5-1-2007

Freeing knowledge, telling secrets: Open source intelligence and development

Cody Burke

Freeing Knowledge, Telling Secrets:

Open Source Intelligence and Development

Cody Burke

There are two key areas under constant pressure as the information revolution accelerates that must be addressed; knowledge and knowledge management, or in other words, collection and production. In relation to security matters, the question is how to find the best information to produce relevant and useful intelligence, and then what is the best method to understand that information and develop the appropriate responses. This task has traditionally been the domain of the varying intelligence agencies, who have cultivated an air of mystery and secrecy that is ill fitted to meet the demands of modern counter-terrorism, or even the level of information sharing that is required in the network-centric warfare championed by many in the Pentagon. As the information revolution continues and more individuals have more access to more and more information, it becomes clear that attempting to restrict and control information flows becomes an exercise in futility. It also is apparent that while society at large, and particularly the business community, have begun to embrace the potential offered by information technology advances, the intelligence community lags behind. This research paper will introduce two constructs for dealing with information flows that take full advantage of technological gains, while challenging traditional methods and assumptions about knowledge and knowledge management. For collection, open source intelligence; for production, open source development.

Intelligence is defined as the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas, also information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The crucial component of this definition is that intelligence is a product that must be created, it is not simply enough to know something; if it is not packaged, analyzed, and filtered, than it has no value to policy makers. The role of the intelligence product itself is to give decision makers relevant information about the outside world so that informed

choices can be made, or put succinctly, "intelligence defines reality for those whose actions could alter it".[1] Increasingly, the focus of intelligence agencies has been to move away from strategic intelligence towards an emphasis on tactical information, or in the words of the Tim Weiner in the New York Times; "The big picture has been bumped by spot news. Strategic intelligence in the power to know your enemies intentions, spot news is what happened last night in Waziristan".[2]

The root of the inability of the intelligence community to effectively counter modern asymmetric threats in the form of netwar and 4GW [fourth generation war] is the culture of secrecy that is the legacy of the Cold War. The obsession with secrecy is the most damaging effect of the intense competition between the two Superpowers, and despite the end of the Cold War, the culture of secrecy still permeates that intelligence community.[3] There is an assumption in the intelligence community that information becomes more valuable as it rises in classification, creating a closed system that values keeping secrets more than accumulating general knowledge that is publicly available.[4] Combined with excessive bureaucracies and competitiveness among agencies, the result is information hoarding, technological ignorance, unaccountability, distrust of public information, and a culture where personal power radiates from the ability to know things that know one else does.[5]

This phenomenon was described by Air Force Lt. General Mike Hayden, speaking as director of the NSA in 2002, as the "stovepipe mentality" that only allows information to move vertically, but not horizontally to the areas where it is actually needed.[6] In addition, the information that is

---

[1] www.jfcom.mil/about/glossary, Quoted from Barlow, J. P. (10/07/2002). Why Spy? Forbes.com., p. 2, and the role of intelligence explained in detail in Rathmell, A. (2000). "Building Confidence in the Middle East: Exploiting the Information Age." Journal of Palestine Studies 29(2): 5-19., p. 8

[2] Weiner, T. (2006). Langley, We Have A Problem. The New York Times. New York.

[3] Barlow, J. P. (10/07/2002). Why Spy? Forbes.com.

[4] Steele, R. D. (2002). Open Source Intelligence: What is it? Why is it important to the Military? NATO Open Source Reader, NATO.

[5] Barlow (2002)

[6] Barlow (2002) Hayden went on to be appointed Director of the CIA in 2006.

developed is often either unusable, or of limited use due to the classified nature of the sources.[7] In one instance, the US detected North Korea breaching safeguard agreements made with the International Atomic Energy Agency(IAEA) using satellite imagery, but to protect the sources and methods used would not provide the raw data to the IAEA, limiting the ability of the IAEA to hold the North Koreans accountable.[8] Classification also creates huge methodological problems for academics attempting to conduct studies on sensitive areas, findings often can not be shared for peer-review, limiting the open discussion that is essential to sound research and undermining the results.[9] For policy makers, intelligence bills that deal with classified material often go unread; due to the legal requirements that they not discuss the contents all debate is stifled and bills dealing with important issues of covert operations and funding are voted on blind.[10]

The current state of intelligence and the emphasis on secrecy also does not take full advantage of the potential that the revolution in information technology provides for information sharing and collaboration. Robert D. Hof writes in Business Week that, "New research indicates that cooperation, often organized from the bottom up, plays a much greater role than we thought in everything from natural phenomena like ant colonies to human institutions such as markets and cities", and goes on to quote eBay CEO Margaret C. Whitman who states, "It is far better to have an army of a million than a command-and-control system".[11]

The success of the exploitation of information technology in the intelligence community has been mixed. The foundations of the modern internet are built upon ARPANET, developed to ensure communication and command and control ability would remain in place in the event of nuclear attack form the Soviet Union; in the event of the loss of one node in the network, communications could be easily routed around the missing node, maintaining the system. The US intelligence community as of 2006 uses Interlink, a secure intranet that provides a network for the

---

[7] Barlow (2002)

[8] Rathmell, A. (2000). "Building Confidence in the Middle East: Exploiting the Information Age." Journal of Palestine Studies 29(2): 5-19.

[9] van Meter, K. M. (2002). "Terrorist/Liberators: Researching and dealing with adversary social networks." Connections 24(3): 66-78.

