supra note 12, at 5 (stating that the Agreement includes access to intelligence and security arrangements, standardized codewords, security agreements that all employees of each UKUSA agency must sign, and procedures for storing and disseminating material); James I. Walsh, Intelligence-Sharing in the European Union: Institutions Are Not Enough, 44 J. Common Market Stud. 625, 630 (2006) (“It establishes common security procedures and standardized technical terms, code words and training across the participating countries’ intelligence services, ensuring that shared intelligence is handled in a consistent manner and is unlikely to be misinterpreted by a receiving state.”).

38. Müller-Wille, supra note 2, at 15 (“All intelligence collectors are concerned about the security of their sources and their methods of collecting information. If these are uncovered, access to the information will be jeopardized. In addition, they may want to protect the information itself.”).


41. Roberts, supra note 39, at 338 (“The principle was central to the agreement signed by NATO members in January 1950.”). Intelligence sharing between domestic agencies of the same national intelligence community also occasionally uses a classification caveat, known as ORCON (originator controlled). The CIA uses ORCON most extensively than any other U.S. agency—perhaps because it receives much intelligence from foreign agencies. Michael A. Turner, Why Secret Intelligence
receiving agency is obliged to guarantee that it will not be disclosed. The provider also sets the classification level, which the recipient is bound to respect, and reserves the right to maintain or change it. Sometimes a sending agency authorizes the future sharing of information with the services of certain other states a priori; at other times, it only approves further distribution on an ad hoc basis. This is to avoid what is known as a “Trojan Horse”—where “a receiver shares the intelligence with third parties that have not obtained the provider’s security clearance.”

To avoid intelligence failure caused by inaccurate intelligence, professional best practices require screening exchanged intelligence for relevance and attaching written caveats to indicate the information’s reliability. These caveats can allow a receiving agency to judge a piece of information’s probative value. If the intelligence has not been tested, the receiving agency should not rely on it without corroboration. Professional standards provide that, in all cases, an agency generally should “test” or corroborate received intelligence through its own independent collection capabilities. Alternately, services can cross-check the information through contacts with other foreign counterparts. For example, if France provides Germany with intelligence indicating that a specific individual is associated with terrorist activities and crossed into Germany in a given month, German intelligence might request information regarding that person from intelligence agencies in bordering states. If other information proved that he or she had been in Singapore for the entirety of that month, France’s shared intelligence would be deemed incorrect.

---

42. Accountability and Transparency Background Paper to Arar Commission, supra note 41, at 7 (noting that much of the intelligence “Canada receives is designated as confidential and released only on the guarantee that it will not be publicly revealed”).


44. Id. (noting senders may stipulate, for example, that information may be shared within NATO or members of the EU’s Partnership for Peace framework who have adequate, pre-approved security agreements).

45. Müller-Wille, supra note 2, at n.21 (setting out reasons a receiving agency might pass on information to a third agency).


47. Paradoxically, for these agencies, the only way the quality of intelligence exchanged can be improved is through further sharing. Müller-Wille, supra note 2, at 16 (“The accuracy can only be verified or falsified if the collection of intelligence is increased, not if it is reduced.”).

48. A disadvantage of this approach lies in the potential for “circular reporting,” where “[a] snippet of data may be passed in a full circle, and thus, when received by the originating nation, may be considered corroboration for what might have been only a tentative assumption in the first place.” Clough, supra note 1, at 606. In our example, if Germany had received the same intelligence from the United States as from France, it might accept that as corroboration—even if the U.S. had simply passed on intelligence received from French intelligence. For examples of networked connections that led to circular reporting, see BAMFORD, supra note 37, at 417.
Between closer network partners, standards may also include agreements to distribute all intelligence gathered on a certain issue or by a specific collection discipline (such as SIGINT), or to refrain from intercepting communications of a partner’s nationals or using the network to gather economic information for national corporate interests.

A reputation for compliance with these norms helps determine the volume, type, and quality of information an agency receives and thus correlates to the network’s overall level of efficiency.\(^{49}\) Highly trusted partners receive intelligence in real-time and on a frequent basis, and may share intelligence gathering resources such as satellites or listening stations.\(^{50}\) At one extreme, the “ECHELON” system between the UKUSA SIGINT agencies represents a tightly integrated—and likely unprecedented—network for sharing intelligence, spanning collection centers worldwide and enabling the agencies to collect an enormous volume of communications, as many as three billion a day.\(^{51}\) According to Nicky Hager, who wrote the first detailed exposé of the system, the network allows the stations of each partner agency to function as “components of an integrated whole.”\(^{52}\) The example of ECHELON shows that networks function mostly efficiently and effectively when composed of partners that can be trusted to abide by professional standards.

In order for an intelligence agency to gain trust within the network, it must establish a good professional reputation.\(^{53}\) Because networks facilitate transmission of information relating to a member’s reputation for competence and trustworthiness,\(^{54}\) intelligence officials are familiar with their peer’s reputations, which vary even among agencies in the same country.\(^{55}\) Many intelligence agencies are acutely aware that their performance will be measured by their counterparts

---

49. Wenpin Tsai & Sumatra Ghoshal, *Social Capital and Value Creation: The Role of Intrafirm Networks*, 41 Academy of Management J. 464, 467 (2004). Chris Clough identifies five levels of intelligence sharing: (1) raw intelligence product revealing the source and product in detail; (2) “all or part of raw product without exposing the source;” (3) summary of data (4) finished analysis of data; and (5) “policy conclusions resulting from the intelligence.” Clough, *supra* note 48, at 603.

50. See Clough, *supra* note 1, at 603–605 (noting examples of close intelligence cooperation between countries).


52. Nicky Hager, *Secret Power: New Zealand’s Role in the International Spy Network* 29 (1996). Nicky Hager’s report is considered among the best informed analyses, although the existence of the ECHELON system have never been officially confirmed. Rudner, *Britain Betwixt and Between*, supra note 12, at n.31. See also Lawrence D. Sloan, Note, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 Duke L.J. 1467, 1470 (2001) (“The closest a representative of the United States intelligence community has come to publicly confirming the existence of ECHELON was when the Director of Central Intelligence, George Tenet, referred to the ‘so-called ECHELON program of the National Security Agency’ in congressional testimony.”).


54. Id. at 54 (noting that “evident violations of those norms would quickly be transmitted across the network, raising the cost of those violations”).

As former intelligence official Michael Herman says, “[i]n secret intelligence more than in most activities, a good reputation is slowly gained, and easily lost.”

C. Reputational Sanctioning to Ensure Compliance with Professional Norms

Whereas numerous civilian controls, including statutory limits, budgetary oversight, and professional rewards, govern actions of law enforcement and military officials, intelligence professionals even in democratic states generally rely on professional norms to delineate the boundaries of their own transnational actions and to hold partners accountable. The written agreements (whether executive agreements or MOUs) and oral understandings that apply to intelligence sharing networks are not legally enforceable; there are no judicial remedies or political sanctions to provide redress for breaches. Nonetheless, networks can create conditions under which professional standards come to be respected, despite the lack of legal sanctions.

Within networks, real and imagined pressures from the intelligence peer group drive compliance with professional norms in a process Ryan Goodman and Derek Jinks have labeled “acculturation.” These pressures “include (1) the imposition of social-psychological costs through shaming or shunning and (2) the conferral of social-psychological benefits through displays of public approval.” Goodman and Jinks suggest this drive toward acculturation may actually work better within a denser network of relationships, because the network partners know one another, have multiple interactions, and seek to remain members in good standing.

Unlike persuasion, acculturation does not require that “actors actively assess the content of a particular message—a norm, practice, or belief—and ‘change their

56. See HERMAN, supra note 9, at 207 (explaining that “most intelligence agencies are producing partly for an international audience of fellow-professionals, as well as their primary national recipients”).


58. Bruneau & Dombroski, supra note 31, at 164. Arthur S. Hulnick & Daniel W. Mattausch, Ethics and Morality in United States Secret Intelligence, 12 HARV. J. L. & PUB. POL’Y 509, 509, 520 (1989) (“Ethics are often defined as behavior relating to professional standards of conduct. As in any other profession, such standards exist in the field of intelligence, even if these standards require behavior that is unacceptable for private citizens.”); SLAUCHER, supra note 53, at 54. See also Harold Hongju Koh, Transnational Legal Process, 75 NEB. L. REV. 181, 204 (1996) (“As transnational actors interact, they create patterns of behavior and generate norms of external conduct which they in turn internalize.”).


61. GOODMAN & JINKS, supra note 60, at 8.

62. Id. at 5–6.
minds. For example, if Jordanian intelligence understands that complying with standards like caveating for reliability or not sharing information obtained through torture is a precondition for inclusion and good reputation in the network, it will obey the standards out of a desire to join or become a respected member of the group. The agency need not have an inherent belief in the normative legitimacy of the rule to comply. It may even consider torture to be a useful interrogation method, but desist from the practice for the purpose of information sharing because of its desire to be an esteemed network partner. Classic social network analysis suggests that the agency—through network interactions—may then come to internalize those norms, resulting in a higher rate of compliance and greater incentives to maintain a good reputation.

Experience shows that when prestigious actors within the intelligence networks transmit network standards and exert pressure on their peers, other intelligence agencies comply even when not admitting the legitimacy of the rule. The United States and the United Kingdom, in particular, have acculturated their partners to relatively arbitrary standards of behavior. At the insistence of U.S. intelligence, for example, positive vetting of intelligence recruits for disloyalty or allegiance to radical groups remains the professional standard—despite its dubious contribution to increasing security. Even the United States’ closest allies must adopt such regulations in order to secure its cooperation. In a similar pattern, the U.S. Drug Enforcement Agency has used its cooperative networks to acculturate partners to drug trafficking detection, investigation, and interdiction; as a result, methods of agencies are now very similar.

63. Id. at 3–4, 5 (“The touchstone of the overall process [of persuasion] is that actors are consciously convinced of the truth, validity, or appropriateness of a norm, belief, or practice.”).
64. Id. at 7 (arguing that compliance can be motivated by the “social-psychological benefits of conforming to group norms and expectations (such as the ‘cognitive comfort’ associated with both high social status and membership in a perceived ‘in-group’”).
65. See GOODMAN & JINKS, supra note 60, at 8 (discussing the various social pressures that cause internalization of and conformation with group behavioral patterns). Initially, however, those less-professionalized services that join the network may abide by network standards out of pure self-interest, rather than any internal sense of normativity. Id. at 8–9.
66. SPIRO, supra note 7, at 39–40 (explaining that “development of intelligence cooperation frameworks would depend on developing effective systems of information classification acceptable on both cooperating sides. It also requires NATO authorities to accept, or at least endorse, the personnel vetting practices and security clearances of potential cooperation partner intelligence services.”). See also SLAUGHTER, supra note 53, at 172 (observing a similar phenomenon with regards to MOUs concluded by the U.S. Securities and Exchange Commission and foreign regulators’ implementation of U.S.-style regulation).
67. Aldrich, supra note 2, at 425 (Soon after U.S.-U.K. peacetime intelligence sharing began, the advisor said “. . . Officials have already offered the procedure now proposed [positive vetting] and nothing short of that offer . . . will secure their cooperation.”).
68. GILL, supra note 2, at 75 (“Americanization’ rather than ‘harmonization’ fairly describes global evolution of law enforcement since the 1960s, especially regarding drugs.”). Foreign drug enforcement agencies are not necessarily persuaded of the value of these techniques, rightly so since international drug enforcement efforts have generally failed. Diane Marie Amann, The Rights of the Accused in a Global Enforcement Arena, 6 ILSA J. INT’L & COMP. L. 555, 556 (2000). However, drug or transnational crime intelligence units in illiberal countries have improved and adopted more professional methods in spite of the otherwise repressive tactics typically employed by other intelligence units. See, e.g., Seth G. Jones et al., Nat’l Security Research Division, Securing Tyrants or Fostering Reform? U.S. Internal Security Assistance to Repressive and Transitioning Regimes, RAND 85 (2006), available at http://www.rand.org/pubs/monographs/2006/RAND_MG550.pdf (noting that Uzbek Sensitive Investigation Unit, charged with countering drug trafficking, now operates within Western norms with the support of the U.S. DEA).
To counteract incentives to depart from professional standards, intelligence networks rely heavily on reputational sanctioning. Anecdotal evidence suggests that professionalized services agonize over their foreign partners’ potential disapproval. The British government, for example, sought an injunction against *Spycatcher*, an exposé of British intelligence, because it would cause “damage to the reputation of the services in the eyes of foreign allies.”

For intelligence officers, “the consequences of exceeding [international professional norms is] unacceptable—personally and professionally, nationally and internationally.”

Exclusion from a network because of a bad reputation is improbable—largely because most partners need the comparative advantage that the other provides. Nevertheless, without a good reputation, the individual agencies (or agents) may find themselves deprived of necessary information. For example, in the early 1960s, the relationship of the British Secret Intelligence Service (MI6) with the CIA fell to a low because security lapses and molehunts damaged the CIA’s trust in MI6. MI6 remained valuable, however, due to high-quality intelligence it gathered from a few select sources behind the Iron Curtain. The history of Communist agent penetration of the German Federal Intelligence Service (or Bundesnachrichtendienst (BND)) resulted in its allies withholding the most sensitive or high-resolution intelligence. Even today, residual fears of Russian infiltration sometimes cause Germany’s allies to hold back intelligence. Although trilateral negotiations between the BND, NSA, and GCHQ resulted in a U.S. eavesdropping station jointly manned by BND and NSA officials, the BND is not allowed access to communications gathered by the NSA. Those services that develop a reputation for providing bad intelligence to the network likewise may find their flow of shared intelligence reduced to a trickle.

Misuse of intelligence may also reduce sharing. For example, connections between the CIA and Mossad were interrupted at least twice. The first time, Israel used U.S. intelligence to bomb Iraq’s nuclear reactor in 1981 over the CIA’s objections; the second time, the Mossad was revealed to have a spy within the U.S.

---

69. Patrick Birkinshaw, *Freedom of Information: The Law, the Practice and the Ideal* 38 (3rd ed. 2001); see also Kent Pakel, *Integrity, Ethics and the CIA: The Need for Improvement*, STUDIES IN INTELLIGENCE 85 (Spring 1998) (stating that in interviews, many intelligence officials at the CIA described a “tyranny of reputation,” in which “a bad call can stay with you for three years”).

70. See Chesterman, supra note 36, at 1097 (arguing that this notion “rings true”). See also Anne-Marie Slaughter & William Burke-White, *The Future of International Law is Domestic (or, the European Way of Law)*, 47 HARV. INT’L L.J. 327, 334 (2006) (“They build trust and establish relationships among their participants that create incentives to establish a good reputation and avoid a bad one.”).

71. Stephen Dorril, MI6: *Inside the Covert World of Her Majesty’s Secret Intelligence Service* 703 (2000). See also Richelson & Ball, supra note 12, at 6 (noting that security lapses have resulted in compromise of UKUSA intelligence numerous times).

72. See James Risen, *BomSniffs for Russian Moles, Worrying C.I.A.* , N.Y. TIMES, June 4, 1998 (One U.S. intelligence officer asserts that the BND has had “a history of penetration, and the truth is we have never really taken them too seriously as an intelligence organization”).


74. Erich Schmidt-Eenboom, *The Bundesnachrichtendienst, the Bundeswehr and Sigint in the Cold War and After, in Secrets of Signals Intelligence During the Cold War and Beyond* 129, 147–50 (Matthew M. Aid & Cees Wiebes eds., 2001); Dorril, supra note 71, at 778.
More recently, Australian intelligence was reportedly frustrated by the degree to which British and American intelligence flooded it with untested, often poor, intelligence in the run-up to the Iraq war, and considered expanding its own collection abilities to reduce its dependence on other intelligence agencies.

