

██████████

Efficacy and Adoption of Central Web 2.0 and Social Software Tools in the U.S. Intelligence Community

American Public University System

American Military University

Department of Security and Global Studies

Charles Town, WV 25414

<http://www.amu.apus.edu>



David A Schroeder

david.a.schroeder@navy.mil

david.a.schroeder2@us.army.mil

<https://www.intelink.gov/wiki/das>

March 2011





Abstract

Over nearly the past decade, the United States Intelligence Community has struggled with how to effectively share information and transform the intelligence production process to leverage the explosion of social software tools. Post-9/11 reports, recommendations, directives, and legislation uniformly point to the need for the IC to move from the existing “need to know” mode to one of “need to share” and “responsibility to provide.” Initiatives like Intellipedia and A-Space have been held out as successes, but they have not fundamentally changed the “finished report” model of intelligence production. Grassroots adoption of new tools by eager young analysts has only gone so far, and the IC is in danger of not achieving the agility it needs to respond to today’s threats. Perils like Wikileaks threaten to undo the progress that has been made. What can be done to transform intelligence into a “living” product?





Abbreviations

CASE	Collaboration and Analyst/System Effectiveness
CIA	Central Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
FOUO	For Official Use Only
HCS	HUMINT Control System
HUMINT	Human Intelligence
IARPA	Intelligence Advanced Research Projects Agency
IC	Intelligence Community
ICD	Intelligence Community Directive
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
JWICS	Joint Worldwide Intelligence Communications System
NCTC	National Counterterrorism Center
NOFORN	No Foreign Nationals
NIB	NGA Intelligence Brief
NIE	National Intelligence Estimate
NIS	National Intelligence Strategy
NIPRNet	Non-classified Internet Protocol Router Network
NGA	National Geospatial-Intelligence Agency
OSINT	Open Source Intelligence
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SIPRNet	SECRET Internet Protocol Router Network
WMD	Weapons of Mass Destruction









Table of Contents

Introduction	6
Purpose	7
Key Research Questions	7
Hypothesis	8
Literature Review	8
Literature Summary	13
A Long Road	14
Tools to the Rescue	17
“Wikipedia for Spies”	19
Trouble Gaining Traction	21
The Road to Solutions	23
The Joint Product Line	24
Living Intelligence	28
Perils of Information Sharing?	30
Conclusion	35
Reference List	37

Tables and Figures

<i>Table 1: Laws and recommendations supporting information sharing</i>	15
<i>Table 2: Availability of Intelink services across security domains</i>	18
	
	
<i>Figure 1: Intellipublia user roles</i>	26
<i>Figure 2: Intellipublia Joint Product Line</i>	27
<i>Figure 3: Google Living Stories</i>	30





“Changing organizational culture is like herding cats. However, organizational change in the IC is more like herding cats, rats, bats, monkeys, tigers, lions, etc., while some of the animals are flying and jumping around in trees, and others are trying to eat them.”

— Pat Gorman, former IC CIO





Introduction

In recent years, the United States Intelligence Community (IC) has undertaken efforts to increase information sharing and collaboration across the sixteen agencies that comprise the IC. Various legislation, commissions, and directives have universally advocated for increased information sharing within the IC, between the IC and Department of Defense (DOD), and among other government elements, state and local authorities, and academia.

In response to this call for increased information sharing, the IC created and deployed tools designed to assist in these efforts. The tools are modeled after successful “Web 2.0” tools on the commodity Internet, such as wikis, blogs, media sharing tools, and other “social software.” Some tools are available only to a particular audience, while other tools, such as those provided by Intelink, are made uniformly available to intelligence and defense users. The goal is to foster their adoption through a combination of accessibility and availability, grassroots efforts, and training.

One of the prime examples of these tools is Intellipedia, a “wiki” similar to Wikipedia.

Four years since the launch of Intellipedia, collaboration is occurring, but the adoption has been limited. Many users express concerns about duplication of work, lack of time and resources to contribute to multiple tools, or uncertainty about how contribution to such tools may impact perception and recognition of work. Furthermore, most collaboration appears to default to the Top Secret environment for a variety of



██████████

possible reasons, limiting the reach and utility of these tools in the extended national security enterprise (e.g., state and local government and academia).

The real impact of these tools on information sharing in the IC remains unclear.

Purpose

To determine ways to increase the efficacy and adoption of central information sharing tools — such as Intellipedia and Intellipublia — to create a more agile and adaptive Intelligence Community.

Key Research Questions

General: Why do members of the US Intelligence Community have so many challenges utilizing central information sharing facilities, in light of numerous mandates to move from a “need to know” to “need to share” philosophy?

Specific: Why are US Intelligence Community agencies unable to effectively transition to utilizing interagency Web 2.0 and social software facilities, instead standing up their own “stove piped” tools or relying on existing, legacy intelligence production processes less conducive to collaboration and sharing?

Corollary: Can a workable model be demonstrated to create topical “living intelligence” resources and “snapshots,” as opposed to traditional finished intelligence products, that replace or supplement “big agency” production processes?



Hypothesis

In order for central information sharing tools to be utilized and succeed in transforming intelligence, existing processes for intelligence production must be changed to accommodate new mechanisms for collecting, sharing, and publishing information.

Literature Review

The deployment of information sharing and social software tools in the IC has been described in a number of articles in the mainstream press hailing the arrival of “Wikipedia for spies” (Calabresi 2009) or “Facebook for spies” (Shaugnessy 2008). The focus has certainly been a result of the interest in the rise in popularity of Web 2.0 tools in the eyes of the public, combined with curiosity about the secretive activities of the IC. However, this coverage does little to address the adoption or usefulness of these tools throughout the intelligence establishment.

Covering Intellipedia, other Intelink tools, and initiatives like A-Space in an unclassified forum is also complicated by the fact that large parts of the application of these tools are classified. Some of these tools are deployed in an unclassified form, for use by IC and DOD elements as well as state and local government. Ironically, even with this much broader audience, the tools deployed in the unclassified environment are the least used (Calabresi 2009). This may reflect the culture of secrecy in a community whose job it is to steal — and keep — secrets. Though unclassified and “open sources often equal or surpass classified information in monitoring and analyzing such pressing problems as terrorism, proliferation, and counterintelligence,” there is an attitude that



██████████

unless information is classified, it is not important. (Mercado 2005) This makes an accurate unclassified assessment difficult.

The CIA's Calvin Andrus (2005) helped to drive the modern IC social software movement by proposing an idea that is the basis for many of the central social software tools used throughout the IC today. Andrus put forth the notion that deploying or allowing the use of tools such as wikis and blogs would enable the agility necessary for the IC in the modern world, allow sharing between the IC and non-intelligence government counterparts, and create a critical mass which would enable the use of these tools to "self organize." In other words, individuals would contribute, review, and correct content, and good ideas would rise to the top while mediocre, chaotic, or poorly formed ideas would be marginalized or ignored. Andrus argues that deploying these tools combined with search and feedback mechanisms would create an environment that would naturally foster the growth of such tools. The core claim is that this will create an IC that can dynamically adapt and adjust itself in response to changing threats. Andrus acknowledges that this change will have challenges, but underestimates the difficulty that the adoption of such tools faces from existing institutional culture, organizational structure, and business processes.