[10] Milligan, S. (August 6, 2006). Classified intelligence bills often are unread. The Boston Globe.

[11] Hof, R. D. (20/6/2005). The Power of Us. Business Week Online.

collection, analysis, production, and dissemination of information.[12] The CIA has also entered into the production of IT technology though the creation in 1999 of In-Q-Tel, a private, non-profit company to develop IT for national security purposes.[13] Denis A. Clift, writing in CIA Studies in Intelligence, certainly sees the intelligence community as on the cutting edge of the IT revolution, and asserts that, "The internet era has become the intelligence community's new strength as well as its new challenge. Cold War assumptions driving intelligence collection and analysis- that enemy targets were closed societies and that superpower rivalry trumped all other issues- are assumptions of the past".[14]

Clift may have been correct in 2003, but by 2005 is disputed by an Army officer who served in Iraq, who in reference to Interlink notes that "it's pretty damn cool, for four years ago".[15] In his article in Wired magazine, Kris Alexander compares Army Knowledge Online, a service launched in 2001 that enables soldiers to keep in touch and share knowledge through virtual personal work spaces, and the Center for Army Lessons Learned, a military blog space that enable soldiers to post white papers relating to any subject, with the relatively crude Interlink used by the intelligence community.[16] Alexander notes that a search for "improvised explosive devices" on the Center for Army Lessons Learned returns over 130 results, all of which have been edited for accuracy by a staff of experts and are based on current field experience, while Interlink is composed of separate portals and data for 15 different agencies, and although all the agencies might be seeing the same data, there is no way to interact with and share analysis across the community.[17] For Alexander, the solution lies in engaging the minds and expertise of more people, by establishing blogs on Interlink that allow for the free exchange of ideas and information not just among the intelligence community, but from those outside who posses the knowledge to

---

[12] Clift, D. A. (2003). "From Semaphore to Predator: Intelligence in the Internet Era." CIA Studies in Intelligence Unclassified Edition 47(3).

[13] Clift (2003)

[14] Clift (2003)

[15] Alexander, K. (2005). We Need Spy Blogs: An Army officer calls for better information gathering. Wired. 3.

[16] Alexander (2005)

[17] Alexander (2005)

contribute: journalists, academics, and the established blogoshere.[18] In this vein Barlow, writing in Forbes, calls for the intelligence community to take its cues from the scientific community, where the scientific method is utilized to arrive at "truth" based on the *widest* possible consensus through peer-review and the distribution of conclusions and analysis, rather then concealment and classification.[19] Barlow refers to a speech given by Dr. Edward Teller comparing the U.S. experience during the Cold War with open and closed systems; the nuclear program, a closed system, resulted in a virtual tie by the end of the Cold War, while the electronic industry, an open system, was decades ahead of the Soviet Union.[20]

The success against the Soviet Union of an open system over a closed system demonstrates that the market often provides the cues and new structures for innovation far before bureaucratic government institutions. Cebrowski noted this in 1998 when calling for the adoption of network-central warfare, positing that if the US economy, business, and IT industry were undergoing fundamental change, then the military, being a reflection of American society, must change as well.[21] Although Cebrowski writing in 1998 was referring to the way what companies were in effect creating situational awareness though networking communications, looking to the market as of 2006 for a solution, the largest innovation and tool to capitalize on increasing information flows is the open source movement. What Alexander and Barlow, and by extension of his own logic Cebrowski, are recommending for the security community (both intelligence and military) is an open source, as opposed to closed source system. The term open source has two different, yet conceptually linked meanings which will now be dissected.

1) The Open Source Development Model

Open source has its root in the creation of software though the release of source codes and the encouragement of modification and redistribution. Open source methods can be traced to 1991

---

[18] Alexander (2005)

[19] Barlow (2002), p. 5, notes that scientists "toil to create systems to make all the information available to one immediately available to all", and describes them as "committed free marketeers in the commerce of thought".

[20] Dr. Edward Teller's speech is quoted in Barlow (2002), p. 4

[21] Cebrowski, A. K., Garstka, John J. (1998). "Network-Centric Warfare: Its Origin and Future." Proceedings(January 1998).

and the development of the Linux operating system by Linus Torvald. Linux was developed though the use of a loose group of volunteer coders that collaborated to create a more stable operating system completely made up of free software.[22] Since then open source methods have been refined and gained in popularity, and have proven to produce high quality and stable programs. The popularity and scope of the open source movement is evident through sites like SourceForge.net, a software development website that has, as of 2006, over 1,000,000 registered users and hosts over 100,000 open source projects.[23] All programs are available to download at no charge, and participation and feedback is strongly encouraged. What was achieved by Torvald and is being continued at sites like SourceForge.net is not significant because of the products produced, but because of the method used.[24] The potential of using large groups to solve programing problems has reached the corporate level as well. One example is TopCoder, a software development that company hosts Code Jam, a contest for the top 100 freelance coders in the world. These coders are then recruited to work on small parts of projects, in competition with each other. The end result is then pieced together from the best of each of the smaller segments, resulting in faster development cycles and a superior product.[25]

Greg Madey provides this helpful summery of open source software development:

> "Open source software development teams, are generally comprised of volunteers working not for monetary return, but for the enjoyment and pride of being part of a successful virtual software development project. Team members often come from around the world and rarely meet one another face-to-face. The open source project are self-organized, employ extremely rapid code evolution, massive peer code review, and rapid releases of prototype code. The open source software movement is a prototypical example of a decentralized self-organizing process. There is no central control of central planning. It challenges conventional economic assump-

---

[22] Goetz, T. (2003). Open Source Everywhere. Wired. 11.