Consequently, other network actors can exercise a powerful form of accountability. Unlike the public, intelligence agencies have the knowledge and means to demand information and compliance from their intelligence sharing partners. Although the secrecy of transnational sharing makes it impossible to evaluate the extent to which network sanctioning results in compliance with professional norms, reputational control is not necessarily less effective than hierarchical control. When all network members subscribe to a norm, internal regulation may be even more effective and efficient than external controls. Nevertheless, as the next section will show, the lack of democratic oversight and control of intelligence networks permits abuses and undermines human rights in a way that calls out for democratic scrutiny and stringent regulation.

II. CHALLENGES OF TRANSNATIONAL INTELLIGENCE COOPERATION FOR DEMOCRACY AND HUMAN RIGHTS

The self-regulating and secret nature of transnational intelligence networks poses a significant challenge to our very conception of democracy and the appropriate role of agencies in the democratic state. A democracy requires that the people set policy. Thus, in liberal democracies, intelligence agencies have the sole function of preserving the democratic state. They are to carry out and inform policy, not to make it. Democracy also entails transparency and oversight of executive agencies and demands accountability, that is, clear standards to guide agency behavior. The coercive power of intelligence agencies is, therefore, to be reined in through statute, treaty, and legislative oversight.

Yet, as this Part argues, the involvement of our intelligence agencies in information sharing networks challenges each of these assumptions. Section A describes the lack of democratic accountability and oversight inherent in these intelligence networks. The opacity with which these networks operate results in


76. Robert O. Keohane, The Concept of Accountability in World Politics and the Use of Force, 24 Mich. J. Int’l L. 1121, 1129–30 (2003) (“Unlike outsiders, they can identify who is responsible for results or for failures: they have information as a result of their organizational activity. Precisely because they are likely to suffer if their organization does badly (insofar as accountability operates at the level of the organization), they have incentives to help correct the problem at the individual level.”).

77. Id. at 1134.

78. Koh, supra note 60, at 1401 (arguing that “the most effective form of law-enforcement is not the imposition of external sanction, but the inculcation of internal obedience”). See also Oran R. Young, International Cooperation: Building Regimes for Natural Regimes and the Environment 71 (1989) (“Most members of social systems comply with the dictates of prevailing institutions most of the time for reasons having little or nothing to do with their expectations regarding the imposition of sanctions.”).

public ignorance and legislative indifference, leaving services largely to determine their own transnational activities even in liberal democracies. Instead of being checked by legislation, information sharing is only minimally regulated by professional standards. Section B argues that without proper oversight, intelligence networks permit domestic foreign policy to be undermined and national and international law to be circumvented. Paradoxically, as Section C explains, Western intelligence agencies attempt to carry out their mission of preserving the democratic state by cooperating with unethical intelligence agencies in illiberal states and lending their support to authoritarian regimes. Moreover, the professional norms agencies set for themselves in these networks prove easy to disregard. With connections to less-reputable agencies, intelligence services from liberal democracies often give in to the temptation to commit human rights abuses and to outsource torture. Even the most professional agencies may trade in unreliable or untested information, to the detriment of the demos.

A. Deficit of Democratic Accountability and Control

A functioning democracy assumes that each executive agency’s actions are subject to executive and legislative approval and control. Yet, intelligence networks effectively shield ever-greater degrees of government activity from public view and domestic structures of accountability. With secrecy and non-disclosure as its cardinal rules, transgovernmental intelligence cooperation often occurs without the knowledge of domestic constituencies. The coercive power and substantial potential for error of intelligence networks are subject to little or no domestic oversight or review. As to terrorism or arms smuggling, the issue of accountability is especially salient, because measures are usually taken against individuals (often citizens of nations lacking strong accountability mechanisms) with little possibility of effective political or legal challenges. Although networks exert some degree of accountability through professional standards and reputational sanctioning, from a democratic standpoint the “view of intelligence as a profession that largely governs itself according to its own definition of responsibility” is alarming.

This section argues that the network connections of agencies of liberal democracies currently operate in a legal void, an anathema to the rule of law and democracy. As Section 1 explains, the secrecy and opacity with which these networks function marginalize democratic institutions. Section 2 shows that democratic oversight at any level is minimal, which in turn means intelligence agencies have few clear statutory or regulatory limits on activities conducted with their foreign counterparts.

80. Although scholars differ on the exact definition of accountability, Robert Keohane explains that “[a]ll satisfactory definitions of accountability include, explicitly or implicitly, two essential features: information and sanctions.” Keohane, supra note 76, at 1124. More specifically, “there must be some provision for interrogation and provision of information, and some means by which the accountability-holder can impose costly sanctions on the power-wielder.” Id.

81. Bruneau & Dombroski, supra note 31, at 166.
1. Lack of Transparency

At the heart of the lack of democratic accountability lies the fact that even though intelligence agencies regularly cooperate with one another, their network arrangements are nearly invisible to national publics, legislators, and international bodies. The opacity and deniability under which networks operate insulate each intelligence agency from criticism. An agency can seldom be reprimanded for sharing or failing to share information with network partners, since it denies having them; nor does it risk major repercussions for other states’ intelligence failures caused by bad intelligence it provided. Put simply, an oversight committee cannot provide input, request information, or impose restraints on arrangements of which it has no knowledge.

Cooperation can take place without public knowledge, legislative consent, or even executive approval. In 1954, for example, the Danish intelligence chief approved and then covered up United States intelligence reconnaissance flights across Danish territory, which could not be cleared through diplomatic channels. Similarly, Turkish government leaders were not informed of the secret agreement between Turkish and American military intelligence agencies to gather SIGINT. More recently, the Lithuanian state security service gave permission to the CIA to run a secret prison in the country, without informing the president or the prime minister.

The perpetual secrecy of information shared through networks further exacerbates the problem. Under current arrangements, any intelligence provided in confidence by another intelligence agency stays perpetually secret and exempt from freedom of information requests, unless the originator consents to its declassification and release. Within tightly knit intelligence agreements such as the UKUSA arrangement, domestic and shared information may become commingled, resulting in the more restrictive rule, intended for foreign information, to become the default

82. Aldrich, supra note 2, at 53 (“[I]n a global era, when clandestine agencies rarely work alone on large issues, the near invisibility of liaison arrangements to oversight by elected representatives is problematic. Oversight mechanisms have not kept pace with global issues.”).

83. Matthew M. Aid & Cees Wiebes, Conclusions, in SECRETS OF SIGNALS INTELLIGENCE DURING THE COLD WAR AND BEYOND 313, 324 (Matthew M. Aid & Cees Wiebes eds., 2001) (“[I]ntelligence chiefs of many of the European Sigint organisations sometimes kept many of the details of their intelligence collaboration with the US and Great Britain a secret from senior civilian officials in their own governments.”). At other times, political sensitivity created incentives to shield intelligence sharing from the public eye. Id. at 326 (“[W]hile the working relationship between NSA and the CIA on one hand and the Norwegian military intelligence organisation, the FO/E, on the other hand was quite close, the political leaders of Norway were constantly fearful that this relationship would become a matter of public record.”).


85. Aid & Wiebes, supra note 83, at 324 (“American military officials in Turkey had to remind their colleagues back in Washington . . . not to mention [this agreement] in any discussions with Turkish political or diplomatic authorities”).


87. See, e.g., Roberts, supra note 39, at 353-357 (listing examples of the continuing influence of NATO’s security of information policy over domestic access-to-information laws accommodation of originator control).
rule for classification and access to information. Based on a study of NATO’s information sharing, Alasdair Roberts concluded that “[t]he connection of governmental networks means that the flow of information through any one government will be increased,” thus increasing incentives to tighten security and classification of all information. Thus, more information becomes permanently withheld from those outside the intelligence community. Even when the originator or sharing agreement provides for declassification after a certain number of years, declassification is not linked to the existence of a justification for continued secrecy.

2. Absence of Democratic Oversight

A constant throughout the globe is that intelligence agencies are considerably insulated from sunshine and sanctions as compared to other government agencies. Even in the United States, which is considered to have some of the most stringent legislative monitoring of intelligence agencies, Congress typically only reviews intelligence policy after an issue becomes public—putting out the fire rather than preventing it. Within Europe, some states do not have any parliamentary body to monitor intelligence, although some employ other means of supervision.

88. See id. at 359. Roberts concludes that intelligence exchange agreements challenge assumptions that “global integration is favorable to increased transparency” and that “domestic policy on matters of state secrecy is increasingly constrained by the thickening web of agreements on security of information.” Id. at 332.

89. Id. at 359 (“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.’”). Romanian intelligence, for example, informed parliament that NATO required that a bill for the classification and protection of shared intelligence as state secrets be passed. Id. at 332 n.10; see also Duke, supra note 43, at 609–10 (discussing increased classification and “very secret” designations required of the EU to gain access to information from member states or other organizations by NATO). Even international tribunals are forced to become more secretive. See Chesterman, supra note 36, at 1122 (observing that the International Criminal Tribunal for the former Yugoslavia, for example, created a national security exemption to its obligation “to produce documents and information”).

90. Walter Laqueur, The Uses and Limits of Intelligence 209 (1993) (stating that it is not “readily obvious why, many years after the event, intelligence files should remain closed. Some suspect that this has less to do with the defense of the realm than with the wish to cover up past mistakes.”); Roberts, supra note 39, at 353–54 (noting that international information sharing agreements cause the Canadian government to continue to deny requests for access to information provided by other states even where disclosure would not cause harm).

91. Under EU regulations, for example, the member state originator determines declassification; originators may either state a date upon which a document may be declassified or review the classification level every five years. Björn Müller-Wille, Improving the Democratic Accountability of EU Intelligence, 21 Intelligence & Nat’l Security 100, 122 (2006). Nonetheless, because of lack of enforceability, “declassification rests fully on the will of the originator, most notably the Member States’ intelligence communities.” Id.

92. William J. Daugherty, Executive Secrets: Covert Action and the Presidency 29 (2004) (stating that according to the former Director of Central Intelligence, “[i]n no other country—including the parliamentary democracies of Western Europe—has intelligence been subject to so much investigation and review by the legislative branch as it has in the United States”).

Central to the absence of democratic oversight and control is the fact that most intelligence agencies, even in Western democratic states, operate either under ambiguous statutes or without any statutory authorization. In Britain, the United States, and Canada, at least one particular intelligence agency has operated (or continues to operate) without any statutory authority or limitations. This represents a near total absence of accountability, the very concept of which “presuppose[s] norms of legitimacy that establish, not only the standards by which the use of power can be judged, but also who is authorized to wield power and who is properly entitled to call the power-wielders to account.”

The absence of limits set by a democratic body poses a serious danger given intelligence agencies’ coercive power and capacity for deception.

Where legal restraints do exist, they impose limits almost exclusively on domestic activity. These include requirements that foreign and domestic intelligence be separated, residents’ and citizens’ information not be intercepted, and, as applies to intelligence networks, residents’ and citizens’ data be shared only in accordance with domestic data protections. Even in democracies, however, there are generally no statutory permissions or limitations on intelligence work outside national borders or intelligence relations to foreign counterparts. From a practical standpoint, this indicates a lack of legislative involvement in setting the proper powers and limits of intelligence. It also confounds democratic accountability because there are no clear standards of what an agency is permitted to do, with whom it may form connections, and under what circumstances intelligence sharing or other operations are authorized.

Similarly, to the extent they do oversee intelligence agencies, national systems by and large fail to address the transnational relationships and activities of their intelligence agencies. Traditional democratic mechanisms used to attain information and impose sanctions—namely, oversight, legal/judicial constraints, and publicity from the media, NGOs, and citizens—pay little attention to transnational intelligence cooperation. For example, it was only after the European Parliament expressed Resolution on ECHELON.

94. See Turner, supra note 41, at 32 (noting that the existence of the National Reconnaissance Office was only revealed in 1994); Stuart Farson, Canada’s Long Road from Model Law to Effective Political Oversight of Security and Intelligence, in WHO’S WATCHING THE SPIES? ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY 99, 101 (Hans Born et al. eds., 2005) (noting that the CSE’s existence was only acknowledged in the mid-1970s); Birkinshaw, supra note 69, at 50 (noting history of lack of statutory authority for U.K. intelligence).

95. Grant & Keohane, supra note 59, at 30.

96. Birkinshaw, supra note 69, at 50 (“It could be argued that, from a constitutional point of view, one of the most glaring omissions is the absence of a precise statutory code covering the powers of the services.”); Müller-Wille, supra note 91, at 103 (“It is crucial that laws regulating the services’ activities are credible and adequate, i.e. that they allow agencies to do what is required to safeguard the democratic system and the people. For the sake of checks and balances, these special powers must be regulated by law and not simply by governmental decrees.”).

97. As Stansfield Turner, former Director of Central Intelligence, observed, “the laws and rules apply mostly to interference with Americans and hence do not greatly affect most foreign intelligence espionage operations.” Stansfield Turner, Secrecy and Democracy: The CIA in Transition 152 (1985).


99. Currently, we depend on the media, NGOs, and social networks to reveal abuses and activities of our own intelligence agencies. Ronald J. Deibert, Deep Probe: The Evolution of Network Intelligence, 18
concern over the ECHELON system that the democratic bodies in the UKUSA countries showed any interest in transnational intelligence agreements. The U.S. investigation into the arrangement only began after illegal interceptions of citizens’ communications were alleged.\(^{100}\)

Apathetic oversight bodies combined with few statutory restraints make intelligence networks and their activities outside the domestic sphere the area of weakest oversight and thus accountability.\(^{101}\) As we will see, the failure to take transnational relationships into account can render statutes limiting intelligence activity in the domestic sphere practically toothless as well.

The transnational aspect of intelligence work can also stymie national efforts at regulation and oversight. Oversight bodies are often specifically excluded from receiving information exchanged through networks—depriving them of the potential to review the use of network arrangements.\(^{102}\) The Arar Commission, a Canadian public inquiry into the extraordinary rendition of Syrian-born Canadian citizen Maher Arar to Syria, is a case in point.\(^{103}\) Without the cooperation of Canada’s intelligence partners, the findings were inevitably incomplete and the appropriate officials and agencies could not be held accountable for wrongdoing. A Dutch government inquiry into intelligence failures at Srebrenica faced similar obstacles to uncovering the role of allied intelligence.\(^{104}\) Likewise, although the U.S. House Permanent Select Committee on Intelligence investigated, requested documents, and held hearings on ECHELON, they were denied information due to its transnational nature.\(^{105}\)


\(^{101}\) Müller-Wille, \textit{supra} note 91, at 107.

\(^{102}\) Birkinshaw, \textit{supra} note 69, at 42–43 (noting the director of the GCHQ can refuse to disclose information to the UK Parliamentary Committee on Security and Intelligence with oversight over GCHQ because it was “provided by, or by an agency of, the government of a territory outside the UK”).

\(^{103}\) Maherarar.ca Home Page, http://www.maherarar.ca/ (last visited April 21, 2010).

\(^{104}\) Aldrich, \textit{supra} note 2, at 53.

