Approaches to "Outreach" for Intelligence

Center for Asymmetric Threat Studies (CATS)

Author: Gregory F. Treverton

NATIONAL DEFENCE COLLEGE

CATS
Center for Asymmetric Threat Studies

MSB
Swedish Civil Contingencies Agency

Title: Approaches to “Outreach” for Intelligence
Author: Gregory F. Treverton

Published by: The Swedish National Defence College
Number of copies: 300

ISBN 978-91-89683-07-5

© Swedish National Defence College
No reproduction, copy or transmission of this publication may be made without written permission. Swedish material law is applied to this book.

Printed by Elanders, Vällingby 2009

Approaches to "Outreach" for Intelligence

Gregory F. Treverton[1]

RAND Corporation and Centre for Asymmetric Threat Studies (CATS)
December 2008

This working paper, part of the second year of CATS' project on intelligence for terrorism and homeland security for the Swedish Emergency Management Agency (SEMA), explores ways that intelligence services, both foreign and domestic, have or might reach out beyond government for information or expertise. The topic is less easily bounded than might appear to be the case, for much of normal intelligence work involves reaching out. Domestic services reach out to ethnic and other groups of interest as a crucial part of their work, and foreign and domestic services often reach out to national companies that might be objects of intelligence interest from the intelligence services of other nations.[2]

Those kinds of outreach are, for this working paper, the boundaries of the topic, and the paper concentrates on ways that services have reached or might reach out to private individuals or organizations in order to have the benefit

1 I happily acknowledge the contribution of my RAND colleague, Andres Villamizar.

2 For instance, the Australian Security Intelligence Organization (ASIO) established its Business Liaison Unit (BLU) in October 2005 as a "direct interface between business and ASIO to enhance the flow of national security information to the private sector." See http://www.theage.com.au/news/Business/ASIO-chief-plans-business-briefings/2006/06/07/1149359792800.html.

of information or expertise on important intelligence issues.[3] It is outreach for the purpose of improving analysis. A recent U.S. intelligence directive defines analytic outreach as "the open, overt, and deliberate act of an IC [intelligence community] analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information."[4]

The paper first describes the current state of outreach; it emphasizes that the change in intelligence's targets has made reaching out all the more important if not always easier. It then lays out a range of forms of outreach, with international examples for each.

The State of Outreach

In one sense, outreach is not new. At its beginnings in the late 1940s, for instance, the CIA's Board of National Estimates established the "Princeton Consultants" – a group of distinguished professors who met with the Board several times at year, in secret in Princeton, to review draft intelligence estimates.[5] It is, though, newly important and newly challenging. Indeed, the challenge is probably better described as "external engagement" than the narrower "analytic outreach."[6]

Because modern intelligence services operate mostly in secret, and because their highest calling is protecting sources and methods, reaching outside fellow intelligence services is something of an unnatural act. Trust and relationship are critical. Too often the flow is only in one direction, with intelligence officers listening but not talking, thus making the process both baffling and unsatisfying for the outsiders being "reached." These government-organized seminars or workshops seem mere collection opportunities, with outsiders giving and officials receiving. To be sure, there are trade-offs, and sometimes immediate needs for information gathering arise. But the real pay-off is long-term building of relationships.

---

3 Thus, this discussion of outreach also excludes activities designed to make agencies good local or national citizens, not produce better intelligence. The U.S. CIA's Directorate of Science and Technology, for instance, provides speakers, prizes and other interactions designed to promote the learning of science and technology, and the U.S. NSA Mathematics Education Partnership Program is a similar set of programs addressed to mathematics. See, respectively, https://www.cia.gov/offices-of-cia/science-technology/in-the-community-across-the-nation.html; and http://www.nsa.gov/mepp/index.cfm.

4 U.S. Intelligence Community Directive 205, "Analytic Outreach" (effective 16 July 2008), available at http://www.dni.gov/electronic_reading_room/ICD%20205.pdf.

5 See Sherman Kent, "The First Year of the Office of National Estimates," available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/7year.html.

6 The broader terms was suggested in a conversation with an official from Britain's MI-5.

Organizational culture can be a powerful obstacle. The mind-set of collection is hard for intelligence organizations to shake, and security procedures not only reinforce that psychological obstacle but can also create more tangible obstacles – like difficulties bringing outsiders into cleared facilities. Most intelligence services undertake both analysis and operations, and some move people back and forth between those functions relatively often. That can further confuse the role tension between outreach and collection. Even in a service like the CIA, which separates operations and analysis in separate components, still operates according to the needs of its operators (the Directorate of Operations), and so many analysts still are wary of announcing where they work, handing out cards, and all the other aspects of building (open) relationships with outsiders. The State Department Bureau of Intelligence and Research (INR) is solely an analytic arm and so finds outreach a less unnatural act.

