© 2011, *Global Media Journal -- Canadian Edition* Volume 4, Issue 2, pp. 95-113
ISSN: 1918-5901 (English) -- ISSN: 1918-591X (Français)

Making Friends in Dark Shadows: An Examination of the Use of Social Computing Strategy Within the United States Intelligence Community Since 9/11

Andrew Chomik

Centre for Military and Strategic Studies, Canada

Abstract:

The tragic events of 9/11 highlighted failures in communication and cooperation in the U.S. intelligence community. Agencies within the community failed to "connect the dots" in the intelligence they had, which was cited by the 9/11 Commission Report as a reason for the terrorist attacks being allowed to happen. Since then, the U.S. intelligence community has made organizational and operational reforms towards intelligence sharing. As part of this reform, the Director of National Intelligence has introduced web-based social computing technology to be used by all members of the intelligence community. This paper argues that while this technology has been adopted into the intelligence environment, it has reached a "plateau" in its use, and that intelligence failures continue to persist in the U.S. post-9/11 world. It identifies and analyzes the challenge of implementing social computing and Web 2.0 technology into the U.S. intelligence community, as well as account for possible deficiencies in the community that might be contributing to these intelligence failures. Finally, the definition of "success" in intelligence analysis and social computing is explored, and critique against information sharing is put forth.

Keywords: 9/11; Crisis Management; Joint Production; Information Sharing; Intelligence; National Security; Social Computing; Social Media

Résumé:

Les événements tragiques du 11/9 ont mis en lumière les défaillances de la communication et de la coopération dans la communauté des services de renseignement aux États-Unis. Les agences au sein de cette communauté ont échoué à relier entre eux les renseignements à leur disposition, un échec cité par le rapport de la commission sur le 11/9 comme une des raisons ayant permis les attaques terroristes. Depuis lors, la communauté des renseignements américains a effectué plusieurs réformes de l'organisation et des opérations de partage de renseignements. Dans le cadre de ces réformes, le Director of National Intelligence a fourni à tous les membres de la communauté du renseignement des technologies Internet du type réseaux sociaux. Cet article explique que, bien que ces technologies aient été adoptées par la communauté du renseignement, elles ont désormais atteint un plafond dans leur utilisation et les défaillances en matière de renseignement persistent dans l'environnement américain post-11/9. L'article identifie et analyse les défis liés à la mise en œuvre de technologies Web 2.0 de type réseaux sociaux dans la communauté des services de renseignement aux États-Unis d'une part, et fait l'inventaire de lacunes possibles dans la communauté pouvant contribuer à ces défaillances d'autre part. Enfin, l'article explore la définition de "succès" en matière d'analyse de renseignements et de réseaux sociaux tout en abordant les critiques à l'encontre du partage d'informations.

Mots-clés: 11/9; Gestion de Crise; Informatique Sociale; Partage d'Information; Production Conjoint; Renseignement; Sécurité Nationale

---

In his seminal piece entitled, "The Wiki and a Blog: Towards a Complex Adaptive Intelligence Community" (2005), Calvin Andrus identified using wikis and blogs in the United States Intelligence Community (USIC) as a possible solution to their information sharing challenges in a world after the September 11, 2001 (9/11) terrorist attacks. Andrus asserted that intelligence-based decision making was moving towards real-time, live environments, and that the "intelligence-decision-implementation cycle", such as when new security issues emerge in Baghdad and are vetted through decision-makers in Washington, can now be as short as 15 minutes. The ability to provide concise and quality intelligence under a compressed cycle requires comprehensive intelligence sharing using central locations of information within the USIC. Andrus argues that such tools have the potential to solve this challenge.

More broadly, it has been debated within academia and the U.S. government that the events of 9/11 could have been prevented had there been more effective interagency communication to "connect the dots" in intelligence gaps. For example, the intelligence the National Security Agency (NSA) held on American Airlines flight 77 hijacker Nawaf al Hazmi in January, 2000, was not communicated effectively with other relevant USIC agencies to assess his level of threat. The National Commission on Terrorist Attacks upon the United States Report (the 9/11 Commission Report; 2004) identified this example and the broader lack of interagency

communication as one of a number of failures that led to the terrorist attacks. Since then, the value of a collective network of intelligence agencies collaborating together in an integrated structure has become a focal point and a strategic aim for the Office of the Director of National Intelligence (ODNI). The community has also been focusing on organizational reform involving greater information sharing, removing the silos (or the practice of "stove-piping") of information between agencies, and moving away from the "need-to-know" treatment of intelligence to a "responsibility-to-provide" model (ODNI, 2008b: 8.) This fundamental shift in strategy has been an attempt to improve on the intelligence gaps that plagued the USIC before 9/11, a period in time which was highlighted by a relative and considerable lack of cooperation among agencies to prevent terrorist attacks and threats to national security (National Commission on Terrorist Attacks upon the United States, 2004).

Social computing and Web 2.0 technology, two concepts that employ using social web-based software to connect users with information, have grown in their use in the USIC since Andrus' study, which chronologically coincided with the recognition of intelligence failures by the 9/11 Commission Report. Examples of this technology include blogs, instant messaging, social networking, social bookmarking, collaborative information building (e.g. wikis), and other forms of engagement that foster two-way, social interaction (Von Kortzfleisch, Mergel, Manouchehri & Schaarschmidt, 2008). Major social computing-based initiatives implemented by the ODNI, such as Intellipedia (a wiki information resource) and A-Space (a social networking platform), have been designed to improve the analysis and provide consumers, such as policy makers, with timely and relevant intelligence products. However, since their adoption in the mid 2000's, these tools have "plateaued". In other words, they have reached their maximum usable potential (Jackson, 2009, Rasmussen, 2010). Similarly, there is an emerging concern within the USIC itself that these Web 2.0 tools are not reaching far enough in sharing intelligence – they serve complementary roles rather than being entrenched as mandatory tools in the intelligence cycle (Dixon, 2009; Dixon & McNamara, 2008). These same processes, including the quality of analytic tradecraft, have also come under much debate in the new millennium, particularly since 9/11.