\(^{105}\) Sloan, \textit{supra} note 52, at 1487.
Because secret written agreements, informal understandings, and professional standards govern network exchanges of intelligence instead of legislation, the judiciary is also almost completely excluded from regulating an intelligence agency’s foreign activities and contacts with foreign counterparts. Although domestic courts rarely visit the issue of intelligence shared through networks, when legal issues implicit in sharing arrangements have arisen, international obligations to network partners have typically trumpped judicial scrutiny and the rights of criminal defendants.\textsuperscript{106} For instance, in the U.K. trial of the IRA’s Nicholas Mullen, intelligence officers withheld information about his allegedly illegal deportation by Zimbabwean intelligence agents from the court and government officials.\textsuperscript{107} Most recently, however, in a decision that may indicate courts’ reassertion of their role in overseeing intelligence, the British Court of Appeals rejected the British government’s argument that release of information regarding the torture of a former Guantanamo prisoner should be kept secret out of concern for its intelligence sharing relationship with the CIA.\textsuperscript{108} As a general matter, however, the result of information sharing arrangements 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.”\textsuperscript{109}

B. Collusion to Avoid Democratically Determined Policies and Statutes

In practice, a unique danger of intelligence networks lies in their tendency to encourage intelligence agencies to collaborate with one another to the detriment of the interests of the democratic nations they are meant to serve. Because of the corporatism agencies exhibit through networks, “the closeness of the practitioners to each other may be greater than to the precise policy objectives and interests of the organizations or states to which they formally belong.”\textsuperscript{110} This is especially likely to occur among tight-knit intelligence services. In the UKUSA intelligence community, “elements of [the community] frequently come to perceive their ultimate loyalties as lying more with the UKUSA community than with their own governments.”\textsuperscript{111} For example, Australian army officers working with the CIA during the Vietnam War were prepared to swear not to divulge details about their joint activities to their own commanding officers and government.\textsuperscript{112} The closeness of ties has sometimes been used counter to the policies of the agencies own governments.\textsuperscript{113} For instance,

\begin{itemize}
\item 106. Martin Rudner, \textit{Canada’s Communications Security Establishment from Cold War to Globalization, in SECRETS OF SIGNALS INTELLIGENCE DURING THE COLD WAR AND BEYOND} 97, 123–24 (Matthew M. Aid & Cees Wiebes eds., 2001) [hereinafter Rudner, \textit{Canada’s Communications Security Establishment}] (“The legal issues implicit in Sigint-derived evidence have never been tested before Canada’s courts. Whenever questions have been raised, mere reference to Canada’s ‘international’ obligations has sufficed to defer detailed inquiries.”).
\item 107. DORRI, \textit{supra} note 71, at 768.
\item 109. Roberts, \textit{supra} note 39, at 355.
\item 110. GILL, \textit{supra} note 2, at 37. \textit{See also} Philip B. Heymann, \textit{International Cooperation in Dealing with Terrorism: A Review of Law and Recent Practice}, 6 AM. U. J. INT’L L. & POL’Y 1, 2 (1990) (“[I]nstitutional constituencies such as law enforcement officials may find that their interests resemble those of their foreign counterparts more than those of other groups within their own country.”).
\item 111. RICHELSON & BALL, \textit{supra} note 12, at 305.
\item 112. \textit{Id}.
\item 113. \textit{Id}.
\end{itemize}
intelligence professionals in various countries were aware of or suspected each other’s knowledge of weapons-smuggling rings operating out of Pakistan to supply weapons to countries including Libya and North Korea, yet they kept this information from the populations that they purported to protect.\footnote{114}

Network partners have also colluded to avoid statutory restraints on domestic activity. Statutes prohibiting eavesdropping on citizens or residents without a warrant, or creating a barrier between intelligence and law enforcement, have been circumvented. The German BND, for instance, reportedly uses the European Counter-Terrorist Intelligence Center in Paris (where agents from Britain, France, Germany, Canada, Australia, and the United States work together against terrorism) to read information from German law enforcement agencies it would be barred from obtaining at home as a matter of domestic law.\footnote{115} In Norway, the CIA was given permission to penetrate Muslim groups and investigate individuals on Norwegian soil without normal review and accountability procedures in place and “with little, if any, control on the part of Norwegian authorities.”\footnote{116}

Numerous revelations involving the UKUSA arrangement disclose the potential for circumventing statutory and constitutional law. Within ECHELON, the partner agencies all submit a list of keywords; every partner station in the world then collects telephone, fax, email, and other electronic communications (and, it is suspected, internet traffic) in which the keywords appear and then sends them to the requesting agency.\footnote{117} Likely as part of this program, at least three of the major telephone lines in Great Britain, each capable of carrying 100,000 calls, are wired through the NSA listening station, allowing direct taps into British Telecom’s network.\footnote{118} The result is that the collecting agency does not necessarily know what its stations are collecting.\footnote{119}

Reports suggest that UKUSA agencies also purposely use ECHELON to exchange surveillance information on each others’ citizens in violation of domestic statutes.\footnote{120} NSA employees have provided details of the use of the network to

\begin{itemize}
    \item \footnote{114} Ron Suskind, The One Percent Doctrine:  Deep Inside America’s Pursuit of Its Enemies since 9/11 269 (2006) (“In the interplay between decisions made by the intelligence professionals and a small circle of policy makers—and the competing claims made by other branches of government or by the public, with its recognized right to understand what truly guides U.S. foreign policy—almost all the options reside with the parties of the first part.”).
    \item \footnote{115} Dana Priest, Help from France Key in Covert Operations:  Paris’s ‘Alliance Base’ Targets Terrorists, WASH. POST, July 3, 2005, A1; European Parliament Resolution on ECHELON, supra note 95, para. 3 (“Whereas the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries’ intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter . . . .”). Privacy protections also risk being violated. See generally Francesca Bignami, Towards a Right to Privacy in Transnational Intelligence Networks, 28 MICH. J. INT’L L. 663 (2007) (stating that privacy “is one of the most critical liberal rights to come under pressure from transnational intelligence gathering”).
    \item \footnote{116} Rudner, Hunters and Gatherers, supra note 10, at 215.
    \item \footnote{117} Hager, supra note 52, at 29; Sloan, supra note 52, at 1476–78 (listing various types of methods and communications intercepted through the ECHELON system); Rudner, Britain Betwixt and Between, supra note 12, at 581–82.
    \item \footnote{118} Lawner, supra note 11, at 453.
    \item \footnote{119} Hager, supra note 52, at 29 (“This means that the New Zealand stations are used by the overseas agencies for their automatic collecting—while New Zealand does not even know what is being intercepted from the New Zealand sites for the allies.”).
    \item \footnote{120} Seth F. Kreimer, Watching the Watchers:  Surveillance, Transparency, and Political Freedom in
intercept politicians’ telephone calls.\textsuperscript{121} CSE also monitored communications of U.K. Prime Minister Margaret Thatcher’s cabinet members on behalf of the GCHQ.\textsuperscript{122} Several GCHQ officials similarly revealed that partners were targeting and distributing information regarding peaceful political groups.\textsuperscript{123} More recently, at a meeting of the UKUSA intelligence heads, U.S. Director of Central Intelligence George Tenet described statutes against eavesdropping as “among the ‘shackles’ that would, at the very least, be loosened, if not in practice discarded.”\textsuperscript{124} He suggested, as Suskind describes, that “[a] country may not be able to tap the lines of its own citizens without legal authorization. But there’s nothing to stop it from listening in on some other country’s citizen, and then filing very thorough reports to that foreign citizen’s government. Just as long as the report does not hand over the specific raw matter—the SIGINT dispatch of nouns and verbs—the letter of various privacy laws would stay intact.”\textsuperscript{125}

Where there is peer accountability, rather than outside oversight, as these examples demonstrate, network norms will check the power of network partners only “insofar as abuses are against the interests or principles of the other entities within the transgovernmental networks.”\textsuperscript{126} Consequently, there is a danger that congruence of goals and close cooperation within intelligence networks will lead to “collusion against the interests of outsiders” rather than improved professional norms.\textsuperscript{127} The next section will examine several such instances.

\textbf{C. Undermining Foreign Policy and Human Rights through Connections to Illiberal Agencies}

Just as intelligence cooperation imperils legal safeguards, so too does it run the risk of intelligence services working with each other against the interests of their domestic publics. In particular, cooperation with intelligence agencies in regimes that have little in common with liberal democracies threatens the promotion of democracy and human rights. As Section 1 argues, information exchange with authoritarian regimes comes with a price. A quid pro quo is expected (and has been provided) by professionalized intelligence services and democratic nations. As Section 2 demonstrates, less-reputable agencies have profited from their inclusion in


121. \textit{See}, e.g., Sloan, supra note 52, at 1485–86 (discussing the claim by an NSA contract employee “to have witnessed firsthand the real-time interception of a telephone call made by United States Senator Strom Thurmond”).

122. Rudner, \textit{Canada’s Communications Security Establishment: From Cold War to Globalisation} 15 (Ottawa: Norman Paterson Sch. of Int’l Affairs, Carleton Univ., Occasional Paper No. 22, 2000) (noting that due to the political sensitivity, GCHQ could not be directly involved, so CSE intercepted the communications at the Canadian High Commission in London and delivered the information to the GCHQ).


124. SUSKIND, supra note 114, at 85.

125. \textit{Id}.

126. Grant & Keohane, supra note 59, at 39.

127. \textit{Id}.; Herman, supra note 3, at 351 (confirming that since 9/11, the balance has tipped against ethical restraints, and commenting that “[i]f the wartime metaphor fits counter-terrorism, it implies relatively few moral restrictions on information gathering on its targets.”).
intelligence sharing networks to crack down on dissenters, demand concessions from the West, and continue systematic torture and indefinite detention. While admitting that these partners engage in rights violations, numerous commentators suggest that no one is harmed by the exchange of information. Section 3 aims to challenge this assumption. The problem is not simply illiberal regimes engaging in violations of individual rights, but also liberal democracies encouraging and soliciting violations for which they are not held accountable.

1. Quid Pro Quo: Intelligence at What Price?

Partner services in illiberal regimes do not offer intelligence out of altruistic motives; like any other intelligence partner, they want something in return. Most commonly, less reputable agencies demand repayment in kind. Russian intelligence warned the United States that information sharing could not be “one-way traffic.” The desirability of sharing with authoritarian regimes, however, depends on the type of information requested. It is one thing for Canadian intelligence to supply “an assessment on the potential for terrorists to use the avian flu virus as a biological weapon with the Libyan, Saudi Arabian and Egyptian intelligence services.” It is quite another to provide intelligence on individual Chechens to Russian intelligence.

Illiberal agencies may also demand that intelligence services in liberal democracies spy on émigré or dissident groups on their behalf. South Africa, for example, was tipped off to the activities of the African National Congress and the location of Nelson Mandela by intelligence services in Western democracies whose publics opposed apartheid. In return for providing the CIA with information on Libyan nationals with ties to international terrorists, Libyan intelligence was allowed to interrogate prisoners at Guantanamo Bay about exiles in London. The FBI also arrested and interrogated one of Qadaffi’s primary opponents and long-time critic of al Qaeda based on information provided by Libya. Unsavory agencies have come to expect such cooperation; British intelligence faced complaints from Egyptian and Jordanian intelligence for failing to act on their requests for information on émigré communities.

128. Peter Gill, Securing the Globe: Intelligence and the Post-9/11 Shift from ‘Liddism’ to ‘Drainism,’ 19 INTELLIGENCE & NAT’L SECURITY 467, 477 (2004) (“Transnational information exchange is one thing, brokering the use of torture is another.”); Herman, supra note 3, at 342 (observing that some say that “[i]intelligence is information and information gathering, not doing things to people; no-one gets hurt by it, at least not directly”).


131. HOLT, supra note 75, at 72 (contrasting this intelligence exchange with “intelligence on Soviet submarine and other ship movements around the Cape of Good Hope in exchange for information on Soviet and Cuban activities in Angola”). Cooperation with apartheid South Africa posed a dilemma for Western intelligence, whose governments officially opposed apartheid. MICHAEL HERMAN, INTELLIGENCE SERVICES IN THE INFORMATION AGE: THEORY AND PRACTICE 40 (2001).


133. Id., at 10.

134. Rudner, Hunters and Gatherers, supra note 10, at 214. Jamie Wilson et al., New Brothers in Arms—and Cash and Intelligence, GUARDIAN (U.K.), Oct. 20, 2001, at 7 (“Britain’s contribution is expected to include the granting of Russian demands that a hard line be taken against Chechen exiles in
A partner agency may also expect Western intelligence to turn a blind eye to its activities in their territory. For instance, out of fear of jeopardizing relations with Iranian intelligence under the Shah, the U.S. intelligence community tolerated operations against Iranian dissidents in the United States.\(^{135}\) Iran later used the information gained from these operations to take reprisals against dissidents’ families in Iran.\(^{136}\) Chinese intelligence cooperation has reportedly generated German intelligence support for surveillance of the Chinese democratic opposition abroad.\(^{137}\) Through these arrangements, intelligence services in liberal democracies help silence domestic and international dissent against authoritarian governments.\(^{138}\)

Another preferred method of compensating network partners is to provide them with funds and equipment. This may seem ethically neutral but often serves to prop up authoritarian regimes and subvert democracy. For example, equipment provided by the German BND was used by: the Indonesian military intelligence service to overthrow President Sukarno; Ugandan dictator Idi Amin to eavesdrop on opponents; a guerrilla organization to destabilize the legal Mozambique government; and, more recently, Chinese intelligence to monitor the movements of journalists and dissidents.\(^{139}\) Similarly, British intelligence officials report that, in return for information on terrorist groups, states like Malaysia receive surveillance equipment they can use against dissidents in their own territory.\(^{140}\) Just a month after 9/11, intelligence partners, like Egypt and Oman, received arms from the United States for their cooperation.\(^ {141}\) The United States has also built counterterrorist intelligence centers for numerous foreign agencies, hoping to gain valuable intelligence from agencies the CIA’s former Deputy Director for Operations described as “utterly unhesitant in what they will do to get captives to talk.”\(^{142}\)

2. Silencing Criticism and Bolstering Authoritarian Regimes

When their intelligence agents aid antidemocratic and human-rights abusive practices of friendly dictators in hopes of good intelligence, liberal democracies sacrifice their leverage to promote rights and damage their reputations at significant political cost.\(^{143}\)

Criticism of repressive governments with cooperative intelligence agencies has dramatically declined. In the past the U.S. condemned Malaysia’s detention of dissidents under the Internal Security Act; today Malaysia is hailed as a “beacon of stability” and the detentions have been praised.\(^{144}\) Other liberal democracies have similarly reduced public criticism.\(^{145}\)

---

\(^{135}\) HOLT, supra note 75, at 129.
\(^{136}\) Id.
\(^{137}\) Schmidt-Eenboom, supra note 74, at 158.
\(^{138}\) HOLT, supra note 75, at 127.
\(^{139}\) Schmidt-Eenboom, supra note 74, at 154–59 (listing more examples).
\(^{140}\) Wilson et al., supra note 134, at 7.
\(^{141}\) Id.
\(^{142}\) SUSKIND, supra note 114, at 87.
As a result, in many countries, progress in improving human rights practices, especially those of security services, has been reversed. For example, in Morocco, a key U.S. intelligence ally, security services resumed indefinite detention of suspects in secret interrogation centers, and the government enacted a broad anti-terrorism bill in which covers almost any violent crime.\footnote{Carol Migdalovitz, \textit{Constitution Research Serv., RS 21579, Morocco: Current Issues} (2005), available at http://www.policyarchive.org/handle/10207/bitstreams/3768.pdf} By labeling dissidents or rebels as “terrorists,” authoritarian states now legitimize repressive practices and shield these practices from criticism by their partners.\footnote{Rudner, \textit{Hunters and Gatherers}, supra note 10, at 217}

Counterterrorism intelligence sharing with the West actively bolsters the power of authoritarian dictators and their ruthless intelligence services. Due to the cooperation of the brutal Uzbek security services, U.S. policymakers refer to Uzbek President Islam Karimov as a partner and ally, strengthening his hand.\footnote{Thomas Carothers, \textit{Promoting Democracy and Fighting Terror}, 82 FOREIGN AFFAIRS 84, 86 (2003).} Indeed, one of the reasons that we may now know so much more about the illiberal agencies involved in information sharing is that certain foreign services disclose their ties to Western intelligence agencies as a way of demonstrating their strength and shoring up their position domestically.\footnote{Holt, \textit{supra} note 75, at 71. The practice of disclosing ties seems to have increased after September 11.} Two instances of it was Libya’s Qadaffi and Syria’s Assad, for example, who revealed their agencies’ intelligence sharing with the West.\footnote{Gawdat Bahgat, \textit{Transatlantic Cooperation: Libya’s Diplomatic Transformation}, 29 FLETCHER F. WORLD AFF. 43, 47 (2005); Rudner, \textit{Hunters and Gatherers}, supra note 10, at 217. Sudanese intelligence officers brag that “American intelligence considers us to be a friend” and “[t]he information we have provided has been very useful to the United States.” Silverstein, \textit{supra} note 132, at A1.}
Political favors that fly in the face of human rights policies of liberal democracies have also been doled out. In the past, the U.S. rejected Sudan’s overtures, refusing to cooperate with its intelligence service in fear it would legitimize the repressive government. Yet, days after CIA officials and Sudan’s deputy intelligence chief concluded a secret intelligence sharing arrangement, the U.S. abstained on a vote at the United Nations Security Council, freeing Sudan from international sanctions. Due to ties with Western intelligence services, Pakistan also succeeded in lifting U.S. prohibitions on arms sales.