In most respects, the change in targets described in table 1 has made outreach all the more important, and taken it in new directions. In one respect, however, it may have made it more difficult. The ponderous and "bounded" nature of the Soviet target provided both time and incentive to develop relationships with knowledgeable outsiders. Now, with many targets, not few, lots of uncertainty and, often, the harder edge of short-term demands, it is tempting for some in intelligence officers to say "why bother?" cultivating outsiders. There is too much to do inside.

The other attributes of the changed target have made external engagement all the more important. For instance, after the end of the Cold War, humanitarian, peacekeeping and other contingency operations mushroomed, often in countries which had not been of high priority for intelligence. In many of them, any foreign presence on the ground was stray academics but also, in particular, non-governmental organizations (NGOs), especially those in the business of humanitarian relief like the International Red Cross, CARE or Médecins san Frontières. They were often skeptical of government and more so of intelligence. But they also came to welcome that someone cared about their issue. They knew a lot about local circumstances, and so became both sources and consumers.

Table 1 lays out the distinctions between traditional state targets of intelligence and non-state targets like terrorists:

Table 1: From Cold War Targets to Era of Terror Targets

	Old: Cold War	New: Era of Terror
Target	States, primarily the Soviet Union	Transnational actors, also some states
Objects of scrutiny	Mostly big, rich and central	Many small, even single individuals, and peripheral
"Story" about Target	Story: states are geographic, hierarchical, bureaucratic	Not much story: non-states come in many sizes, shapes
Location of target	Mostly "over there," abroad	Abroad and at home
Consumers	Limited numbers: primarily federal, political military officials	Enormous numbers in principle: including state, local and private
"Boundedness"	Relatively bounded: Soviet Union ponderous	Much less bounded: terrorists patient but new groups, attack modes
Information	Too little: dominated by secret sources	Too much: broader range of sources, though secrets still matter
Interaction with Target	Relatively little: Soviet Union would do what it would do	Intense: terrorists as the ultimate asymmetric threat
Form of intelligence product	"Answer" for puzzles; best estimate with excursions for mysteries	Perhaps "sensemaking" for complexities
Primacy of Intelligence	Important, not primary: deterrence not intelligence rich	Primary: prevention depends on intelligence

As the humanitarian example drives home, the transition to targets that are small, peripheral and perhaps unpredictable means than intelligence must often expect *not* to have an edge over experts outside government. Given closed foes, Cold War intelligence gave pride of place to secrets – information gathered by human and technical means that intelligence "owned." Terrorists are hardly open, but an avalanche of open data is relevant to them: witness the September 11th hijackers whose true addresses were available in California motor vehicle records. During the Cold War, the problem was too little (good) information. Now, it is too much (unreliable) information. Then, intelligence's secrets were deemed reliable; now, the torrents on the web are a stew of fact, fancy, and disinformation.

Because of the unbounded and high profile nature of transnational threats, intelligence must wade through a sea of information that contrasts sharply with the much more limited information that was available on closed societies such as the Soviet Union. And much of the information is, at best, of uncertain reliability. Given that most of the torrent of information is not secret, intelligence services not only can but need to reach out to outsiders to process or validate information.

Next, while various countries, especially the United States, hoped that their policies would influence Cold War Moscow, intelligence agencies could pre-

sume that, as a first approximation, those efforts at influence would fail. The Soviet Union would do what it would do. The challenge, in the first instance, was figuring out its likely course, not calibrating influence that other nations might have over that course. The terrorist target, however, is utterly different. It is the ultimate asymmetric threat, shaping its capabilities to our vulnerabilities. The September 11th suicide bombers did not hit on their attack plan because they were airline buffs. They had done enough tactical reconnaissance to know fuel-filled jets in flight were a vulnerable asset and defensive passenger clearance procedures were weak. They could get box cutters through airport security, and the scheme obviated the need to face a more effective defense against procuring or importing ordnance.

To a great extent, we shape the threat to us; it reflects our vulnerable assets and weak defenses. In that sense, the capabilities of terrorists are a mystery, not a puzzle, for those capabilities depend on their continuing adaptation to the vulnerabilities of their targets, not on counts of missiles, guns or even cells.[7] For instance, Al-Qaeda-linked plotters in 2006 planned to blow up airplanes over the Atlantic with liquid explosives smuggled onto planes as sport drinks or other permitted carry-ons. They had adapted to the airport security procedures then in effect, knowing that drinks were then permitted as carry-ons and that most detectors in place could not identify explosives.