This paper examines the current use of social computing tools in the USIC, and will analyze their effectiveness within the larger intelligence cycle process. This paper assumes that the social computing tools used in the USIC are part of a larger information sharing strategy as established by the ODNI, which itself is part of a larger national intelligence strategy currently in place (ODNI, 2009a). Additionally, the assumption is made that intelligence failures still persist since 9/11, and that social computing tools and the intelligence cycle have challenges that will require reforms if the ODNI envisions acceptance and thorough use of these tools to meet organizational objectives.

Web 2.0 and Social Computing Use in the U.S. Intelligence Community

An analysis of social computing cannot be made without understanding these new technologies and their roles in the context of a cultural shift towards a more collaborative and cooperative environment as a whole-of-community approach (that is, bringing all of the relevant agencies within the USIC and their partners together cooperatively to achieve this shift as a whole.) Breaking down the barriers of distrust and promoting interagency collaboration is a focal point from recent information sharing challenges in the USIC. The 2009 National Intelligence Strategy

identifies these challenges as central to building greater success in gathering intelligence and collecting reliable data (Enterprise Objectives #1 and #4) (ODNI, 2009a).

The idea of social computing (and Web 2.0) technology was a nebulous area of Information Technology (IT) solutions for organizations large and small. While the technology seemed to offer greater collaboration efforts and ways for normal people with little or no programming experience to engage user content on the web (e.g., the growth in use of Web 2.0 sites such as Wikipedia, Myspace and Facebook in the early and mid 2000s), how it could be applied into an organizational setting was not entirely clear. It was in this same timeframe that United States suffered the devastating terrorist attacks of 9/11, and raised a multitude of concerns and questions in the U.S. government and the public about the effectiveness of the USIC's knowledge of terrorist activities and the actionable intelligence they had (National Commission on Terrorist Attacks upon the United States, 2004). The security landscape was rapidly changing due to the amorphous nature of unconventional non-state threats such as al-Qaeda and the Taliban, along with their increasing ability to use technology for nefarious means (Kohlmann, 2006). A changing landscape required a fundamental shift in national security strategy; terrorism and national security threats were becoming increasingly decentralized and sophisticated. The USIC needed methods to become more responsive and to transform into a more cohesive unit of cooperating agencies that shared their resources, rather than 16 different silos operating independently of each other.

The 9/11 Commission Report (2004) identified information sharing as one of the primary weaknesses that led to the attacks, which was brought about by a failure among the various U.S. government agencies and departments to communicate effectively. It identified the "need-to-know" culture as a crucial bottleneck to effective intelligence sharing, and suggested that security requirements at the time were "nurturing overclassification and excessive compartmentation (compartmentalization) of information among agencies" (2004: 417). The Commission went further in recommending that intelligence and data collected should be in its most shareable and accessible form to all, but still subject to the proper security clearances and with an audit trail on queries. More decentralized data among the USIC should also be accessible across agency lines, and a "trusted information network" was recommended to be designed for facilitating greater cooperation in information sharing (2004: 418).

Legislative action soon followed. The U.S. Congress created the Director of National Intelligence role by passing the Intelligence Reform and Terrorist Prevention Act in 2004, a body of legislation designed "to ensure maximum availability of and access to intelligence information within the Intelligence Community consistent with national security requirements" (ODNI, 2008b: 6). The legislation brought together all 16 U.S. intelligence agencies under one umbrella organization, a structure needed to provide central direction for better information sharing. Subsequent legislation was entrenched through Executive Orders 12333 and 13470 and Intelligence Community Directive Number 501, which refined the guidance provided to agencies on the new technologies and methods to be implemented (ODNI, 2008b; 2009b).

Michael McConnell, the Director of National Intelligence (DNI) from 2007 to 2009, brought forth two implementation plans for parlaying information strategy into action. The "100 Day Plan for Integration and Collaboration" introduced a number of initiatives, including launching a civilian joint duty program, improving research capabilities and upgrading analytical tools for analysts, and prioritized information sharing as one of the primary objectives (ODNI, 2007a). Part of this information sharing effort was to draw lessons from the "Web 2.0 revolution" and create the same type of social networks, collaborative knowledge and data

"push" found on publicly available social websites (Wertheimer, 2008). The same plan was extended further in McConnell's "500 Day Plan for Integration and Collaboration", focusing on "core" and "enabling" initiatives that provided more detail for achieving collaboration goals, such as introducing new hiring practices and web training, tradecraft improvements and administration changes, new IT programs such as the Single Information Environment, data collection strategies, and system and architecture planning (ODNI, 2007b).

For the USIC, the primary social computing tools that were introduced included Intellipedia, a community-wide, crowd-sourced wiki used to build a database of information that is only accessible within the USIC and across secure internal networks JWICS, SIPRNet and Intelink-U (and built using the same technology as popular online reference site Wikipedia), and A-Space, a social networking tool that allows USIC analysts to connect and collaborate in online workspaces. Additional tools used in the USIC include CompanyCommand, an online forum for servicemen to share expertise (Dixon, 2007), microblogging services such as eChirp, Yammer and IBM SameTime, Google search functionality, and enterprise content and collaboration software such as Microsoft SharePoint (Hoover, 2009; Intelligence Community Chief Technology Officer, 2010; Jacks, 2009).

It should be noted that during the increasing adoption of these Web 2.0 tools, intelligence successes were being made that had major impacts on both military and foreign policy. Two such successes included the assassinations of Abu Musab al-Zarqawi in 2006 and Osama bin Laden in 2011, which signalled major intelligence victories for the White House. Both of these events have reflected positively on the White Houses' ability to use intelligence to eliminate key threats to American interests at home and abroad, although caution was issued that these successes do not signal the end of the larger "war on terror" (Rutenberg, 2006; They got him; After Osama bin Laden, 2011).