3. Complicity of Liberal Democracies in Rights Violations

Liberal states and their authoritarian partners are subject to various international and domestic legal obligations that constrain the scope of action against individuals. Citizens in many liberal democracies see themselves as devoted to human rights and have enshrined protections against torture and other fundamental rights violations into national law. Although it is expected that intelligence agencies violate the domestic laws of other states in their collection activities, they are not authorized to circumvent these international and domestic restraints.

Yet, as has become apparent since 9/11, intelligence agencies from liberal democracies sometimes intentionally solicit torture or coercive action from illiberal partners. At others, they innocently ask for help within the normal course of investigations, but may be reckless as to the consequences of their requests. Always, however, connections to illiberal regimes will raise the specter of complicity in or encouragement of the violation of individual rights.

In their hunt for terrorist operatives, Western intelligence has depended on counterparts in countries around the world to conduct interrogations and report information gleaned. Western intelligence agencies provide lists of questions and

152. Id.
154. E.U. NETWORK OF INDEPENDENT EXPERTS IN FUNDAMENTAL RIGHTS, THE BALANCE BETWEEN FREEDOM AND SECURITY IN THE RESPONSE BY THE EUROPEAN UNION AND ITS MEMBER STATES TO THE TERRORIST THREATS 20 (Mar. 31, 2003), available at http://www.humanrights-observatory.net/dhangles/tematic2.pdf (“It is important to keep in mind that the Member States of the European Union, which are party to the European Convention of Human Rights, are bound to comply with that instrument, including in the context of interstate cooperation that they choose to enact with nonmember States.”). As a matter of international law, a state that solicits or assists in a human rights violation is responsible for it. Report to the International Law Commission to the General Assembly, 56 U.N. GAOR Supp. (No. 10) at 64, U.N. Doc. A/56/10 (2001), reprinted in [2001] 2 Y.B. Int’l L. Comm’n 31, U.N. Doc. AA/CN.4/SER.A/2001/Add.1 (Part 2). (“[I]nternationally wrongful conduct often results from the collaboration of several States rather than of one State acting alone.”). See also id. at 66 (“An aiding or assisting State may not deliberately procure the breach by another State of an obligation by which both States are bound; a State cannot do by another what it cannot do by itself.”).
155. See HUMAN RIGHTS WATCH, REPORT TO THE CAN. COMM’N OF INQUIRY INTO THE ACTIONS OF CANADIAN OFFICIALS IN RELATION TO MAHER ARAR 7 (May 17, 2005) [hereinafter HUMAN RIGHTS WATCH] (“If we are getting everything we need from the host government, then there’s no need for us to [conduct interrogations],” a former U.S. government official told Human Rights Watch. “There are some situations in which the host government can be more effective at getting information.”). See, e.g., INT’L CAMPAIGN AGAINST MASS SURVEILLANCE, supra note 144, at 47 (noting the CIA station chief in Tashkent “readily acknowledged torture was deployed [in Uzbekistan] in obtaining intelligence [from U.S. suspects]”).
accept answers that are almost certainly coerced from the suspects, while knowing that many of these agencies engage in acts of torture. Involvement is not limited to U.S. intelligence services, but rather includes a wide variety of intelligence agencies from democratic states.\footnote{156. See, e.g., Rudner, Hunters and Gatherers, supra note 10, at 219 (observing that Australia and Southeast Asian partners submitted lists of questions to be put to terrorist suspect Hambali). Canadian intelligence has also implicated individuals and sent questions to foreign counterparts. For example, Maher Arar’s brother-in-law was questioned by the Tunisian police after moving there from Canada, based on information to which only Canadian agents would have had access. In a similar incident, “Kassim Mohamed, who divides his time between Toronto and Egypt, was questioned by CSIS in Canada after videotaping Toronto landmarks . . . . When he arrived in Egypt, he was arrested and held for two weeks, handcuffed and blindfolded, in a prison in Cairo.” INT’L CAMPAIGN AGAINST MASS SURVEILLANCE, supra note 144, at 26. See also Philip B. Heymann, Civil Liberties and Human Rights in the Aftermath of September 11, 25 HARV. J.L. & PUB. POL’Y 441, 455 (2001) (noting that many abuses occur in cases “in which the CIA will know of the capture of individuals and may make known to the international security apparatus of a foreign nation exactly what it would like to know”).}

In the most egregious cases, Western services have exploited the lack of accountability and rights protection in partner nations to circumvent human rights law and violate individual rights. The case of Maher Arar provides a well-known example. Arar is a Canadian citizen entirely innocent of wrongdoing who was detained at a U.S. airport, sent to Syria, and interrogated and tortured by Syrian Military Intelligence (SMI).\footnote{157. Id. at 38} Despite knowing that the SMI, an agency notorious for its torture practices, had custody of a Canadian citizen, the Royal Canadian Mounted Police (RCMP) offered “large volumes of highly sensitive documents and information, seized during investigative efforts or obtained from confidential informants associated to terrorist cells operating in Canada.”\footnote{158. Id.} The RCMP also sent questions for Arar and other detainees in Syria against advice that the SMI would likely use torture to seek answers and would consider the questions proof that the individuals were in fact terrorists.\footnote{159. Id. at 56–57.} Arar was indeed tortured—beaten and kept alone in an unlit cell the size of a grave.\footnote{160. Id. at 56.} A proper appreciation of the SMI’s practices and lack of professionalism should have suggested that answers obtained from these interrogations would be untrustworthy. The SMI, for example, found Arar’s salary and job description unbelievable.\footnote{161. Id. at 56.}

In another instance, the U.K. security service MI5 solicited abuse from its network partners in Africa. When several of acquaintances of cleric Abu Qatada traveled to the Gambia, MI5 cabled a “foreign intelligence agency,” labeling them “Islamic extremists” and disclosing their destination.\footnote{162. Craig Whitlock, Courted as Spies, Held as Combatants: British Residents Enlisted by MI5 After Sept. 11 Languish at Guantanamo, WASH. POST, Apr. 2, 2006, at A1. See also HUMAN RIGHTS WATCH, CRUEL BRITANNIA: BRITISH COMPlicity IN THE Torture AND ILL-TREATMENT OF TERROR Suspects IN Pakistan 1–7 (2009), available at http://www.hrw.org/en/reports/2009/11/24/cruel-britannia-0 (investigating U.K. complicity in torture in Pakistan and concluding that it is inconceivable that security services were not aware their partners were engaging in torture of detainees about whom they were providing questions and receiving information).} Upon arrival, CIA and Gambian intelligence agents were waiting. When one of them, a British citizen,
asked to meet with the British consul, an American agent replied, “Who do you think asked us to arrest you? Where do you think this information came from, the questions we are asking you?” All were detained for over a month. The two non-British citizens were subsequently sent to Guantanamo Bay and remain there (MI5 has paid them several visits). Because it only shared information, the United Kingdom denies responsibility because it did not specifically request that the individuals be detained.

Even where a Western agency attempts to mitigate rather than capitalize on the tactics of disreputable or brutal agencies, the possibility of torture, disappearance, or detention remains a serious risk. The tendency of intelligence officers to focus on worst case scenarios increases the likelihood that information, will be acted upon often to the detriment of individual human rights. Repressive countries’ intelligence services are particularly unlikely to exercise restraint when called upon to conduct interrogations on behalf of Western services, especially where allegations of Islamic terrorism are involved. The simple act of providing questions about an individual to a less professional agency can cause it to conclude that the sharing agency considers the individual to be a serious terrorist threat.

The brutal nature of some partners of Western intelligence agencies blurs the line between acceptable and unacceptable requests. For example, in an attempt to confirm reports of the death of al Qaeda leader Zawahiri, a CIA operations manager called an Egyptian intelligence chief for a DNA sample from Zawahiri’s brother, who had been detained in Cairo. The Egyptian officer reportedly responded, “No problem. We’ll get his brother, cut off his arm, and send it over.” Even well-intentioned and necessary requests for intelligence may, therefore, create a “ripple effect” beyond the requesting country’s borders “with consequences that cannot be controlled” by that country. Western intelligence should thus carefully evaluate the risks posed by requesting information from illiberal services, meticulously phrase requests for information, and attempt to ensure treatment of persons in accordance with legal obligations. Unless they do so, requests for information may become, in fact, requests for violation of human rights law.

164. Id.
165. Id. Even if the United Kingdom did not specifically ask for the detention (which seems unlikely), Western agencies provide specific intelligence with the intent that their partners act on it. RONALD KESSLER, THE CIA AT WAR: INSIDE THE SECRET CAMPAIGN AGAINST TERROR 273 (2003) (“By the middle of 2002 the CIA had rolled up three thousand terrorists in a hundred countries. Usually a foreign service made the arrest based on CIA information.”).
166. HOLT, supra note 75, at 86. As a general matter, there are fewer repercussions for acting against individuals or on terrorist information since it generally does not engage geopolitical concerns.
167. See Heymann, supra note 156, at 453–54. (“[P]rotections [available in the United States] are often not available in anything like the same measure in states where terrorists are likely to seek haven. Those countries’ internal structure and police apparatus are likely to be far less constrained if activated by the CIA on behalf of America.”).
169. SUSKIND, supra note 114, at 132.
170. Id.
171. See National Security Background Paper to Arar Commission, supra note 26, at 16 (discussing effect from Canadian perspective).
172. Heymann, supra note 156, at 455.
Western agencies also have subverted human rights and endorsed abuse by receiving information from their new “allies.” The case of Craig Murray, former British ambassador to Uzbekistan, is one example of Western knowledge of abuse. When he urged the British Foreign Office to stop using intelligence elicited from terrorism suspects through torture and other coercive means, he was told that the intelligence could still permissibly be used “even if it was elicited by torture, as long as the mistreatment was not at the hands of British interrogators.”

Using information obtained through torture or indefinite detention is not in the interest of accuracy or effectiveness. Mistreatment typically results in information replete with false positives, on the basis of which innocent persons are then detained and mistreated, continuing the cycle. The cost of receiving information of dubious reliability from illiberal states is paid not only by persons in or sent to repressive countries but also by residents of liberal democracies throughout the world. As the Arar Commission determined, “[r]eceipt of . . . information may lead to significant personal consequences for individuals . . . such as surveillance, further collection of personal information, or interrogation.”

Services in repressive regimes are of questionable reliability because of their use of torture. They are doubly dubious as their chief functions are to lend blind allegiance to the regime and to repress dissidents. They also often have contradictory interests: providing financing and support to some designated terrorist groups, and offering to work against others (or sometimes the same group).

Western services’ apparent credulity has already resulted in numerous errors. A human source identified by the Libyan intelligence head was responsible for allegations that Saddam Hussein provided biological and chemical weapons training to al Qaeda. The Bush administration acted upon it even though the CIA already doubted the source’s veracity. New intelligence sharing arrangements between U.S. intelligence and the Russian security intelligence services (FSB) have also generated unreliable information and rights violations. A naturalized U.S. citizen,

173. Don Van Natta, Jr., U.S. Recruits a Rough Ally to be a Jailer, N.Y. TIMES, May 1, 2005, at A22.
174. Tony Pfaff, U.S. Army, Bungee Jumping Off the Moral Highground: The Ethics of Espionage in the Modern Age, http://www.usafa.edu/isme/JSCOPE02/Pfaff02.html (“It is a well-established fact that information gained under the duress of torture is rarely reliable.”). See also Shane O’Mara, Torturing the Brain: On the Folk Psychology and Folk Neurobiology Motivating ‘Enhanced and Coercive Interrogation Techniques,’ 13 TRENDS IN COGNITIVE SCI. 497, 497–98 (2009) (showing with scientific evidence that coercive intelligence techniques and torture make it less likely for the subject to accurately recall information, and more likely for false memories to replace real ones).
175. National Security Background Paper to Arar Commission, supra note 26, at 17 (“[I]nformation obtained from other countries may not have been acquired in ways consistent with rights and freedoms protected [in Canada]. It may, for example, have been obtained through torture or other unacceptable investigation techniques, or in the absence of checks and balances to ensure reliability.”).
176. See Herman, supra note 5, at 229. Moroccan intelligence, for example, spends a great deal of its resources on extensive surveillance of “three particular classes of foreigners: US citizens (for their ‘own safety,’) Spaniards, and journalists, the latter two to ensure they were engaging in approved activities.”
178. See SUSKIND, supra note 114, at 187–88 (discussing the CIA’s concerns over intelligence on WMDs in Iraq). This is not a new experience for the CIA and Mossad, which together created the Iranian intelligence agency and the Korean Central Intelligence Agency (known for their “heavy-handed brutality and torture”) and received much “intelligence of dubious validity” from both. HOLT, supra note 75, at 71.
Omar Shishani was accused of having links to terrorism, based on information provided by the FSB.\textsuperscript{179} The FSB and witnesses it supplied identified Shishani as an Islamic radical who introduced Wahhabism to Chechnya in the 1990s. In the end, this information was revealed to be inaccurate—a case of false identity.\textsuperscript{180} Yet, U.S. intelligence appeared willing to accept this information unconditionally.

In the end, it is clear that the sort of compliance enforced through professional network sanctioning does not necessarily produce strong compliance or good behavior on the part of intelligence services. A real risk is the proliferation of lower, rather than higher, standards. Because acculturation relies on the pull of peer pressure rather than the legitimacy of the norm, it is value-neutral as to the norms transmitted through the network. Thus, “actors systematically conform (under the right conditions) even if the group is clearly wrong . . . .”\textsuperscript{181} In the case of transnational intelligence sharing networks, the norms have both been positive—good investigative tactics—and negative—most recently, torture and indefinite detention.\textsuperscript{182} Though professionalized intelligence services may generally be relied upon to achieve high standards, greater cooperation with intelligence agencies of dubious virtue has strained the professional ethos.\textsuperscript{183}

### III. A PROPOSAL FOR MORE PROFESSIONAL, DEMOCRATIC INTELLIGENCE EXCHANGE

While the days immediately after 9/11 may not have permitted reflection on the proper safeguards for efficacious, humane arrests and interrogations, the problems that have emerged from recent intelligence cooperation call for their institution.\textsuperscript{184} This section proposes two mutually enforcing methods to reduce human rights abuses and poor intelligence, support policies in favor of democracy and rights, and reassert democratic control over intelligence activities. This section offers hope that the combination of internal controls and democratic rules can allay some of the excesses and irrationalities that arise from the participation of democratic states in intelligence networks that often include repressive states.


\textsuperscript{180} Id.

\textsuperscript{181} GOODMAN & JINKS, supra note 60, at 8. Another danger, which Jinks and Goodman consider an identifying characteristic of acculturation, is “decoupling” which involves adoption of structural commitments that do not correspond to local practices such that true human rights compliance does not occur. \textit{Id.} at 33–34. For example, Uzbekistan, a U.S. partner in the “war on terror,” now understands that other states attach importance to human rights and accountability and has enacted legislation and brought prosecutions against police for torture; yet, no conviction based on coerced confessions has been overturned. Jones et al., \textit{supra} note 68, at 78.