As central shared tools were deployed for the IC under the auspices of the Director of National Intelligence (DNI), many media outlets watched with great interest. Thompson (2006) covered the launch of Intellipedia and blogs on Intelink, the IC's longtime information sharing environment, for *New York Times Magazine*. Thompson notes that the intelligence failures relating to the terrorist attacks of September 11, 2001, were found to be the result of a "failure to connect the dots," (Thompson 2006) and

██████████

relates the thinking among proponents of social software in the IC that such tools can help to do just that. One early assertion was that the unclassified Intellipedia, because of its much larger audience and potential user base, would grow the most rapidly. This assumption, widely held in the early days of these tools, proved to be incorrect. Thompson also observes that the failure of any Web 2.0 and social software initiatives could forever doom any reform efforts that hope to use such technologies in the IC. Thompson further notes that such tools, if successful, threaten to run afoul of traditional walls built between various intelligence components designed to protect the rights of American citizens. Thompson does aptly describe the existing organizational culture, which is resistant to the notion of a grass-roots social software movement that enables information sharing and crosses traditional organizational boundaries.

Subsequent media coverage is still enthusiastic about the prospects of the use of Web 2.0 and social software tools by the intelligence establishment. Calabresi (2009) covered the growth of Intellipedia for TIME and, interestingly, three years later still references the same failed attempt to create an NIE for Nigeria as Thompson (2006). However, Calabresi observes that the greatest benefit of social software in the IC is that individuals from varying backgrounds and agencies may collaborate on a topic outside of traditional organizational channels. Interestingly, Calabresi notes that the instance of Intellipedia operating on the Top Secret network is the most active, contrary to early predictions that it would be the unclassified Intellipedia that would stake this claim. However, because of a lack of emphasis on unclassified and open source products, analysts tend to migrate to the highest classifications instead of the lowest (Mercado 2005). Today, no finished intelligence products are created with Intellipedia. However,

██████████

experts argue that the reliance on such products is too heavy, and that “snapshots” of intelligence information about any given topic should be given precedence.

Jackson (2009) summarizes many of the problems as due the fact that grassroots adoption can only go so far. Chris Rasmussen of the National Geospatial-Intelligence Agency (NGA) explains that Intellipedia and other social software tools have not replaced existing intelligence production systems, meaning that analysts may have to enter and maintain the same data multiple times, or that analysts may be less likely to participate in the new tools because the old systems still exist. Rasmussen argues that top-down management support, coupled with replacing “big agency production systems,” is required to realize the true potential of the new tools.

The Director of National Intelligence (DNI) is continuing the push to expand information sharing throughout the IC. Intelligence Community Directive 501 (DNI 2009), or ICD 501, codifies in policy much of the letter and spirit of information sharing recommendations put forth by various commissions since September 11, 2001. One of the primary purposes of the policy is to “foster an enduring culture of responsible sharing and collaboration within an integrated IC,” (DNI 2009) while promoting the notion of a “need to share” and “responsibility to provide” versus “need to know” — alongside this is a “responsibility to discover”. These responsibilities require the establishment of information sharing environments to properly support information search and discovery, with the IC CIO “develop[ing] the IT architecture that supports this Directive” (DNI 2009). However, this directive has not resulted in significant change with respect to Intellipedia and other central tools provided by the DNI via Intelink.

██████████

De Rose *et al.* (2008) propose a model for community participation in wikis like Intellipedia with human contributors augmented with automated contributions from existing resources. This method is proposed as a way to add data from existing information systems and databases. This model keeps data up-to-date, eliminates the duplication of effort for users having to bring data in from other systems, and provides incentives for users to contribute additional information. This hybrid approach could provide an answer for the gulf that currently exists between existing intelligence production systems and new Web 2.0 and social software tools utilized by the IC.

The CASE Program Completion Report (IARPA 2008) is perhaps the most relevant attempt to measure the impact of information sharing tools on intelligence analysis throughout the Intelligence Community. The CASE report notes that “[t]he dominant view in 2005 both inside and outside government was that—despite post-9/11 reform efforts—the IC continued to be plagued by a culture of secrecy, compartmentation of information, and ‘need to know.’” It is precisely this problem that post-9/11 legislation and recommendations sought to overcome. By discovering ways to apply metrics to analyst performance, CASE hoped to demonstrate the effectiveness of various information sharing tools. CASE’s approach also dealt with what they referred to as “tacit collaboration,” as opposed to explicit, purposeful collaboration. This approach endeavored to measure what some call the “serendipitous interaction” enabled, in part, by social software tools. CASE’s efforts were hampered because measures of analytic quality are largely subjective in nature and impacted by many other variables. Because CASE was discontinued when the Intelligence Advanced Research Projects Agency (IARPA) absorbed the project, it issued only a program completion report at the time of

██████████

termination. However, the lessons learned from CASE provide a framework for future investigation.

Mergel *et al.* (2009) observed one positive aspect of the current landscape: the early growth of Intellipedia has outstripped that of public counterparts like Wikipedia, in part due to a “set of highly motivated and engaged employees.” However, the challenges of integrating such tools into a daily workflow are also highlighted, as are the roadblocks to success that exist, such as encouraging the sharing of knowledge and the voluntary utilization of available tools. Critically, there is a lack of incentive to “go the extra mile,” or to contribute to an additional system; thus, structures for incentive must be developed, and, notably, “standard operating procedures might have to be reengineered,” and well-established routines scrutinized (Mergel 2009). Mergel further notes that metrics to measure and incentivize performance must be established and included within the framework for employee performance evaluations. All of this is necessary to work against the *status quo* and to challenge the defensive attitude against innovation and change.

Literature Summary

Nearly all of the literature on the topic of information sharing tools in the IC makes reference to post-9/11 legislation and recommendations revolving around increasing information sharing and breaking down barriers to such sharing. The success of Web 2.0 and social software tools in the public realm has translated into a hope that the tools would have the same revolutionary impact on intelligence processes.



One shortcoming discussed in many of the articles, particularly earlier articles, is that there is an assumption that the mere existence of these tools would encourage increased information sharing organically. However, this assumption has not been borne out by reality. Subsequent coverage and analysis (e.g., Joch 2009) has begun to observe that the IC has traveled as far as it can go with “organic” adoption, and that existing, established intelligence agency production processes must change to utilize the new tools.

Another issue discussed is the assumption that the tools would grow fastest in unclassified environments, and slower in classified environments. In practice, the opposite has proven true. None of the literature examines the cause of this discrepancy, which may hold valuable information regarding barriers to adoption.

While the hope of organic adoption has been realized for a small number of early adopters and grassroots supporters, it has not been the case for most analysts throughout the Intelligence Community. An examination of the underlying reasons for barriers to adoption is needed to establish changes that would increase utilization of shared tools.

A Long Road

Since the terrorist attacks of 9/11, there has been a collection of reports, commissions, executive orders, directives, and legislation that have attempted to identify and address the information sharing deficiencies in the IC (Table 1).

The recommendations all share the common theme of challenging the status quo to shift from a “need to know” culture to one of “need to share” and “responsibility to provide.” The recommendations begin with the 9/11 Commission Report, and continue as a common theme through an array of subsequent reports and findings.

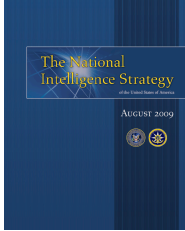





The power of these recommendations lies chiefly in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which establishes the DNI as the authority on these matters. Recommendations made by the DNI carry the weight of the authority to execute the law and act as the leader of the IC. The real power of the DNI to compel IC agencies to act has been a subject of significant debate.



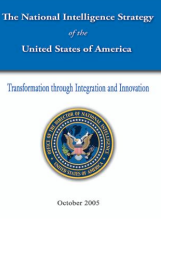



While the authority of the recommendations may be clear, the path to implementation and compliance has been murky. Metrics for demonstrating compliance do not exist, and there is no system of incentives to reward collaboration. These may be the core issues that hinder needed changes, and the adoption of the tools that could act as a vehicle for that change.

