AU/AFF/NNN/2009-0712

AIR FORCE FELLOWS

AIR UNIVERSITY

LEVERAGING TECHNOLOGY AND SOCIAL MEDIA FOR INFORMATION SHARING

by

Kenneth W. Backes, Colonel, USAF

A Research Report Submitted to ESS/FO
In Partial Fulfillment of the Graduation Requirements

Advisor:
Dr. Stephen Burgess
Department of International Security
US Air War College

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **Leveraging Technology and Social Media for Information Sharing**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Air Force Fellows Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

Improving information sharing, as a sub-set of reforming the interagency process, is a much talked about endeavor. This research paper looks at a few solutions leveraging social networking and emerging technologies for the tactical and operational levels of planning and execution. Each solution is subjectively assessed by ease of use, security, and suitability. HARMONIEWeb is an internet accessible environment for the exchange of information across the civil-government boundary. Two social networking capabilities are assessed: facebook and Twitter. Both help people communicate with others. Facebook has a wider audience and is mostly web enabled with some provisions for mobile (cellular) updates. Twitter has grown into a real-time microblogging/short messaging service that works over multiple networks and devices. FrontlineSMS is free stand-alone software that turns a laptop and a mobile phone into a central communications hub. The leveraging of technology and social networks appears to be an inevitable course of action in the day-to-day interaction of any government agency. Once security concerns are properly addressed and mitigated, organizations should select a social networking system accessible by a variety of devices or inputs (i.e. Twitter) and establish an on-line presence and network with interested collaborators. If requirements dictate information sharing and communications in a stand-alone (or technologically isolated) environment, adopting a software system specifically tailored to facilitating communication within and between non-governmental organizations using indigenous mobile phone carriers or pairing with a deployable mobile phone facility (i.e. FrontlineSMS) is applicable.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **38**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

Acknowledgments

I would like to thank the faculty and staff at the Hoover Institution on War, Revolution and Peace at Stanford University for their assistance and encouragement during the duration of this project. Special thanks to Senior Fellows Victor Davis Hanson and Richard Burress for their wisdom and guidance as well as Mr. Bob Oster for his keen insight. I appreciate the wise counsel from my Air University faculty advisor “Doc” Burgess and the support from the research project sponsors at U.S. Africa Command especially my friend Colonel Mark Nickson. Early interviews with key personnel at the Departments of Defense and State as well as the U.S. Agency for International Development helped me scope this endeavor. I enjoyed the camaraderie with my colleagues in the National Security Affairs Fellowship: Mr Richard Boly, State Department, Colonels Joe Felter (USA), Dave Ottignon (USMC), and Kevin Dixon (USAF) in addition to our “minder” Ms Joy Kelley. Finally, I appreciate the patience and understanding of my lovely wife as well as her coaching and tutoring on the finer points of facebook.

Abstract

Improving information sharing, as a sub-set of reforming the interagency process, is a much talked about endeavor. This research paper looks at a few solutions leveraging social networking and emerging technologies for the tactical and operational levels of planning and execution. Each solution is subjectively assessed by ease of use, security, and suitability.

HARMONIEWeb is an internet accessible environment for the exchange of information across the civil-government boundary. Two social networking capabilities are assessed: facebook and Twitter. Both help people communicate with others. Facebook has a wider audience and is mostly web enabled with some provisions for mobile (cellular) updates. Twitter has grown into a real-time microblogging/short messaging service that works over multiple networks and devices. FrontlineSMS is free stand-alone software that turns a laptop and a mobile phone into a central communications hub.

The leveraging of technology and social networks appears to be an inevitable course of action in the day-to-day interaction of any government agency. Once security concerns are properly addressed and mitigated, organizations should select a social networking system accessible by a variety of devices or inputs (i.e. Twitter) and establish an on-line presence and network with interested collaborators. If requirements dictate information sharing and communications in a stand-alone (or technologically isolated) environment, adopting a software system specifically tailored to facilitating communication within and between non-governmental organizations using indigenous mobile phone carriers or pairing with a deployable mobile phone facility (i.e. FrontlineSMS) is applicable.

Chapter 1

Introduction

Improving information sharing, as a sub-set of reforming the interagency process, is a near-universally heralded concept. It seems, much like motherhood and apple pie, no one is against improvement in communication and collaboration. The interagency process is ripe for both evolutionary and revolutionary reforms and improvements in the realm of exchanging information.