[23] http://sourceforge.net/

[24] Goetz (2003)

[25] Arnoldy, B. (November 1, 2006). How to build software? Henry Ford, meet eBay. The Christian Science Monitor.

> tions, it turns conventional software engineering and project management principles inside out."[26]

Open source development is enabled by the internet, allowing unlimited numbers of participants in projects, and rooted in software coding, but is not limited to technological developments; politics, culture, and the Creative Commons movement for the release of non-copyrighted material all draw inspiration from the philosophy of open sources.[27] The most successful project in open source development is Wikipedia, with as of 2006 over 1,298,000 user published articles that can be edited by anyone. Founded by Jimmy Wales in 2001, by 2003 Wikipedia was receiving more hits than Britannica.com. In a 2005 study by Nature Magazine the two online encyclopedias tied at four each for serious errors, and Wikipedia had 162 factual errors, omissions or misleading statements, only slightly more then the 123 that Britannica.com had.[28] Another significant open source project is Project Gutenberg, an effort to release works that have fallen into the public domain as free e-books. Books are typed in manually by volunteers and proofread by Distributed Proofreading, another open source project that breaks down newly enter e-books into individual pages so multiple editors can work on the same e-book, speeding up the process.[29] Open source scientific journal distribution projects have been launched with some success as well, in an attempt to bypass the expensive subscription costs that limit readership and to stay true to the principal that freely available knowledge aids in the scientific process.[30]

A related open source concept and buzzword is "crowd sourcing", basically the enlistment or in some cases employment of large groups to work on projects. Marketocracy, an online community of stock traders, tracks the picks of its top 100 traders and bases its mutual fund investments on those picks. NASA has enlisted the help of the online community to help pour over the images from Mars to create a map of the planet. Perhaps more significant, the newspaper publishing company Gannett announced in 2006 that it would begin crowd sourcing newsroom func-

---

[26] Madey, G., Freeh, Vincent, Renee Tynan (2002). The Open Source Software Development Phenomenon: An Analysis Based on Social Network Theory. Eighth Americans Conference on Information Systems.

[27] http://en.wikipedia.org/wiki/Open_source

[28] Giles, J. (2005). "Internet encyclopedias go head to head." Nature(438).

[29] Goetz (2003), www.gutenberg.org, www.pgdp.net

[30] Goetz (2003)

tions, even renaming newsrooms as "information centers", and allowing the public to participate in the generation of stories by acting as watchdogs, whistle-blowers, and researchers.[31] In a security related example, the state of Texas announced in November 2006 that live feeds from digital cameras placed at border crossings known to be used by illegal immigrants would be made available on the internet, to allow members of the public to assist in spotting and reporting illegal crossings.[32] The Operation Iraqi Freedom Documents project is another instance of security related crowd sourcing. To speed up the translation process, 55,000 documents, audiotapes, and videotapes seized in the 2003 invasion were put online and made available for public access.

The open source model, while seemingly a positive and somewhat idealist notion of cooperative collaboration to reach a shared goal, is also useful in understanding the activities of modern global terrorist groups. Both an open source community and a global terrorist group are based on a flat organizational structure that eschews top-down hierarchies in favor of large groups of technically savvy semi-autonomous actors working toward a common goal. Innovation is encouraged and weak spots and vulnerable faultlines are targeted, in the case of open source development the weak spots are the bugs or redundancies in the system that can be eliminated by the open source process. Drawing from Eric Raymonds seminal open source ethnographic project on the history of hacking and open source, *The Cathedral and the Bazaar*, John Robb identifies five key characteristics of open source thought that are applicable to terrorism;

1) Release early and often;

2) By using a large enough pool of collaborators eventually a solution will be found that can then be passed on and replicated;

3) The collaborators are the most important asset and will provide valuable ideas that should be recognized and take advantage of;

4) Simplicity is the best solution and enables swarming tactics and a high speed development cycle; and finally,

---

[31] Howe, J. (November 3, 2006). Gannett to Crowdsource News. www.wired.com/news.

[32] BBC (November 4, 2006). Web users to 'patrol US border. http://news.bbc.co.uk/.

5) Available resources can often be used in unexpected ways.[33]

To take this train of thought a step further and into the abstract, the shared goal that holds together an open source community, be it a software project or encyclopedia, is fundamentally an idea; an idea that can be modified and tinkered with to meet an individuals specific situation, but ultimately in service to the larger project. Substitute ideology for shared goal, and global terrorism can be seen as operating on this model. By providing what amounts to a source code in the form of what has been termed the "global jihadist" agenda, these actors encourage the localized innovation that drives the agenda and can result in dynamic and unpredictable movement. The open source model of a shared goal that guides the network also attempts to address a principal weakness of networks, the difficulty in controlling one after it is created. Matthew and Shambaugh see networks acting as a "stable force multiplier" for terrorists, but not a means to impose that kind of control that would be necessary to pose a serious sustained threat to western interests.[34] While effectively putting the terrorist threat into perspective, if the open source model is applied to Matthew and Shambaugh's thesis it becomes apparent that the goal of the network is not strict top-down control, but the creation of a loose bottom-up open source community that in pursuing their localized objectives also further the larger cause.