Unfortunately, while gains in strategy and information sharing were being made, intelligence failures continued to plague the post-9/11 security environment. One of the most criticized failures was the prewar intelligence assessments on Iraq's weapons of mass destruction program. The Senate Selection Committee on Intelligence (SSCI) concluded that serious analytical errors were made by analysts, collectors and managers, and that a pervading sense of "groupthink" was evident in the assembly of such intelligence (Rosenbach & Peritz, 2009). Among other well-known incidents, President Barack Obama has also cited the "mix of human and systemic (intelligence) failures" by the USIC to thwart the December 25, 2009 attempted bombing of a Northwest flight by a Nigerian-born extremist as "completely unacceptable" and that there was information that "should have been pieced together" (Meyer, Nicholas & Semuels, 2009). The 2011 Arab Spring has also raised concerns about intelligence failures. Dianne Feinstein, chairwoman of the SSCI raised issue with the intelligence collected on the uprisings, saying the United States "missed warnings" on the events that took place in Tunisia and Egypt (Associated Free Press, 2011), and that the situation revealed intelligence "was way behind the times" and "inadequate" (Rogin, 2011).

Where Has Intelligence Gone Wrong Since 9/11?

Failures in intelligence analysis since the formation of the ODNI and 9/11 have not ceased to continue. Research and academia is rife with studies and analysis of failures in the intelligence cycle, with one of the most maligned phases being analysis. However, there are additional reasons for why such failures occur, and it would be ignorant to conclude that only one part of

the intelligence cycle is broken, or that the intelligence process alone is the culprit for continued failures. An examination of challenges in social computing, then, cannot discount the larger issues that are often cited as to why intelligence failures happen. Although by no means an exhaustive list, the following subthemes provide some insight into these very gaps, although each can undoubtedly stand alone as their own fields of research.

The Intelligence Community Has Become Large and Costly

In 2010, the *Washington Post* published a series of investigative articles on the state of the USIC called Top Secret America, which the newspaper put together based on government documents, contracts, job descriptions, property records, corporate and social networking sites, records, and hundreds of interviews with USIC staff and officials. The findings of the investigation included that 854,000 people had "Top Secret" security clearance, 50,000 intelligence reports are produced each year, and that public spending on the USIC amounted to $75 billion, a number almost 250 per cent larger than it was on 9/11 (Priest & Arkin, 2010). However, while the investigation is a journalistic effort to shed light on the size of the community, others argue that the community is simply making up for the downsizing it suffered between the end of the Cold War and 9/11. In this sense, the community may not be coming to full terms with its size and expansion, and thus, not understanding its own reform in a post-9/11 world (Kerbel, 2008; Zagert, 2005).

Wasteful spending is also another critique of the expansive USIC. The Federal Bureau of Investigation, for example, spent $170 million on case-handling software that, after too many bugs and frustrations with the system, was scrapped (Thompson, 2006; Zegart, 2005). Another example points to overly-expensive satellite programs for technical information collection and processing, perpetuated by competing requirements between the intelligence community and the Department of Defense, which was compounded by a lack of effective Congressional oversight (Best, 2011). These examples are microcosms of larger (and chronic) spending problems. However, such problems of wasteful spending and the overall size of the intelligence community budget are on the radar of the Senate Select Committee to reform (Feinstein, 2010), but are indicative of strategic issues through budgetary matters.

Processes in the Intelligence Cycle are Problematic

There is much debate about how the analytical process in the intelligence cycle is faulty. Similarly, there is also debate whether the intelligence that is created is disseminated appropriately and in full disclosure. Since consumers often rely on intelligence analysis to make bureaucratic decisions, these two processes are inextricably tied. The connection between intelligence failures and the effectiveness of the analysis and dissemination processes are subfields of research on their own and are beyond the scope of this paper. However, the analysis process and social computing tools are inextricably tied if they are considered tactical tools at the disposal of the analyst to perform their tasks.

The USIC often reflects on its intelligence deficiencies. The *Studies of Intelligence* journal that is produced by the Central Intelligence Agency or the numerous reports and papers that are produced by the U.S. military are just two of the many internal sources of critique for policy makers to consider. It is often that the community points to a lack of "strategic warning" or an ability to see beyond tactical levels of intelligence analysis. Citing the failure to provide

strategic warning during the 1990 Iraqi invasion of Kuwait, one report suggests that intelligence gathered amounted to nothing more than "story-telling", and that the only proper way to move forward is through better analysis of potential developments (or, according to Davis (2002), "linchpin analysis"). The production cycle also puts a premium on being agile and flexible, but often results in producing intelligence that lacks strategic foresight or identifying trends for which to communicate effectively to policy makers and consumers (Davis, 2002; Petersen, 2011). Other government-produced studies often indicate flaws with analysis interpretation and critical thinking skills as problematic.

Academic research is also supportive of the assertion that there is a lack of strategic foresight. Lefebvre (2004) argues that critical thinking is important, and that there may be too much emphasis on current intelligence, although intelligence analysts should not be expected to "predict the future" with perfect measures of accuracy. Similarly, Kerbel (2008) identifies that, if intelligence were compared as an "art" versus a "science", the artistic side would need to be cultivated, as it is this that can provide reason and hypothesis to an otherwise scientific process of data collection and systematic information process.

Again, a common theme among the analytic process is that analysis is not reaching the intended strategic level required to make informed policy decisions through disseminated intelligence. The finished intelligence model might be serving to inhibit good analysis, as data-focused reports captured at a specific time may not be sufficient to "connect the dots" required to improve the quality of disseminated analysis. Intelligence analysis may also be negatively affected by other factors, including (but not limited to) cognitive bias (Lefebvre, 2004; Johnston, 2005), misunderstandings of requirements between policy makers and intelligence analysts (Petersen, 2011; Kerbel & Orcott, 2010), or a lack of proper training (Ackerman, 2007; Heuer, 2005). Still, technology (and thus, social computing tools) can play a large role in the improving the quality of an analyst`s work (Lefebrve, 2004).

Information Sharing—A Chronic Challenge

Information sharing among departments and agencies within organizations has historically been a difficult task to achieve, particularly with federal agencies. Trust is a central requirement for agencies to engage in consistent and friendly information sharing activities with other agencies. Federal agencies, in particular, require a degree of trust that is unlike other organizations. Liu and Chetal (2005) argue that these agencies suffer "conflicts of interest" when they are forced to share information, which results in a lack of trust between agencies that does not mutually benefit each agency involved. This "lack of trust" between agencies has been a historical characteristic of the USIC, as numerous academic and government-produced reports have identified this and the "stove-piping" of information from each other as chronic challenges. The *9/11 Commission Report* (2004) refers to the latter issue multiple times as one of the gaps in intelligence coordination that allowed the 9/11 attacks to happen.