The focus of this research will be at the lower levels of interaction and execution and will suggest a few "solutions" that leverage social networking, emerging technology, or both. Most will be at what the military classifies as the tactical level and in no case higher than the operational level. However, some knowledge of the landscape at the strategic level of planning and execution will inform the discussion. This paper will touch briefly on just some of the barriers to information exchange. Ultimately, it will suggest a few tactics, techniques, and procedures that may be useful in future operational planning and execution.

While not a technical paper, the solutions suggested will be focused on technological innovation from a lay person's perspective. The evolution of the cyber space environment from the dawn of the internet age through the emergence of Web 2.0 (and the nascent Web 3.0) has radically altered the way people and organizational hierarchies communicate, collaborate, and cooperate. Development of Web 2.0 technologies are again radically affecting the way the world communicates and conducts business. Web 2.0 platforms are primarily user oriented. The users are an integral part of the data and information streams and content. The US government has been slow to take advantage of Web 2.0 approaches and tools. However, several government agencies have experimented with some of these tools.[1] Future innovation is inevitable and many developments have occurred just in the course of this research. Apart from the US Government, the use of social networks has exploded across governments, business and industry, as well as organizations of all sizes and, of course, individuals. No less than the Pope has praised as a "gift to humanity the benefits of social networking sites such as Facebook and MySpace in forging friendships and understanding.[2]" The Israeli government, in the most recent conflict in Gaza, used the twitter mircoblog to hold news conferences.[3]

The paper will examine the roles emerging social media concepts might play in the future and examine where they might be most applicable. To date, the major efforts in leveraging social networks and using unclassified access technologies have been in the public affairs arena—in effect to define and shape perceptions and report on events that have already occurred. Little has been done in the realm of actual operations—e.g. making things happen instead of reporting on what has happened. Therefore, the paper will frame the discussion around the suitability of using the social media or emergent technology in a variety of situations outside of the public affairs arena (though public affairs lessons learned can be utilized for operational use). Each solution will be subjectively assessed, by the author, on its ease of use, security vulnerabilities, and suitability for collaboration and communication. The paper will then cover a few examples of recent utilization of social media and other technology to address collaborations, communications, and other cooperative efforts to seek to draw out lessons learned from them.

It should be noted that leveraging technology and/or social networks is not without risks and presents some unique challenges and several potentially serious pitfalls. Prior to implementing any suggestions, organizations are cautioned to do a thorough assessment of the attendant risks, including operational and communications security, to determine if the potential benefits outweigh the risk exposure. The cyber space realm is extremely dynamic and new capabilities (and vulnerabilities) are revealed frequently. John Brennan, President Obama's top adviser for counterterrorism and homeland security said: "The national security and economic health of the United States depend on the security, stability and integrity of our nation's cyberspace, both in the public and private sectors[4]." President Obama ordered a review of the nation's cybersecurity to examine how federal agencies use technology to protect secrets and data. The effort will examine all the government plans, programs and activities underway to manage large amounts of data -- including passport applications, tax records, personal tax returns and national security documents[5]. The security of cyberspace is far from a settled domain. In fact, the US government's Director of the National Cybersecurity Center recently resigned over concerns that the National Security Agency improperly controls the nation's cybersecurity efforts.[6] This is illustrative of the dynamic nature of the problem. A government agency's or organization's use of technology or social media will undoubtedly need to be scrutinized carefully for compliance with review guidelines when they are published.

An additional aspect to be addressed is the availability of the suggested solution sets in a wide variety of technologically diverse environments. One cannot assume ubiquitous access to an internet connection and the world-wide web with sufficient band-width to accommodate the latest in technology and web design. In fact, for a large segment of the world population, lower tech solutions suggest themselves as being superior to higher tech options in regard to availability, training, and ease of replication.

Notes

[1] Environmental Protection Agency Web 2.0 Whitepaper, Web 2.0 Workgroup, February 2008, available on-line at http://www.collaborationproject.org/download/attachments/11206698/ EPA+Web+2.0+White+Paper.pdf

[2] "Vatican launches Pope YouTube Channel" *Associated Press*, January 23, 2009, accessed at: http://tech.yahoo.com/news/ap/20090123/ap_on_hi_te/eu_vatican_youtube

[3] "Can Social Networking Fix U.S. Image?" Victoria Esser, Politico.com, February 4, 2009, accessed at: http://www.politico.com/news/stories/0209/18353.html

[4] "Obama Asks For Review Of Online Security" *Associated Press*, Washington Post, February 10, 2009, Pg. 3

[5] Ibid.