The intelligence community, in an effort to address failures leading up to 9-11, has made some small steps to adopt open source methods. Significantly, in 2004 the CIA launched CIA Wiki, and in 2006 the Director of National Intelligence introduced a community wide wiki called the Intellipedia.[35] These projects allow for subject experts across the intelligence community to submit and edit content to build a base of knowledge that is to be used to compile National Intelligence Estimates and country reports, in the hopes that it will encourage debate and produce a better product. To protect security and ensure accountability the wiki has three levels of classification and participants have to attach their names to submissions, in what is an attempt to build

---

[33] Raymonds project is available at www.catb.org/~esr/writings/cathedral-bazaar/, and Robb outlines these points further at http://globalguerrillas.typepad.com/globalguerrillas/2004/09/bazaar_dynamics.html

[34] Matthew, R., Shambaugh, George (2005). "The Limits of Terrorism; A Networked Perspective." International Studies Review 7(4).

[35] Kaplan, D. E. (October 30, 2006). Wikis and Blogs, Oh My!, U.S News and World Report., Miller, G. (November 1, 2006). U.S. using Wikipedia software for intelligence reports. Los Angeles Times., and Reuters (November 1, 2006). U.S. Adds Wiki to Spy Arsenal.

an open system enclosed within a closed one. Also significant is the actual software being used in the creation of the Intellipedia, MediaWiki, the free open source program that also powers Wikipedia.[36] Not only is the value of the open source method being recognized, but the advantages presented in terms of cost and quality of programing by open source development are as well.

Although the intelligence community would benefit from applying open source methods to the intelligence process, it is illustrative to remember one indisputable characteristic of a network; any network is only as strong as the information that is on it. Analysis of intelligence would be aided by open source methods, and in keeping with the premise that transparency (openness) and optimization of available technology is preferable, then the discipline of open source intelligence must be examined.

2) OSINT

Open source as a term can also refer to the intelligence discipline of open source intelligence (OSINT). OSINT is defined as unclassified information obtained from any publicly available source in print, electronic, and even verbal form.[37] Radio, television, newspapers, journals, internet, commercial databases, and video all fall under this category, and can be successfully exploited to gather intelligence. This kind of data can be extremely useful, and is often the only means of penetrating dark and covert networks. The process begins with open source data (OSD), the raw information from the primary source, and must then be assembled through an editing process to filter and validate. This then results in open source information (OSIF) that can be disseminated as newspaper articles, books, TV and radio broadcasts, and on the internet.[38] Only after the OSIF has been deliberately discovered, analyzed, and disseminated to a select audience in reference to a specific question is true OSINT created.[39]

---

[36] Miller (2006)

[37] NATO (2001). NATO Open Source Intelligence Handbook, NATO., NATO leads the field in OSINT, and has produced three technical manuals for OSINT practitioners that are heavily referenced in the majority of works reviewed for this paper. Two of which, the OSINT Handbook and OSINT Reader, are the reference points for the technical aspects of OSINT described in the this chapter.

[38] NATO OSINT Handbook (2001)

[39] NATO OSINT Handbook (2001)

The value of OSINT is not new, if anything it is the oldest intelligence discipline, and was of particular value during the Cold War for all sides involved. In World War II, the Cold War, and the Vietnam War, radio and print sources accounted for the majority of intelligence gathered. It is estimated that 80% of valuable intelligence comes from open sources.[40] The IT revolution has dramatically increased the access to and value of open sources, allowing for faster and cheaper collection and analysis.[41] The key drivers for the shift towards open sources can be identified as the exponential growth of the internet as a tool for disseminating information, the huge rise in the amount of published and broadcast information, and the collapse of many formerly denied areas.[42] What has happened is a movement away from the Cold War mentality. When the task of the intelligence agencies was dealing with closed societies that did not release the information that was needed, covert methods were necessary to ascertain the motives and strategy of the other. The new environment is one in which an analyst is faced with an abundance of information that can be obtained quickly and cheaply.[43] In effect the problem is no longer how to get information, but what to do with the mass amount that is available.

The process of creating OSINT products is similar yet distinct from the production of other methods of intelligence, and relies on four key elements to create interactive, outwardly engaged, and consumer oriented products.[44] The first element is the report; traditional intelligence is produced with the end result being a report that is presented to the customer/policy maker, often with vague or little referencing due to security concerns. The lack of referencing makes validation of the contents of a report by the consumer next to impossible, often leaving policy makers in the position of making decisions based only on information that is credited to a "reliable source", as was the case with the assertion that Iraq possessed WMDs.[45] The role of the report

---

[40] Mercado, S. C. (2004). "Sailing the Sea of OSINT in the Information Age." CIA Studies in Intelligence Unclassified Edition 48(3).

[41] Mercado (2004)

[42] NATO OSINT Handbook (2001)

[43] Clift (2003)

[44] NATO OSINT Handbook (2001)

[45] Mercado, S. C. (2005). "Reexamining the Distinction Between Open Information and Secrets." CIA Studies in Intelligence Unclassified Edition 49(2), Mercado states that "With open information, sources are often unclear. With secrets, they almost always are."

itself represents the crux of the difference between traditional intelligence analysis and open source methods. The report is the beginning of the OSINT process, and provides both analysis and sources to enable the customer to access the raw data to meet specific needs.[46] In essence the same as citing in an academic work or showing every step of a mathematical equation, the end result is a clear path that shows how the analysis was arrived at, leading to greater reliability and accountability.