However, agencies and departments within the newly-structured USIC were thrust into a hierarchy that imposed overarching strategies and mandates while still having to maintain their already pre-existing internal agency strategies, goals and resources. This new layer of hierarchy, supported by numerous ODNI strategies (ODNI, 2007a; 2007b), imposed immediate pressure on these agencies to improve intelligence quality through better information sharing. Such an immediate organizational shift and imposition of new strategy has created compartmentalized units of specialization, much at the expense of interagency collaboration and information sharing

practices, especially as tailored intelligence for consumers (particularly policy makers) is in strong demand (Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security [CBSSRIIANI], 2011). However, assistance has been set up to support analysts and their collaboration requirements. The Analytic Transformation program provides solutions for analysts to organize large volumes of data and improve the quality of analysis through better training standards and technology use (ODNI, 2008a). In other words, the program seeks to "change how (intelligence analysts) approach analysis" with a focus on better interagency collaboration (Lowenthal, 2009: 144).

Why Have Social Computing Tools Plateaued in the Intelligence Community?

The Tools are Complementary and not Official

This requires an examination of how we measure success, and how these tools are viewed as essential to those who use them. Consider that both users and proponents of these tools have suggested that their unofficial status as part of the analysis phase in the intelligence process is a contributing factor to the problem. In the case of Intellipedia and A-Space, it has been suggested these tools only serve as complementary rather than mandatory roles to pre-existing bureaucratic processes, and that duplication of work is a likely consequence of using them (Dixon & McNamara, 2008; Jackson, 2009). While these studies opine from the users' perspective, Chris Rasmussen, Living Intelligence System Program Manager in the USIC and one of the community's most well-known Web 2.0 technology proponents, also makes the case that this is problematic, and prevents a true "reform" in the intelligence system (Rasmussen, 2010).

An Environment for Failure

It is also possible that the increase in intelligence spending since 9/11 has created an environment where social computing tools are too ineffective to provide any significant solution to policies and strategies asking for better collaboration and information sharing. Rasmussen suggests that the spending surplus not only created duplication of data and efforts, but also led to a sprawling IC structure and a fragmented intelligence process that perpetuates siloed analytical reporting and cemented the bad habits of "stove-piping" (Rasmussen, 2010). Such problems were echoed by the Pentagon, identifying data duplication as problematic from supporting two wars since 2001 (Ferguson, 2010). Rasmussen continues by arguing that the most effective innovations in organizational technology are those that are considered disruptive rather than incremental. Intellipedia and A-Space were not entrenched in the intelligence cycle workflow to complete disseminated products, which then relates back to the `complementary` role problem discussed earlier. Zagert (2005) also considers that the entrenched policies and cultures of each individual agency within the USIC serve as reoccurring problems when information sharing attempts are made, or when agencies are expected to collaboration with each other. One such opinion from within an agency in the USIC demonstrated a stark reminder of this engrained culture resistant to change when he commented that "real men don't type" (Zegart, 2005).

What Measures Success?

To examine this question, two areas of study must be acknowledge and examined—intelligence analysis and Web 2.0 adoption. Since preventing intelligence failures pertains to the intelligence cycle and the technology used within it, these two areas of study are inextricably tied.

Measuring Success in Intelligence Analysis

Defining success in intelligence analysis is not an easy undertaking. Consider that intelligence, by its nature, is meant to prevent possible threats from happening, both on home soil and broad. Is success measured, then, by the number of threats foiled (and subsequently is failure compounded by the number of threats that were not countered)? Or is there another classification? Success is a fragile and complicated function to measure, especially as the USIC is routinely subject to demonization if a threat goes undetected, or if intelligence is considered faulty.

Lowenthal (2009: 147) challenges that "good" intelligence meets certain requirements:

- Intelligence is timely: it can be served to consumers when needed;
- Intelligence is tailored: it contains specific information that does not lose objectivity or is not politicized;
- Intelligence is digestible: it has to be understood by consumers with no obscure analysis; and,
- Intelligence is clear: declaration is made about what is known, and what is unknown, and should indicate confidence in its material.

While these are general considerations, much has been studied on what constitutes effective intelligence analysis. Some suggest a revamping of the analytical process, including solving some of the earlier problems mentioned (e.g., cognitive bias issues and training). Regardless, defining success and failure in intelligence is a field of research that both academia and the intelligence community regularly attempt to explain.

Additionally, it should be noted that in producing intelligence products, there is a history of focusing on failed intelligence rather than successful intelligence. The IC is often critiqued by policy makers, media and the public on the failures it suffers, and tends to have the proverbial finger pointed at when intelligence fails, which damages credibility (Petersen, 2011). John F. Kennedy once said of the CIA that "its successes will be secret and its failures will be trumpeted" (Ibid: 15). As such, failures that occur result in much debate about where the process went wrong, or where the gaps are that need to be addressed. The definition of success in intelligence analysis is also difficult to measure when high-ranking, public officials such as the President or the SSCI issue warnings about intelligence methods, shaking public confidence in the effectiveness of their intelligence community.

Measuring Success in Web 2.0 and Social Computing Adoption

By the same token, social computing, or Web 2.0 technology has its own set of measurements for success. There is considerable material published on the success of Web 2.0 and social computing adoption in the private and public sector, both from industry professionals and

academia. There are, however, some commonalities among successful adoptions of these technologies. In an article produced in McKinsey Quarterly by leading management consultancy firm McKinsey & Company, Eric Lui, Andy Miller, and Roger P. Roberts (2009) identified six factors for successful adoption of Web 2.0 technology in large organizations:

- bottom-up "grassroots" use of the technology (with "champions" of the technology at the top of the organizational hierarchy);
- acceptance of natural use in these technologies (that is, letting users define what works and what doesn't);
- these tools must be in the business workflow; participation must be made mandatory so as to reduce duplicating work;
- appeal to the participants needs; reward and recognize contributors for their content;
- target heavy users for pushing the technology; certain users need to serve as motivation for others to participate; and,
- balance risk and freedom; organizations need to find a balance between risk management over the content posted and the ability for users to post without fear of reprisal.