As military planners would put it, it is impossible to understand red, potential foes, without knowing a lot about blue, ourselves. This interaction between "us" and "them" has very awkward implications for intelligence, especially foreign intelligence that has in many countries been enjoined from examining the home front and, less formally, worried that getting too close to "policy" is to risk becoming politicized. The task has now become net assessment of threats and vulnerabilities, of red against blue, and that provides powerful incentive to reach out beyond intelligence and beyond government – especially perhaps to those private sector managers of critical "public" infrastructure.

A final driver of increased interest in outreach is the nature of the new people coming into intelligence. The young recruits are a wonderful opportunity for intelligence services but also a challenge. They grew up on Google and are used to reaching out, not sitting back and waiting for information to come to them. They are used to being connected in a hundred directions, not limited by

---

7 On the distinction between puzzles and mysteries, see Gregory F. Treverton, "Estimating Beyond the Cold War," *Defense Intelligence Journal,* 3, 2 (Fall 1994); and Joseph S. Nye, Jr., "Peering into the Future," *Foreign Affairs*, 77, 4 July/August 1994, 82-93. For a popular version, see Treverton, "Risks and Riddles," *Smithsonian,* June 2007

"need to know."[8] If they find their communications gear at home a generation ahead of what they have at work, with business practices to match, they will be lost to intelligence agencies.

In sum, intelligence services may spy but don't do enough "looking."[9] Nor are they adept at hiring or otherwise making use of lookers. Terrorist targets are secretive, but in a more transparent world, one with fewer denied areas, lots of intelligence can be obtained by simply looking, better still drawing on those outside government who have done the looking in their work as business people, NGO members or cops on the beat. One commentator, Robert Steele, talks about the emergence of the six "intelligence tribes" that will join the traditional national intelligence tribe: i) the military, ii) law enforcement, iii) business, iv) academia, v) nongovernmental and media, and finally vi) religious or citizen intelligence tribes. While, for him, "smart clans" or "smart mobs" will challenge the power and influence of "dumb nations," still, in "specific areas generic to all tribes" cooperative advances can be made. Furthermore, "multilateral information sharing, rather than unilateral secrecy" will be the primary characteristic of intelligence in future. Intelligence will become personal, public and political, will be taught at every school and will emerge as a mixed private-public good. [10]

To be sure, the incentives have different degrees of effect in different countries. That fact, plus national traditions and cultures, mean that outreach varies enormously in extent and form across nations. For instance, the German external service, the Bundesnachrichtendienst (BND), does not cooperate with any non-governmental organizations or groups other than private companies whose technological secrets are vulnerable to attack from abroad (Russia, China etc.). The domestic service, the Bundesamtes für Verfassungsschutz (*BfV*), seeks help from various communities, for example Muslim organizations, in order to get a better understanding of their inner workings. That, however, is doing normal business, not "cooperation" or outreach.

In Spain and other European nations outreach activities mostly revolve around the concept of "open source." Spain's CNI, *Centro Nacional de Inteligencia*, which is attached to the Ministry of Defense, aims to promote and expand an "intelligence culture" in support of the activities of the Spanish Intelligence Community. "We [the CNI] understand 'intelligence culture' as

8 This point came through loud and clear in interviews throughout the analytic elements of the Intelligence Community in 2004. See Gregory F. Treverton and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis,* TR-293, (Santa Monica: RAND Corporation, 2008).

9 See Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information,* (Cambridge: Cambridge University Press, 2001), p. 161ff.

10 Robert David Steele, "Information Peacekeeping and the Future of Intelligence", *The Journal of Intelligence and Counterintelligence*, 17, 2 (Summer 2004), 265.

the knowledge base a society must have about the needs, functions and goals of the intelligence service, in order to perceive intelligence activities as an integral part of society itself, as it pertains to its security, liberty and defense of its interests." As such, the CNI views this "culture of intelligence" as particularly relevant for the entrepreneurial and academic sectors. Within this last one, it seeks to make intelligence "an academic discipline to be studied at universities and other learning centers." To accomplish this it will foment both the inclusion of intelligence topics in academic curricula and of the scholarly research pertaining to these subjects.[11] At the same time, the CNI hopes to benefit from the "experience and knowledge base" that the academic world has about topics of interest to the CNI, both in terms of information and analysis.[12]

In general, European governments are more self-contained than the United States (and Canadian), and so reaching across the private-public membrane is rarer, though that is changing: witness the SEMA interest in this topic. In Britain, for instance, explicit reaching across the public-private boundary in intelligence is limited, and contacts tend to be less formal and centered on a few elite universities, with an "old boys' (now including girls) network" flavor to them. As a result, many of the explicit forms of outreach suggested here arise from U.S. (or Canadian) experiences.