To enable the customer to access information independently without having to request a report on a specific issue, and to overcome the limitations of search engines, the second element of OSINT production is link tables that are progressively created to reflect various areas of interest.[47] With ranking by importance and relevance, URL, and a brief summary of content, these link tables grow and can be exchanged between agencies to facilitate quick and efficient information gathering when the need arises.[48] Third, to increase productivity, internet based distance learning centers are utilized to provide one-stop reference points for basic information needed by analysts and customers alike.[49] The CIA World Factbook, EMM News Explorer, and the MIPT Terrorism Knowledge Base are examples of civilian versions of these, as well as commercial services such as Silobreaker.[50] The fourth key to OSINT production is the use of expert forums. Expert forums provide a net of expertise on topics that can be broken down and reorganized to meet the requirements of the specific task at hand, and can use the knowledge of members to build a database of information and analysis that is outside the institutional culture of the intelligence community.[51]

---

[46] NATO OSINT Handbook (2001)

[47] NATO OSINT Handbook (2001)

[48] NATO OSINT Handbook (2001)

[49] NATO OSINT Handbook (2001)

[50] Silobreaker is a subscription based open source facilitator program, www.silobreaker.com, EMM News Explorer is a free version incorporating many of the same features, http://press.jrc.it/NewsExplorer/home/en/latest.html, and MIPT Terrorism Knowledge Base contains information on terrorist groups including incident tracking, graphing functions, and background information, http://www.tkb.org/Home.jsp

[51] NATO OSINT Handbook (2001)

Open Source data and information come from a variety of places, with the only stipulation being that it is unclassified. The first and obvious source is from traditional media outlets, which remain the core of OSINT efforts.[52] The Foreign Broadcast Information Service (FBIS) translates foreign media in the U.S. and is credited with several early warnings that were missed by the CIA, including the Sino-Soviet split in the early 1950s.[53] The FBIS has now been incorporated into a new agency, the Open Source Center (OSP), but remains based within the CIA and now serves an expanded role.[54] Many countries exploit open sources, with efforts by the Netherlands and Sweden as examples of attempts at full integration of the intelligence, government, business, and academic communities.[55] One of the many private internet sites that allow for the surveying of foreign media is watchingamerica.com, a service that uses translation software to remove the chance of bias. Analysis of media has proven to be of immense value, particularly in closed societies like North Korea. The North Korean media consists of only two newspapers, one run by the communist party and one run by the government, and make up one of the sole reference points for analysts to determine the motivations and priorities of the North Korean government.[56] The failure of the U.S. and Japan to penetrate North Korea by covert means demonstrates the difficulty in securing closed covert sources, as opposed to the relative ease of exploiting open sources with the proper methods and viewed through the appropriate lens.[57]

The internet, driven by the corresponding revolution in IT and knowledge management, is a crucial enabler for OSINT for two reasons. One, the ability to network and communicate with other people to share information and insights, and two, the ease with which information can be accessed through both free and commercial databases.[58] The internet poses challenges as well; in

---

[52] NATO OSINT Handbook (2001)

[53] Mercado (2005)

[54] Ackerman, R. K. (March 2006). "Intelligence Center Mines Open Sources." Signal.

[55] Steele (2002), Open Source Intelligence: What is it? Why is it important to the Military?.

[56] Mercado (2004) and Carlin, R. L., Wit, Joel S. (2006). North Korean Reform: Politics, economics and security. Adelphi Paper 382. IISS, International Institute for Strategic Studies. Carlin describes the way in which even the controlled media of North Korea gives valuable insight into internal politics though the timing and context of what is printed, as well as the omission of certain topics.

[57] Mercado (2004), Carlin (2006)

[58] NATO OSINT Handbook (2001)

the absence of quality products from analysts, the customer can be driven to use the internet as a crutch, thus necessitating proper validation and contextualization of internet sources by the analyst.[59] Sources on the internet must be checked for validity to ascertain accuracy, relevancy, currency, and objectivity.[60] From a security standpoint, the internet must be seen as a two way street, and poses two distinct challenges. First, potential adversaries can and will use the internet themselves to obtain open source information. The internet and the information obtained can be used in a legal manner that may not raise suspicion. The Operation Iraqi Freedom Documents project was pulled offline in November 2006 when it became apparent that the some of the documents posted for translation contained the instructions of building a crude nuclear weapon.[61] For intelligence and military purposes, information on the internet that is posted by third parties and thus not under the direct control of the organizations involved is a serious potential danger, as is the sheer amount of information that is under control of the organization but is unmanageable due to size.[62] The second challenge is the trails that are left on the internet that can reveal intentions and priorities, and information about the systems that could compromise security of networks.[63] This necessitates "laundering" a search to disguise interest and intent, reducing the amount of information shared online, and maintaining an anonymous persona online.[64] To address the possible threats posed by the internet to security, two approaches must taken; first, what is available online must be determined so countermeasures can be prepared and vulnerabilities addressed, and second, an understanding of the technological issues must be reached to minimize the information leakages during online activity.[65]

---

[59] NATO OSINT Handbook (2001)

[60] The process to evaluate web sites is detailed in Web Site Authentication and Source Analysis in NATO OSINT Handbook 2001, p. 24-26

[61] Broad, W. J. (November 3, 2006). The Struggle for Iraq; U.S. web archive is said to reveal nuclear primer. New York Times. New York.