Table 1. Review of legislation, IC or other directives, and recommendations that support information sharing, and “need to share” vs “need to know” model (Courtesy Intellipedia Need to Share).

Document	Title and excerpt	Reference
	<p>National Intelligence Strategy 2009</p> <p><i>“Radically improve [...] information management, integration and sharing practices, systems and architectures (both across the IC and with an expanded set of users and partners) — meeting the responsibility to provide information and intelligence...”</i></p>	<p>August 2009</p> <p>p. 14</p> <p>DNI</p>
 <p>INTELLIGENCE COMMUNITY DIRECTIVE 501</p>	<p>Intelligence Community Directive (ICD) 501</p> <p><i>“IC elements shall treat information collected and analysis produced as national assets and, as such, shall act as stewards of information who have a predominant ‘responsibility to provide.’”</i></p>	<p>January 2009</p> <p>p. 2</p> <p>DNI</p>


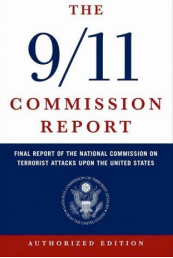




	<p>Intelligence Community Information Sharing Strategy</p> <p><i>“Together, we must challenge the status quo of a ‘need to know’ culture and move to one of a ‘responsibility to provide’ mindset.”</i></p>	<p>February 2008</p> <p>p. 9</p> <p>DNI</p>
	<p>100 Day Plan for INTEGRATION and COLLABORATION</p> <p><i>“[S]hift from the current ‘need to know’ mindset to create appropriate tension in the system to more effectively balance the ‘responsibility to provide’ while still addressing the requisite need to protect sources and methods...”</i></p>	<p>April 2007</p> <p>p. 9-10</p> <p>DNI</p>
	<p>National Intelligence Strategy 2005</p> <p><i>“Remove impediments to information sharing within the Community, and establish policies that reflect need-to-share (versus need-to-know) for all data, removing the ‘ownership’ by agency of intelligence information.”</i></p>	<p>October 2005</p> <p>p. 14</p> <p>DNI</p>
	<p>WMD Commission Report</p> <p><i>“[O]verly stringent protective requirements play too decisive a role in the decision to whether to share information [and] undervalue the need to share...”</i></p>	<p>2005</p> <p>Chapter 9</p> <p>WMD Commission</p>
	<p>Executive Order 13388</p> <p><i>“[G]ive the highest priority to the interchange of terrorism information between agencies and appropriate authorities of state, local, and tribal governments...”</i></p>	<p>October 2005</p> <p>White House</p>
	<p>Executive Order 13381</p> <p><i>“[A]gency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal.”</i></p>	<p>June 2005</p> <p>White House</p>





	<p>Intelligence Reform and Terrorism Prevention Act</p> <p><i>“The [DNI] shall have principal authority to ensure maximum availability of and access to intelligence information [...] establish policies and procedures to resolve conflicts between the need to share intelligence information and the need to protect intelligence sources and methods.”</i></p>	<p>December 2004</p> <p>118 STAT. 3650</p>
	<p>9/11 Commission Report</p> <p><i>“[A] system that requires a demonstrated “need to know” [...] assumes it is possible to know, in advance, who will need [it, and] that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate. The culture of agencies feeling they own information must be replaced by a culture [where] agencies feel they have a duty to mak[e] that information available. Agencies uphold a ‘need-to-know’ culture of information protection rather than promoting a ‘need-to-share’ culture of integration.”</i></p>	<p>2004</p> <p>p. 417</p> <p>9/11 Commission</p>

Tools to the Rescue

As Table 1 illustrates, information sharing has been a perennial challenge for the IC. Failures in information sharing have been blamed for intelligence failures related to the terrorist attacks on 9/11, the assessments of WMDs in Iraq, and the Christmas Day 2009 bombing attempt of Northwest Flight 253. A number of efforts have been undertaken in an attempt to address the information sharing problem.

While many information sharing tools exist throughout the agencies, the focus of this analysis is information sharing tools centrally provided for the IC by the DNI. Indeed, part of the problem is fragmentation of tools, or an avoidance of central tools in favor of standing up agency-specific tools, which defeats the purpose of such tools for





cross-agency sharing.

Intelink provides central Web 2.0 and social software resources available to the intelligence and national security communities. The mission of Intelink is to:

Enable ubiquitous web-based information sharing and collaboration capabilities that enable members of the extended national intelligence enterprise to collaborate in a common shared space (Intelink 2009).

Intelink has existed as an information sharing environment since 1994, but it has only been since about 2005 that major efforts have been undertaken to deploy Web 2.0 and social software tools. Intelink is unique in that it provides a consistent set of tools and services across the three security classification domains (Table 2).

Table 2. *Availability of Intelink services across security domains.*

Security domain	Network and function	Access
UNCLASSIFIED SBU	Intelink-U, for handling of unclassified information up to the Sensitive But Unclassified (SBU) or Controlled Unclassified Information (CUI) levels, such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and similar.	NIPRNet or peer networks designed to handle official unclassified traffic. Intelink-U Remote Access (RA) to DNI-U, from any internet connection.
SECRET	Intelink-S, for handling information up to the Secret level, with caveats such as NOFORN.	SIPRNet, a network designed to handle Secret traffic.
TOP SECRET SCI	Intelink-TS, for handling of information up to the Top Secret level, with facilities for handling Sensitive Compartmented Information (SCI) up to SI/TK/HCS/G.	Joint Worldwide Intelligence Communications System (JWICS), a network designed to handle Top Secret traffic.





Intelink services available on each security domain include (IC-CIO 2009):

- Intellipedia — Shared wikis which enable collaboration on topical articles and other content, based on MediaWiki, the same software which powers Wikipedia.
- Search — Enterprise search system supporting search and discovery across each security domain, powered by Google Search Appliance.
- Blog — Service familiar to many internet users, enabling individuals or workgroups to easily publish information to the web, and allow others to follow items of interest.
- Microblog — eChirp, a Twitter-like secure microblogging service that can be used to enhance situational awareness and information discovery across agencies.
- Instant Messaging — Provides instant, real-time chat functionality and chat rooms to support collaboration, crisis management, current event monitoring, etc.
- Document and media sharing — Share documents, media, and other content via a document management system, photo gallery, or a YouTube-like video sharing facility.

“Wikipedia for Spies”

The most popular of these tools — and the most commonly hailed in the press — is Intellipedia. Intellipedia is a “wiki.” Wikis are web-based tools which allow users to create, edit, and delete content in a collaborative fashion. The concept of an IC wiki originated from Dr. Calvin Andrus (2005) of CIA's Technology Innovation Center after studying the successful and popular wiki known as Wikipedia. Intellipedia does,



[REDACTED]

however, have critical differences from Wikipedia:

- Intellipedia does not enforce a neutral point of view to the same degree as Wikipedia, thus, allowing some differentiation to occur with the hope that a consensus view will emerge.
- Intellipedia can contain some non-encyclopedic content such as meeting notes and items of internal, administrative interest.
- Because of the flexibility, several offices throughout the IC are using Intellipedia to maintain and transfer knowledge on daily operations and events.
- Every edit on Intellipedia is attributed to a user — thus ensuring full transparency and accountability.