Forms of "Outreach"

Given the focus on analytic outreach, this scanning defines the process broadly, including practices that might be more likely to be thought of as "in-reach." The spectrum of possible forms no doubt could be widened, but a first listing might include:

- Co-production, in which outsiders are an integral part of producing inside products.
- Virtual co-production, with wikis or blogs open to (selected) outsiders, for example.
- Outsiders on retainer for occasional consultation or analysis.
- Joint inside-outside working groups on particular issues.
- Ongoing collaboration in detail, on methods if not products.
- Systematic debriefing of willing "lookers" among nation's citizens or others.
- Publications targeted or available to outsiders.
- Occasional conferences, involving outsiders.
- Use of Web sites, to invite tips or other information.

11 https://www.cni.es/05/05_index.cfm
12 Ibid.

Here is more detail and example on each form or method:

Co-Production. One form of this is simple outsourcing, paying an outside company or group to collect information or conduct analysis, with guidance from the intelligence agency but only limited interaction with it. At the extreme, intelligence agencies can now simply buy – from Bloomberg, Oxford Analytica and other organizations – economic and political analysis they used to do in-house. In the next step, the RAND Corporation and lots of similar institutions do analysis – usually unclassified but sometimes classified as well – for a number of American intelligence agencies. The arguments for outsourcing range from information and expertise, to access, to method, to simple time. Insiders may want to tap particular expertise or methods unique to an outsider or group. Or that group may have easier access to information or expertise; a few years ago, for instance, RAND organized workshops bringing Russian and American experts on North Korea together to share notes – which would have been awkward for an American intelligence service to organize. Often, RAND does longer-term analysis that the CIA or others could do but lack the time, given the press of current intelligence.

Sometimes, outsourcing approaches co-production, but more often the relationships is pretty standoff-ish. An interesting recent CIA initiative, infelicitously named "iD8," sought to do co-production inside the government. It was to be based outside Washington to both symbolize and make use of its openness to outside expertise of all sorts. It would work on hard problems with outsiders, keeping the work unclassified and moving up the ladder of classification only when it absolutely had to. Alas, it is far from certain that iD8 will actually happen.

Another U.S. initiative, this one by intelligence at the Department of Energy, seeks to reshape strategic intelligence through co-production. The challenge is to do strategic intelligence on climate and energy together. For that task, secret information is not very useful, and international collaboration is. So far some 24 nations have been represented at 3 international workshops. The project is conceived explicitly as co-production, or co-creation, joint exploration, *not* the traditional producer-consumer interaction. To a great extent, the conversation *is* the product.

Virtual Co-Production. An example might be wikis or blogs open to (some) outsiders. There seems not yet to be a good example of this in intelligence. The U.S. Intellipedia is a classified version, thus limiting the role of outsiders. But the wiki technology – producing a clear trail of who edited what and why – makes is a natural way to involve expert outsiders on problems where the premium is on expertise, not secrets. In general, intelligence agencies have only

begun to examine the range of uses the web might serve for them. The so-called terrorism futures market, was an intriguing case in point. Developed by the U.S. Defense Department, it was a web-based market in which investors would buy futures on the likelihoods of specific events or conditions occurring in the Middle East. When it came to light, it provoked political outrage, betting on death. Yet, later, analysts across the political spectrum rallied to the idea, as a way of using the market to gain information. Financial analysts bet their own money before they are willing to make specific recommendations to clients. In this case, too, with uncertainty large and information in short supply, using a futures market to get experts to bet their hunches made a good deal of sense.

Outsiders on Retainer. The Spanish intelligence community and others make use of "reserve intelligence officers" – that is, ex-insiders, now outsiders who may be called upon to carry out certain activities as needed. This generates an expanded network of analysts and information gatherers, since most of these "reservists" work for private security firms. Another model from the U.S. National Intelligence Council (NIC) is the NIC Associates, now IC (Intelligence Community) Associates. Chosen from the ranks of academia, the corporate world, or think tanks, they are asked to bring their understanding to bear on a wide spectrum of issues. Paid a small retainer, they ordinarily are asked to prepare periodic background reports within their area of specialization and meet with analysts at informal seminars.

Joint Working Groups on Particular Issues. One interesting model, at the edge of intelligence, is that of the British Defence Academy's Advanced Research and Assessment Group (ARAG). [13] It organizes its work in "research clusters." ARAG holds thematic seminars, based on research, where the results are discussed in a circle of intelligence and area experts, plus intelligence customers. It is a model between conferences and "targeted research." Participants have found it a useful way of bringing knowledge directly to the customers in a setting, where there is plenty of space for probing interaction. With consumers present, it provides instant feed-back as well as proposals for new research.

