No More Secrets:

National Security Strategies for a Transparent World

Report

March 2011

American Bar Association Standing Committee
on Law and National Security

Office of the National Counterintelligence Executive

National Strategy Forum

American Bar Association Standing Committee on Law and National Security

The Standing Committee on Law and National Security, since 1962, has sustained an unwavering commitment to educating the Bar and the public on the importance of the rule of law in preserving the freedoms of democracy and our national security. Founded by five farsighted individuals, among them Chicago lawyer Morris I. Leibman and then ABA President and later Supreme Court Justice Lewis F. Powell, the Standing Committee focuses on legal aspects of national security with particular attention in recent years to the issues raised by legal responses to terrorist events. The Committee conducts studies, sponsors programs and conferences, and administers working groups on law and national security related issues. Its activities assist policymakers, educate lawyers, the media and the public, and enable the Committee to make recommendations to the ABA. It is assisted by an Advisory Committee, Counselors to the Committee, and liaisons from ABA entities. For more information, visit www.abanet.org/natsecurity.

Office of the National Counterintelligence Executive

The Office of the National Counterintelligence Executive (ONCIX) is part of the Office of the Director of National Intelligence and is staffed by senior counterintelligence (CI) and other specialists from across the national intelligence and security communities. The ONCIX develops, coordinates, and produces: annual foreign intelligence threat assessments and other analytic CI products; an annual national CI strategy for the U.S. government; priorities for CI collection, investigations, and operations; CI program budgets and evaluations that reflect strategic priorities; in-depth espionage damage assessments; and CI awareness, outreach, and training standards policies. For more information on the Office of National Counterintelligence Executive, visit www.ncix.gov.

The National Strategy Forum

Since 1983, the National Strategy Forum, a nonprofit, nonpartisan think tank in Chicago, Illinois, has focused on the issues and trends affecting US national security strategy. The NSF's principal mission is to enhance the public's understanding of national security related topics through a monthly lecture series and the National Strategy Forum Review, a thematic quarterly journal. In addition to its public education programs, the NSF also conducts conferences on various subjects related to national security, including homeland defense, counterterrorism, nuclear nonproliferation, catastrophe preparedness and response, and international relations. Post conference reports, issues of the National Strategy Forum Review, and more are available at www.nationalstrategy.com.

Workshop Convener
Suzanne E. Spaulding

Report written by Alane Kochems

Disclaimer:

The "No More Secrets: National Security Strategies for a Transparent World" Workshop was not for attribution. The materials contained herein represent the opinions of the discussants and do not reflect the official policy of their respective agencies, private sector organizations, or any entity of the United States government. The materials do not represent the policy position of the Office of the National Counterintelligence Executive or the American Bar Association or the Standing Committee on Law and National Security. These materials and any forms and agreements or views herein are intended for educational and informational purposes only, and imagine a world where technological intrusion coupled with insider threats has threatened the ability for secure communications. This discussion was based on this hypothetical situation and is intended to help spark discussions to assist policymakers, educate lawyers, the media and the public.

ISBN: 978-1-61632-878-8 (pbk.)

ISBN: 978-1-61632-879-5 (pdf.)

No More Secrets: National Security Strategies for a Transparent World

Post Workshop Report –March 2011

Table of Contents

Introduction

Individuals, organizations, and governments are far more interconnected now than ever before. Technology and its impact on social, economic, and government behavior is bringing ever greater transparency and raising exponentially the cost and difficulty of keeping information secret. Social networking media, Web 2.0[1], new technology, and laws protecting personally identifiable information all exemplify a world of increasing transparency and complexity. There are significant implications for governments, businesses, and individuals living and operating in a world without secrets. The US national security community, in particular, faces tremendous challenges as it considers a world in which its competitors and adversaries are likely to have access to much, or even most, of its information.

There is a shadow race between those trying to keep information secret and those seeking that information – and the seekers are rapidly gaining the upper hand. The U.S. government and the private sector must be sufficiently nimble and adaptive to the tsunami wave of information that is available to adversaries and competitors at every level, including state and non-state actors. The nature and scale of this challenge calls for a careful assessment of the U.S. government's traditional approach to counterintelligence and its dependence on secrecy as the key to gaining and maintaining a competitive advantage. The United States may be approaching a time when there will be virtually "no secrets." How can the United States adjust to survive and thrive in an increasingly transparent world?

The United States may be approaching a time when there will be virtually "no secrets." How can the United States adjust to survive and thrive in an increasingly transparent world?

[1]For an explanation of the concept, see Tim O'Reilly, "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software," Sept. 30, 2005, available at http://www.oreillynet.com/lpt/a/6228 (last viewed 7/12/10).

[2] See, e.g., the recent theft of approximately 260,000 documents and cables from the State Department. Kevin Coleman, "Those 260,000 Stolen Documents from the State Dept.," July 7, 2010, available at http://defensetech.org/2010/07/07/those-260000-stolen-documents-from-the-state-dept/ (last viewed 7/7/10).

The most damaging threat to both government and the private sector has traditionally been from insiders stealing information for personal use or for sale to the highest bidder. As malefide actors take greater advantage of advancing cyber capabilities and better technology, the insider threat only becomes more dangerous. Ames and Hanssen did significant damage to the United States. However, with today's technologies, they could have removed gigabytes of information rather than hundreds of pages.[2] The recent WikiLeaks releases of over 70,000 Afghan war documents, nearly 400,000 from the Iraq war, and over 250,000 State Department cables from all over the world provide dramatic evidence of the problem's scope. [3]

Technology has outraced the country's defensive posture. As the price for protecting secrets increases, both in terms of resources required and opportunity costs incurred, individuals, companies, and governments will need to determine what information is so vital that they must protect it. The U.S. government wishes to protect serious national security information, protocols, and proprietary information. However, in addition to the practical obstacles alluded to earlier, it faces legal, moral, and ethical constraints on its defensive actions that many of its adversaries do not. Going forward, the government and private sector will need to develop thoughtful strategies and policies to address these issues if they are going to retain their competitive advantages.