Similar arguments have been made by other pieces of literature, especially in the field known to some as "Government 2.0". Bartoski and Hadden (2010) recommend that supplementing "management thinking" with "design thinking" in the public sector will encourage the best ideas and technologies to surface from a pool of many (akin to the acceptance of natural use put forward by Lui, Miller, and Roberts). They also suggest that "viral" change is needed to build faith in the product, and participation in conversations and peer networks are expectations that should happen in all levels of the organization. Similar conclusions were found in journalist and author James Surowiecki's The Widsom of Crowds (2004), a seminal and popular piece on the effective use on the power of crowds to build knowledge bases of information.

While these recommendations are put forth by private sector authors, there are common factors that public sectors share in terms of organizational requirements for social computing and Web 2.0. One such example of a public sector adoption of Web 2.0 is NASA's introduction of "Spacebook" a social networking platform for NASA employees used to "create a culture of engagement and collaboration among employees" (Thornton, 2009). The service was introduced to also create a secure social network separate from publicly available social computing sites Twitter and Facebook in order to help alleviate security concerns, as well as provide tools for the next generations of scientists and engineers to support their work (Ibid).

From a pragmatic perspective, social computing has proven to be a popular endeavour among USIC employees. Intellipedia now has over 1.28 million pages, used by over 180,000 users contributing content (Intelligence Community Chief Information Officer, 2010). A-Space has also achieved significant adoption rates and usage among USIC analysts (Dixon, 2009). Intellipedia was also integral to information sharing during the 2008 Mumbai terrorist attacks, and won Homeland Security Awards in 2009 for the improvements it made in information sharing among analysts (Wu, 2010). This, however, does not mean that Web 2.0 has been effective for producing intelligence. An attempt to produce a National Intelligence Estimate solely on Intellipedia itself was ultimately rejected and sent back into the conventional stream of intelligence analysis and dissemination (Joch, 2009). Having this particular product revert back

to conventional bureaucratic processes suggests that using Intellipedia and other social computing tools as channels for building and disseminating intelligence are problematic, and lacking in a cohesive, fluid workflow of collaboration among agencies

Effective Use of Social Computing in the Intelligence Community

Ultimately, the success of social computing tools will have to be measured on the basis of how the users see its benefits, and whether the larger intelligence analysis process is considered successful by bureaucrats, policy makers and academia. These tools, however, are still in their infancy; epistemic knowledge around the use of social computing tools has so far been limited to a handful of industry professionals and academic experts with varying levels of expertise on team dynamics and social computing technology. While studies such as those of Dixon and McNamara (2008; 2009) provide observational insight into what users think of these tools, these studies are neither comprehensive enough nor do they measure long-term effects that social computing have on the actual analysis process. Additionally, academic research on collaboration efforts and information sharing, for which social computing tools would be associated with, tend to focus on the analysis process itself rather than the actual tools used.

Review of currently analytic processes is also not up to par. While the Office of Analytic Integrity and the ODNI work with IC agencies to evaluate internal analysis procedures, the USIC mainly relies on the judgments of experts in analysis assessment to provide direction, rather than systemic or scientific methods to deliver results that might otherwise generate more accurate tool assessment (CBSSRIIANI, 2011). Perhaps the closest official attempt to measure the effective use of information sharing tools came from the CASE Program Completion Report (Sickels, 2008), but this program was plagued by issues of analytic quality and the subject nature of its variables (Schroeder, 2011). Furthermore, these tools have not been implemented long enough to understand their long-term effects on the analytical process, which itself may pose challenges in that these tools serve a complementary role rather than being firmly entrenched into the intelligence production workflow.

Similarly, conventional security problems have persisted in the adoption of new technologies and Web 2.0 products. Leaders within the ODNI (including former directors themselves) have expressed concern of the difficulty in keeping up with the Web 2.0 "revolution" (Ackerman, 2008), in addition to having to focus on the security issues that accompany full, integrated data systems among all 16 agencies. These conventional challenges include trusting their own workforce to safeguard shared information, and dealing with the resistance that still exists among some of the USIC workforce in adopting new technologies (Ibid). To complicate matters further, USIC leaders have also explicitly stressed that cyber terrorism is their primary concern when it comes to web issues; a lack of a comprehensive cyber strategy will only serve to inhibit overall web use within the USIC at home and abroad (McConnell, 2010).

Critics of Information Sharing in the USIC

Information sharing is also not without its risks. Particularly for the USIC, the issues of privacy and information leaks are a common theme among critics of information sharing theories. These fears have also been substantiated in recent events. The controversy surrounding diplomatic cables stolen from the Top Secret computer network SIPRNet, which is shared by the military

and intelligence community, and given to whistle-blowing website Wikileaks have raised concerns about how far information sharing has extended under the ODNI. The leak occurred when Pvt. Bradley Manning, a low-ranking serviceman, stole hundreds of thousands of diplomatic cables and sensitive information documents, which led to public embarrassment on the part of the U.S. government and left questions about the ease of accessibility into otherwise secure networks used in the USIC, such as SIPRNet or the Joint Worldwide Intelligence Communications System (JWICS), both of which Manning had access to (Perlow, 2010). Hilary Clinton, Secretary of State, remarked that the leaks amounted to an "attack on America's foreign policy interests" and on the "international community", and has "put people's lives in danger" (Aroon, 2010). Director of National Intelligence James Clapper commented in October 2010 that the leaks posed a "chilling effect" on the community's willingness to share information, although in March, 2011, he determined that the fallout was "still being assessed" (Ackerman, 2011).

Support, however, has leaned on the side of continued information sharing. Jay Bosanko, director of the National Archives' Information Security Oversight Office, remarked that it would be a step backwards to roll back information sharing initiatives, while Ellen McCarthy, president of the Intelligence and National Security Alliance suggested that the benefits of information sharing "far outweigh the costs" and said the community should focus on "operational security and counterespionage" instead (Reilly, 2010). Defense Secretary Robert Gates has also reiterated that the impact on American foreign policy was "modest" and not the "melt down" others were making it out to be (Ackerman, 2010). It remains to be determined the long-term effects that Wikileaks will ultimately have on the information sharing policies in the USIC.