A U.S. experiment, dubbed the Summer Hard Problems workshop, or SHARP, was modeled after a highly successful program by the National Security Agency, which has a long tradition of collaboration with top mathematicians charged with developing new encryption algorithms. Begun in 2006, SHARP is a four-week workshop with 20 outside experts and 20 top analysts from the CIA and eight other intelligence agencies. Their mission is to better understand

13 The ARAG website is http://www.da.mod.uk/colleges/arag.

some of the most basic questions confronting U.S. intelligence: What's driving the spread of extremism around the globe, and how can it be stopped.[14]

Ongoing Collaboration in Detail, On Methods If Not Products. Here, the widest venture has been the CIA-sponsored Global Futures Forum, which grew out of another similar initiative, the Global Futures Partnership, which aimed to be a strategic "think and do tank" that undertakes unclassified global outreach for CIA and other U.S. intelligence community elements on the most important issues facing the intelligence community today and in coming years. It conceptualized and implemented interdisciplinary and multi-organizational projects on key intelligence issues with leading thinkers from academia, business, strategy, and intelligence consultants.

In late 2005, the Partnership launched the Global Futures Forum (GFF) as a multinational, multidisciplinary intelligence community embracing intelligence, national security, and non-government experts to engage in strategic level, unclassified dialogue and research to better understand and anticipate transnational threats.[15] GFF members from more than 35 countries worked together in a number of topic-based communities of interest, including:

- terrorism and counterterrorism studies
- radicalization
- illicit trafficking
- proliferation
- foresight and warning
- practice and organization of intelligence
- social networks
- genocide prevention
- pandemics
- environment and resource challenges
- failed and failing states

GFF participants met in community of interest gatherings in the United States and abroad, in larger annual forums, and in a groundbreaking, unclassified, password-protected Web site that enables conversations begun in face-to-face meetings to continue around the clock and around the world. The last GFF plenary conference brought representatives from 40 countries together in Vancouver with the war in Iraq still raging. As another instance, the Community of Interest: Practice and Organization of Intelligence met in December 2008 in Antwerp on managing intelligence, and in Ottawa in March on cognitive issues.

14 David E. Kaplan, "Let's Play Ball", *U.S. News & World Report*, November 6, 2006.

15 See https://www.cia.gov/offices-of-cia/intelligence-analysis/organization-1/gfp.html

In mid-2008, however, the CIA pulled most funding from the GFF. GFF apparently fell afoul of two themes that have run through this paper. Its process of long-term relationship building looked interesting but unproductive for an analytic organization that gives pride of place to writing short, immediate items for the President's Daily Brief. If GFF looked aimless to the CIA's analysts, it looked threatening to the agency's operators, who feared it would intrude on their premier liaison relationships (with Canada and Britain, for instance) and who, to boot, thought they monopolized the agency's dealings with non-Americans. There is the hope that other U.S. agencies and other countries, like Canada, will pick up at least some of the GFF activities.

Systematic Debriefing of Willing Citizens. CIA case officers working in the National Resources (NR) Division, which has stations in major U.S. cities, routinely debrief, on a voluntary basis, U.S. business executives and others who work overseas. There are two defects with this arrangement. One is the reluctance some people still may have to deal with the CIA, still more the operations directorate where NR sits. Second, if the task is thought of as "collection," then it will be colored by a short-term, slightly predatory perspective. Instead of collection, the task should be thought of as facilitation or mediation: if I'm just back from Sakhalin Island, I don't want to be debriefed by an all-purpose interviewer but rather to share notes with the intelligence agency's expert on Sakhalin (and he or she should want my view directly, not in a report produced by a debriefer who is unknowledgeable about the subject).

Canada and other countries do better. Since 1953 Canada has been systematic in interviewing, first, immigrants from the Cold War's "denied areas," and more recently those of interest for more general reasons.[16] Originally part of the Department of National Defence, the Interview Program (IP) was transferred to the Department of External Affairs in 1968. For Canada, and for others, doing this through the foreign service or some other-than-intelligence agency makes sense.

Publications Targeted or Available to Outsiders. *Commentary* is published by the CSIS Intelligence Assessments Branch (IAB).[17] It provides unclassified information on current topics related to the security of Canada, and is written by strategic analysts and subject experts in the security intelligence field. The publication of *Commentary* is intended to provide a platform for public discourse on issues related to national security. The CIA's *Studies in Intelligence* contains articles mostly written by insiders and often classified, but it does

16 See Kurt F. Jensen, "Canada's Foreign Intelligence Interview Program, 1953-90," *Intelligence and National Security*, 19, 1 (2004), 95-104.