To that end, the American Bar Association Standing Committee on Law and National Security, the Office of the National Counterintelligence Executive (ONCIX), and the National Strategy Forum sponsored a one day workshop in Washington, DC, on June 29, 2010. The workshop brought together over two dozen members of academia, government, and the private sector to discuss whether the world is rapidly approaching a time when secrets no longer exist and how the government might prepare for and function in such circumstances. The workshop focused on the national security context but many of the issues discussed are also relevant for other government functions, as well as businesses and individuals. The discussion occurred under Chatham House Rules – participants' comments were for the public record, but comments were not for attribution.

The workshop report you are now reading is the result of that discussion.[4]

---

[3] Bridget Johnson, "WikiLeaks: Rest of War Documents To Be Released in a Few Weeks," Aug. 14, 2010, available at http://thehill.com/blogs/blog-briefing-room/news/114279-wikileaks-rest-of-afghanistan-documents-to-be-released-in-a-few-weeks (last visited 8/17/10). Iraq documents: http://www.nytimes.com/2010/10/23/world/middleeast/23intro.html . State Department cables: http://www.guardian.co.uk/media/wikileaks (last visited December 2, 2010).

[4] The workshop was not designed to produce a consensus on the issues. This report, therefore, is intended as a summary and should not be taken as reflecting the views of any individual participant, the ABA, the ONCIX, or the National Strategy Forum.

Chapter 1: Examining the Premise

Intellipedia Doyen Don Burke stated at a conference in 2008 that "[i]n 15 years, there will be no more secrets." [5] Burke made this prediction in the context of discussing the wealth of information already available through unclassified sources. This provocative statement became the seed that two years later led to this discussion of how the United States, specifically the Intelligence Community (IC), would address national security issues in a completely transparent world. The workshop attendees first examined the likelihood that the IC would be operating in a completely, or nearly, transparent environment by 2023.

An assumption underpinning Burke's statement is that the world is currently in a period of punctuated equilibrium. These periods occur when an organism undergoes minimal evolutionary change for geologic time periods interrupted by short periods (i.e., within a single organism's lifespan) of incredibly rapid change.[6] Such periods of rapid change can alter the world order. Even if the world is not in a period of punctuated equilibrium, it continues to increase in complexity and connectivity, a byproduct of which is access to incredible quantities of information and data.

As humans developed through history, they relied on oral traditions, and later, written methods, for retaining important information. Significant resource costs limited what humans would record using these methods. For instance, early humans used songs to recall their origin stories. As they moved to writing, they kept more information such as census data and tax rolls. It is only with the advent of computers with their rapidly increasing, inexpensive storage capacity that humans have been able to store large quantities of data with minimal thought to cost. Even 50 years ago, a person traveling in a foreign country would be fairly cut off from family, friends, and co-workers left at home. The traveler might send a letter using international air mail but the cost to send such a letter would ensure that the traveler only included the most pertinent details and mailed only a few letters. Now, with the Internet and other communication technology, travelers remain connected regardless of where they are. In fact, not having a digital trail is a red flag when crossing international borders.

[5] Suzanne E. Spaulding, "No More Secrets: Then What?", blog entry for June 24, 2010, available at http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html (last viewed 7/16/10).

[6] Stephen Jay Gould and Niles Eldredge, "Punctuated equilibria: the tempo and mode of evolution considered," Paleobiology, vol. 3, No. 2, Spring 1977, p. 115, available at http://www.nileseldredge.com/pdf_files/Punctuated_Equilibria_Gould_Eldredge_1977.pdf (last viewed 7/16/10).

Fewer resource constraints and ease of recording and storage have led to people capturing and saving ever greater amounts of data and keeping it indefinitely. Furthermore, there is more data available now for people to gather. Google's CEO recently observed that "Every two days, we now create as much information as we did from the dawn of civilization up until 2003."[7] The Intelligence Community, like society at large, has been collecting and storing all the data and information it believes useful in achieving its missions. However, because of the Community's nature, the IC has protected most of its information through classification. If the world is becoming increasingly transparent, the IC will have an increasingly difficult time protecting that classified material.

The national security community traditionally relies upon information monopoly providing it with strategic advantage. This assumes that that the government has information that its competitors or adversaries do not. Given the ubiquity of information in open sources, the irresistible benefits that come from networking information, and the vulnerability of cyberspace, this assumption should be seriously challenged inside and outside of government. It is increasingly likely that others will have the same information, either because they have stolen it from you or because they have been able to develop it independently.

As secrecy's price increases, organizations will have to calculate which secrets are so sensitive that protection outweighs the efficiency advantages of sharing and collaborating.

With organizations and governments able to keep fewer secrets, they must change how they act if they want to remain competitive. Assuming that a document or piece of information remains secret, and acting based on that assumption, has become more dangerous. Already there have been public reports of adversaries penetrating classified defense networks and waging cyber attacks.[8] A major impediment to the U.S. government changing its assumptions about the security of its classified networks is the great difficulty of writing policies and procedures on how to act when an adversary could conceivably know any and all supposedly classified information – including the policies.

[7] Stacy Cowley, "Unprofitable Demand Media Files for IPO," CNNMoney.com, Aug. 8, 2010, available at http://money.cnn.com/2010/08/06/technology/demand_media_ipo/ (last viewed 8/18/10).