Intellipedia has been remarkably popular, and is most used in its classified variants [REDACTED]. This is surprising, because the unclassified variant has far more potential users since it is available to state and local government and other members of the extended national security enterprise (Intelink 2006). One major issue may be awareness, and individual organizations adopting their own tools to manage information. A Twitter-like microblogging tool, eChirp, shows similar higher usage in the Top Secret domain [REDACTED].

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

The usage patterns show that most users are still defaulting to utilizing classified resources, even when such use may not be necessary. When the Intelink tools are used, their use often duplicates work analysts may be performing within the constraints of their own agency's tools and processes. (Jackson 2009)

Trouble Gaining Traction

While central information sharing tools have enjoyed use from all IC and DOD components, much of the usage has come from voluntary early adopters. IC agencies are still reluctant to rely on these tools, out of a fear they may not be able to be "trusted." In other instances, analysts may have to duplicate work, entering information into both Intellipedia and an internal agency production system (Jackson 2009). Central tools like Intellipedia are not seen as an authoritative source of information because of the perception that wiki-based content is less "real" (Joch 2009, Jackson 2009).

██████████

While previous press coverage had been largely positive, in 2009 both Federal Computer Week (Joch 2009) and Government Computer News (Jackson 2009) published reports highlighting the difficulties in the adoption of these tools. The IC was described as “wrestling” with how best to utilize such tools, even suggesting that tools like Intellipedia may be suffering from a “mid-life crisis.” The articles asserted that the way forward is unclear. The main areas identified as problems were:

- Agencies feeling the need to “own” information, rather than sharing it
- Cultural and process differences between organizations
- Concern that differing analytic outlooks may be masked or lost
- Fear of losing control over information in a wiki, therefore making the information less accurate, timely, complete, or trustworthy
- Utilization of tools at higher levels of classification than necessary

A failed attempt to create a National Intelligence Estimate (NIE) on Nigeria using Intellipedia has been cited as an example of why such tools cannot be used for serious intelligence work. However, the issue wasn’t one of discovering relevant information, it was one of not fully trusting the information that was found, because of caveats which labeled information as not being “finished intelligence.”

Meanwhile, success stories shared a common element. In each case, a decision was made to use the wiki as the official — or only — facility for managing information. This makes the wiki the source of record, and eliminates duplicate or shadow systems. However, even these examples often represented usage within a single organization, not

[REDACTED]

for joint or interagency functions.

The Road to Solutions

In order for central information sharing tools like Intellipedia to be a success, legacy “big agency” production systems must be eliminated in favor of a new, joint production model. Indeed, the 2009 National Intelligence Strategy speaks to just this point in Enterprise Objective 4 (DNI 2009):

***Assure the environment.** Develop a world-class, Community-wide, assured information environment based on a common, effective, reliable, and secure infrastructure capable of providing information wherever IC elements or their customers are positioned.*

***Rationalize solutions.** Enable the rapid implementation of simple, logical, effective, cross-cutting solutions (materiel and non-materiel), recognizing the need to terminate and eliminate legacy systems.*

***Enable information flow.** Integrate assured and authorized discovery and access of information to the IC workforce, while ensuring timely and tailored dissemination of information at appropriate classification levels.*

***Improve information aggregation and analysis.** The IC must narrow the gap between our capacity to “sense data” and our capabilities to “make sense of data” in handling an exponentially increasing volume and variety of data and information.*

A persistent concern with the usage of Intellipedia for intelligence production has been losing control of the vetting and approval process for information. If two or more agencies’ analytic perspectives on an issue differ, how can that difference be maintained and highlighted if consensus is not reached? How can a “living intelligence” product maintain a “finished,” approved version, while still also allowing edits and updates, all

██████████

without compromising the integrity of the latest vetted version approved by a single agency or the community as a whole? The answer has more than one part.

One part of the answer is that agencies must actively choose to transition from existing production systems and business processes to new joint production methods. This will require a major cultural shift, significant management support, and performance metrics to judge and reward participation, the mechanics of which are beyond the scope of this paper. However, reasons given why these changes are not possible or practical usually revolve around limitations in control of production processes in tools like Intellipedia.

The other part of the answer is that tools must be specifically designed to address these concerns. They must operate in a joint/interagency environment, and enable agency-specific approval and signoff on approved content (maintaining a major feature of agency production), while still allowing edits and additional information and perspectives to be added by any other agency (maintaining the benefits of community-wide information sharing and the agility provided by a wiki).

The brief video “Toward Living intelligence” highlights the problems and solutions in this realm: <http://youtube.com/watch?v=nbgQ1V2BLEs> (Rasmussen 2009a).

The Joint Product Line

Intellipublia is an enhanced wiki tool, also built on MediaWiki as Intellipedia, but with enhancements to support interagency production. Intellipublia seeks to migrate existing knowledge creation and dissemination processes into a community collaborative environment.

██████████

The present factory-modeled IC production systems generate over 50,000 products per year, many of which are redundant and unread (Rasmussen 2009a). While tools like A-Space and Intellipedia are faster and more collaborative, they suffer from their separation from the traditional production process. They are considered “good for collaboration but not for official production” (Rasmussen 2009a).

The long-term goal of Intellipublia is to make the process faster and less redundant, while providing customers with the most reliable information available. This can be achieved by moving the review process into the same spaces where collaboration takes place.

The short-term goal of Intellipublia is to generate transparent wiki-based intelligence in the same channels as finished intelligence. The long-term goal of Intellipublia is to generate joint living analysis where tailored snapshots are the exception, not the rule, and where “products” are the by-product of the collaborative process, not the end state (Rasmussen 2009b).

Intellipublia seeks to:

- “Build upon best practices of the open collaboration model while preserving the spirit and idea of the traditional review process;” and
- “Reduce siloed production and duplication through transparent drafting, review, and dissemination (Intellipublia builds on common information, while highlighting different analytic lines in the context of the information at hand).”

Intellipublia accomplishes this by integrating drafting, review, and dissemination

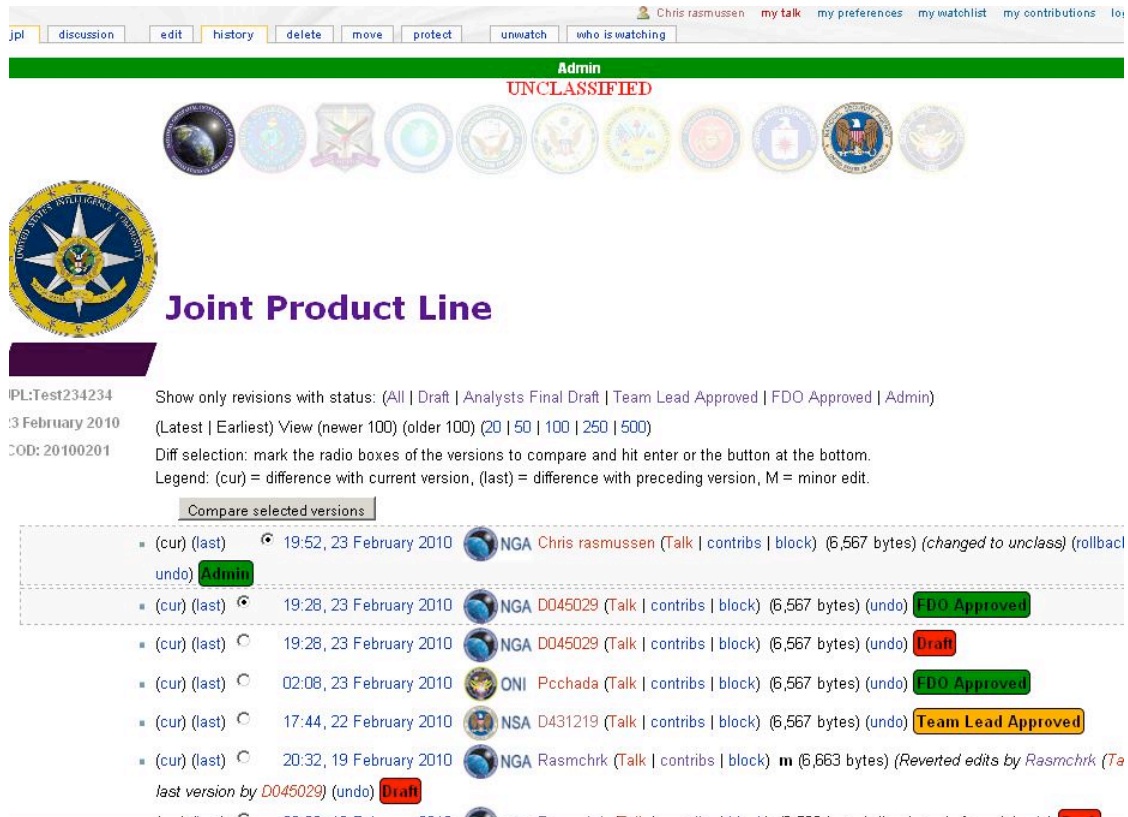
markings into the workflow of an Intellipedia-like solution (Figure 1 and Figure 2). The Joint Product Line will consist of topical articles to which all agencies can contribute information and analysis. In October 2009, Intellipublia was used to produce an NGA Intelligence Brief (NIB), an official NGA intelligence product (Rasmussen 2009b).