\textsuperscript{182} Another example of negative norm transmission is the pressure exerted through a “strong lobby of the foreign intelligence functionaries, who in order to maintain their influence successfully pressured to maintain a post-Soviet model of the secret services in Poland,” despite significant concern that such services were persistent rights violators and extremely politicized. Andrezej Zybertowicz, \textit{An Unresolved Game: The Role of the Intelligence Services in the Nascent Polish Democracy}, in \textit{WHO’S WATCHING THE SPIES? ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY} 145, 147 (Hans Bora et al. eds., 2005).

\textsuperscript{183} This is confirmed by the network literature, which suggests that smaller or more-cohesive networks exhibit a higher degree of internalization of and compliance with network standards. \textit{See, e.g.}, Slaughter, \textit{supra} note 22, at 359.

First, regulation internal to intelligence networks must be strengthened, as Section A argues. Agencies purporting to represent the interests of democratic governments should ascribe to more stringent and ethical professional norms for the sake of accuracy, human dignity, and overall efficacy. They must use the reputational sanctioning of network relations to acculturate repressive partners to more ethical rules of the game. While there is substantial room for improvement of intelligence’s democratic accountability, a number of networked intelligence services, especially in the global counterterrorism effort, are not held to account in any way. All intelligence agencies are, however, subject to reputational sanctioning from their fellow professionals. Professional standards within the network, therefore, offer the most promising basis for accountability.

Second, efforts internal to intelligence networks must be supplemented by greater public and legislative involvement. Section B argues that the protection of democratic governance and mitigation of intelligence excesses requires oversight, accountability, and some measure of transparency. As they currently exist, traditional means of accountability systematically fail to provide any of these. Legislative oversight and public involvement are imperative to set proper limitations and permissions on our intelligence services. Greater transparency in turn will facilitate democracy and rule of law. Ultimately, as Section C contends, problems related to the accountability and accuracy of intelligence may be best solved by prioritizing law enforcement.

A. Acculturation of Intelligence Agencies to Ethical Professional Norms

If the experience of the last nine years is any indication, existing professional standards in network arrangements are inadequate to ensure that intelligence services act both in the most effective way and in the best interests of democracy. Connections to untrustworthy, unreliable intelligence partners create a substantial risk of bad foreign policy decisions, false positives, and subversion of democracy. This section proposes ways to mitigate some of these problems. Section 1 argues in favor of clear ethical professional standards to advance reliable intelligence sharing and human rights compliance. Section 2 contends that the most effective way to institute compliance with such standards is through acculturation within the network—that is, communitarian pressure on illiberal agencies to adopt more professional, rights-respective behavior. Official training and aid, the “quid pro quo” delivered by Western intelligence, must also support these efforts and the wider foreign policy goals of democratic states. Ultimately, however, Western intelligence may need to establish limits and cut or minimize ties to certain partners.

1. New Rules for Intelligence Cooperation

It is vital that information exchanged be precise and accurate and that the means used to collect it be ethical and minimally intrusive on individual rights. This section proposes clear, ethical professional standards to further information sharing against transnational threats—in both the long and short term.

The first section contends that professional norms must include prohibitions on torture and indefinite or arbitrary detention. The second section proposes professional rules that make caveating information mandatory, rather than
discretionary. The third section argues in favor of use restrictions to ensure that information sent to other states does not foster human rights abuses.

a. Ethical Standards in Compliance with International Human Rights Law

Abuses generate inaccurate information, alienate populations, and impede successful, rights-respecting cooperation. They do not constitute an effective strategy to counter transnational threats. In order to deter rights violations and mitigate their effects, professional intelligence standards should include principles relating to the handling of intelligence and the arrest, detention, and interrogation of suspects. There must be clear norms barring the use of coerced information. This will avert Western complicity in human rights violations and incentivize placing greater pressure on rights-violating partners to comply with proper intelligence gathering techniques.

As a general rule of thumb, intelligence ethics should include principles of justification, proportionality, necessity, and accuracy. All intelligence partners should understand that “individuals will be targeted only when it is justified, authorised and the information gathered will be properly recorded and only retained or made accessible where legitimate need can be established.”\footnote{185} As the 9/11 Commission recommended, the “United States should work with friends to develop mutually agreed-on principles for the detention and humane treatment of captured international terrorists . . . .”\footnote{186} Such norms must bring the principle of harm minimization to the forefront with the result that individual intelligence officials confronting ethical dilemmas recognize them, seek guidance in codes of practice, and ultimately minimize the potential harm to democracy, individuals, and consumers of intelligence.\footnote{187} Like military professionals, who are governed largely by their professional ethical rules, intelligence officials should “take care not to act in such a way that disregards the notion that individual human life and dignity are valuable for their own sake and that people should be treated as an end in themselves and not merely a means.”\footnote{188}

Professional intelligence services should abide by international prohibitions on torture, summary execution, and cruel, inhuman, and degrading treatment. As the Harvard University Project on Justice in Times of Transition has proposed in the Intelligence Bill of Rights, “agencies must conduct their work in a manner consistent with respect for human rights as such standards are defined by international law,” including prohibitions on “[t]orture and other [c]ruel, [i]nhuman or [d]egrading [t]reatment or [p]unishment.”\footnote{189} Agencies should further refrain from “measures

\begin{itemize}
\item \textit{Gill, supra} note 2, at 153.
\item \textit{Gill & Phytyian, supra} note 79, at 155 (“[N]ot just individual security officials are ‘moral agents’; so are the agencies and governments of which they are part, so statutes, guidelines and codes of practice must all be drawn up within the context of ethical agreements . . . . Since intelligence cannot be disinvited, and current practice is dominated by realist ethics, perhaps the most we can strive for is harm minimization . . . .”).
\item \textit{Pfaff, supra} note 174, at 2.
\item Project on Justice in Times of Transition, Harvard University, Safeguarding Human Rights in Relation to Intelligence Activities: An Intelligence Bill of Rights, para. 6 (Nov. 17, 2004) (on file with
designed to interfere with the normal political or judicial processes or with the lawful internal workings of parties and organizations engaged in lawful activity,” such as spying on émigré communities or peaceful protesters.  

A commitment to refrain from exploiting information obtained through coercive tactics should similarly travel in the toolbox of Western intelligence norms. The determination of whether information has requisite reliability and credibility should include an evaluation of whether the information was obtained through torture or cruel, inhuman, or degrading treatment. If coercion has been used, the information should be designated of dubious reliability. As recommended by the Ottawa Principles on Anti-Terrorism and Human Rights, it should not be used as a basis for:

(a) the deprivation of liberty;
(b) the transfer, through any means, of an individual from the custody of one state to another;
(c) the designation of an individual as a person of interest, a security threat or a terrorist or by any other description purporting to link that individual to terrorist activities; or
(d) the deprivation of any other internationally protected human rights.

While this limit would not eliminate rights violations, it would curtail receiving states’ ability to exploit those violations. This is in contrast to the current system under which Western agencies encourage coercive tactics by gladly accepting information gained through them. Over time, limits on use of coerced intelligence might reduce torture by intelligence services. Just as the exclusionary rule serves as a deterrent for the use of coercive tactics in the domestic context, these restrictions would bolster incentives for services to professionalize and train partners to engage in more humane practices.

b. Caveats as a Requirement

Because intelligence is used to inform decision making on vital foreign and domestic issues and may have serious consequences for individuals, it is imperative that agencies institute clear requirements for quality control of shared information. First of all, before information is shared, it ideally should be checked against other available sources.

author) [hereinafter Intelligence Bill of Rights] (proposing basic guidelines for intelligence based on a study of intelligence systems and their regulation).

190. Id. paras. 6–7.


192. This is not a perfect analogy because intelligence agencies use information less often than law enforcement agents. In the context of terrorism intelligence sharing, this rule would be stronger if more criminal prosecutions for violent criminal acts were brought—as they indeed should be. See infra part III.C.

193. New Challenges, supra note 51, para. 6 (“It is vital that intelligence should be reliable, which means sound intelligence that can be cross-checked against different sources. Complementary sources are an operational requirement.”).
information quality." Second, proper caveating on shared intelligence should be required, rather than discretionary. Lacking definitive guidance, agencies engage in “indiscriminate reporting of unverified information, without regard to the information quality, reliability or usefulness, or without considering the receiving agency’s ability to analyze the information”—generating a highly ineffective information sharing environment.

The findings of the inquiry into Arar’s case amply demonstrate the importance of proper caveating to ensure accuracy and minimize the negative repercussions of false positives. According to the inquiry, as part of the RCMP’s terrorism intelligence responsibilities, it provided a great deal of misleading, inaccurate, and piecemeal information to the United States. For example, the RCMP reported that Arar and his wife were “Islamic Extremist individuals suspected of being linked to the Al Qaeda terrorist movement,” had refused to be interviewed, and had connections to known terrorists. Officials systematically failed to attach written caveats that indicated the reliability of the source and relevance to the investigation. This failure to caveat was not an isolated occurrence, but rather a direct consequence of the informal and often implicit nature of understandings and requirements between networked actors. By contract, requiring caveats could protect individuals implicated, prevent unwise foreign policy decisions, and ensure the integrity of intelligence sharing and collection processes.

In all cases, agencies should attach quality and reliability caveats. Each piece of information shared should indicate whether it has been cross-checked and confirmed. Reliability scales, contextual data, and the greatest information possible about the source and method of collection should be indicated along with doubts or conflicting data. Codes for different sources could make information possible to track without exposing sources’ identifying features, and meters of credibility could reduce circular reporting and intelligence agencies “intoxicating each other.” Since intelligence agencies are charged with analyzing the reliability of information as accurately as possible, the requirement that intelligence be caveat should not be overly burdensome.

194. U.S. DEP’T OF JUSTICE, PRIVACY AND INFORMATION QUALITY POLICY DEVELOPMENT FOR THE JUSTICE DECISION MAKER 3 (Sept. 2005) ("Promoting information quality by internal safeguards and procedures helps to ensure the accuracy of the information you handle."). See also MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT 23 (2006), available at www.markle.org/downloadable_assets/2006_nstf_report3.pdf, [hereinafter MARKLE FOUNDATION] ("If users do not believe that the information is reliable and comprehensive . . . they will implement their own collection systems and may keep the information to themselves.").

195. MARKLE FOUNDATION, supra note 194, at 19.


197. Id.

198. Id.

199. MARKLE FOUNDATION, supra note 194, at 30 (arguing there also must be “mechanisms to make any limitations on the reliability or accuracy of data known to those using the information”).

200. Müller-Wille, supra note 91, at 118–119 (“The exposure of intelligence products to a formalized quality control would raise the demand for ‘trackability’ of sources (codes can be used to prevent exposure) and for clarity concerning what facts, assumptions and interpretations different conclusions are based on.”).

201. HERMAN, supra note 9, at 104.
In the interest of accuracy, receiving agencies should only retain properly caveated information that is accurate and complete. Given the number of false positives (and negatives) caused by mistaken identity and misspellings, a receiving agency similarly should take care when combining information from various sources that it all relates to the same individual. At an institutional level, creating a position for quality control might be helpful. Indeed, after the debacle over allegations of weapons of mass destruction in Iraq, British MI6 created the position of senior quality control officer to review and determine the credibility and veracity of gathered intelligence.

In a similar vein, agencies should adopt rules to correct inaccurate information. This would involve a duty to investigate allegedly erroneous information and to implement a process to correct inaccurate or materially unreliable information. Because of the transnational nature of intelligence cooperation, correction of inaccurate information at the domestic level will not suffice. Informing network partners upon the discovery of an error is crucial. In the Arar case, for example, this would have meant Canadian intelligence had a duty to notify both U.S. and Syrian intelligence of the inaccuracy of information they had previously forwarded.

c. Restrictions on the Use of Shared Information

Intelligence agencies should also attach use restrictions to prevent the use of information to facilitate torture, arbitrary detention, or other abuses, as they already do in other contexts. Some Western agencies screen intelligence for relevance and personal information that, as a matter of domestic law, can only be shared in certain circumstances and attach caveats limiting the information’s uses. Several of the

202. U.S. DEP’T OF JUSTICE, PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES: POLICY TEMPLATES FOR JUSTICE INFORMATION SYSTEMS C.3.10(c) (Sept. 2006), available at http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf. See also Ottawa Principles, supra note 191, at 8.2.2 (“All state agencies involved in the collection and storage of personal information must ensure that: (a) data are protected against unauthorized access, use or disclosure; (b) data are only used in connection with the purpose for which they were collected; and (c) data are only held for as long as necessary and are destroyed thereafter.”).


204. MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 315–16 (4th ed. 2009).

205. Close allies may already tend to correct one another and withdraw inaccurate information. See Senate Report on Iraqi National Congress, supra note 46, at 59, 167, 172 (providing examples of a foreign agency withdrawing intelligence previously shared and indicating as an intelligence error the failure to withdraw from circulation information shown to be unreliable).

206. MARKE FOUNDATION, supra note 194, at 30; U.S. DEP’T OF JUSTICE, supra note 202, at C.3.10(e) (“Investigate in a timely manner any alleged errors and correct or delete information found to be erroneous . . . .”); U.S. DEP’T OF JUSTICE, supra note 194, at 7 (proposing as a central principle that agencies “[i]mplement safeguards to ensure information is accurate, complete, and current, and provide methods to correct information discovered to be deficient or erroneous”).

207. U.S. DEP’T OF JUSTICE, supra note 202, at C.4.20 (“When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated . . . .”); Ottawa Principles, supra note 191, at 8.3.3 (“States sharing information have an obligation to correct information once they learn of its unreliability. States agencies and/or private companies involved must be subject to shared, joint and several liability where errors or abuses occur.”).

United States’ Western partners attach use restrictions to law enforcement information, prohibiting the use of shared information to impose the death penalty.209

Although there is a danger that use restrictions could chill intelligence sharing,210 misuse of intelligence and abuses by Western intelligence services is likely to have a similar impact on the willingness of agencies to share intelligence with those services.211 Cruel treatment at the hands of U.S. and other intelligence partners has already prompted some Western intelligence agencies to consider restricting uses of shared information as well. One of the Arar Commission recommendations was that Canada evaluate sharing on a case-by-case basis and carefully limit potential uses of shared information.212 Canadian agencies are now required to consider limiting cooperation with agencies in cases where individuals might be exposed to human rights abuses or torture.213 In other instances, partners have withheld information unless they receive assurances it will not be used for proceedings in military commissions or with relaxed evidentiary standards.214 Still others have considered limiting intelligence support to the United States out of fear that this relationship will make them targets for attack.215

To supplement use restrictions for individual pieces of intelligence, the amendment of MOUs or formal agreements for the sharing of information may be necessary. Such action would not be unprecedented. For example, when Israel used U.S. satellite images to strike Iraq’s Osirak reactor, against American intentions and

209. E.U. NETWORK OF INDEPENDENT EXPERTS IN FUNDAMENTAL RIGHTS, supra note 154, at 19–20 (noting that the first example was the refusal of France to cooperate with the United States in the case of Zacarias Moussaouii until it received commitments that information provided by France would not be used to impose the death sentence); Rudner, Hunters and Gatherers, supra note 10, at 214 (“[A]llies like Britain, France, Germany, and Spain have refused to extradite suspected al-Qaeda terrorists to the United States, where they might face capital punishment.”).

210. Melchers, supra note 99, at 42 (“[S]ubsequent recommendations pertaining to the sharing of investigative information and intelligence with foreign governments may provoke some degree of chill in Canada-U.S. relations, though not unreasonably so.”); Rudner, Canada’s Communications Security Establishment, supra note 106, at 124 (“[F]or Canada (or another partner country) to impose national legal or human rights standards unilaterally onto Sigint interceptions might well jeopardize future UKUSA collaboration against transnational crime and other sensitive targets.”).

211. MARKLE FOUNDATION, supra note 194, at 24.


213. Melchers, supra note 99, at 43. The Canadian Security Intelligence Service has restricted its cooperation with at least one foreign counterpart because of human rights concerns. Rudner, Hunters and Gatherers, supra note 10, at 214.