[8] E.g., Julian E. Barnes, "Pentagon Computer Networks Attacked," Nov. 28, 2008, Los Angeles Times, available at http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28 (last viewed 7/16/10). See also Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, Aug. 21, 2007, available at http://www.wired.com/politics/security/magazine/15-09/ff_estonia (last viewed7/16/10).

Individuals, businesses, and governments are also deciding that connectedness and information access provide greater benefits than secrecy. There are often strong business reasons for sharing information and collaborating (e.g., efficiency) that outweigh the advantages of keeping information locked away and work stovepiped. As secrecy's price increases, organizations will have to calculate which secrets are so sensitive that protection outweighs the efficiency advantages of sharing and collaborating. There is already evidence that organizations are doing such calculations and choosing sharing over stovepiping. For instance, Eli Lilly has opened an e-research subsidiary to harness the expertise and work of thousands of researchers because the company determined it was more cost effective to have many minds working on the project than trying to protect research developed by a small, isolated group.[9] Another example is a group of scientists who gave computer gamers the opportunity to assist with optimizing protein structures via a computer game.[10]

The working group participants generally concluded that efforts to keep secrets are unlikely to completely cease as long as there is an economic incentive to maintain them, but conceded that the remaining secrets will be challenging to keep for any length of time. Increased transparency will likely force governments and businesses to expend significant resources to protect their most sensitive information and to use that information rapidly while it still can provide them with an advantage.

[9] BW Healthwire, "e.Lilly Announces Plans to Launch New Startup; InnoCentive Introduces Novel Approach to Drug Discovery Using the Internet," Jun. 28, 2001, available at http://www.thefreelibrary.com/e.Lilly+Announces+Plans+to+Launch+New+Startup%3B+InnoCentive+Introduces...-a075992581 (last viewed 7/16/2010).
[10] John Timmer, "Gamers Beat Algorithms at Finding Protein Structures," ars technica, last updated Aug. 4, 2010, available at http://arstechnica.com/science/news/2010/08/gamers-beat-algorithms-for-finding-protein-structures.ars (last viewed 8/5/10).

Chapter 2: "Secrets" Today

The working group discussed several different ways to define today's "secrets." There was some consensus that how one defines the concept will radically affect the way one classifies, uses, and protects critical information.

One participant suggested that the U.S. government primarily classifies information to protect sources and methods. However, it may also classify information:

(1)because the information indicates that the government is thinking about certain topics and that interest could indicate policy directions; [this is part of "sources and methods"]
(2) in order to exploit the information;
(3) in order to use a technical capability to collate and make something from it; or
(4) to have information to trade or to use with others to create something.

Operating in a classified environment seriously constrains how and with whom the Intelligence Community conducts business. For instance, if there were a high-tech instrument that could determine the presence of trace amounts of radioactive material at a great distance, some in the federal government would almost certainly want to classify that information. However, that classification does not necessarily make the United States safer. In some situations, it might be better to share that information and instrument with allies and in other situations it might be best to tell the entire world that the United States has that kind of technology as a deterrent. There is little analysis currently on the costs and benefits of classifying particular information and that will likely need to change in the future.

The working group then discussed alternative definitions of secrets. One could consider secrets to be information asymmetries. The national security community has been thinking about asymmetric warfare for years. Secrets would become one more possible asymmetry to exploit. From this perspective, a secret is merely something that one actor knows when others do not, which allows the knowledgeable actor to behave differently because of the known information. Another, related, view is to consider secrets to represent decision advantages. Secrecy includes both absolute and competitive advantages; it involves protecting both an entity's strengths and its weaknesses.

Regardless of how one defines "secret," that secret has a limited time value. When it took years to master a process or to build a weapon system, it was necessary to protect the relevant information for years. As some activities have become easier, the related information often becomes irrelevant in the span of seconds to months. Unfortunately, the U.S. government has retained the idea that it must protect all of its sensitive information for as long as possible even though much of the information is rapidly losing its value. With the short half-life of information, it becomes necessary to guard that decision advantage only long enough to use it. Once the decision advantage expires, the government (or business) can then redirect its finite resources to protect other critical information. However, some participants cautioned that in 2010, most organizations cannot accurately identify what critical information will give them a decision advantage in 2016.

The U.S. government is having problems appropriately handling, storing, managing, and sharing classified information. Controlled unclassified information further muddles the situation; the federal government has over 107 unique markings and 130 different labeling or handling procedures for data it considers sensitive but unclassified.[11] It is becoming increasingly difficult for people to understand what should be classified and at what level. Moreover, the amount of information collected is growing significantly. Since there are disincentives for not collecting information but few for over-collecting, one can understand how the U.S. government arrived at the current situation. No government agency wants to testify before Congress on why it lacked critical information during a disaster or crisis. With a default of classifying information and long retention times, the U.S. government faces the growing burden of protecting its ever-expanding cache of sensitive information.

Regardless of how one defines "secret," that secret has a limited time value.

In preparation for increased difficulty in keeping secrets, some participants argued that the U.S. government should de-incentivize classifying information. It should no longer be easier, or considered "safer," to classify something than to keep it unclassified. In addition to having a strong reason for classifying information, one member suggested a few ways to minimize overclassification such as (1) incorporating into performance evaluations whether an individual is classifying information properly, and (2) having periodic audits of documents to ensure that classifiers list real, specific reasons for classifying something. (Other participants disagreed with the latter suggestion as being excessively bureaucratic and ineffective.) Classification guidance needs to take into

[11] "About CUI," n.d., available at http://www.archives.gov/cui/ (last visited 7/27/10).

account the full costs of classifying information.