One concern also revolves around trusting users to contribute in an appropriate manner to information-based, crowd-sourced material. There is little preventing an intelligence analyst from providing incorrect data or misinformation, nor is there from analysts making mistakes by error or by negligence while managing data in these systems—allowing them to the freedom to contribute content is one of the risks taken with Web 2.0 technology (although under Surowiecki's idea of crowd-sourcing, such information would theoretically be subject to the quality control and vetting by other analysts, and likely subject to other pre-existing methods of information proofing). The National Intelligence Strategy explicitly states that the USIC needs to have strong identity management and secure networks to prevent disclosure of sensitive material and from such negligence or errors taking place (ODNI, 2009a). Particularly for Web 2.0 technology, risk can manifest from sharing information or conversations on tools that can perpetuate to other areas of shared networks. For example, an analyst writes sensitive content using an internal microblogging system (such as Yammer or in a collaboration space), which may be captured in another analysts' newsfeed on A-Space or propagated as "pushed" information to Intellipedia which might be classified as sensitive. The inherent danger in Web 2.0 use is the very factor that makes it useful—it interlinks multiple social computing tools and data together; information can be transmitted without a user knowing how far that information travels. However, such is the risk inherent in using social networks and social computing tools, as other industry and academic studies that have examined the use and governance of social computing have shown (Maximize benefits . . ., 2011; Strufe, 2010). Critics may also point to the ease in which Web 2.0 technology integrates with publicly available services on the Internet. Again, this risk pertains to the leakage of information, but from a security standpoint, the USIC is behind a sophisticated firewall system that is significantly "insulated" from public networks (Kenyon, 2010). Similarly, data duplication may also pose a problem if aggregated data from

different networks and databases are not vetted against each other (Francis, 2011; Rasmussen, 2010).

Conclusion

Andrus asserted that a critical mass must be established before a fundamental change can truly take hold. Even though the USIC has adopted social computing and Web 2.0 technologies to improve interagency information sharing, it remains to be seen whether the current state of social computing tools in the USIC will elevate to a point where not using them is a failure in itself. The issue is further complicated as intelligence agencies begin to migrate their data to federated, central locations, and direction from the top of the community implies that collaboration and information sharing are the goals and objectives of the USIC. There is no shortage of collected data and analyzed intelligence: 50,000 intelligence products produced each year inevitably create huge knowledge bases for reference and usage, most of which go unread (Thompson, 2006). By the same token, the large mass of information must be vetted and filtered to collectors and analysts entrenched in the intelligence cycle so only useful and relevant data will help build products ready for dissemination. This information must similarly reflect in the quality of the analysis being conducted, which will ultimately be judged by bureaucrats who, for better or worse, use the information in guiding American policy.

Additionally, measuring the success of social computing tools cannot be done without looking at the larger information sharing strategy in the USIC, which itself is a strategy within an even larger national intelligence strategy. While the ODNI has made it clear what these strategies are, social computing tools must not be considered exclusive from the intelligence process, particularly in the analysis phase. Tactical success of these tools may be measured in statistics of usage, contributions and satisfaction made by analysts who use them, but success will undoubtedly be tied to how effective the intelligence cycle as a whole is measured. Removing the "stove-pipes" and "connecting the dots" are continually scrutinized concepts, particularly by policymakers, the media and the general public, especially as the USIC continues its strategy of openness and transparency. However, conflict and power are ever-present in politics, and agencies have deeply entrenched, bureaucratic processes that, while the *9/11 Commission Report* viewed these as structural problems, points to larger organizational and culture changes that need to be made for true reform (Zegart, 2005). To this end, success, in the absence of a clear, industry-wide definition, is likely to be viewed in the eye of the beholder, for which zero intelligence gaps entirely will be the expected goal.

Areas for Future Study

Some in the intelligence community have begun to voice possible directions in where to take social computing use in the USIC. Using social software as part of a reformed intelligence cycle that augments existing production systems and introduces a new "joint production method" is one such solution advocated by some (Rasmussen, 2010; Schroeder, 2011). Social computing tools must be reinforcing of the intelligence cycle, and used as a set of mandatory (not complementary) technologies that advance the collection, analysis and dissemination of intelligence products. Since such reforms would potentially be considered "disruptive technology" (Dixon, 2008), these changes will likely require a paradigm shift in organizational culture, management support, and a check and balance system so as to continually measure the

performance of analysts in the intelligence cycle who use these entrenched technologies on a regular basis.

If such production reforms are implemented, it will likely have a considerable impact in making reforms in analytical tradecraft within the USIC. While there are many works of literature that exist in determining the best course of action for the USIC to improve the intelligence cycle, technology-based analytical reforms have shown potential in overcoming the challenges posed by chronic "stove-piping" of information, a lack of trust among USIC agencies, and better interagency collaboration through intelligence sharing. However, much more sustained use of social computing tools and analysis of their use are likely required before any clear and effective strategy can be sufficiently developed. There can be no nebulous use of these tools going forward if the United States is to prepare their intelligence efforts for the rapid-response, digitally-oriented future of national security and to operate under a "responsibility-to-provide" information sharing strategy, something the USIC has struggled with ten years after 9/11.

References

Ackerman, Robert K. (2007, May 1). Cultural changes drive intelligence analysis. *SIGNAL Magazine*, *61*, 56-57. Retrieved August 22, 2011, from http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1311&zoneid=31.

Ackerman, Robert K. (2008, April 1). Future threats drive U.S. intelligence. *SIGNAL Magazine*. Retrieved April 18, 2011, from http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1548&zoneid=231.

Ackerman, Spencer. (2010, November 30). Pentagon boss is not sweating WikiLeaks. *Danger Room-WIRED*. Retrieved August 30, 2011, from http://www.wired.com/dangerroom/2010/11/pentagon-boss-is-not-sweating-wikileaks/.

Ackerman, Spencer. (2011, February 11). Spy chief: Damage from WikiLeaks is unclear. *Danger Room-WIRED*. Retrieved August 30, 2011, from http://www.wired.com/dangerroom/2011/02/spy-chief-damage-from-wikileaks-is-unclear/.