214. AMERICAN COLLEGE OF TRIAL LAWYERS, REPORT ON MILITARY COMMISSIONS FOR THE TRIAL OF TERRORISTS 22–23 (March 2003) (noting that “France and Germany have announced that they will not disclose information to U.S. law enforcement authorities is that information could be used to convict an alleged terrorist who might then be subject to the death penalty”). See Walsh, supra note 37, at 629–30 (“[C]oncerns about civil and political rights might preclude one state from sharing intelligence with another. Such states might be reluctant to share intelligence in their possession with receivers who have weaker data protection laws or norms.”); James Igoe Walsh, Intelligence-Sharing and United States Counter-Terrorism Policy, in EMERGING TRANSNATIONAL (IN)SECURITY GOVERNANCE: A STATIST-TRANSNATIONALIST APPROACH 44, 47 (Ersel Aydinli ed., 2010) (“Governments have legitimate reasons to surround their intelligence gathering and analysis with considerable security.”).

215. Simon Tisdall, Fighting Terror the Malaysian Way, Not the US Way, GUARDIAN (U.K.), June 8, 2005, at 16 (reporting that Malaysia was focused on not becoming a target and was only cooperating quietly); see also ALFRED B. PRADOS, CONG. RESEARCH SERV., IB 93085, JORDAN: U.S. RELATIONS AND BILATERAL ISSUES 8 (2006), available at http://www.fas.org/sgp/crs/mideast/IB93085.pdf (“Jordan’s cooperative relationship with the United States has made it vulnerable to terrorist attacks, particularly from organizations operating from Iraq.”).
interests, U.S. intelligence amended its agreement with Israeli intelligence so as to limit Israel’s use of U.S. intelligence to defensive purposes only. At the domestic level, several proposals have suggested use caveats or authorized use principles as a way of facilitating information sharing.

Respect for these information sharing standards, which promote accuracy and ethical intelligence behavior, can be developed in two reinforcing ways. First, pressure from well-respected network partners can help acculturate illiberal agencies to professional and rights-respecting norms, as Section 2 will discuss. Second, as Section B will argue, standard setting and oversight through democratic bodies can reinforce network acculturation to ethical intelligence standards and encourage intelligence behavior in the interest of liberal democracies.

2. Professionalization of Illiberal Agencies

To the extent that Western intelligence must cooperate with services in illiberal regimes, it is in the interest of all network partners that illiberal agencies be professionalized and acculturated to professional norms through reputational sanctioning within the networks. Unless the network acculturates less reputable agencies to accept accurate, reliable information gathering skills and safeguards for the humane treatment of suspects, it will be unable to provide consistently useful information—especially in the long-term. Successful transnational cooperation may necessitate maintaining contact with certain repressive regimes, but consistent pressure should be exerted on partners to improve their practices and become more professional.

Professional standards, rather than legislative or other domestic oversight, are the prime mechanism to sanction and professionalize network partners. Therefore, the use of peer accountability and reputational sanctioning to enforce ethical professional norms, including prohibitions on mistreatment, may present the most effective mechanism to professionalize repressive intelligence agencies. Changing the culture of intelligence agencies is without a doubt a difficult task, and “[l]egal and ethical standards have to be taken seriously if they are to become part of the organizational culture, rather than just window dressing.” Effective acculturation to ethical professional standards will require concerted reputational sanctioning and targeted use of intelligence aid and training. If leading intelligence powers set

216. Lefebvre, supra note 4, at 536.
217. U.S. DEP’T OF JUSTICE, supra note 194, at 7 (setting forth a use limitation principle, which would require purpose specification and subsequent use only in conformance with such purposes); MARKLE FOUNDATION, supra note 194, at 35 (proposing an authorized use criterion which must be articulated and recorded prior to sharing).
218. Ian Cameron, Beyond the Nation State: The Influence of the European Court of Human Rights on Intelligence Accountability, in WHO’S WATCHING THE SPIES? ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY 34, 41 (Hans Born et al. eds., 2005) (“It is probably correct to say that a system of internal controls, in particular the maintenance of the democratic sensibilities of the staff themselves, is the most important safeguard against abuse of power.”).
219. Id.
standards through intelligence collaboration, restraint, and objective assessment, other professional norms can spread to less professionalized agencies.\footnote{See Herman, supra note 5, at 238.}

This section recommends using professional sanctioning and transmitting norms through intelligence networks to encourage more effective long-term counterterrorism information sharing and overall strategy. It relies primarily on the theory of acculturation and argues that where hegemons or groups of influential intelligence agencies encourage compliance with certain norms, other intelligence agencies may adopt and comply with them. The idea of communitarian pressure operating within intelligence networks to induce human rights compliance may seem unlikely, but changes may occur, especially where well-respected intelligence agencies target their support and sanction violators collectively and consistently.\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).}

In the past, Western intelligence powers exported their professional standards and methods through networked contacts and transparent foreign aid. As Michael Herman notes, because of the involvement of the U.S. and U.K. in the development of various intelligence agencies worldwide, “[i]ntelligence to some extent has its own international patterns. Different national structures have points in common, with influence and imitation operating on transnational intelligence networks.”\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).} Concepts beyond immediate operational capabilities have long been prominent in Western attempts to acculturate and train foreign partners. Assistance from Britain has focused on “‘training to improve the objectivity of threat analysis, especially on the civilian side of government’ and ‘strengthening the capacity of intelligence services to assess genuine outside threats’” with the understanding that depoliticized, objective intelligence “figures among the attributes of good governance and responsible international citizenship.”\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).} Similarly, after the Cold War, the U.K. and U.S. both focused on building the democratic accountability of intelligence services in Central Europe.\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).}

Such use of intelligence networks suggests the capacity of intelligence contacts to provide a lever for change.\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).} Inclusion in a network can lead to pressure to imitate and identify with the group, which is likely to generate compliance with the group’s norms.\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).} Within intelligence networks, interactions among partners and concern over the development of reputation can drive compliance with professional norms.\footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).} In order to accomplish this, the network must provide clearly identifiable

\begin{itemize}
\item \footnote{See Herman, supra note 5, at 238.}
\item \footnote{Herman, supra note 131, at 219 (“[T]he OECD nations plus some others signed a ‘bribery convention’ in which ‘the United States has got all the right countries to play by roughly the same rules.’ This is still far removed from intelligence; but it is still a reminder that unexpected things can happen when states are persuaded of common interests.”); Herman, supra note 5, at 238 (noting that during the Cold War, the U.S. and USSR agreed not to extend some of their encryption for the mutual benefit of facilitating verification).}
\item \footnote{Herman, supra note 9, at 277.}
\item \footnote{Herman, supra note 5, at 230 (quoting the British Secretary of State for International Development). Herman suggests that “[p]erhaps Canada, Australia and New Zealand could make particular contributions where US and UK advice is suspect, as perhaps could Germany whose post-1945 intelligence has fewer associations than most with covert activities.” Id. at 237.}
\item \footnote{Jones et al., supra note 68, at 18.}
\item \footnote{See id. at 34 (suggesting that the difficulty of reforming El Salvador’s security forces after the human rights tragedies of the civil war is an example of this pressure to imitate group norms).}
\item \footnote{Raustalia, supra note 8, at 51 (concluding that “when networks promote regulatory change, change occurs more through persuasion than command”).}
\end{itemize}
membership benefits. For less reputable agencies, the anticipated long-term benefits of a good professional reputation may then outweigh the present value of violating network standards. Rewarding good behavior similarly may help induce compliance by less reputable intelligence agencies. Rewards must, however, be carefully constructed and include incentives for progress toward greater respect for democracy and human rights.

Agencies should also use the capacity of intelligence networks to more consistently penalize violations of rules. Intelligence professionals are those most likely to become aware of impropriety by partner agents and are therefore the best actors to conduct oversight and demand compliance with professional guidelines. Clear rules, sanctions, and rewards facilitate efficacious intelligence sharing and create predictable and consistent standards of professional behavior. For, “[i]f there is no expectation that misuse of the system will result in a penalty, there is little disincentive for misuse.”

Maintaining full contact with a partner who continually violates professional norms may impede sharing and trust-building. Communicating an agency’s violation of network standards, by contrast, can shame the agency and incentivize replication of more professional, well-respected agencies in the network. When a partner agency fails to make progress toward professional and accountable behavior, several alternative responses are possible: “[a]t the lowest level, the system terminates access by an offending user. If the problem is more pervasive in the agency, it can terminate access by the agency. Finally, there is the option of maintaining access but working with the agency to improve its practices and compliance.”

Partner agencies might similarly only share information with violating partners on a case-by-case basis or in limited areas less likely to result in repression such as countering biological weapons.

The goal of intelligence network sanctions and rewards should be to cultivate capable, accountable, and professionalized network partners who can be trusted to gather, analyze, and use information in humane and professional ways. As is the aspiration of Western intelligence generally, intelligence networks should employ reputational sanctions and aid in order to “keep[] the players honest, not permit[] disreputable arguments to thrive, [and] point[] out where positions are internally contradictory or rest on tortured readings of the evidence.”

The combination of network sanctioning and targeted support can lead to greater professionalization of our network partners. Regarding all contact with less reputable agencies, Western

230. GILL & PHYTHIAN, supra note 79, at 158 (“[T]here is increasing recognition of the need for some international oversight mechanism to reinforce changes made to operational guidelines and training”).
231. U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-02-04, INFORMATION SHARING: PRACTICES THAT CAN BENEFIT CRITICAL INFRASTRUCTURE PROTECTION 8 (2001) (concluding that there must be procedures for handling rules violations because a violation of partners’ trust will undermine purpose and diminish willingness to share information).
232. MARKLE FOUNDATION, supra note 194, at 29 (“[A] clear, calibrated, and predictable system of accountability for misuse of the system should be an important part of the information sharing environment . . . . Penalties should be known, and they must be applied consistently.”).
233. GOODMAN & JINKS, supra note 60, at 7.
235. HERMAN, supra note 9, at 152 (quoting R. Jarvis).
intelligence should seek to minimize potential harm and foster greater accountability and respect for professional standards. In contrast to current practice, Western intelligence should recognize when the costs outweigh the benefits and when withdrawal of support is in order. Ultimately, raising the professional level of partners through training, aid, and support is imperative. The next section will examine the most effective way to attain this goal.

3. Limits on Quid Pro Quo

This section argues that training and aid should be tailored to further professionalization, and that the quid pro quo for counterterrorism support should minimize potential contribution to rights violations. It relies on studies that show that professionalization through training, aid, and network contact of security services can enhance accountability and efficiency of security services.

To foster greater respect for accuracy, depoliticization, and proposed prohibitions on cruel treatment and arbitrary detention, it is imperative that Western nations seriously consider the most appropriate and effective form of assistance to less professional agencies. Future aid should specifically take into account the short- and long-term costs of counterterrorism efforts. Although long-term costs are frequently ignored, counterterrorism efforts have substantial short-term costs as well. For example, not only did U.S. support to Pakistani intelligence and security forces feed anti-American sentiment and religious extremism there (a long-term cost), it also caused the Pakistani economy to lose in excess of $10 billion in two short years. 236

Assistance to intelligence services should encourage progress toward competence and accountability. Studies show that properly designed training and aid can enhance the accountability and efficiency of more illiberal security services. 237 In El Salvador, for example, qualitative and quantitative evidence reveal the success of UN and U.S. efforts to improve the security services. 238 In less than a decade, security services that had been responsible for thousands of summary executions and systematic torture were called to account and made subject to external review and human rights vetting. 239 The same study also found that aid and training of security intelligence forces generally does not work in highly authoritarian countries, but can have significant effects in emerging democracies. 240 Such findings should be a key consideration when and where the United States decides to provide aid. All aid should be evaluated on the basis of its effects on human rights as well as its contribution to security.

To avoid contributing tools to its repressive partners that facilitate human rights abuses or subvert democracy, Western intelligence should focus on areas with less...
risk of rights violations. Some assistance—such as bomb-squad training and counter-proliferation support—may increase security with little impact on rights, and thus provide a mechanism for continued intelligence contact and the promotion of mutual interests. Other apparently innocuous techniques can create the potential for further repression. Where possible, money should be targeted to certain specific benchmarks, because due to its fungibility it carries risks of undermining foreign policy and reform. In all cases, assistance should be assiduously conditioned, and further aid should depend on progress made toward improving practices.

Training must consistently impart the lesson that arbitrary arrests, detention, and torture are unacceptable. In the United States, in the late 1970s, executive policy mandated just such training in a move that was welcomed by many within the intelligence community. Jack Devine, the former acting head of the CIA’s worldwide operations observed that the refusal to descend to the level of repressive and Communist regimes gave the United States an ideological advantage. Discarded in the heady post-9/11 days, these standards gave credence to the principle that Western intelligence agencies acting as an arm of democratic governments would uphold, not undermine, the values of liberal democracies. Since 9/11, U.S. and other Western intelligence agencies have wandered far from the promotion of these values and have faced significant dilution of professional norms and damage to their reputations.

Ultimately, Western intelligence agencies should know when to cut ties with certain partners. While they should not expect perfect compliance with professional standards and rights norms to result from these efforts, they must weigh the costs of associating with a service that continues to commit abuses. Agencies from liberal democracies should consider the danger of bolstering the capacity of their partners that carry out the policies of brutal authoritarian governments. Certainly, an agency “should end, reduce, or significantly restructure assistance,” when it bears no fruit.

B. Establishing Democratic Oversight and Accountability

This section argues in favor of more watchful and involved legislative and transnational bodies, engaged public debate, and a greater degree of transparency. So doing, it sets out the general principles that should underlie proposed domestic and international mechanisms. Fundamentally, there should be more comprehensive and transparent debate over the purpose, guidelines, and limits of transnational intelligence networks. Because the tension between the demands of democracy and

---

241. Id. at xiv.
242. Id. at 87 (“[E]ven forensic training (including training in explosives) raises concerns that it could enable Uzbek personnel to more effectively fabricate evidence in criminal and counterterrorism proceedings.”).
243. See, e.g., Van Natta, supra note 173, at A22 (reporting that the U.S. State Department cut off $18 million in aid because the Uzbek government failed to improve its human rights record, but the U.S. military then provided an additional $21 million for removal of biological weapons).
244. GREY, supra note 184, at 13.
245. Id.
246. Jones et al., supra note 68, at xviii-xix.
247. Id. at 85.
the secrecy of intelligence networks is particularly acute, the argument focuses on democratic states with professional intelligence services.

Section 1 tackles the problem of the secrecy that obscures the activities of transnational networks from public and legislative awareness. It proposes that intelligence network agreements and MOUs be declassified and that, with the passage of time, originator controls not be permitted to trump Freedom of Information Act requests and declassification of documents. Section 2 calls for democratic bodies to turn their attention to transnational networks. For too long, legislatures and the public have been unaware of and uninvolved in the transnational activities of agencies that purport to serve democratic interests, but often subvert them. Clear statutory permissions and limitations should be devised by democratic representatives. While not without cost, the involvement of the legislatures and the public would convey substantial advantages for intelligence agencies in terms of greater rationality, consistency, and accuracy.

Section 3 argues that, as a general matter, law enforcement networks offer greater potential to counter terrorism in an accurate, reliable, and rights-respecting way and should, therefore, be the focus of international cooperation. Intelligence and law enforcement officials have long worked together to counter and prosecute terrorist groups. Law enforcement intelligence must be prioritized, and any genuine problems involved in prosecutions and information exchange should be the focus of international and transnational cooperation.