There is a real risk that the Intelligence Community is squandering its resources attempting to keep non-secrets secret. There is a false presumption that classified resources provide higher quality and more data than open source ones. By using open source tools first, the IC would better grasp what information is already within the public sphere (and, thus, easily accessible by its competitors and adversaries) and spend less effort, risk, time, and money using classified sources when they are unnecessary. One participant noted that the Netherlands has a law which requires its intelligence agencies to exhaust all open sources of information before using classified ones. Some participants cautioned that privacy advocates may object to open source intelligence gathering as a privacy invasion. Others warned that even when data comes from unclassified sources, the government could classify it, but should do so only if it is reasonable to conclude that others do not have the same information—which one participant emphasized would rarely be the case for open source data— and only for the length of time that monopoly is likely to last and the information remains useful.

To remain competitive in a more transparent environment, governments must make some hard decisions about what they absolutely must keep secret and for how long – and at what cost.

When considering what information is already in the public realm, it is important to recognize the limitations of "anonymization." With greater computing power now available, releasing incomplete information or redacted data can still provide adversaries or competitors with a wealth of intelligence. [12] In the last few years, organizations have released what they believed to be redacted data only to have outsiders quickly tag the data to specific individuals.[13] For instance, while Twitter and flickr only have a 15 percent overlap in users, both networks can be de-anonymized with only a 12 percent error rate.[14] This makes opens source intelligence (OSINT) a valuable tool for the U.S. government and its competitors.

[12] E.g., BJS, "Data Sorting World Record: 1 Terabyte, 1 Minute," July 27, 2010, available at http://scienceblog.com/36957/data-sorting-world-record-falls-computer-scientists-break-terabyte-sort-barrier-in-60-seconds/ (last viewed 7/27/10).

[13] E.g., by using only gender, zip code, and birth date, a Carnegie Mellon researcher identified William Weld, a Massachusetts governor in the 1990s. Seth Schoen, "What Information Is 'Personally Identifiable'?" Electronic Frontier Foundation, 9/11/2009, available at http://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable (last viewed 7/16/10).

[14] Arvind Narayanan and Vitaly Shmatikov, "De-anonymizing Social Networks," n.p., n.d., available at http://userweb.cs.utexas.edu/~shmat/shmat_oak09.pdf (last viewed 7/16/10).

Determining what information is a crown jewel or creates a decision advantage is not a theoretical task. The United States has been increasingly fighting wars as part of international coalitions, which requires it to share information with its partners. For instance, in Afghanistan, some service members have been sharing information using mobile phones, computers, and other electronic devices over the local internet service provider's network. This has led to a difficult counterintelligence issue. Using smart personal digital equipment on the battlefield to share information with others across public service providers leads to an immediate tactical advantage; however, it may cause a strategic loss if enemies monitor those public pathways and then train based on the information gathered. The United States must recognize the difficulty of keeping this information secret and develop strategies based on that understanding. To remain competitive in a more transparent environment, governments must make some hard decisions about what they absolutely must keep secret and for how long – and at what cost.

Chapter 3: Strategies for Prevailing in an Increasingly Transparent World

There was a general consensus among workshop participants that while we will never reach a point at which there are no secrets, the world is becoming increasingly transparent and governments need to learn to operate with far fewer secrets. While the participants generally agreed that the Intelligence Community needs to define its vital secrets, members offered different ways to do that. The IC might consider any information that provides a competitive advantage or decision advantage as a secret. If it were to adopt such a definition, then it would need to maximize the advantages provided while minimizing any penalties for keeping secrets. Often information that offers a decision advantage is only worth protecting for a limited time since others can often generate the same information given sufficient time. For the IC, secrets will have varying half-lives depending in part on how the government plans to use them. Different secrets will produce different protection and use requirements.

Another way to evaluate the IC's current body of secrets is to separate the true "crown jewels" that are critical to the security of the country. Every data point or bit of information cannot be considered a crown jewel if the Community intends to protect truly vital information. If everything is a tightly held secret, then nothing is. Maintaining the current default that everything should be considered secret is becoming (if not already is) dangerous and impractical. The U.S. government should evaluate whether its data is (1) critical for it but useless to anyone else (e.g., internal process documents); or (2) valuable to it and to its adversaries/competitors (e.g., weapons technology secrets, sensitive intelligence gathering collection methods, sources, and tools. Knowing whether to keep information and whether others have an interest in such information allows the federal government to appropriately assign resources to protect the most important information that it reasonably believes its competitors do not have and that they would find valuable. One participant suggested that the U.S. government should only protect two types of information: (1) decision advantages and (2) anything that puts agents at risk. Ultimately, it was suggested, the government needs to do a careful cost/benefit analysis before deciding to treat something as a secret.

Some in the business community are already responding to the increasing transparency by reducing their secrets and sharing more information to enhance innovation. For example, Eli Lilly has turned to thousands

of researchers outside the corporation to help it solve some its most difficult challenges. It relies on creative uses of patents and licenses, rather than secrecy, to ensure appropriate return on investment. In contrast, Google relies on trade secrets law to protect its algorithms because it believes it would have a harder time proving patent infringement.

Currently, the IC has multiple business lines, including: (1) collecting data; (2) analyzing data; (3) specialized journalism; and (4) handling, transferring, and storing massive amounts of information. Each of these business lines requires different priorities and has different critical data that the managers believe they must guard. As protecting secrets becomes more arduous and resource intensive, the Intelligence Community must determine what its core business is, which will then help it define its critical information.