Andrus, Calvin. (2005). Toward a complex adaptive intelligence community: The Wiki and the Blog. *Studies in Intelligence*, *49*(3). Retrieved August 30, 2011, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Wik_and_%20Blog_7.htm.

Aroon, P.J. (2010, November 29). Clinton: WikiLeaks disclosure is 'attack on the international community'. *Madam Secretary | Foreign Policy*. Retrieved August 30, 2011, from http://hillary.foreignpolicy.com/posts/2010/11/29/clinton_wikileaks_disclosure_is_attack_on_the_international_community.

Associated Free Press. (2011, February 8). Top US senator: 'No real warning' on Egypt unrest. *Google*. Retrieved August 30, 2011, from http://www.google.com/hostednews/afp/article/ALeqM5i4URLBnwqSuNdzQiJLwJnoLJSX2A?docId=CNG.ca75d68733ba56c6dff1582ac6bf480a.8a1.

Best, Richard A. (2011, January 20). *Intelligence authorization legislation: Status and challenges.* Ft. Belvoir: Congressional Research Service. Retrieved August 29, 2011, from http://www.fas.org/sgp/crs/intel/R40240.pdf.

Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security. (2011). Challenges for the intelligence community. *Intelligence analysis for tomorrow: advances from the behavioral and social sciences* (pp. 5-22). Washington, D.C.: National Academies Press.

Davis, Jack. (2002). *Improving CIA analytic performance: strategic warning*. Central Intelligence Agency. Washington, DC: Sherman Kent Center. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA526569&Location=U2&doc=GetTRDoc.pdf.

Dixon, Nancy M. & McNamara, Laura A. (2008, February 5). *Our experience with Intellipedia: An ethnographic study at the Defense Intelligence Agency*. Retrieved August 30, 2011, from http://www.au.af.mil/au/awc/awcgate/sandia/dixon_mcnamara_intellipedia.pdf.

Dixon, Nancy M. (2007). CompanyCommand: A professional community that works. *Ask, Summer*. Retrieved April 16, 2011, from http://askmagazine.nasa.gov/issues/27/27i_company_command.html.

Dixon, Nancy M. (2009, June 22). *How A-Space is shaping analysts' work*. Defense Intelligence Agency Knowledge Laboratory. Retrieved April 26, 2011, from http://conversation-matters.typepad.com/A_Space_Study.pdf.

Feinstein, Dianne. (2009). Intelligence authorization act for fiscal year 2010. S.C.O. Intelligence, U.S. Government Printing Office.

Ferguson, Barbara. (2010, July 21). Clapper and secret America in the spotlight. *Arab News*. Retrieved August 27, 2011, from http://arabnews.com/world/article87375.ece.

Francis, Steven. (2011). The most insidious operational risk: Lack of effective information sharing. *The Journal of Operational Risk, 6*(1), 55-56.

Heuer, Richard. (2005). Limits of intelligence analysis. *Orbis, 49*(1), 75-94.

Hoover, Nicholas. (2009). CIA, NSA adopting Web 2.0 strategies; In addition to Intellipedia, social and Web-inspired software is becoming the next great tool for the intelligence community. *InformationWeek*, Retrieved August 30, 2011, from Academic OneFile via Gale: http://go.galegroup.com.ezproxy.lib.ucalgary.ca/ps/start.do?p=AONE&u=ucalgary.

Intelligence Community Chief Technology Officer. (2010, August). *Intelink*. Retrieved August 30, 2011, from http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/Breakfast%20Presentations/2010%20Presentations/Intelink%20Basic%20presentation.pdf.

Jacks, Jason. (2009). Updated global information grid would bring Web 2.0 to the Defense. *National Defense, 94*(669), 47.

Jackson, Joab. (2009, February 18). Intellipedia suffers midlife crisis. *Government Computer News*. Retrieved April 18, 2011, from http://gcn.com/Articles/2009/02/18/Intellipedia.aspx?Page=2.

Joch, Alan. (2009, May 14). Intelligence community wrestles with Web 2.0 tools for information sharing. Federal Computer Week: Latest news for government IT and federal employees. Retrieved August 28, 2011, from http://fcw.com/Articles/2009/05/18/Data-sharings-new-mandate.aspx?Page=1.

Johnston, Rob. (2005). *Analytic culture in the US intelligence community: an ethnographic study*. Central Intelligence Agency, Center for Study of Intelligence. Washington, DC: Goverment Printing Office. Retrieved August 30, 2011, from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA507369&Location=U2&doc=GetTRDoc.pdf.

Kenyon, Henry. (2010, September 20). DOD adds social media tools behind the military firewall. *Defense Systems*. Retrieved August 28, 2011, from http://defensesystems.com/Articles/2010/09/20/DOD-Social-Media-Tools.aspx?Page=1.

Kerbel, Josh & Olcott, Anthony. (2010). Synthesizing with Clients, not analyzing for customers. *Studies in Intelligence*, *54*(4). Retrieved August 30, 2011, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-4/synthesizing-with-clients-not-analyzing-for.html.

Kerbel, Josh. (2008). Lost for words: The intelligence community's struggle to find its voice. *Parameters*, *38*(2), 102-112.

Kohlmann, Evan F. (2006). The real online terrorist threat. *Foreign Affairs*, *85*(5), 115-124.

Lefebvre, Stéphane J. (2004). A look at intelligence analysis. *International Journal of Intelligence and CounterIntelligence*, *17*(2), 231-264.

Liu, Peng & Chetal, Amit. (2005). Trust-based secure information sharing between federal government agencies. *Journal of the American Society for Information Science and Technology*, *56*(3), 283-298.

Lowenthal, Mark M. (2009). *Intelligence: From secrets to policy*. Washington, D.C.: CQ Press.

Maximize benefits, minimize risks with social media in the workplace. (2010, May). *Design Firm Management & Administration Report*, *10*(5), 13-15.

McConnell, Michael. (2010, February 28). Mike McConnell on how to win the cyber-war we're losing. *The Washington Post*. Retrieved April 16, 2011, from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR10/02/25/AR2010022502493_pf.html.