[62] Umphress, D. A. (Winter 2005). "Diving the Digital Dumpster: The Impact of the Internet on Collecting Open-Source Intelligence." Air & Space Power: 82-91., p. 87-88

[63] Umphress (2005), p. 88 provides a technical explanation of the potential vulnerabilities to a secure network, and NATO OSINT Handbook 2001, p. 27-29 gives detailed instructions on how to work online anonymously.

[64] NATO OSINT Handbook (2001)

[65] Umphress (2005)

Commercial online premium sources offer access to edited information that has been at least partially validated, cataloged, and formated.[66] As of 2001, 8,000 commercial databases had been identified with possible commercial value.[67] These range from the leading services Lexis-Nexis, Factiva, and Dialog to the more specialty services such as Jane's Information Group, Stratfor, and Oxford Analytica. To utilize the larger commercial premium sources effectively, it is necessary to employ a professional information broker, who has experience with the search engines on these services, while the smaller more specialized services generally will offer customized products fitted to exact specifications.[68] The role that commercially available open sources can play is best illustrated by Robert D. Steele, who describes a war game on Somalia conducted by the UN in which a UN officer grew impatient with the U.S. intelligence that was available. With three phone calls and $5,000, the UN officer received an overnight delivery of: from Jane's, a complete county profile with maps of clan areas, order of battle for each clan, and every article published in any of Jane's publications in the last two years related to Somalia; from Oxford Analytica, reports suitable for presentation to Prime Ministers and Presidents on UN operations in Somalia, U.S. foreign policy towards Somalia, and U.S. operations in Somalia; and from the Economist Intelligence Unit, a complete country risk report, including logistic difficulties likely to be encountered such as port and airfield limitations.[69]

For information that exists outside of published literature and commercial channels, OSINT relies on Grey literature and information, encompassing all legally and ethically available information that is obtained through specialized channels and is not controlled by commercial publishers, booksellers, or subscription agencies.[70] Examples are working papers, technical reports, white papers, data sets, conference summaries, etc.; generally produced by non-profit organizations, commercial organizations, government, and clubs and associations.[71] The value of the exploita-

---

[66] NATO OSINT Handbook (2001)

[67] Sudemen, W. (2002). Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community. NATO Open Source Reader, NATO: 56-63.

[68] NATO OSINT Handbook (2001)

[69] Steele (2002)

[70] NATO OSINT Handbook (2001), and discussed in detail in Soule, M. H. a. R. R. P. (2002). Grey Literature. NATO Open Source Reader, NATO.

[71] NATO OSINT Handbook (2001) and Soule (2002)

tion of Grey information lies in the amount of information that exists outside traditional channels, yet this presents a serious challenge for collection, as does the non-standard format that grey information is likely to appear in.[72] To collect and analyze it effectively, specific collection strategies have to be put in place, and the necessary language and technical specialists have to be utilized. Competitive intelligence in the corporate world relies on grey sources, for example using the topics of speeches at conferences or the subjects discussed on blogs and user groups to deduce corporate strategies and weakness.

Perhaps the OSINT source with the broadest application is the commercial imagery industry. The rapid growth of the commercial satellite imagery industry has to some extent been so successful as to endanger the discipline of overhead imagery intelligence (IMINT) as a covert entity.[73] The growth of this industry has had a dramatic effect on the intelligence community, as images become available, states that previously did not have the technical means to launch satellites are able to gain access to imagery, and various non-governmental organizations are able to utilize satellite imagery to suit their purposes.[74] In the case of NGOs, the use of high-quality overhead imagery is an asset for bringing issues to the attention of media and governments. The use of satellite images to document mass graves in Yugoslavia in 1995 and 1999 and spur military intervention was driven by the U.S. government, but now that the same capabilities are in the hands of the private sector, groups outside of traditional channels of power are empowered to call attention to humanitarian disasters such as refugee flows, environmental damage, and ethnic cleansing.[75] In June of 2006, Amnesty International went public with commercially obtained satellite images showing for the first time the destruction of the Porta Farm settlement in Zimbabwe that displaced over 30,000 people[76]. Satellite photos are also routinely used to illustrate the consequences of global warming on the polar ice caps and other environmental issues. The increasing transparency that is brought on by the availability of these kinds of images pressures

---

[72] Soule (2002)

[73] Mercado (2004)

[74] Dehqanzada, Y. A. a. F., Ann M. (2002). Secrets for Sale: How Commercial Satellite Imagery Will Change the World. NATO Open Source Reader, NATO.

[75] Dehganzada (2002)

[76] AP (01/06/2006). Mugabe's obliteration of township exposed. The Australian.

governments to be more accountable for their actions, and the international community to take stronger action when presented with this kind of hard evidence.