The Intelligence Community must find ways to adapt to an environment where speed in using decision advantages trumps secrecy

If the Intelligence Community's goal is to find and acquire secrets, then the IC must determine what secrets will be useful to decision makers tomorrow and what it will need to retain for decision makers' use in 5-10 years – as well as what does not need to be retained. For instance, knowing someone's social network provides one with a lot of data but one still must have the capability to turn that data into information and then act on the generated information. In some cases, the capability may not yet exist. The inclination, then, may be to retain vast amounts of data in case it might prove useful in the future. However, this increases the risk that the data will be compromised or misused. Since analysts attempt to extract intelligence about future actions from past data, understanding what information might be useful and when, and what the costs are of retaining information, should help guide the IC's collection policies and its valuation of secrets.

The Intelligence Community must find ways to adapt to an environment where speed in using decision advantages trumps secrecy. To that end, the Intelligence Community will have limited resources and will have to carefully choose its business lines. For instance, creating covers for spies has become much more expensive since any piece of information is identifiable.[15] It is likely that in the future the IC will use covers less frequently and expend more resources creating deeper covers or non-official covers[16].

[15] "Spycraft: A tide turns," July 15, 2010, available at http://www.economist.com/node/16590867/ (last viewed 7/28/10).

[16] Non-official cover is a term used to describe an intelligence operative who assumes a covert position that does not have ties to the government for which the individual works.

The participants discussed different security approaches for protecting truly sensitive information. For years the federal government (and organizations) have approached protecting secrets from a perimeter-based, physical security perspective: guards, guns, walls, specially compartmentalized information facilities, etc. For instance, on sensitive projects, governments or corporations may ban the use of unauthorized thumb drives, CDs, or other storage devices to prevent employees from using such devices to steal sensitive data. However, by emphasizing perimeter-based physical security, organizations ignore that the human brain is essentially a storage container which can pass through such measures. Instead of trying, and failing, to prevent access, organizations should architect their security systems as if malefide actors are already present in their systems.

Another security approach would be for the U.S. government to use a public health model to protect its secrets. As connectivity increases, the world starts to look more like an organism. The greater the resemblance, the better the chance is that an immune response approach would succeed, with sensors able to detect "pathogens" that threaten the system and counter them. Biomedical models deal with threats through barriers, resiliency to attacks, and recovery rather than attempting to stop all threats at a border. Such models can provide a framework for treating known threats by engaging in surveillance, swarming resources to infection sites, and quarantining as necessary.[17] Recovery and resilience form part of a defensive strategy since the very difficulty in succeeding with a crippling blow becomes a disincentive for attacking.

The participants also recognized the value of open source intelligence (OSINT) in an increasingly transparent world. Concern was expressed that while the IC has been talking a lot about OSINT, the leadership has not supported it. To function effectively in a transparent world, the IC will need to move from talking about OSINT to championing it. Such support might include modifying IC members' authorizing statutes which presume classified collection methods and altering funding streams to give greater resources to OSINT efforts. Since OSINT also tends to generate privacy concerns, at least one participant advocated for internal audits at high levels.

Somewhat related to conducting more OSINT, some working group members criticized the government's default of classifying information. In preparation for increased difficulty in keeping secrets, some members

[17] For more information, please see the recommended readings in the appendix.

[18] Congress recently enacted legislation that includes requirements similar to those recommended. See H.R. 553, The Reducing Overclassification Act, authored by Rep. Jane Harman (California), September 2010: http://www.whitehouse.gov/blog/2010/10/07/president-signs-hr-553-reducing-over-classification-act http://www.fas.org/sgp/congress/2010/overclass.html

argued that the U.S. Government should de-incentivize classifying information. It should no longer be easier to classify something than to keep it unclassified. In addition to having a strong reason for classifying information, one member suggested a few ways to minimize over classification such as (1) incorporating classification frequency into performance evaluations and (2) having the Inspector General review documents to ensure that classifiers list real, specific reasons for classifying something.[18]

From a training and organizational culture standpoint, the group discussed the tendency of younger members to readily share information without necessarily considering the security risks. The Intelligence Community and U.S. military need to train and educate staff regarding the costs and benefits of sharing information and when it is appropriate to collaborate and share. At the same time, these organizations have to work against an entrenched culture of compartmentalizing information, stovepiping, and overclassification.

The group also discussed efforts within the Intelligence Community to build a social media capability, which allows IC members to work in a different way. A major part of functioning in a world with minimal secrets is transitioning to work processes that allow people to contribute in multiple ways in discussions about which they have knowledge or expertise. These individuals have used a three-pronged strategy to measure return on investment: measure the collaborative environment by (1) vibrancy, (2) social communication (productive, good information exchanges), and (3) relevance to missions. Some working group members believed that the IC should create incentives for those activities where mission value increases in relation to vibrancy and social communication and brings about better outcomes. Some suggested incentives include pay and promotions based on the return on investment measures.

The participants also discussed secrecy in the context of information sharing with allies or state, local, or tribal law enforcement. A group member suggested that the U.S. government should develop the capacity for selective secrecy. It may need strategic secrecy regarding where decision makers are and who are the country's allies and competitors on any given issue at any given time. However, the federal government also needs to develop localized secrecy policies and practices which might allow the IC to share critical decision advantages with state, local, tribal, territorial, and private sector parties.

[19] E.g., see Steven Kotler, "Vision Quest: A Half Century of Artificial Sight Research Has Succeeded. And Now a Blind Man Can See," Wired, September 2002, available at http://www.wired.com/wired/archive/10.09/vision.html (last viewed 7/27/10) or Gary Wolf, "Futurist Ray Kurzweil Pulls Out All the Stops (and Pills) to Live to Witness the Singularity," Wired, Mar. 24, 2008, available at http://www.wired.com/medtech/drugs/magazine/16-04/ff_kurzweil?currentPage=all (last viewed 7/27/10).