Figure 1. Intellipublia user roles are denoted with colored stamps (Rasmussen 2009b).

Diff selection: mark the radio boxes of the versions to compare and hit enter or the button at the bottom.
 Legend: (cur) = difference with current version, (last) = difference with preceding version, M = minor edit.

Compare selected versions		
<input checked="" type="radio"/>	(cur) (last)	14:55, 18 June 2009 Didebap (Talk contribs) (1,943 bytes) (undo) FDO Approved
<input checked="" type="radio"/>	(cur) (last)	13:45, 22 May 2009 Dieckcx (Talk contribs) (1,943 bytes) (undo) Team Lead Approved
<input type="radio"/>	(cur) (last)	14:17, 20 May 2009 Disieam (Talk contribs) (1,943 bytes) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	14:12, 20 May 2009 Disieam (Talk contribs) (1,943 bytes) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	13:22, 20 May 2009 Disieam (Talk contribs) (1,943 bytes) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	14:42, 14 July 2008 Dieckcx (Talk contribs) (undo) Team Lead Approved
<input type="radio"/>	(cur) (last)	18:21, 30 June 2008 Disieam (Talk contribs) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	15:27, 26 June 2008 Disieam (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	13:38, 26 June 2008 Disieam (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	12:50, 18 June 2008 Disieam (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	19:20, 22 January 2008 Didavjy (Talk contribs) (undo) FDO Approved
<input type="radio"/>	(cur) (last)	10:32, 22 October 2007 Cnboyjx (Talk contribs) (undo) Team Lead Approved
<input type="radio"/>	(cur) (last)	10:31, 25 September 2007 Cnboyjx (Talk contribs) (undo) Team Lead Approved
<input type="radio"/>	(cur) (last)	10:31, 25 September 2007 Cnboyjx (Talk contribs) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	10:30, 25 September 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	17:00, 21 August 2007 Yrnacaj (Talk contribs) (undo) FDO Approved
<input type="radio"/>	(cur) (last)	16:33, 7 August 2007 Dieckcx (Talk contribs) (undo) Team Lead Approved
<input type="radio"/>	(cur) (last)	16:33, 7 August 2007 Dieckcx (Talk contribs) (undo) Analysts Final Draft
<input type="radio"/>	(cur) (last)	16:33, 7 August 2007 Dieckcx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	15:30, 3 August 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	15:29, 3 August 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	12:41, 9 July 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	09:35, 6 July 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	16:15, 5 July 2007 Cnboyjx (Talk contribs) (undo) Draft
<input type="radio"/>	(cur) (last)	16:14, 5 July 2007 Cnboyjx (Talk contribs) (undo) Draft

Figure 2. *Intellipublia’s Joint Product Line combines official agency review with emergent social content for joint output. Users can consume and compare “authorized” versions to the emergent “living” version. Agency logos quickly denote that official vetters have reviewed the content (Rasmussen 2009b).*



Unfortunately, existing legacy intelligence analysis and production processes continue to dominate. The massive increases in intelligence budgets after 9/11 created an environment that fostered even more “duplication of effort, fragmentation, and sprawl throughout the [IC]” (Rasmussen 2010). The push for increased information sharing and “jointness” in the IC is embodied in legislation, directives, and other recommendations in the wake of 9/11 (Table 1). The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) is one of the key elements in the focus on collaboration in the IC.

However, IC agencies awash in post-9/11 spending also built upon existing

[REDACTED]

business processed and old habits resulting in “massive duplication of effort,” with “each intelligence agency still behav[ing] much like an independent newspaper writing whatever it wants with limited coordination with other agencies” (Rasmussen 2010). Thus, tools that are designed to break the old models and enable collaboration across organizational boundaries have not made significant inroads into the core business function of the IC: intelligence analysis and production. Old behaviors and stove piping were reinforced because the process remained the same.

One key observation about just why this is so is that “each agency, command, and fusion center controls every process associated with production and can conduct each process in a vacuum,” (Rasmussen 2010) and there is no mandate, beyond recommendations to increase sharing of *finished* intelligence products, to coordinate the intelligence *production* process across agency boundaries. While some analytic collaboration has been enabled by social software, these tools still remain at best as a complement to and not a replacement for existing production processes across the IC.

Living Intelligence

A new to effort to move forward the notion of “living intelligence” is a joint project undertaken as part of a competition to transform intelligence work at the National Geospatial-Intelligence Agency (NGA). Known as the “Living Intelligence System,” the project proposal asserts that the IC “has virtually exhausted the limits of technology working within the framework of the proprietary, vertically vetted finished intelligence model,” and proposes a model with “the flexibility to meet consumer-defined needs by replacing a user interface dominated by static, traditional [intelligence discipline]

██████████

reporting methods with integrated, topical and ‘living’ production that consolidates access into one intuitive place under one topic[al article]” (Rasmussen 2011a).

The Living Intelligence System uses software from Google Labs’ Living Stories project, an “experiment in presenting news [...] designed specifically for the online environment,” in which “complete coverage of an on-going story is gathered together and prioritized on one [page]” (Figure 3, Google 2010). Instead of having multiple news outlets create multiple — but slightly different — articles about the same topics, information from a variety of sources is gathered using a topical methodology. The analogy for the IC is that different news outlets represent IC agencies, and news articles become topics of intelligence interest.

The Living Intelligence System moves “away from static, duplicative reporting toward joint, living stories that weave in micro-updates, deep-dive analysis, multi-media, GIS projects, and ‘apps’ related to an intelligence topic” (Rasmussen 2011a). This approach can be combined with the with the vetting, agency voice, and approval component of the Joint Product Line while leveraging the “crowd sourcing” benefits of social software and Web 2.0 technologies. This is the missing piece in efforts to increase information sharing: not only must information and intelligence be shared, but **the intelligence analysis and production process must be shared.**


This project will feature a web site to present topical output, and two content generation engines: a Wordpress blog, and a MediaWiki site using the same software as Intellipublia. All development and testing will occur on the public Internet. See <http://youtube.com/watch?v=9ft3BBBg99s> for supporting video (Rasmussen 2011b).