While the collection of information in physical form, be it electronic or print, is the core of intelligence, the real revolution in OSINT and IT is the networks of experts that can be developed. In areas of the world where access is limited, the most cost effective and efficient method of gathering OSINT is through direct human observation and human expertise.[77] The human contribution to OSINT is separated into three levels: internal experts, external experts, and local knowledge.[78] The true merger of open source development concepts with OSINT is the way in which systems can be developed to exploit all three levels effectively. The separate pieces of information that can be gathered through a network of observers, experts, and even amateurs can result in a product that is superior to one prepared by a security cleared analyst. This is in large part due to the relative numbers; a network of human sources not limited by classification is huge, case officers are in short supply.[79] The idea of casting a broad net to encourage participation from outside the intelligence community is advocated by Robert R. Steele, an OSINT advocate and founder of Open Source Solutions (OSS.net). Steele makes two arguments; first, that to be effective, intelligence must draw upon what he refers to as the "seven tribes" of intelligence, government, military, law enforcement, business, academic, ground truth (non-governmental and media), and civil (citizens, labor unions, religions).[80] Second, that the contributions of these varied sources must be then communicated to the masses, to create "citizen centered intelligence" by enabling citizens to not only participate, but to draw upon the pooled knowledge created.[81] The SHARP program that was unveiled by the CIA in July 2006 is an attempt to bring in the outside community to the intelligence process, bringing in anthropologists, sociologists, psychologists, and religious

---

[77] NATO OSINT Handbook (2001)

[78] NATO OSINT Handbook (2001)

[79] Mercado (2005)

[80] The "seven tribes" are detailed on www.oss.net, and in Steele, R. D. (2006). Reinventing Intelligence, www.oss.net

[81] See Steele, R. D. (2002). The New Craft of Intelligence. Oakton, Virginia, OSS International Press, for an full discussion of "citizen centered intelligence", essentially an argument for the creation of web based portals where people can type in their zip code and be able to access all manner of reports on local issues, hard data on areas of concern, overviews of applicable laws, etc., to democratize information.

study experts in a four week conference with top CIA analysts.[82] This is perhaps a first step toward the creation of what Steele refers to as "Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing (M4IS)" that can reshape the intelligence community.[83]

OSINT contributes to the overall intelligence process in four main ways. First, open sources can provide the a "tip off" for classified sources though newsgroups, blogs, and traditional media[84]. Due to the speed at which events develop, and the impossibility of blanket coverage of all areas of the world with intelligence assets, analysts and policymakers must rely on open sources for cues.[85] The most striking example is the image of CIA officers watching the Berlin Wall fall on television, clearly a case of what a CIA veteran referred to as, "a time when public political activity proceeds at such a rapid and fulminating pace that secret intelligence, the work of agents, is overtaken by events publicly recorded".[86] Second, OSINT contributes to the efficiency of the overall intelligence effort by allowing classified assets to be targeted where they are most needed. If a question can be addressed using open sources, this gives the more expensive and in-demand covert programs more time to deal with assignments that are more suited to their skill sets, while still being available to validate open sources when necessary.[87] The third contribution is providing context and validation for closed sources by supplementing the classified data with general background information that is sometime lacking, such as economic data, political trends, and local "on the street" knowledge.[88] The forth and final contribution is in providing plausible cover for classified sources.[89] If a open source is found that validates a closed source, than the information can be shared more extensively with NGO's, other nations, and the public,

---

[82] Kaplan, D. E. (October 29, 2006). Hey, Let's Play Ball, U.S News and World Report.

[83] Steele (2006), Reinventing Intelligence

[84] NATO OSINT Handbook (2001)

[85] Mercado (2005)

[86] Quoted and discussed in more detail in Mercado (2004), p. 2

[87] NATO OSINT Handbook (2001)

[88] NATO OSINT Handbook (2001)

[89] NATO OSINT Handbook (2001)

increasing the usefulness and value of the information. This is particularly relevant in the context of multinational efforts like NATO, the UN, and coalition forces in the war on terror.[90]

When applied practically, OSINT can have a uniquely stabilizing effect in some situations where confidence building measures (CBMs) are being employed, as a mechanism to address problems posed by information imbalances, lack of trust in third party verification, and information sharing.[91] The pursuit of "information dominance" by advanced nations can exacerbate the threat perceptions held by weaker nations, and can increase reluctance to engage in transparency on arms control initiatives and other CBMs.[92] The U.S. pursuit of "information superiority" is driving the intelligence community[93], and contributing to an information imbalance that must be addressed. Problems arise through this somewhat shortsighted approach to the handling of information: not only are external threat perceptions and suspicions elevated, but information sharing is not facilitated by "dominance", if the information cannot be shared across borders to address common issues.[94] CBMs and regional cooperation initiatives are based on the assumption that a common view of reality can be established, consequently, if information can not or will not be shared to protect classification, then the whole process is flawed and seriously handicapped.[95] The role of third parties can also be addressed with OSINT, in that while intelligence provided by a regional power with superior capabilities will arouse suspicion, the ability of less powerful states to engage in effective OSINT collection will empower them by providing information that is either self originating or from a third party vendor such as a commercial satellite company, which will inspire more trust.[96]

---

[90] NATO OSINT Handbook (2001)

[91] Rathmell (2000)

[92] Rathmell (2000)

[93] Clift (2003)

[94] Rathmell (2000)

[95] Rathmell (2000)

[96] Rathmell (2000)

To these ends, OSINT can be employed to create Regional Conflict Prevention Centers (RCPCs), to share data and establish common perceptions in conflict prone regions.[97] An example of this concept can be seen in the Europe, with NATO/EU cooperation and the process towards a common intelligence policy (CIP).[98] In Europe, the foundation is built upon the intelligence sharing and cooperation mechanisms developed by the Western European Union (WEU), and specifically the WEU Intelligence Section and WEU Satellite Center.[99] The use of satellite imagery to verify treaty implementation, monitor arms control initiatives, provide general security surveillance, and maritime and environmental monitoring for use by member states represents a positive step toward regional intelligence integration.[100] The role of NATO in the CIP was addressed in the Petersberg Tasks, as well as the establishment of dialogues between the WEU and Russia and non-WEU Mediterranean countries.[101] In 1992 the first formal meeting of the WEU and NATO occurred, with one of the key outcomes an agreement to exchange classified information, and an agreement that the WEU could make use of NATOs integrated communication networks.[102] These and other measure established the frameworks for further integration, and explain why NATOs publications on OSINT are seen as the foundations of the discipline. Open sources hold high value to an organization that must communicate effectively across many nations and cultures. The European Security Strategy 2003 states, "common threat assessments are the best basis for common actions", a clear acknowledgment of the need for at the very least a shared view of reality.[103]

---

[97] This concept is explored in detail by Rathmell (2000), specifically in relation to the Middle East, where he proposes centers for the Levant and the Gulf to implement the Arms Control and Regional Security(ACRS) CBMs initiated in the Madrid peace process.