Some also noted that with the world's current level of connectedness and recent advances in technology, the boundary between biology and silicon is rapidly dissolving.[19] However, the U.S. government continues to treat cyber issues as distinct and separate from physical or personnel security concerns. This is quickly leading to a situation where culturally and legally there is a distinction between cyber and physical when, in actuality, the difference may not exist. For instance, most people would agree that conducting an intelligence espionage operation against a computer is a reasonable and necessary activity. Would those same individuals still find the operation reasonable if the computer were connected to someone's brain?

It is becoming increasingly difficult to determine where to draw the line between privacy and the ability to protect, gather, exploit, and leverage secrets. In a highly connected, technology-infused world, it will be difficult for governments to operate secretly when competitors and adversaries have access to such a rich information environment. Since information quality varies considerably, one participant suggested that it may be beneficial to cloak valuable information with either misinformation or false information. Some participants strongly disagreed with this suggestion. They believed that it is too easy to identify and strip the false data from a data set. For instance, the Defense Advanced Research Agency (DARPA) sponsored a "Network Challenge," where it placed 10 red weather balloons at 10 fixed locations within the continental United States and asked the public to collaborate in finding them. The study explored "the roles the Internet and social networking play in the timely communication, wide-area team-building, and urgent mobilization required to solve broad-scope, time-critical problems."[20] Participants were able to quickly strip out false data while searching for the balloons.

...organizations should assume that they will fail to protect their secrets

One participant argued that organizations should assume that they will fail to protect their secrets. It more accurately depicts the reality of the situation and prompts them to use that sensitive information to their advantage while it still provides a decision advantage. If a government believes that others have full access to its secrets, then the government will need to change its behavior to remain competitive. For instance, if the U.S. government believes that its adversaries have access to its military networks, then it may change its war-fighting behavior. Instead of large-scale buildups and deployments, the country might switch to quick actions with minimal buildup and rapid deployment to prevent adversaries from capitalizing on knowledge about its deployment plans and logistics stores.

[20] "Darpa Network Challenge," available at https://networkchallenge.darpa.mil/Default.aspx (last viewed 10/8/10).

Chapter 4: Conclusion

While the members of the working group did not all agree with Don Burke's prediction of no more secrets, there was a general consensus that the government, as well as the private sector and individuals, confront an enormous challenge in trying to learn how to prevail in an increasingly transparent world. The business community may be farthest ahead in addressing this challenge, and government should engage with private sector players who are developing new ways of doing business that enhance innovation and require far fewer secrets. Government must learn what businesses already understand: those who figure out how to operate with fewer secrets will gain a significant advantage over those who continue to cling to traditional notions of indefinite information monopoly.

Government must learn what businesses already understand: those who figure out how to operate with fewer secrets will gain a significant advantage over those who continue to cling to traditional notions of indefinite information monopoly.

Appendix I: Agenda

No More Secrets: National Security Strategies
for a Transparent World

Tuesday, June 29, 2010

**American Bar Association Standing Committee
on Law and National Security
Office of the National Counterintelligence Executive
National Strategy Forum**

Underwritten in part by the McCormick Foundation

Tuesday, June 29, 2010

Bingham McCutchen LLP
2020 K Street, NW
Washington, D.C. 20006

10:00am Welcome and Introduction
Harvey Rishikof, Chair, American Bar Association Standing Committee on Law and National Security; Professor of National Security Law, National War College

10:15am Opening Remarks by the National Counterintelligence Executive
Robert "Bear" Bryant, Director of National Counterintelligence

10:30am Session One: Examining the Premise
Moderator: *Suzanne E. Spaulding, Principal, Bingham Consulting Group*

Are we approaching a time when there will be no more secrets, or at least far fewer secrets?
The growing challenge and cost of keeping secrets/maintaining a monopoly on information:
Espionage
Dependence upon the Internet
Technology convergence
Societal behavior
Ubiquitous IT tools for finding/understanding/managing information
Unprecedented "digital permanence" of previously ephemeral moments/transactions/data
Will we find new ways to keep information secret?

11:15am SESSION TWO: "Secrets" Today
Moderator: *N. John MacGaffin III, Senior Director, CENTRA Technology, Inc.*

What are "secrets"? (governmental, private sector, personal)
Why are there "secrets?"
Current Secret Protection (counterintelligence, cybersecurity, legal protections, etc.)
Secrecy System Strengths and Vulnerabilities
The Intersection of Corporate and State Secrets

Noon Working Lunch/Session Three

SESSION THREE: The Results of Divulging or Otherwise Losing Secrets
Moderator: *Joel F. Brenner, Senior Counsel, National Security Agency*

Vital Secrets
Non-Vital Secrets
Examples of Competing Without Secrets

12:45pm SESSION FOUR:
Strategies for Prevailing in an Increasingly Transparent World
Moderator: *Harvey Rishikof, Professor of National Security Law, National War College*

Technology
Policies and Practices
Training
Legislation

2:45pm SESSION FIVE: Wrap-Up
Moderator: *Suzanne E. Spaulding, Principal, Bingham Consulting Group*

Statement of Principles
Recommendations
Implementation

4:30pm Informal Reception

5:30pm Final Adjournment

Appendix II: List of Workshop Participants

Joel F. Brenner
Senior Counsel
National Security Agency (NSA)

Robert M. Bryant
Director of National Counterintelligence & Security Office of the Director of National Intelligence

Richard Burge
Chief Executive
Wilton Park

Don H. Burke
Intellipedia Doyen
Central Intelligence Agency (CIA)/CIO

Angeline G. Chen
General Counsel and COO
Marinette Marine Corporation

Jeffrey R. Cooper
Chief Innovation Officer
Science Applications International Corporation (SAIC)