Figure 3. Google Labs Living Stories displays topical news articles from multiple sources on a single page, with ability to organize chronologically and “deep dive.”



Perils of Information Sharing?

In 2010, a major controversy erupted when an organization called WikiLeaks released on the Internet large amounts of classified information relating to US activities in Iraq and Afghanistan, including hundreds of thousands of field reports and State Department cables. It has been suggested that this breach was a result of increased information sharing or the lack of adequate controls on information sharing, but the IC and DOD have taken a balanced approach in response.



Background

WikiLeaks defines itself as a “not-for-profit media organization” with a goal to “bring important news and information to the public” (WikiLeaks 2010), “founded by Chinese dissidents, journalists, mathematicians and start-up company technologists, from the US, Taiwan, Europe, Australia and South Africa” (WikiLeaks 2008). At its launch, WikiLeaks stated that its “primary interest is in exposing oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East, but we also expect to be of assistance to people of all regions who wish to reveal unethical behavior in their governments and corporations” (WikiLeaks 2008).

WikiLeaks is a flat, decentralized, volunteer organization. WikiLeaks has no headquarters or leadership, *per se*, though Australian Julian Assange is often described as the site's founder (Mey 2010). However, Assange does not identify himself as a founder and its creators have not been formally identified (Marks 2007). Some accounts describe Assange as having a disproportionate amount of power (Taylor 2010). As of January 2010, the WikiLeaks team consisted of five people working full time and about 800 people who work occasionally, mostly anonymously and via the Internet (Mey 2010). WikiLeaks has an advisory board, which guides its direction, and receives significant legal and other assistance from a number of major media and journalism organizations (Mey 2010).

The function of WikiLeaks is to provide a vehicle for the release of secret or sensitive information, without fear of repercussions for the individual leaking the information. Via this capability, WikiLeaks hopes to affect political change. WikiLeaks’

██████████

Assange has said that if asked to choose between “advocate” and “journalist,” he would choose “advocate.” (Cohen 2010) The leaks of classified materials to WikiLeaks related to the wars in Afghanistan and Iraq have constituted the largest leak of classified information in history. These disclosures were “designed to weaken support for both wars” (Ackerman 2010).

WikiLeaks’ primary mechanism for enabling leaks of information is a web site hosted by a “refugee hosting” site in Sweden. Via this web site and other means, WikiLeaks provides a secure and anonymous mechanism to submit files with strong encryption. WikiLeaks then analyzes the submissions to test their veracity (WikiLeaks 2010). If deemed acceptable for publication, a WikiLeaks author writes a story explaining the relevance of the material, and posts that analysis along with the source material itself. The hallmark of WikiLeaks is complete anonymity for sources, reducing the level of fear many may have of leaking sensitive information. (WikiLeaks 2010)

WikiLeaks’ initial mission statement focused on “exposing oppressive regimes.” Some analysts believe that it is open societies, not oppressive regimes, which suffer the most from the existence of organizations like WikiLeaks (Aftergood 2010). Nearly all of the highlighted material WikiLeaks features on its web site are leaks from the United States and other democracies.

Information Sharing to Blame?

The classified information obtained by WikiLeaks is thought to have originated from a single source, US Army PFC Bradley Manning. Manning has been charged with 23 counts of various offenses relating to these disclosures, including a capitol offense

██████████

(AFPS 2011). In his position as an intelligence analyst, Manning had access to a number of different networks and information repositories. This included Situation Reports (SITREP) from soldiers in the field in Iraq and Afghanistan, and State Department cables shared with the DOD via a program called Net-Centric Diplomacy (NCD) (Calabresi 2010). Under NCD, certain cables could be marked for SIPRNet distribution (SIPDIS). Cables marked SIPDIS were then automatically shared with cleared DOD personnel.

After the Wikileaks disclosures, a number of media outlets began to analyze whether the government's increased information sharing efforts were to blame, saying that WikiLeaks "proved that there's a downside to better information-sharing." (Nakashima 2010) James Clapper, the Director of National Intelligence, has said he believes the Wikileaks disclosures will have a "chilling effect" on information sharing (Nakashima 2010). Ranking House Intelligence Committee member Rep. Pete Hoekstra argued that the Wikileaks disclosures were a result of information being shared too broadly (Strohm 2010). Indeed, after the disclosure of the State Department cables, the State Department removed access to NCD from SIPRNet (Calabresi 2010).

In response, the DOD has made a number of changes to workstations on SIPRNet, including limiting the number of systems that can download data to removable media, and requiring approval from another authority to do so (Nakashima 2010). The DOD is also considering controls similar to those used by credit card companies to detect anomalous behavior in real-time (Christie 2010). Deputy Secretary of Defense William Lynn said the balance was "how to better protect information without denying soldiers the real-time battlefield intelligence they need to win wars" (Christie 2010). The challenge, according to DNI Clapper, is to discover when "somebody's downloading a

[REDACTED]

half-million documents [such that] we find out about it contemporaneously, not after the fact” (Nakashima 2010).

A number of former IC and DOD officials and other experts cautioned against an overreaction to WikiLeaks that would harm improvements in information sharing (Horowitz 2010). Former NSA director General Michael Hayden (2010) warned that we should not “conclude that this is too much information and too many people, and [...] once again trad[e] off potential physical safety for information security.” Andrew McAfee (2010), a Fellow at Harvard’s Berkman Center for Internet and Society and principal research scientist at the Center for Digital Business in the MIT Sloan School of Management, worried that a return to the “need to know” *versus* “need to share” model would be a misguided response, and undo progress in intelligence sharing. McAfee argues that technology and information sharing are not to blame, but rather the individual who chose to leak classified information. Others have argued that while the individual may be to blame, information sharing and modern technology enable breaches that may not have been possible or practical in the past, with James Lindsay of the Council on Foreign Relations arguing, “Back in the pre-internet days you would have needed a semi-trailer to walk off with a quarter million documents. Today you can fit that information on a thumb drive” (Lindsay 2010).

While Wikileaks has resulted in tightening of security policies (Nakashima 2010), it appears to not have significantly impacted information sharing. Secretary of Defense Robert Gates observed that the disclosure was an embarrassment, but that the actual consequences for US foreign policy are “fairly modest” (Ackerman 2010a). Michael Leiter, head of the National Counterterrorism Center (NCTC) said that the “much-

██████████

predicted halt in intelligence agencies' sharing has yet to manifest itself," and that the IC is in a "a relatively healthy place on information sharing" (Ackerman 2010b).

Conclusion

Information sharing has been identified as an area of major deficiency in the Intelligence Community in the years since 9/11. At the same time, the rise of Web 2.0 and social software on the open Internet has demonstrated its effectiveness for sharing information quickly and broadly. The Intelligence Community has sought to apply the success of Web 2.0 and social software to its own information sharing problems.

Intelligence Community innovators have suggested that such tools could enable the Intelligence Community be more adaptive, agile, and effective. A collection of Web 2.0 and social software tools has been made available, both centrally and within individual agencies. It is the central tools that will have the most utility and benefit for interagency information sharing.

The fact that the tools simply exist, though, is not enough. There have been numerous clear directives since 9/11 laying out the need to enhance information sharing and collaboration. However, this has not changed the fundamental culture of the Intelligence Community, which has long been one of discovering and keeping secrets — even from other agencies. This creates an environment where information is something to be hoarded, rather than shared.