[98] Rathmell (2000)

[99] Pforzheimer, W. L. (1999). "Prospects for a European Common Intelligence Policy." CIA Studies in Intelligence Unclassified Edition 44(3).,

[100] Pforzheimer (1999), p. 5, provides a critique of the Satellite Center that is valid, but misses the key point, that it represents a multinational effort to jointly combat shared interests though the collection and dissemination of data to the member nations.

[101] NATO (2001). NATO Handbook: Implementation of the Petersberg Tasks, NATO.

[102] NATO Handbook: Implementation of the Petersberg Tasks (2001)

[103] EU (2003). A Secure Europe in a Better World: European Security Strategy. Brussels, EU.

The use of OSINT has been stymied by the mistaken belief that only secrets hold intelligence value. NATO identifies this as "excessive secrecy and compartmentalization", an over reliance on select methods in the name of operational security.[104] Traditionally the intelligence community has done what Eliot A. Jardines, the assistant deputy director of national intelligence for open source at the Open Source Center (OSC), refers to as "developing high", meaning building systems that are geared for the highest classification level possible. To address this Jardines advocates a culture of "low" development, to start at an unclassified level, and then move upward if necessary.[105] He is echoed by the Director of the OSC, Douglas J Naquin, who envisions the community changing to move away from the belief that the higher the classification, the more valid the information.[106] Both Naquin and Jardiens see a move toward open sources as advantageous not only because of the value of the information, but the freedom that lower or no classification can grant in the application of technology. It is far easier and more cost effective to integrate off-the-shelf products to use for intelligence purposes then to try to get hardware and software cleared for classified use.[107] Using off-the-shelf products allows for the use of the technology while it is still state of the art.[108] This keeps the intelligence community on the same level with potential foes like terrorists organizations and non-state actors who by default will be using the most current products on the market, as they have no capacity to develop classified systems. Using the best tools available is necessary to avoid the pitfalls of Interlink, which despite being hailed as a state of the art network in 2003, is behind the curve when compared to the internet that is used by the general public.[109]

The old model of operations is based upon a top-down chain of command, with short term time frames and a reliance on closed (classified) sources to support unilateral action by either nations

---

[104] This and other problems that can arise in intelligence analysis are discussed in Appendix C: Categories of Misconception and Bias(p. 46-47), in the NATO OSINT Handbook 2001

[105] Ackerman, R. K. (March 2006). "Culture Changes Weigh Heavily on Center Success." Signal.

[106] Ackerman (2006)

[107] Ackerman (2006)

[108] Barlow (2002)

[109] Clift (2003) writes that Interlink is "highly advanced" and "ever evolving", and connects government and military at the national, theater, and tactical level, but the experience of Alexander (2005) contradicts this praise by noting that in 2003, when Clift was writing, Interlink used an "outdated version of AltaVista", and there was no simple way to find data or communicate across the network.

or coalitions.[110] The new model, developed to address the growing role of larger coalitions and NGOs in any eventual action taken, has to be a bottom-up, multicultural, consensus based approach. This model has been shown to be the most effective method for arriving at consensus, particularly in the case of multinational organizations like NATO, who have to balance varying cultural, linguistic, and national interests.[111] The obvious choice to support for this model of operations is open source development and OSINT, due to the ease with which information can be shared when it is unclassified and the power of large peer-driven networks. In this manner, the expertise of government agencies, diplomatic corps, business communities, religious organizations, NGOs, and the academic community can all be drawn upon.[112]

Open source development and OSINT are conceptually linked because of their inherent collaborative nature and wide focus, as well as an emphasis on transparency in methods and sources. When employed jointly, these two methods can serve to force a break from the culture of secrecy in the intelligence community to an more open system that is better suited to the challenges presented by increasingly networked adversaries. The interaction between a new kind of knowledge management (open source development) and collection (OSINT) indiscriminately empowers government affiliated groups, positive social activist networks, as well as terrorist and criminal networks. Groups who take advantage of open source methods gain access to huge pools of collective knowledge and the means to build networks to both collect and distribute it, facilitating the horizontal movement of information and knowledge. The possibility of the application of an open source development system to the intelligence process allows for the best practices of the IT industry to be applied to the exponentially expanding quantity of open source material available to create the highest quality intelligence products with the greatest utility.

---

[110] NATO OSINT Handbook (2001)

[111] NATO OSINT Handbook (2001)

[112] NATO OSINT Handbook (2001), Barlow (2002) calls for the inclusion of librarians, journalists, scientists,, philosophers, sociologists, theologians, economists, artists, and cultural historians, to form a global "neighborhood watch", and Alexander (2005) envisions a CIA blog to attract interested people from all disciplines.