Richard E. Friedman
President and Chair
National Strategy Forum

Albert C. Harvey
Chair, Advisory Committee
ABA Standing Committee on Law and National Security

Eliot A. Jardines
Chief Knowledge Officer
CENTRA Technology, Inc

Donald M. Kerr
Research Professor
Volgenau School of Information Technology and Engineering
George Mason University

Robert K. Knake
International Affairs Fellow
Council on Foreign Relations

Susan Landau
Fellow
Radcliffe Institute for Advanced Study

Dennis J. Lehr
Of Counsel, Hogan & Lovells

James A. Lewis
Director and Senior Fellow
Technology and Policy Program
Center for Strategic and International Studies (CSIS)

N. John MacGaffin III
Senior Director
CENTRA Technology, Inc.

Elliot E. Maxwell
Fellow, Communications Program
Johns Hopkins University

Judith A. Miller
ABA Standing Committee on Law and National Security

Gregory T. Nojeim
Director
Project on Freedom, Security and Technology
Center for Democracy and Technology

Richard P. O'Neill
President
The Highlands Group

Peter Raven-Hansen
Professor of Law
The George Washington University Law School

Harvey Rishikof
Chair, Standing Committee on Law
and National Security
American Bar Association (ABA)

Paul Rosenzweig
Principal
Red Branch Consulting, PLLC

Michael Schrage
Research Fellow
Sloan School of Management Center
for Digital Business
MIT Security Studies Program (SSP)

Frederick A.O. Schwarz, Jr.
Chief Counsel
Brennan Center for Justice at
New York University School of Law

David M. Shapiro
Counsel, Liberty and National
Security Project
Brennan Center for Justice at
New York University School of Law

Jennifer E. Sims
Professor and Director of
Intelligence Studies
Security Studies Program
Georgetown University

Suzanne E. Spaulding
Special Advisor to the Standing Committee
on Law and National Security
American Bar Association
Principal, Bingham Consulting Group
Bingham McCutchen LLP

K.A. (Kim) Taipale
Founder and Executive Director
Stilwell Center for Advanced Studies
in Science and Technology Policy
Rapporteur

Alane Kochems
Observers

Hyon Kim
Program Manager
Office of the Director of National
Intelligence (ODNI)

Adriane Lapointe
Visiting Fellow
Center for Strategic and
International Studies (CSIS)

Holly McMahon
Staff Director
Standing Committee on Law and National
Security
American Bar Association (ABA)

Piper Treece
Master's Candidate
Security Policy Studies
The George Washington University

Denise E. Zheng
Program Manager
and Research Assistant
Technology and Public Policy
Center for Strategic and
International Studies (CSIS)

Appendix III: Recommended Readings

Links

Huffington Post link to an item posted by Suzanne Spaulding:
http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html

IBM's Internet of Things video:
http://www.youtube.com/watch?v=sfEbMV295Kk
"The planet has grown a central nervous system"

Don Burke's comment on the following video: "I continue to find this video that explains accelerating change to be a powerful tool for conveying this hard-to-understand topic: 'Are Humans Smarter Than Yeast'"
http://www.youtube.com/watch?v=hM1x4RIjmnE

Blog post about the new Chevy Volt is illustrative of how everything is being connected:
http://gm-volt.com/2010/06/23/exclusive-chevy-volt-will-come-with-more-than-one-year-free-onstar/

Biology and silicon joining together:
http://www.computerworld.com/s/article/9141180/Intel_Chips_in_brains_will_control_computers_by_2020
http://www.botjunkie.com/2010/06/10/monkey-brain-controls-7-dof-robot-arm/
http://www.technologyreview.com/biomedicine/25341/?ref=rss&a=f

Intelligent aggregators
http://venturebeat.com/2010/06/22/semantic-startup-primal-builds-pages-around-your-thoughts/

DailyPerfect (http://www.dailyperfect.com/), an "innovative personalization technology, which can predict a user's interests through an automated semantic analysis of publicly available information. Our predictive content engine will generate a personalized news feed customized just for you. If you are a publisher, ad network or direct marketer and are interested in learning how our B2B content personalization and behavioral targeting solutions can help improve your business, please contact us."

escience news is compiled by an artificial intelligence engine
http://esciencenews.com/about

Sensored planet (and bodies)
http://www.readwriteweb.com/archives/the_internet_is_a_series_of_tubes_real-time_mappin.php
http://www.readwriteweb.com/archives/sensors_next_big_wave_of_computing.php#more
http://nextbigfuture.com/2010/01/wireless-body-monitoring-system-and.html
http://singularityhub.com/2010/01/27/the-win-human-recorder-a-patch-to-monitor-your-health/
http://www.ats.org/site/News2?page=NewsArticle&id=6063&security=1141&news_iv_ctrl=1261

The AI Revolution is On
By Steven Levy, Wired, January 2011
Overview on the state of AI and how its permeating society in ways we never expected and don't readily see.
http://www.wired.com/magazine/2010/12/ff_ai_essay_airevolution

Watson
IBM's Computer Jeopardy Champion
There has been much coverage but the February 2011 Nova Special "The Smartest Machine on Earth" is a fascinating look at Watson
http://www.pbs.org/wgbh/nova/tech/smartest-machine-on-earth.html

Cisco's Global Mobile Data Traffic Forecast Update, 2010-2015
February 2011
Two astounding tidbits from the many in the report:
- There are 48 million people in the world who have mobile phones, even though they do not have electricity at home.
- Mobile-connected tablets will generate as much traffic in 2015 as the entire global mobile network in 2010.
http://newsroom.cisco.com/dlls/ekits/Cisco_VNI_Global_Mobile_Data_Traffic_Forecast_2010_2015.pdf