[6] Rod Beckstrom, Director, National Cybersecurity Center, to Secretary Janet Napolitano, Department of Homeland Security (DHS), memorandum, March 5, 2009, accessed at: http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf

Chapter 2

Reform Efforts Framing this Discussion

The Project for National Security Reform, headed by James Locher III and a distinguished group of academic and government leaders, published a report, "Forging a New Shield[1]" that seeks to address the challenges to the national security interagency system. It provides an analysis of the system's performance and proposes reforms for the Executive Branch and Congress. One of the major areas addressed in the report is directly applicable to this research project—the management of the Knowledge Base. Within this area is a discussion of information sharing.

The report notes that "Sharing information across organizational boundaries is difficult[2]" and "One of the most obvious challenges to effective decision-making in the national security system is sharing information across organizational boundaries: within a federal agency, between federal agencies, between different levels of government, or among governmental and nongovernmental organizations." The report also notes "Because there is no system in place to hold collectors accountable for inappropriately withholding information[3], the incentives to not share information often outweigh the best interests of the nation. The benefits of sharing information are not immediately apparent, but the costs are apparent and also immediate.[4]

In the context of this paper an example of a deficiency in information sharing highlighted during the 2004 tsunami in Indonesia: "no open source database existed to give responding organizations information about the scene on the ground. There was also no formal mechanism for sharing information between the U.S. government, non-governmental organizations, government organizations (NGOs), and foreign governments.[5]"

Using this example as a departure point,[6] the research focused on solutions that could assist in ameliorating these deficiencies. The availability and accessibility of a database or central "pool" of information is a major consideration as well as the ability to share with other actors and interested parties.

Notes

[1] Project on National Security Reform, *Forging a New Shield*, 2008, Washington DC, on-line internet, available from: www.pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf

[2] Ibid. pg. 341

[3] United States, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction Report to the President of the United States*, (Washington: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005) <http://www.wmd.gov/report/index.html> pg. 288.

[4] Project on National Security Reform, *Forging a New Shield*, 2008, pg. 342

[5] "International Interagency Response to the 2004 Indian Ocean Tsunami" Project on National Security Reform Case Study, *Forging a New Shield*, 2008, pg. 344

[6] There were dozens of other examples available; for brevity, the author chose just this one.

Chapter 3

Current Dynamics

One of the critical issues at the center of collaboration efforts and challenges, especially with foreign governments and non-governmental agencies, is a perceived association with the US government or, in particular, the US military. The International Committee of the Red Cross for example, maintains a strict policy of neutrality to maintain its status as "…an impartial, neutral and independent organization whose exclusive humanitarian mission is to protect the lives and dignity of victims of war and internal violence and to provide them with assistance[1]." Because of this imperative to remain neutral, the organization will refuse to associate with any country's military if there is a perception of taking sides. They do this not only to protect their personnel in an on-going situation, but also to assure their neutrality is accepted at face value elsewhere. While associating a solution with the US government or military is not a "show stopper," the visibility must be a consideration as a solution is evaluated.

In addition, with the explosion of social media venues, some care must be taken to select the correct ones to utilize for collaboration or information sharing. There are far too many sites, and some with very narrow niche users, to try to cover all possible avenues for sharing information. The cyclic trend of popularity of one site over another cannot be overlooked. It would, at a minimum, be a waste of resources to devote effort to a particular networking site that was declining in popularity while other, more viable sites were ignored and not used.

This ever-changing nature of the world-wide web and emerging technologies requires a constant and consistent review of the "terrain" where information is shared and propagated. The utilization of these tools requires a frequent "refresh" on information and content, both for currency and relevancy. An outdated web page, for example, arguably causes more mis-information than no web page at all.