The tools are available to enable the beginning of a cultural shift in the Intelligence Community. IC management must carefully assess the meaning of the numerous directives on information sharing, and discover how to implement new



intelligence production processes in place of the old. If this challenge can be met, it will be a win for the Intelligence Community, and the people it is charged with protecting.

The unclassified literature is enthusiastic about the prospects for these tools, but provides only a cursory look at the landscape, with sometimes ill-suited comparisons to public tools. A comprehensive unclassified study would have the benefit of much wider scrutiny, allowing for broader examination of the reasons for limited adoption of the tools for intelligence purposes. Sadly, the recent disclosures of classified information by WikiLeaks threaten to hamper or even reverse gains in information sharing and collaboration (Nakashima 2010). New tools such as Intellipublia's Joint Product Line and the Living Intelligence model (Rasmussen 2010, Rasmussen 2011) provide a way forward, but management buy-in and support will be required for success.



Reference List

- Ackerman, Robert. 2009. "Intelligence Community Embraces Virtual Collaboration." *SIGNAL*, May.
<http://www.afcea.org/signal/articles/templates/200904SIGNALConnections.asp?articleid=1918&zoneid=258> (accessed January 18, 2011).
- Ackerman, Spencer. 2010. "Pentagon Boss Is Not Sweating WikiLeaks." *WIRED*, November 30. <http://www.wired.com/dangerroom/2010/11/pentagon-boss-is-not-sweating-wikileaks/> (accessed February 5, 2011).
- Ackerman, Spencer. 2010. "WikiLeaks Hasn't Broken U.S. Intelligence. Yet." *WIRED*, November 30. <http://www.wired.com/dangerroom/2010/12/counterterrorism-chief-doesnt-see-info-freeze-from-wikileaks-yet/> (accessed February 5, 2011).
- Aftergood, Steven. 2010. Wikileaks Fails "Due Diligence" Review. *Secrecy News*, June 28. http://www.fas.org/blog/secrecy/2010/06/wikileaks_review.html (accessed February 26, 2011).
- American Forces Press Service (AFPS). 2011. "Army Adds 22 Charges Against Intelligence Analyst." *Defense.gov*, March 2.
<http://www.defense.gov/news/newsarticle.aspx?id=63002> (accessed March 3, 2011).
- Andrus, D. Calvin. 2005. "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence* 49, no. 3 (September 2005): 63-

██████████

70. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=755904 (accessed January 18, 2011).

Bray, David. 2008. "Knowledge Ecosystems: Technology, Motivations, Processes, and Performance" (Ph.D. diss., Emory University), in Social Science Research Network. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1016486 (accessed January 18, 2011).

Calabresi, Massimo. 2009. "Wikipedia for Spies: The CIA Discovers Web 2.0," *TIME*, April 8. <http://www.time.com/time/nation/article/0,8599,1890084,00.html> (accessed January 18, 2011).

Calabresi, Massimo. 2010. "State Pulls the Plug On SIPRNet," *TIME*, November 29. <http://swampland.blogs.time.com/2010/11/29/state-pulls-the-plug-on-siprnet/> (accessed February 5, 2011).

Christie, Michael. 2010. U.S. mulls credit card-type monitoring to halt leaks. *Reuters*, October 27. <http://in.reuters.com/article/idINIndia-52465720101026> (accessed February 26, 2011).

Cohen, Noam, and Brian Stelter. 2010. Iraq Video Brings Notice to a Web Site. *New York Times*, April 6. <http://www.nytimes.com/2010/04/07/world/07wikileaks.html> (accessed February 26, 2011).

De Rose, Pedro et al. 2008. "Building Community Wikipedias: A Machine-Human Partnership Approach," *IEEE Data Engineering* 24: 646-55.



<http://pages.cs.wisc.edu/~whshen/papers/madwiki-icde08.pdf> (accessed January 18, 2011).

Director of National Intelligence. 2009. "Intelligence Community Directive 501: Discovery and Dissemination or Retrieval of Information within the Intelligence Community." Director of National Intelligence Electronic Reading Room, January 21. http://www.dni.gov/electronic_reading_room/ICD_501.pdf (accessed January 18, 2011).

Director of National Intelligence. 2010. "ODNI Fact Sheet." Director of National Intelligence Electronic Reading Room, July 16. http://www.dni.gov/press_releases/20100716_Fact%20Sheet.pdf (accessed February 5, 2011).

Google. 2010. "Living Stories." Google Labs. <http://livingstories.googlelabs.com> (accessed February 26, 2011).

Harris, Brian. 2008. "Intellipedia: Leading a Transformation in Knowledge Management within the Intelligence Community." In "Knowledge Management," Special issue, Military Intelligence Professional Bulletin 34, no. 1 (January - March). http://www.fas.org/irp/agency/army/mipb/2008_01.pdf (accessed February 5, 2011).

Hayden, Michael V. 2010. "Who's to blame for damage from WikiLeaks?" *CNN*, December 7. <http://www.cnn.com/2010/OPINION/12/07/hayden.wikileaks.damage/> (accessed February 5, 2011).





Herzog, Ari. 2009. "Looking at Government 2.0 Social Tools." *Ari Herzog*, January 26.

<http://ariherzog.com/guest-interview-with-chris-rasmussen-looking-at-government-20-social-tools/> (accessed February 5, 2011).

Horowitz, Michael C. 2011. "After WikiLeaks: Overreaction could do more damage than anything revealed in the leaked diplomatic cables." *Penn Gazette*, Jan-Feb.

<http://www.upenn.edu/gazette/0111/expert.html> (accessed February 5, 2011).

Howard, Alex. 2010. "Connecting the dots with Intellipedia: U.S. intelligence agencies are using an internal wiki for knowledge sharing." *O'Reilly Radar*, June 3.

<http://radar.oreilly.com/2010/06/connecting-the-dots-with-intel.html> (accessed February 5, 2011).

Intelligence Advanced Research Projects Agency. 2008. "Collaboration and Analyst/System Effectiveness (CASE)," Program Completion Report, December.

Intelink (Director of National Intelligence), "Intelink-U Eligibility Criteria," Intelink Enterprise Collaboration Center, 4 December 2006,

<http://ra.intelink.gov/eligibilitycriteria.pdf> (accessed February 5, 2011).

IC-CIO (Director of National Intelligence). 2009. "ICES Overview," FOSE Conference AFFIRM Luncheon, June 20. [http://www.powershow.com/view/b084-](http://www.powershow.com/view/b084-NGM2N/ICES_Overview_AFFIRM_Luncheon_FOSE_Conference)

[NGM2N/ICES_Overview_AFFIRM_Luncheon_FOSE_Conference](http://www.powershow.com/view/b084-NGM2N/ICES_Overview_AFFIRM_Luncheon_FOSE_Conference) (accessed January 18, 2011).





Jackson, Joab. 2009. "Intellipedia suffers midlife crisis," *Government Computer News*, May 7. <http://gcn.com/Articles/2009/02/18/Intellipedia.aspx> (accessed January 18, 2011).

Joch, Alan. 2009. "Intelligence community wrestles with Web 2.0 tools for information sharing," *Federal Computer Week*, May 14. <http://fcw.com/articles/2009/05/18/data-sharings-new-mandate.aspx> (accessed January 18, 2011).

Kash, Wyatt. 2010. "Reduced funding might actually improve intelligence work." *Federal Computer Week*, May 28. <http://fcw.com/articles/2010/05/28/reduced-funding-might-help-intelligence-work.aspx> (accessed February 5, 2011).