17 See http://www.csis-scrs.gc.ca/pblctns/cmmntr/index-eng.asp.

include articles written by outsiders, and selected editions are unclassified.

A related category of outreach (and "in reach") involves relations with outside academics designed to build long-term relationships, not produce much immediate information or analysis. For instance, the CIA's Center for the Study of Intelligence not only publishes *Studies in Intelligence* but also runs a program of academic relations.[18] It arranges for CIA historians who are invited to lecture on intelligence-related topics. Through the Officer in Residence Program, up to a dozen CIA officers teach intelligence-related courses at American colleges or universities for a two-year tour as visiting professors. Since the program started in 1985, CIA has sponsored officers at over 50 academic institutions, including Harvard, Princeton, Georgetown, University of South Carolina, University of Oregon, University of Kentucky, Texas A&M, Marquette University, Ohio State University and the military academies. CSI also holds conferences with outsiders, usually on specific historical episodes in intelligence – like the publication of declassified U.S. estimates on the Soviet Union – or about teaching intelligence in universities. The CIA and other U.S. agencies also do "in reach," inviting interested academics to work in the agency for a year or more.

Occasional Conferences. Many countries do these in one form or another, and at least two services, Canada's CSIS and Britain's MI-5 have in recent years created special focal points in the service for outreach. Indeed, one Canadian former official observed in an interview that demand may exceed supply, at least in Canada, with representatives from several services knocking on the same academic expert's door.

In the United States, many of the agencies, especially CIA but also DIA, INR and others, hold a variety of meetings, consultations and conferences with outsiders, usually closed but unclassified. Many of them still suffer from the mentality of "collection" mentioned earlier, but both the scope for and the nature of the meetings in changing. For instance, a decade ago the U.S. military's Transportation Command requested a National Intelligence Estimate (NIE) or similar paper on future humanitarian emergencies, on the simple logic that it would be the deliverer of assistance and thus might ask in advance whether likely hardship locales had airstrips or seaports. The people who knew most about this issue were not in intelligence but rather in CARE and the other humanitarian non-governmental organizations (NGOs). Despite their misgivings about government and intelligence, they all came to a conference, with short paper that in effect wrote the first draft of the estimate.

18 See https://www.cia.gov/library/center-for-the-study-of-intelligence/academic-relations/index.html

For Canada's CSIS, much of outreach is focused on local communities and so straddles the line between simply doing business and outreach. But the range is striking, as a few recent examples will suggest:

- November 7, 2005, Ottawa, Ontario –"Understanding Islam: Engaging Canadian Youth to Fight Extremism". Guest speakers included Mayor of the City of Ottawa, Parliamentary Secretary to the Minister of Public Safety, and senior government officials from Public Safety and its agencies. Teachers, students, youth organizations, religious leaders, community groups and citizens also participated in the dialogue.
- November 25-26, 2005, Regina, Saskatchewan – In conjunction with Muslims for Peace and Justice and the Muslim Students Association, organized a local community event called the 'National Security and the Canadian Mosaic.' Community leaders, students, and government officials participated in the event.
- February 5, 2006, Fredericton, New Brunswick – Day-long meeting called 'Atlantic Regional Symposium: Engaging Canadian Society in Keeping Canada Safe.' Participants of the symposium included members of various ethno-cultural communities, the public at large, academia and government officials from Public Safety, RCMP, CSIS, the Canadian Border Services Agency (CBSA), Justice and Canadian Heritage. The regional symposium also drew youth participants from across the Atlantic Provinces. See the Atlantic Provinces Report (PDF 9KB)
- March 18, 2006, Calgary, Alberta – Half-day local community event called 'National Security is Everyone's Concern'. Representatives from Calgary's ethno-cultural communities, along with government officials from Public Safety, RCMP, CSIS, CBSA and the Department of Justice participated in the event. See their Security Report (PDF 9KB).
- May 28, 2006, Edmonton, Alberta – In conjunction with the Edmonton Council of Muslim Communities, Edmonton Interfaith Centre for Education, and Action and Northern Alberta Alliance on Race Relations, hosted the 'Symposium on Security and Civil Liberties.' Members of Edmonton's ethno-cultural communities and government officials from Public Safety, RCMP, CSIS, CBSA, and Justice participated in the half-day local community event.

Use of Web Sites. A survey of various intelligence service web sites is summarized in appendix A. Not surprisingly, the range is wide and none is very venturesome, as suggested above. The FBI site provides an opportunity to provide tips, particular about crime, and most of the other domestic services do provide tip lines or other ways of getting in touch with the agency. The DIA site is more

venturesome is providing opportunities for interaction.[19]

While these forms of outreach – or better, external engagement – are suggestive, they just begin to scratch the surface of what can be possible. If intelligence services are to meet the challenge of transnational threats, like terrorists, they will have to both collect more information on private citizens at home and reach out to those citizens as collaborators. The latter means interacting with society in dramatic new ways. It means opening up.