Meyer, Josh, Nicholas, Peter & Semuels, Alana. (2009, December 30). Obama cites intelligence failures in Northwest airline attack. *Los Angeles Times*. Retrieved August 30, 2011, from http://articles.latimes.com/2009/dec/30/nation/la-na-terror-obama30-2009dec30.

National Commission on Terrorist Attacks upon the United States. (2004).*The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. New York: Norton.

Office of the Director of National Intelligence. (2007a). 100 Day Plan. Retrieved April 17, 2011, from http://www.fas.org/irp/dni/100-day-plan.pdf.

Office of the Director of National Intelligence. (2007b). 500 Day Plan. Retrieved April 17, 2011, from http://www.odni.gov/500-day-plan/500-day-plan.pdf.

Office of the Director of National Intelligence. (2008a). Analytic transformation: Unleashing the potential of a community of analysts. Retrieved April 14, 2011, from http://www.dni.gov/content/AT_Digital%2020080923.pdf.

Office of the Director of National Intelligence. (2008b). United States intelligence community information sharing strategy. Retrieved April 10, 2011, from http://dni.gov/reports/IC_Information_Sharing_Strategy.pdf.

Office of the Director of National Intelligence. (2009a). National intelligence strategy (of the United States of America). Retrieved April 8, 2011, from http://www.dni.gov/reports/2009_NIS.pdf.

Office of the Director of National Intelligence. (2009b). Intelligence community directive number 501. Retrieved August 27, 2011, from http://www.dni.gov/electronic_reading_room/ICD_501.pdf.

Perlow, Jason. (2010, December 1). Wikileaks: How our government IT failed us. *Technology News, Analysis, Comments and Product Reviews for IT Professionals | ZDNet*. Retrieved April 26, 2011, from http://www.zdnet.com/blog/perlow/wikileaks-how-our-government-it-failed-us/14988?tag=mantle_skin;content.

Petersen, Martin. (2011). What I learned in 40 years of doing intelligence analysis for US foreign policymakers. *Studies in Intelligence, 55*(1). Retrieved August 30, 2011, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-1/index.html.

Priest, Dana & Arkin, William M. (2010, July 19). A hidden world, growing beyond control. *The Washington Post*. Retrieved August 26, 2011, from http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/.

Rasmussen, Chris. (2010, October 6). Increasing "jointness" and reducing duplication in DoD intelligence [Web log post]. *CTOvision.com – Context on enterprise technology*. Retrieved April 18, 2011, from http://ctovision.com/2010/10/increasing-%E2%80%9Cjointness%E2%80%9D-and-reducing-duplication-in-dod-intelligence/.

Reilly, Sean. (2010, December 5). WikiLeaks fallout leads to an info-sharing clampdown. *Federal Times*. Retrieved August 29, 2011, from http://www.federaltimes.com/article/20101205/IT03/12050306/.

Rogin, Josh. (2011, March 8). Feinstein complains to Panetta about intelligence gaps on Arab revolutions. *The Cable | Foreign Policy*. Retrieved August 30, 2011, from http://thecable.foreignpolicy.com/posts/2011/03/08/feinstein_us_intelligence_community_s_got_nothing_on_arab_revolutions.

Rosenbach, Eric & Peritz, Aki J. (2009). Confrontation or collaboration? Congress and the intelligence community. Cambridge, Mass: John F. Kennedy School of Government,

Harvard University. Retrieved August 30, 2011, from http://belfercenter.ksg.harvard.edu/files/IC-book-finalasof12JUNE.pdf.

Rutenberg, Jim. (2006, June 9). Bush responds to the killing of a terrorist with caution. *New York Times*. Retrieved August 26, 2011, from http://www.nytimes.com/2006/06/09/world/middleeast/09prexy.html.

Schroeder, David A. (2011). Efficacy and adoption of central Web 2.0 and social software tools in the U.S. intelligence community. Charles Town, WV: Department of Security and Global Studies, American Military University. Retrieved August 24, 2001, from http://das.doit.wisc.edu/amu/Schroeder_Thesis_MAR11_Redacted.pdf.

Sickels, Stephen J. (2009). Collaboration and Analyst System Effectiveness (CASE) Connect. Fairfax, VA, General Dynamics Advanced Information Systems. Retrieved August 29, 2011, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA495972.

Strufe, Thorsten. (2010). *Security and privacy in online social networks*. Boston, MA: Springer.

Surowiecki, James. (2005). *The wisdom of crowds*. New York: Anchor Books.

They got him; After Osama bin Laden. (2011, May). *The Economist*, *399*(8732), 21-25.

Thompson, Clive. (2006, December 3). Open-source spying. *The New York Times Magazine*, News, *54*(L).

Von Kortzfleisch, H., Mergel, I., Manouchehri, S. & Schaarschmidt, M. (2008). Corporate Web 2.0 Applications. In Berthold H. Hass, Gianfranco Walsh and Thomas Kilian (Eds.), *Web 2.0* (pp. 73-87). Berlin: Springer.

Wertheimer, Michael. (2008). Gazette - Arming intelligence with Web 2.0. *The Gazette*, *70*(3). Retrieved April 12, 2011, from http://www.rcmp-grc.gc.ca/gazette/vol70n3/2-0-eng.htm.

Wu, Tzeyoung M. (2010). Wikis within the DoD. *IAnewsletter*, *13*(2), 26-28.

Zegart, Amy B. (2005). September 11 and the adaptation failure of U.S. intelligence agencies. *International Security*, *29*(4), 78-111.

About the Author

Andrew Chomik is a graduate student with the Centre for Military and Strategic Studies, University of Calgary, Canada. His research focuses on the use of social computing tools and social computing strategy in intelligence communities, primarily the United States intelligence community. Andrew is also a technology consultant with the Canadian-based consulting firm Ideaca Knowledge Services, advising clients in various sectors, including the petroleum and energy sectors, on social computing methods and the use of portals and collaboration enterprise technology.

Citing this paper:

Chomik, Andrew. (2011). Making friends in dark shadows: An examination of the use of social computing strategy within the United States intelligence community since 9/11. *Global Media Journal -- Canadian Edition*, *4*(2), 95-113.