Krzmarzick, Andy. 2010. "The high-impact approach to knowledge sharing." *Federal Computer Week*, May 19. <http://fcw.com/articles/2010/05/24/back-talk-govloop-knowledge-management.aspx> (accessed February 5, 2011).

Lindsay, James. 2010. "Wikileaks cables expose world leaders' sensitive diplomacy." *Washington Post*, November 29. <http://www.washingtonpost.com/wp-dyn/content/discussion/2010/11/29/DI2010112902197.html> (accessed March 3, 2011).

Marks, Oliver. 2010. "Wikileaks: Collaboration vs Silos & Stovepipes." *ZDNet Collaboration 2.0*, November 29. <http://www.zdnet.com/blog/collaboration/wikileaks-collaboration-vs-silos-stovepipes/1747> (accessed February 5, 2011).



██████████

Marks, Paul. 2007. How to leak a secret and not get caught. *New Scientist*, January 12.
<http://www.newscientist.com/article/mg19325865.500-how-to-leak-a-secret-and-not-get-caught.html> (accessed February 26, 2011).

McAfee, Andrew. 2006. "Enterprise 2.0: The Dawn of Emergent Collaboration." *MIT Sloan Management Review* 47, no. 3 (Spring). <http://sloanreview.mit.edu/the-magazine/articles/2006/spring/47306/enterprise-the-dawn-of-emergent-collaboration/> (accessed January 18, 2011).

McAfee, Andrew. 2010. "Did WikiLeaks' "Cablegate" Result From Too Much Information Sharing?" *Harvard Business Review*, November 29.
<http://blogs.hbr.org/hbr/mcafee/2010/11/did-wikileaks-cablegate-result.html>
(accessed February 5, 2011).

McAfee, Andrew. 2011. "Living Intelligence." *Andrew McAfee's Blog*, January 28.
<http://andrewmcafee.org/2011/01/living-intelligence/> (accessed February 5, 2011).

Mercado, Stephen. 2005. "Reexamining the Distinction Between Open Information and Secrets," *Studies in Intelligence* 49, no. 2. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm (accessed March 5, 2011).

Mergel, Ines, Charlie Schweik, and Jane Fountain. 2009. "The Transformational Effect of Web 2.0 Technologies on Government," University of Massachusetts National Center for Digital Government.



http://www.umass.edu/digitalcenter/research/pdfs/Mergel_Web20.pdf (accessed January 18, 2011).

Mey, Stefan. 2010. Leak-o-nomy: The Economy of Wikileaks: Interview with Julian Assange. *Media, money and beyond*, January 4.

<http://stefanmey.wordpress.com/2010/01/04/leak-o-nomy-the-economy-of-wikileaks/> (accessed February 26, 2011).

Nakashima, Ellen. 2010. “With better sharing of data comes danger.” *Washington Post*, November 29. <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/28/AR2010112804138.html> (accessed January 18, 2011).

Rasmussen, Chris. 2009a. “Toward Living Intelligence” (video). June 2.

<http://www.youtube.com/watch?v=nbgQ1V2BLEs> (accessed March 5, 2011).

Rasmussen, Chris. 2009b. “Intellipublia’s first official wiki-based output,” Need-to-Share Guy, October 16. https://www.intelink.gov/blogs/chris_rasmussen/?p=175 (accessed February 5, 2011).

Rasmussen, Chris. 2010. Increasing “Jointness” and Reducing Duplication in DoD Intelligence. *DoD INVEST*, October 6. <http://ctovision.com/2010/10/increasing-jointness-and-reducing-duplication-in-dod-intelligence/> (accessed January 18, 2011).

Rasmussen, Chris, Michael Preville, Peter Voth, Ben Josefson, Arwen Vidal, Matt Topper, Jon Ruark, and Nick Livingston. 2011b. “Living Intelligence.” Project for





NGA Director's Online Contest on the NGA Vision to "fundamentally change the user's experience."

Rasmussen, Chris. 2011b. "Living Intelligence System" (video). January 21.

<http://youtube.com/watch?v=9ft3BBBg99s> (accessed March 5, 2011).

Reilly, Sean. 2011. "Despite WikiLeaks, Joint Chiefs vice chairman endorses info-sharing." *Federal Times*, December 8.

<http://www.federaltimes.com/article/20101208/DEPARTMENTS01/12080301/1001> (accessed February 5, 2011).

Shane, Scott. 2010. "Keeping Secrets WikiSafe." *New York Times*, December 11.

<http://www.nytimes.com/2010/12/12/weekinreview/12shane.html> (accessed February 5, 2011).

Shaugnessy, Larry. 2008. "CIA, FBI push 'Facebook for spies'." *CNN*, September 5.

<http://www.cnn.com/2008/TECH/ptech/09/05/facebook.spies/> (accessed January 18, 2011).

Stewart, Phil. 2010. "Analysis: WikiLeaks may set back U.S. intelligence sharing."

Reuters, November 29. <http://www.reuters.com/article/2010/11/29/us-wikileaks-intelligence-idUSTRE6AS67F20101129> (accessed February 5, 2011).

Strohm, Chris. 2010. "WikiLeaks Sparks Debate Over Pentagon's Secret Network."

National Journal, December 2.

<http://nationaljournal.com/member/daily/wikileaks-sparks-debate-over-pentagon-s-secret-network-20101202> (accessed February 5, 2011).



██████████

Taylor, Jerome. 2010. Secret War at the Heart of Wikileaks. *The Independent*, October 25. <http://www.independent.co.uk/news/media/online/secret-war-at-the-heart-of-wikileaks-2115637.html> (accessed February 26, 2011).

Thompson, Clive. 2006. "Open-Source Spying." *New York Times Magazine*, December 3. <http://www.nytimes.com/2006/12/03/magazine/03intelligence.html> (accessed January 18, 2011).

Warrick, Joby. 2010. "WikiLeaks cable dump reveals flaws of State Department's information-sharing tool." *Washington Post*, December 31. <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/30/AR2010123004962.html> (accessed February 5, 2011).

WikiLeaks. 2008. About WikiLeaks. WikiLeaks. <http://web.archive.org/web/20080314204422/http://www.wikileaks.org/wiki/WikiLeaks>About> (accessed February 26, 2011).

WikiLeaks. 2010. About WikiLeaks. About WikiLeaks. <http://wikileaks.org/media/about.html> (accessed February 26, 2011).

Wilshushen, Gregory. 2010. "Challenges in Federal Agencies' Use of Web 2.0 Technologies." *Government Accountability Office*. Testimony Before the Subcommittee on Information Policy, Census, and National Archives, Committee on Oversight and Government Reform, House of Representatives, July 22. <http://www.gao.gov/new.items/d10872t.pdf> (accessed February 5, 2011).



About the Author

David A. Schroeder is looking for ways to help the Intelligence Community work with others — and with itself. Schroeder serves as an Information Warfare Officer in the US Navy Reserve, working on the Navy’s cyber and SIGINT missions. He is also working to grow [an initiative](#) within the Navy’s new Information Dominance Corps (IDC) to enhance its collective situational awareness and facilitate the development of a common IDC culture. In the civilian world, Schroeder works as a Continuity of Operations planner for critical IT infrastructure at the University of Wisconsin–Madison. As a social software evangelist, Schroeder has been an active participant in the Intelligence Community’s social software initiatives. Since 2007, he has served as an administrator on Intellipedia, the Intelligence Community wikis on Intelink. Schroeder holds a Master of Arts degree in Information Warfare from American Military University. He can be reached at david.a.schroeder@navy.mil.