Zite
Similar to "Siri", a new application for your iphone or iPad will watch the web for signals and then crawls over 500,000 web sites to find content relevant just for you.
http://online.wsj.com/article/SB10001424052748704758904576188621188047068.html

Hashable
One of the hottest applications at 2011 SXSW is a new social application called hashable that seeks to replace the business cards and enable real-time and ongoing tracking of interactions with your contacts.
http://www.readwriteweb.com/archives/5_absolute_must-have_apps_to_rock_sxsw_interactive.php

The Leaky Corporation
Digital information is easy not only to store but also to leak. Companies must decide what they really need to keep secret, and how best to do so
The Economist
Feb 24, 2011
http://www.economist.com/node/18226961

Justspotted.com
Website's tag line: "Justspotted is a fun new way to keep up with your favorite celebrities".
This application uses posts from social networking sites to track the location and whereabouts of celebrities
http://www.justspotted.com/

Survey of 10,000 Yammer Users Reveals Benefits of Enterprise Social Networking
Yammer.com, January 2011
http://blog.yammer.com/blog/2011/01/survey-of-10000-yammer-users-reveals-benefits-of-enterprise-social-networking.html

The Connected Company
Communication Nation
8 February, 2011
http://communicationnation.blogspot.com/2011/02/connected-company.html

French Company, Atos Origin, sets out its ambition to be a zero email company within three years
January 2011
http://www.atosorigin.com/en-us/Newsroom/en-us/Press_Releases/2011/2011_02_07_01.htm

8 Predictions for IT in 2015 from Gartner
by Klint Finley, November 30, 2010
http://www.gartner.com/it/page.jsp?id=1480514

Banks open up to iPhone, Android as IT consumerization continues
By Jason Hine, ZDNet, September 10, 2010
"a new report, [by Bloomberg], suggests that two big banks are not only letting Apple iPhones and Android devices in the door in place of the standard-issue BlackBerrys, but are also looking at supporting employee-owned devices."
http://www.zdnet.com/blog/btl/banks-open-up-to-iphone-android-as-it-consumerization-continues/39055

Is That a Computer in Your Sweater or Are You Just Glad to See Me?
Extremetech, January 14, 2011
This article reviews some smartclothing products
http://www.extremetech.com/article2/0,2845,2375741,00.asp?kc=ETRSS02129TX1K0000532

The Eyeball Camera Can Also Zoom
Technology Review, January 2011
http://www.technologyreview.com/computing/27105/?p1=A1&a=f

Smart Contact Lenses for Health and Headup Displays
New Scientist, 10 January 2011
http://www.newscientist.com/article/mg20927943.800-smart-contact-lenses-for-health-and-headup-displays.html

Argus II Retinal Implant approved in Europe for treating Blindness
Announcement:
http://2-sight.eu/images/stories/2-sight/pdf/20110302%20second%20sight%20release%20en

The Files Will Get Out
The Atlantic
http://www.theatlantic.com/technology/archive/2011/02/the-files-will-get-out-a-lesson-from-wikileaks-gawker-the-riaa-and-libya/71628

A Free and Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate
By Yochai Benkler of Berkman Center for Law at Harvard
http://benkler.org/Benkler%20Wikileaks%20CRCL%20Working%20Paper%20Feb_8.pdf

Anonymous speaks: the inside story of the HBGary hack
by Peter Bright
Arstechnica, Feb 2011
http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/2

What They Know
By Jennifer Valentino-Devries
Wall Street Journal, July 31, 2010
http://online.wsj.com/public/page/what-they-know-digital-privacy.html

Spike Bowman: "Dysfunctional Information Restrictions"
http://www.fas.org/sgp/eprint/bowman.pdf

Reinventing Invention: Fixing the Engine of Biopharmaceutical Innovation
http://www.lilly.com/news/speeches/091030/default.html

Lilly's Science Grid Goes Open Source
http://www.bio-itworld.com/BioIT_Article.aspx?id=75790

Additional Reports and Recommended Readings

Report: "New Approaches to Cyber-Deterrence: Initial Thoughts on a New Framework" by Jeffrey R. Cooper, SAIC, December 29, 2009
This report, done under USD(I) auspices, built on three years of previous Highlands Forum work to appreciate the implications of identity and attribution on cyber-security as well as attempts to better understand the relationship of the evolving international security environment and cyber issues. It includes a lengthy discussion of the "cooperation, competition, conflict" (3Cs) framework that Richard O'Neill mentioned at the workshop as well as introducing the concept of "networked deterrence."

CISP Report: "Towards a National Information Strategy: Aligning Responsibility, Authority and Capability to Provide for the Common Defense" by Jeffrey R. Cooper, September 1, 2009
From the Introduction: "The Information Revolution, as with previous technological "disruptions," promises to bring another in a the series of fundamental transformations in how society functions ... – including how we plan and execute critical national security tasks..."

IT Journal, Winter 2007-2008, "No More Secrets"

Report by the Digital Connections Council of the Committee for Economic Development – April 2006 – "Open Standards, Open Source and Open Innovation: Harnessing the Benefits of Openness"

Bob Brewin, No More Secrets, bbrewin@govexe.com, September 15, 2008

Privacy and Security: Myths and Fallacies of "Personally Identifiable Information"
By: Arvind Narayanan and Vitaly Shmatikov
Introduction: Developing effective privacy protection technologies is a critical challenge for security and privacy research as the amount and variety of data collected about individuals increase exponentially.

A Practical Attack to DeAnonymize Social Network Users
By: Wondracek, Holz, Kirda, and Kruegel
Int. Secure Systems Lab
Vienna University of Technology
Brief presentation on the attack results and methods used against social network sites such as Facebook, LinkedIn, and other widely utilized social networking sites.