19 For an interesting discussion of possible private-public cooperation against cyberterrorism, see Peter R. J. Trim, "Public and Private Sector Cooperation in Counteracting Cyberterrorism," *International Journal of Intelligence and CounterIntelligence*,16:4 (2003), 594-608.

Appendix A

Organization	Web Site	Information Exchange	Articles	Comments
USA				
CIA Central Intelligence Agency	https://www.cia.gov/index.html	• Doesn't have public interfaces to receive information from the public. • Shares some internal products with the public. • By phone: through contact points at each division.	Strategic Investment Plan for Intelligence Community Analysis (To see it: https://www.cia.gov/library/reports/general-reports-1/unclass_sip/index.html)	The CIA has the "Iraqi Rewards Program", which could mean a flow of information from the public. (See: https://www.cia.gov/about-cia/iraqi-rewards-program.html)
NSA National Security Agency	http://www.nsa.gov/home.cfm			
FBI Federal Bureau of Investigation	http://www.fbi.gov/	• Invites the public to provide tips and information about most wanted criminals and ways to prevent economic espionage.		The FBI provides tips to the private sector on how to avoid economic espionage. See: http://www.fbi.gov/hq/ci/economic.htm Also asks for tips regarding most wanted criminals and other threats: https://tips.fbi.gov/
NIC National Intelligence Council	http://www.dni.gov/nic/NIC_home.html	• Doesn't have public interfaces to receive information from the public. • Shares some internal products with the public. • By phone: "Global Expertise Reserve Program" contact point.	http://carapace.weblogs.us/archives/492	The NIC has an outreach mechanism called "GlobalExpertiseReserve Program" whose mission is to make contact with thematic experts to improve the scenarios and expand the intelligence coverage. (See: http://www.dni.gov/nic/NIC_associates.html)
DIA Defense Intelligence Agency	http://www.dia.mil	• The "terrorist recognition cards" program is used by the DIA as a strategy to collect information about the individuals fixed in cards. The outreach is based on public request of information, which could be rendered to justice, defense and diplomatic agencies. • Has public interface to receive information from the public. (See at: https://www.rewardsforjustice.net/index.cfm?page=tip&language=english)		http://www.dia.mil/site6_images/cards/index.htm

Organization	Web Site	Information Exchange	Articles	Comments
INR Bureau of Intelligence and Research	http://www.state.gov/s/inr/	• Doesn't have public interfaces to receive information from the public.		The web site has only basic information.
CANADA				
CSIS	http://www.csis-scrs.gc.ca/index-eng.asp	• Four programs without an active interface Information exchange by phone and email. – Liaison/Awareness Program – Public Liaison and Outreach Program – Media Relations Program – Cross-cultural Roundtable on Security • National Security Tip Line (Phone line)	• http://ww2.ps-sp.gc.ca/publications/backgrounders/2005/20050711_e.asp • http://www.dominionpaper.ca/articles/1119 • http://www.militantislammonitor.org/article/id/1993 • http://www.fas.org/sgp/bulletin/sec63.html	
CSEC	http://www.cse-cst.gc.ca/index-e.html	• IT Security Program • Without an active interface. • Information exchange by phone and email.	• http://www.carleton.ca/cciss/outreach.htm	Working in partnership with departments, agencies and the private industry, CSEC's focus is on shaping new IT products, services and service strategies that directly align with Government of Canada operational needs and priorities – to ensure critical information systems are secure.
OTHER FOREIGN SERVICES				
ASIS Australian Secret Intelligence Service	http://www.asis.gov.au/index.html	• Doesn't have public interfaces to receive information from the public. • Doesn't share internal products with the public. • Public exchange only for recruitment		The web site is designed only to give background to citizens about the org and their mission. Also plays an important role as a means of enrolment.
ASIO Australian Security Intelligence Organisation	http://www.asio.gov.au/	• Business Liaison Unit. The BLU administers a secure, password access website for business users. http://www.asio.gov.au/About/Content/blu.aspx	• http://www.hsaj.org/?fullarticle=3.2.2 • http://www.asio.gov.au/Publications/Content/CurrentAnnualReport/Content/Cover.aspx	"ASIO's statutory responsibilities are outlined in the ASIO Act of 1979. Although Australia is similar to the United Kingdom, there is a greater distinction between executive and legislative oversight roles. The Intelligence Services Act of 2001 expanded the role of the Parliamentary Joint Committee on Intelligence and Security in overseeing Australia's intelligence apparatus.