1. Improve Transparency through Declassification

Greater transparency is essential to proper accountability, oversight, and vigilance on both the domestic and international levels. Democratic governance, which depends on the consent of the governed, requires the public to have some knowledge of intelligence activities. Tension between secrecy and accountability is inevitable, but democratic states have erred too far in the direction of secrecy, especially with regard to transnational intelligence sharing arrangements. This Article proposes that sharing agreements be made public and that there be a presumption in favor of declassifying information shared through networks, especially as time progresses.

a. Declassification and Legislative Approval of Intelligence Sharing Agreements

Disclosure of the details of intelligence-sharing agreements (what quid pro quo is promised) is key to public scrutiny and accountability. Other regulatory and enforcement agencies regularly publish their MOUs. It is not clear why formal intelligence agreements, some of which have been in existence for half a century, remain classified as top secret. As Richelson and Ball argue, with regard to the UKUSA relationships, “the citizens of the five democracies [should] be officially and fully apprised of the nature and operations of these agencies, and of the consequences (both beneficial and disadvantageous) of the international cooperative

248. RICHELSON & BALL, supra note 12, at 310 (“[T]he conflict of interest between the requirements of secrecy and the basis of democratic government itself has come to be reconciled in each of the UKUSA countries too far in favour of secrecy.”).
arrangements among them—to the extent permitted by the genuine requirements of national security.”249 Under existing rules, however, declassification of the agreements would likely require the consent of all agencies party to them. Additionally, despite practical difficulties, future intelligence sharing agreements that permit the exchange of personal information should be reviewed by legislatures to ensure their compliance with international and national data protection and human rights legislation.250

Some fear that making information about networks public would endanger security by permitting our enemies to know too much about the quantity and quality of intelligence and the methods of sharing. This concern, however, is largely overstated since other nations’ intelligence services already know a great deal more about our intelligence agencies and their information sharing arrangements than the public does.251 While the level of transparency characteristic of other government agencies cannot be expected, some measure of transparency is important to democratic accountability and well-functioning, accurate intelligence. Equipped with the knowledge of the intelligence partners and the mechanisms of sharing, citizens would be able to engage with intelligence policy.252

b. Presumption in Favor of Declassification of Shared Information

Declassification of information shared through networks is central to improving accountability for actions taken through network arrangements. Declassification creates the potential for delayed scrutiny. As we have seen in the United States, historians, intelligence experts, and the National Security Archives have made valuable use of information declassified and released years later.253

It is likely that—as with other government agencies—intelligence shared through networks is significantly over-classified.254 To remedy this, more precise, uniform classification standards for national security information should be developed to ensure that information only remains classified so long as “there are specific and articulable facts suggesting that disclosure of such information would cause identifiable harm to national security or critical infrastructure and that harm

249. Id. at 309. See also Ottawa Principles, supra note 191, § 7.5 (“Confidentiality rules that apply to information-sharing agreements between states may not take precedence over the right of citizens to access information from their governments.”).

250. Ottawa Principles, supra note 191, §§ 8.3.5–6.

251. See Aldrich, supra note 2, at 51–52 (suggesting that the United States has long maintained a ‘clandestine kinship’ with intelligence services in Syria and Libya, despite public condemnation of these services during the 1990s for their association with terrorists).

252. Steven C. Boraz, Establishing Democratic Control of Intelligence in Colombia, 19 INT’L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 84, 102 (2006) (arguing that intelligence accountability calls for an engaged citizenry, public debate, training civilians to understand intelligence, and opening intelligence training schools for those who engage in oversight).


outweighs the public interest in disclosure.”

Failure to declassify information whose sources and methods no longer need protecting is irrational, as it responds to no national security or foreign policy objectives.

Subject to the requirement that classification supports a legitimate national security interest, a presumption in favor of declassification should be instituted and gradually grow heavier over time. The interest in secrecy recedes with the passing years as targets change, sources die, and methods become outdated. Sometimes, this can occur very quickly; for example, the release of information relating to Saddam Hussein’s regime should raise no serious concerns, as the regime has been toppled, and no one doubts that foreign intelligence agents were actively spying there.

Under such circumstances, the consequences of declassification generally will be beneficial, not harmful, to proper intelligence work. Intelligence operatives report that the current system’s “presumption of secrecy makes it tempting to ignore longer-term costs.” Transparency, therefore, can be expected to generate more effective and efficient intelligence over time. The knowledge that their activities will be made known in the future should generate intelligence policies and behavior that resonate more clearly with democratic values. For example, French intelligence agents might have reconsidered engaging in surveillance of peaceful Iraqi dissident groups in France and providing reports to Iraqi intelligence had there been a system that would eventually declassify their wrongdoing. Instead, this collusion, which the French people did not support, was revealed by documents seized during the Iraq invasion.

Indeed, wrongdoing often eventually emerges to the detriment of an intelligence service’s reputation and respect—through media reports, whistleblowers, or eventual declassification. The result is that policymakers and other intelligence consumers question the judgments of intelligence agencies and doubt their


256. Müller-Wille, supra note 91, at 121–22 (“The issue of releasing intelligence is merely a matter of determining the date for declassification, not a matter of principle and national security. The argument of the necessity to protect sources and methods disappears with time.”); Thomas Blanton, The World’s Right to Know, FOREIGN POL’y 50, 56 (Jul./Aug. 2002) (“Former U.S. Secretary of State Lawrence Eagleburger has said most of the secrets he saw in his government career could easily be released within 10 years of their creation.”).

257. TURNER, supra note 41, at 139 (citing veteran CIA operative Gregory Treverton); see also Bruneau & Dombroski, supra note 31, at 163 (“If the intelligence agencies know that in the future their files will be open for public scrutiny, they are logically more likely to keep a rein on the behavior of their members.”); RICHELSON & BALL, supra note 12, at 310 (“Secrecy has shielded these agencies from full accountability and effective supervision and led to their being less effective and less efficient than they otherwise might be.”).

258. Blanton, supra note 256, at 52 (noting that “openness fights terrorism by empowering citizens . . . and holding officials accountable”).

259. Rudner, Hunters and Gatherers, supra note 10, at 220.

260. RICHELSON & BALL, supra note 12, at 310 (“The truth inevitably prevails, and operations which have been undertaken on the premise that they could be plausibly denied will in the end only damage the reputation of the UKUSA countries and the faith of their citizens in their governments.”).
What is reported and leaked regarding intelligence largely brings transgressions and errors to the public attention with a “negative effect on motivation and morale” among intelligence agents. By contrast, greater transparency through declassification of information should help bring intelligence successes as well as failures to light and result in greater legitimacy for intelligence agencies.

2. Establish Democratic Control and Oversight

Hand in hand with greater transparency must come more rigorous oversight. While the precise features of oversight are specific to the historical and institutional experience of each country, it is clear that current oversight mechanisms in every nation must be rethought. The principle of national control—compelled by democratic accountability—should guide the development of new mechanisms. To counter agencies’ temptation to use networks to subvert democratically determined policy, standards of legality and propriety of intelligence cooperation must be decided and enforced at the national level. Each democratic state should institutionalize a regular reassessment of the costs and benefits of intelligence relationships with its partners. Decisions should be made by elected officials, instead of a closed group of professionals who are largely insulated from the demands of their constituent publics or, worse, a group of foreign intelligence officials who make changes in policy through their influence on domestic intelligence services. Such oversight mechanisms will contribute to, rather than detract from, the effectiveness of intelligence services and ensure that engagement in transnational networks advances the protection and promotion of democracy.

Clear statutory permissions and limitations, as Section a sets out, are imperative to proper oversight and democratic involvement in the transnational activities and connections of agencies. So too is budgetary control, as Section b argues.

a. Set Clear Statutory Authority and Limitations on Intelligence Cooperation

The lack of democratic involvement in setting clear statutory permissions and limitations must be remedied. The rule of law demands that no intelligence agency be established in secrecy and that its legislative mandate, limitations, funding

261. Liaropoulos, supra note 2, at 11–12.
262. Laqueur, supra note 90, at 231 (“[B]ecause the work of intelligence has always proceeded at least somewhat in the shadows, open recognition is seldom heard . . . there has been little encouragement and many public attacks for U.S. intelligence.”).
263. Gill & Phythian, supra note 79, at 152 (“[A] legal framework for security intelligence is a necessary, but not a sufficient, condition for democratic oversight.”). See also Ottawa Principles, supra note 191, at 9.1 (setting forth a monitoring regime for security intelligence activities that focuses on the effectiveness, propriety, legitimacy, and accountability of intelligence activities).
264. Richelson & Ball, supra note 12, at 307 (“As the Australian Royal Commission on Intelligence and Security found in 1977, ‘We . . . need constantly to re-assess the benefits to Australia from intelligence relationships with other countries against the costs.’”).
sources, and oversight mechanisms be public. As compared to professional standards that currently regulate transnational networks, legislation and formal democratically approved agreements have the advantage of clarity and precision. They would focus expectations and set forth proscribed, permitted, and required behavior.

Through legislation, domestic legislatures could play a significant role in better evaluating the costs and benefits of intelligence agencies’ associations. They could ensure that intelligence sharing networks respect basic human values and form part of long-term, well-functioning strategy to deal with transnational threats. Such legislative measures have been enacted in the past, but have suffered from inconsistent application and fallen into desuetude. In the 1960s and 1970s, the CIA’s training of foreign partners in countersubversion, counterguerrilla, and intelligence gathering techniques often increased these foreign entities’ capacity for repression. The U.S. Congress responded with a prohibition on the provision of U.S. funds and support to any internal security service, police, or law enforcement. This law likely went too far. Some support, especially to security services in emerging democracies, can improve the human rights practices of those services. Nevertheless, the brutality of many current intelligence partners calls for legislative involvement to minimize potential complicity in rights violations and to ensure effective foreign policy. Legislative dialogue would take into account the panoply of foreign policy goals and would consider international and national legal limits. It would therefore be a promising starting point to reduce intelligence networks’ potential for complicity in violation of rights and repression of democracy.

Legislatures in liberal states should require intelligence agencies to vet their partners, weigh the potential for abuse against a clearly articulated benefit of cooperation, and advance professionalism and humane treatment through their support to foreign counterparts. The United States requires vetting to prohibit funding or association with known human rights violators, but applies the policy inconsistently; the policy also does not apply to the CIA’s funding of foreign intelligence partners—leaving a gaping hole in enforcement. By establishing

266. Intelligence Bill of Rights, supra note 189, para. 2 (“Intelligence services must be established pursuant to duly enacted legislation by a democratically elected government. The establishment of the agency, its mandate, its funding sources and the nature of its oversight must be made part of the public record.”).

267. See BIRKINSHAW, supra note 69, at 33 (observing that Canada’s Commission of Inquiry on the Royal Canadian Mounted Police concluded that “[t]he agency’s activities in relation to security and its responsibilities should be defined in statute and not ‘diffuse and ambiguous’ sources arising as they did from a ‘melange of Cabinet directives, ministerial correspondence and unstated RCMP assumptions’”). Within Western democracies, these should include measures to ensure appropriate levels of privacy protection not be undermined by transnational networks. See Ottawa Principles, supra note 191, at 8.2.5, 8.3; U.S. DEP’T OF JUSTICE, supra note 194, at 3–4 (discussing importance of agents’ adherence to and understanding of privacy restrictions).

268. Jones et al., supra note 68, at 11.

269. Id. at 11. Though still in effect, this law has been rendered toothless by widespread waivers and exemptions. Id.

270. Id. at 15; see also U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-06-850, SECURITY ASSISTANCE: LAPSES IN HUMAN RIGHTS SCREENING IN NORTH AFRICAN COUNTRIES INDICATE NEED FOR FURTHER OVERSIGHT (2006) (concluding that human rights vetting was not done or was insufficient when counterterrorism training and equipment were provided to security forces in Algeria, Morocco, and Tunisia); U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-05-793, SOUTHEAST ASIA: BETTER HUMAN RIGHTS REVIEWS AND STRATEGIC PLANNING NEEDED FOR U.S. ASSISTANCE TO FOREIGN SECURITY
proper vetting procedures, legislatures could set uniform guidelines and clarify the
criteria agencies should use to evaluate partners. 271 Specific to intelligence sharing,
legislatures in democratic states should seriously consider requiring, as Canada does,
a case-by-case evaluation and a finding that the disclosure to a service of a
government that violates rights “is justified by Canadian security or law enforcement
interests . . . can be controlled by specific terms and conditions; and does not have a
negative human rights connotation.” 272 With consistent national oversight and
statutory control, some of the excesses of involvement in transnational intelligence
networks might be reduced.

Domestic oversight mechanisms will be insufficient to counter all the abuses
and inefficiencies in intelligence networks. These oversight mechanisms will be
biased toward the protection of citizens, sometimes to the detriment of the interests
of non-citizens affected by the activities of intelligence agencies. They also will not
exist in the many states without robust democratic systems, with the result that their
agencies’ international cooperative arrangements will go unchecked.

These oversight deficits may call for an international or transnational
monitoring body. Slaughter suggests that once aware of networks of government
agencies, legislators will “expand their oversight capacities and develop networks of
their own.” 273 Within close-knit arrangements like the UKUSA network, some
cooperative oversight body might be plausible even if subject to more executive than
legislative control. It certainly would present an interesting and possibly more
effective way to regulate international networks. 274

Already, some small measure of contact between legislatures has resulted from
increasing awareness of intelligence agency network relations. For example, the
U.K. oversight body, the Intelligence and Security Committee, “takes part in
international liaison and exchanges, both by visiting oversight agencies abroad and
receiving such visits (these have included many European and former Eastern bloc
countries, the United States, and the other Commonwealth states)”; it also conducts
many visits a year to agencies’ premises to examine their functioning. 275 Similarly, in
response to requests from Poland and Argentina during their transitions to
democracy, the U.S. Senate Select Committee on Intelligence provided assistance in
creating mechanisms for legislative oversight and direction of intelligence agencies,
including sending staff to those countries. 276 The Church Commission and U.S.
establishment of intelligence agency oversight also influenced legislatures in other

---

271. Jones et al., supra note 68, at 173 (“Congress can play a critical role by seeking to establish
uniform guidelines [for vetting practices] and providing further clarification regarding the criteria
executive branch agencies should use in identifying and vetting both units and individuals.”).
274. Aldrich, supra note 2, at 53. See generally Post Cold-War International Security Threats:
that an international terrorism court run by the agencies of the G-8 would benefit intelligence sharing and
enable coordination of standards and procedures).
275. Leigh, supra note 98, at 90.
countries to move toward increased regulation and oversight of their intelligence services. 277

Especially within the European Union, there are calls for harmonization and more transnational or regional oversight of intelligence sharing and cooperative networks. In light of the ECHELON investigation, the European Parliament appealed to member states to draw up a common code of conduct establishing proper levels of protection against intelligence operations that would bind each national agency as to operations against anyone within the European Union. 278 It further advocated including the United States in a common code so as to provide maximum protection for EU citizens. 279 Within the European context, Björn Müller-Wille suggests a “model building on an independent oversight body composed of professional experts.” 280 As he envisions it:

 Experts, e.g., from national oversight bodies, could be appointed by Member States and representatives from the [European Parliament] . . . EU oversight bodies should report to their national equivalents (and through them to national parliaments), the Council and, if not to the responsible committee of the EP as a whole, at least to the five MEPs with security clearance . . . . [T]hese bodies should be responsible for ensuring that agencies act within their mandate and that they do not violate civil liberties and constitutional rights. 281

Some form of transnational oversight, whether expert, executive or legislative, may ultimately be necessary in order to solve some of the inconsistencies and dangers particular to intelligence networks. Pre-existing networks, such as the UKUSA agreements, or regional institutions, such as the European Union, might provide a foundation for the development of such mechanisms.

b. Develop Budgetary Control

Key to democratic oversight and the prevention of intelligence agency subversion of statutory or policy limits is budgetary control. Participation in intelligence networks offers numerous benefits, but comes at a cost to democratic rule, especially when agencies receive or impart funds without democratic involvement.

Networks can prevent legislatures from exercising fiscal accountability, which is a central and, in many countries, constitutionally-mandated tool to check the executive. 282 Imagine a democratic country that attempted to limit the power of its

277. See Farson, supra note 100, at 226 (stating that within the UKUSA network, “it was not until attitudes shifted in the US, by then the alliance’s leading partner, that reforms occurred elsewhere”).