Organization	Web Site	Information Exchange	Articles	Comments
		• Protective security and T4. A division specialized in technical security measures to protect government and, by authorization, private sector companies or individuals. http://www.asio.gov.au/Work/Content/ProtectiveSecurity.aspx • The T4 service is typically for governmental agencies, but the Attorney General would authorize to provide advice about technical measures for security to private sector companies or individuals. • Non-public interface for share security reports with private associates.		64 The committee can initiate investigations or respond to requests from the Attorney General. 65 Australia's executive oversight is also more robust. The Inspector General of Intelligence and Security (IGIS) is an independent officer appointed by the Governor-General and located within the prime minister's office. This unique arrangement allows the IGIS to assist the government and parliament in oversight matters, but allows the office to act independently. The IGIS also enjoys total access to all intelligence and possesses the power of independent inquiry. 66 This oversight also includes access to case files, warrant powers, and financial records.
				Although not a method of oversight, the Australian government also has an aggressive public outreach program. The federal government has established National Security Public Information Guidelines for all agencies engaged in national security issues to promote the public's understanding of the missions and threat. A National Security Public Information Campaign also seeks to encourage public vigilance. Security information is pushed via a variety of media to inform the Australian public of the government's efforts against terrorism and to create a safer environment.

Organization	Web Site	Information Exchange	Articles	Comments
				67 These efforts directly support ASIO's efforts in engaging communities to derive community-based information conduits to support its assessments. This is in stark contrast to MI5's historical outlook regarding public engagement, which took the major step of instituting a public website only after 9/11. 68 Despite these strong oversight mechanisms, ASIO has also been criticized for heavy-handed and intrusive tactics in the past against leftwing groups. 69"[20]
MI-5 The Security Service	http://www.mi5.gov.uk/	• The "How You Can Help" site is an effort to bring citizens the available options to give them info about threats. • Share internal products with the public (Business) through the "Centre for the Protection of National Infrastructure". • To give information: Anti-Terrorist Hotline number. • Has public interface to receive information from the public. See at: https://www.mi5.gov.uk/output/Page18.html o http://www.cpni.gov.uk/aboutcpni188.aspx		
MI-6 Secret Intelligence Service SIS	http://www.mi6.gov.uk/output/sis-home-welcome.html	• Doesn't have public interfaces to receive information from the public. • Doesn't share internal products with the public. • Public exchange only for recruitment		If a citizen wants to share information with SIS, should use the MI-5 mechanisms.
DGSE Direction générale de la sécurité extérieure	http://www.defense.gouv.fr/dgse	• Don't have public interfaces to receive information from the public. • Don't share internal products with the public. • Collect information from the public by mail.		The DGSE outreach is not public. The agency process information brought by "honorables correspondants" (clearance people who collaborate with the agency

20 http://www.hsaj.org/?fullarticle=3.2.2

Organization	Web Site	Information Exchange	Articles	Comments
DRI Direction centrale du renseignement intérieur		• Without Web Site		This new French agency (Jul, 08) is responsible for internal intelligence and counter terrorism. Absorbed the DST. Outreach about counter terrorism in France from "La France face au terrorisme"[21]: "• The first level of contact: the police station or the gendarmerie brigade (for any report or even in case of doubt) or the diplomatic and consular service for French people abroad; • For public services or private companies having already developed sectoral links at the regional level: one of the zonal directorates or territorial brigades in the Direction de la Surveillance du Territoire (Territorial Surveillance Directorate, DST), the Direction de la Protection et de la Sécurité de la Défense (Defence Protection and Security Directorate, DPSD), the gendarmerie, or, as appropriate the regional centres in the fight against radical Islamism, in each regional directorate of the Renseignements Généraux (Central Directorate of General Intelligence, DCRG). • For specific economic or administrative sectors: direct contact with the DST, the DCRG, the DPSD or the gendarmerie"
CESID Centro Superior de Información de la Defensa		• Without Web Site	• http://www.globalsecurity.org/intell/world/spain/cesid.htm	

21 http://lesrapports.ladocumentationfrancaise.fr/BRP/064000275/0000.pdf

Organization	Web Site	Information Exchange	Articles	Comments
CNI Centro Nacional de Inteligencia	https://www.cni.es/00/00_index.cfm	• Don't have public interfaces to receive information from the public. • Don't share internal products with the public.		If a citizen wants to share information with the Spanish government should make contact through the National police – have a public interface to brought information about terrorism. The Guardia Civil shares information about security tips with citizens, but don't have any special interface to exchange information. See: http://www.policia.es/linea/denu_sp.htm?reload_coolmenus http://www.guardiacivil.org/consejos/index.jsp