278. EUROPEAN PARLIAMENT RESOLUTION ON ECHELON, supra note 93, para. 13. See also Ottawa Principles, supra note 191, at 8.3.7 (“The UN member states should develop and adopt an international instrument affirming privacy and data protection as fundamental human rights and laying down minimum standards for protection in accordance with these principles.”).

279. EUROPEAN PARLIAMENT RESOLUTION ON ECHELON, supra note 93, para. 14.

280. Müller-Wille, supra note 91, at 124.

281. Id.

282. Keohane, supra note 76, at 1132 (“Fiscal accountability describes mechanisms through which funding agencies can demand reports from, and ultimately sanction, agencies that are recipients of funding.”); 9/11 COMMISSION REPORT, supra 186, at 410 (“When Congress passes an appropriations bill to allocate money to intelligence agencies, most of their funding is hidden in the Defense Department in
national intelligence agency by restricting funding or issues on which it can gather intelligence. Through networking with partners, however, an agency could escape these funding limits—expanding its available resources and areas of interest. Even more problematically, the intelligence service could receive money or equipment in return for network cooperation, which if kept from legislators could allow it to become self-funded and more powerful than the people, through their legislators, intended.

This may seem far-fetched, but it is not unprecedented. For instance, until the 1990s, ninety percent of the budgets of the Norwegian Secret Services came from the United States and NATO without public or parliamentary knowledge.\(^\text{283}\) Similarly, the National Reconnaissance Office, a U.S. military intelligence agency, whose existence was only publicly disclosed in 1994, accumulated a $4 billion slush fund of appropriations without congressional knowledge.\(^\text{284}\)

Oversight mechanisms should therefore take into account funds received from partners. With regard to large intelligence agencies which sometimes fund extremely repressive partners, national overseers should be aware of how appropriations are being dispensed. Under the current system, many countries’ budgets obscure the most basic facts regarding the amount of funds available and how they are spent; intelligence funds often simply “disappear” in the defense budget.\(^\text{285}\) In the United States, the 9/11 Commission advised Congress to “pass a separate appropriations act for intelligence, defending the broad allocation of how these tens of billions of dollars have been assigned among the varieties of intelligence work.”\(^\text{286}\) In this way, overseers could limit improper funding of illiberal regimes.

Budgetary control can be remarkably successful. As the former U.S. Director of Central Intelligence Colby remarked, in order to convince the CIA to abandon a plan, “an [Intelligence] Committee chairman needs only to say to the DCI at the end of the briefing: ‘Write down in your notebook $100 million, because—if you go ahead—that is what is coming out of your CIA budget next year.’”\(^\text{287}\)

C. Rely on and Bolster Law Enforcement Intelligence

Due to the persistent human rights and democratic accountability problems manifested by intelligence networks, the best way to counter transnational crime, ensure accurate information, and reduce rights violations is to improve information


\(^{284}\) JOHNSON, supra note 6, at 103.

\(^{285}\) Müller-Wille, supra note 91, at 113.

\(^{286}\) 9/11 COMMISSION REPORT, supra 186, at 416.

\(^{287}\) JOHNSON, supra note 35, at 135 (quoting DCI William Colby); accord Müller-Wille, supra note 91, at 113 (“At the national level, budgetary control represents one of the most powerful means by which parliaments can influence and sanction the executive’s policies.”).
sharing networks for law enforcement and criminal convictions. Treating terrorist violence as a criminal act—to be handled through legal systems in accordance with the rule of law, democracy, and human rights—represents the most consistent and successful way to reduce violence and terrorist threats. Arrest and prosecution of suspects, instead of detention and torture at the hands of less reputable partners, would check abuses and engender public support. It would also involve the single most valuable tool to discern inaccuracies, mistakes, and manipulation: an adversarial process before an independent court.

1. Improve Law Enforcement Sharing Networks

Because of the benefits inherent in criminal prosecutions, the focus of the international community and national legislatures should be on improving the law enforcement networks, which link police, prosecutors, and judges.

With regard to transnational threats and actors, the primary approach has long been law enforcement. Terrorist organizations generally rely on criminal acts for their financing; criminal prosecution for lesser crimes, therefore, offers a mechanism to disrupt terrorist activities and turn would-be terrorists into witnesses against higher-ups. Successful investigation and prosecutions of these crimes have long demanded regular contact among law enforcement agents. As a result, police and law enforcement intelligence agencies typically have relied on close and often long-standing connections to their counterpart agencies to counter transnational threats. Only after the end of the Cold War did intelligence professionals, in an attempt to remain relevant, begin to take over the field.

Prior to 9/11, law enforcement was effective against suspected terrorism. Intelligence and law enforcement officials jointly operated against transnational crime, including terrorism. U.S. intelligence and law enforcement (primarily the CIA and FBI) routinely targeted leaders of terrorist groups together. In the context of their “rendition to justice” program, the CIA used connections to foreign intelligence services to coordinate the arrest of terrorists and hand them over to the FBI for prosecution in U.S. courts. Immediately after 9/11, states and their respective agencies worked to improve law enforcement intelligence sharing. Through informal


290. Heymann, supra note 110, at 14 (noting that “[p]olice agencies have a greater tradition of sharing information across borders” than intelligence agencies).


292. MARGARET SATTERTHWAITE & ANGELINA FISHER, CTR. FOR HUMAN RIGHTS & GLOBAL JUSTICE, N.Y. UNIV. SCH. OF LAW, BEYOND GUANTANAMO: TRANSFERS TO TORTURE ONE YEAR AFTER RASUL v. BUSH 9–11 (2005), available at http://www.chrgj.org/docs/Beyond%20Guantanamo%20Report%20FINAL.pdf. See also HUMAN RIGHTS WATCH, supra note 155, at 4 (“During the decade prior to 1998, the U.S. government used extraordinary rendition to bring 13 terrorist suspects to the United States to stand trial on criminal charges.”).
MOUs and formal agreements, states bolstered existing mechanisms of exchange, such as Interpol and Europol. 293 States also concluded mutual legal assistance and recognition treaties in order to alleviate some of the difficulties in arrest and extradition of terrorist suspects. 294 Many experts still believe “a more coordinated law enforcement and intelligence approach would better combat both international crime and terrorism.” 295 As they did in the past, liberal democracies could harness the connections of their intelligence agencies to help rather than hinder criminal prosecutions. To encourage the arrest, prosecution, and conviction of perpetrators of terrorism, intelligence should be “preferably produced in a way that allows it to be exploited as evidence,” and law enforcement officials should use the tools at their disposal, such as witness protection programs, to protect those intelligence sources that might be endangered. 296

Aligning intelligence and law enforcement work is no easy task, 297 but the conclusion that intelligence should automatically trump law enforcement is by no means the logical one. Prosecution in civilian criminal courts undeniably exacts cost and effort, requiring officials to assemble evidence, meet evidentiary thresholds, and locate and arrest perpetrators abroad. 298 Nevertheless, most liberal democracies are equipped with criminal statutes applicable to terrorist acts committed at home and abroad. As a general matter, they boast successful records of prosecuting terrorist acts and other transnational crimes. 299 Although some fear that court procedures will reveal classified information and pose risks to intelligence sources and methods, 300 courts are adept at finding creative solutions to protect information while allowing for an effective defense. Legislatures also can and have enacted statutes to protect classified information while maintaining the integrity of criminal proceedings.

2. Benefits of Law Enforcement Intelligence and the Involvement of Courts

Though affected by some of the same problems as intelligence cooperation, law enforcement networks benefit from greater transparency and the involvement of courts. The involvement of courts has several distinct advantages. It advances Western intelligence’s interests in accuracy and the pursuit of truth, which facilitates

293. WAGLEY, supra note 288, at 13 (discussing various mechanisms for exchange of criminal information transnationally). See also Jorg Monar, Anti-Terrorism Law and Policy: The Case of the European Union, in GLOBAL ANTI-TERRORISM LAW AND POLICY PAGE, 425–30 (Victor V. Ramraj et al. eds., 2005) (analyzing the law enforcement cooperation mechanisms adopted within the EU, including Europol).


295. WAGLEY, supra note 288, at 11.

296. Müller-Wille, supra note 2, at 19.


298. Bay, supra note 20, at 356–57 (describing several difficulties with criminal prosecution).


300. Bay, supra note 20, at 357.
the protection of democratic states, a task at the heart of these agencies’ missions. It also tempers the impulse to rely on illiberal partners to extract information through coercive tactics. Even if the safeguards to prohibit the use of coerced information proposed in previous sections were adopted, one could imagine that an agency might still receive, use, and forward intelligence that has been obtained in violation of human rights law.\(^\text{301}\) The best way to reduce this potential is to facilitate challenges to the information. Criminal trials afford the affected individual the means to challenge the credibility, reliability, and accuracy of information. The rights to present a defense, to confront one’s accusers, to protect against self-incrimination, and to assistance of counsel reduce the risk of error and incidence of government wrongdoing.

Anecdotal evidence from post-9/11 counterterrorism efforts indicates the importance of these procedural safeguards. A U.K. court review of the detention of several individuals found that MI5 had relied on very weak evidence, and falsely claimed that weapons had been found in order to detain them.\(^\text{302}\) The court’s involvement also enhanced MI5’s accuracy. After the proceedings revealed that “the purpose behind a group of Muslim men’s visit to Dorset had not been to elect a terrorist leader [as MI5 had asserted] but to get away from their wives for the weekend,” MI5 withdrew its assessment of their dangerousness.\(^\text{303}\)

In the United States, courts played a similar role. In one case, intelligence officers and prosecutors were willing to accept intelligence and witnesses provided by a Russian agency indicating a U.S. citizen was a well-known terrorist financier. The information turned out to be utterly unreliable as a case of false identity.\(^\text{304}\) Yet only because the individual concerned was prosecuted in a court of law did the falsity of this information come to light.

Court proceedings lessen the risk of Western involvement in or reliance on coerced evidence, inherent in cooperation with less-reputable partners, by exposing wrongdoing and improprieties. For example, a U.S. court uncovered allegations of torture when Wang Zong Xiao, a defendant arrested and charged in China, came to the United States to testify against other defendants and recanted his confession, claiming coercion.\(^\text{305}\) Similarly in Britain, an MI5 officer admitted in court that MI5 possibly assessed evidence obtained through torture as reliable and that administrative agencies likely relied on that evidence.\(^\text{306}\) By creating incentives for Western intelligence to demand high professional and ethical standards from their intelligence partners, participation of courts may generate more credible, efficient intelligence exchange against transnational threats.

Court proceedings help ensure that the right person is subject to sanctions for wrongdoing. Interrogation by intelligence officials can subject individuals to the

\(^{301}\) Müller-Wille, supra note 91, at 108.

\(^{302}\) Mark Phythian, Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture, 18 INT’L J. OF INTELLIGENCE AND COUNTERINTELLIGENCE 653, 669–70 (2005). Among the intelligence that MI5 relied upon was the observation that the detainees were “excessively security conscious” while shopping. Id.

\(^{303}\) Id. at 669.

\(^{304}\) Id.

\(^{305}\) Id., supra note 68, at 557–58 (“The desire to proceed with the joint effort seemed to have blinded the United States prosecutor to earlier indications that the confession might have been coerced and unreliable.”).

\(^{306}\) AMNESTY INTERNATIONAL, supra note 145, at 23.
impossible situation of having to disprove an allegation, in many countries under the threat of torture. By contrast, criminal procedures place the burden on the government to make a case, permit the defendant to engage in discovery, and require disclosure of exculpatory information known to or in the possession of the government. Whereas the current transnational system which errs by not prosecuting those who have committed violent acts and by detaining innocent people who have not, criminal procedures aim to convict the guilty and release the innocent, in the best interest of Western states and their intelligence agencies.

Accuracy—getting the right guy—has a better outcome both in terms of the reputation of liberal democracies and of the promotion of the rule of law in our partner nations. The involvement of courts bestows counter-terrorism efforts and the agencies that implement them with greater legitimacy and public support. By upholding the rule of law, trials give the countries involved moral legitimacy and encourage the development of international legal norms to deal with terrorism. Their capacity for verification portends some measure of quality control, which could remedy certain irrationalities in current intelligence gathering and sharing arrangements.

Although this discussion has focused largely on the use of courts independent of the executive, certain administrative procedures might also be developed to permit challenges to and correction of inaccurate intelligence information and to trigger investigation of possible wrongdoing or statutory violations through intelligence networks. Some states have already developed an administrative right for redress of abuses produced through improper intelligence gathering. The United Kingdom instituted a tribunal where a person can file complaints regarding actions taken by or on behalf of the intelligence’s services with regards to him, his property, or communications. Similarly in Australia, a Security Appeals Tribunal, which has a high-level of security clearance, provides a forum for complaints of illegal intelligence activity. In addition, an Inspector-General of Intelligence and Security acts as an ombudsman for the public and has the power to demand information, examine the records of departments, and investigate complaints about the propriety and accuracy of information gathered.

International tribunals present another intriguing alternative. Some contend that trials before an ethnically and nationally diverse panel of judges offer the most appropriate forum for criminal prosecution of transnational crimes. International tribunals have the comparative advantage of involving the global public, standardizing cooperation and punishment, and enhancing legitimacy of

308. See Intelligence Bill of Rights, supra note 189, para. 10 (advising that “[c]itizens and resident aliens who believe that their rights were violated by intelligence agencies . . . be able to apply to the intelligence agency concerned for access to information held by the state and or such agency about them”).
309. BIRKINSHAW, supra note 69, at 47.
310. Id. at 54.
311. Id. at 60–61, 242.
counterterrorism efforts and factual narratives developed at trial. Laura Dickinson argues that international trials “could help to strengthen the needed intelligence-sharing networks and could help to provide a framework for screening sensitive information that would have greater legitimacy than a purely U.S.-run process.” Accordingly, Muslim states might more willingly extradite suspects and provide full cooperation.

Whatever national or international, judicial or administrative, court proceedings conducted with respect for due process and individual rights should diminish the affinity of many civilians for terrorist groups and strengthen resolve against such groups. The criminal process establishes a historical record of events and exposes evidence of wrongdoing, which can serve to dissipate terrorists’ cult status. Perhaps the greatest value is that “[l]aw enforcement, with its focus on the illegal act itself, removes the temptation to try to judge between just and unjust motivations, legitimate and illegitimate concessions, worthy and unworthy political causes.”

CONCLUSION

If anything is certain in the murky world of intelligence collection, it is that intelligence sharing will continue. Though the partners and the level of sharing may change, intelligence sharing will remain an indispensable component of any effective strategy against transnational threats. But, as this Article has shown, intelligence sharing networks must not remain as they are. As they function now, these networks strain the principles of democracy and accountability. They create ample opportunities for even the most professionalized agency to subvert international and national legal restraints through collusion with network partners, and resulting in untold human rights abuses. More fundamentally, the operation of intelligence sharing networks challenges our democratic system, eviscerating notions of national jurisdiction and traditional mechanisms of managing intelligence agencies.

Reconciling the necessity of transnational cooperation and the constraints of liberal democracy should therefore be a top priority for national executives, legislatures, and international bodies. Network sanctions and high professional standards, although desirable, should not be the only means to evaluate and improve intelligence cooperation. National democratic bodies, international institutions, and regional alliances all have a role to play. As implausible as it may seem, executive and legislative engagement with their counterparts in allied states may prove necessary to ensure intelligence cooperation that is effective and furthers the larger interests of Western democracies. A return to law enforcement and use of the judiciary is essential for the accuracy and legitimacy of efforts to counter transnational threats.

Without real concerted change, we will continue to see the proliferation of inaccurate information, brutal tactics, and intelligence failures due to improper information sharing. Accountability and democracy will continue to suffer. And the network arrangements of our intelligence agencies will continue to challenge our

314. Dickinson, supra note 312, at 1448.
conceptions of international law, accountability, and ultimately the role of our own state in the world.