Access to technologically advanced solutions often implies some connection to the world-wide web. The organization kiwanja.net has pioneered the effort to get developing countries access to technological solutions with innovation not always requiring web access. Kiwanja.net states:

> The adoption and widespread innovative use of mobile phone technology makes Africa an ideal candidate for the development of localized mobile phone applications. These applications could have profound implications for the economic development of some of the poorest African communities, not to mention in improvements in areas such as education and health.…Today's phones are programmable, powerful, and capable of accessing the internet. Lacking a traditional PC, many Africans are turning to their mobile phones to connect with people, information and services. Empowering African mobile owners with the skills necessary to program these increasingly ubiquitous devices is the first step towards nurturing an African mobile phone application developer community. This new community of programmers will be focused on building entrepreneurial applications, designed specifically to meet the unique needs of the African people in a range of social, economic and environmental contexts.[2]

This solution, paired with a deployed telecom capability such as Télécoms Sans Frontières (TSF) can expand the "reach" an organization would need for effective sharing of information.

As technology solutions surface, government agencies must evolve and adapt procedural and access protocols to assure maximum utility. The U.S. Air Force, for example, chose to restrict access to "Troop Tube," a Department of Defense web site modeled after YouTube, the popular video sharing site. Major David Smalls said in an e-mail: "The Air Force must balance network security requirements with competing requests for wide-ranging access to a vast array of public internet services for our Airmen. Air Force-wide policy restricts access to categories of sites that are generally not mission related, and put adverse performance demands on our networks. As a result of this general policy, access to Troop Tube is blocked at Air Force bases.[3]"   While blocking might be entirely appropriate in this case, the utilization of technology solutions will have to address the access issues.

Notes

[1] International Committee of the Red Cross (ICRC) Mission Statement, accessed at www.redcross.org

[2] Kiwanja.net website accessible at: http://mobility.kiwanja.net/

[3] Noah Shachtman, "Air Force Blocking the Military's Own Video Site," *Wired.Com Danger Room Blog,* March 27, 2009, accessible at: http://blog.wired.com/defense/2009/03/air-force-were.html

Chapter 4

Options and Approaches

There are several methods and platforms for sharing information that may be useful at the operational or tactical level. The use of HARMONIEWeb, facebook, and Twitter will be examined as suggested options along with a communications architecture known as FrontlineSMS.

HARMONIEWeb is an internet accessible environment for the exchange of information across the civil-government boundary associated with stability, security, transition and reconstruction operations or humanitarian assistance and disaster relief. It provides an internet accessible virtual environment for the exchange of unclassified information across the civil military boundary associated with Stability, Security, Transition and Reconstruction Operations (Stability Operations) of Humanitarian Assistance and Disaster relief (HADR) operations. It seeks to improve the ability to exchange timely information with non-DoD organizations and non-traditional partners, synchronize DoD and non-governmental organization (NGO) efforts, improve situational awareness for all actors and accelerate successful mission completion. US Joint Forces Command hopes HARMONIEWeb will be an enduring joint enabling capability.[1]

Facebook is an on-line social networking site headquartered in Palo Alto, California. Founded in February 2004, Facebook is a social utility that helps people communicate with their friends, family and coworkers. The company develops technologies that facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. According to the facebook web site: “Anyone can sign up for Facebook and interact with the people they know in a trusted environment.[2]”

Twitter is a privately funded startup in San Francisco, California. Twitter has grown into a real-time microblogging/short messaging service that works over multiple networks and devices. It allows people around the world to follow the sources most relevant to them and access information as it happens—from breaking world news to updates from friends.

FrontlineSMS is free software that turns a laptop and a mobile phone into a central communications hub. Once installed, the program enables users to send and receive text messages with large groups of people through mobile phones.

Evaluation Criteria

Before looking at various solution sets, a review of the questions addressed in the subjective evaluation of each is in order. Each solution will be assessed on Ease of Use, Security, and Suitability.

Ease of Use will be evaluated by actually obtaining rights to or installing the solution for use by a non-technical[3] user. The complexity of the sign-up or installation process will be examined as well as trouble shooting or help-desk support. On-line tutorials or demonstration modules will enhance the user-friendly attributes of a solution as will the ability to easily navigate through the various features of the software or program

Security discussion will answer the question “How ‘protected’ is the information that is available on this platform?” Since all these solutions are unclassified networks, an assumption is made that all the data is vulnerable to a highly proficient and well-funded hacker that could compromise the data integrity. Therefore, none of these solutions will be examined for an environment where transmission would have to be restricted to secure government networks.[4] The log-on protocols will be evaluated as well as the security of the encapsulated applications or other programs in addition to the raw data.

Suitability will be determined by the applicability of the solution set to an operational environment and whether it will be effective in achieving a desired outcome. Inherent in this evaluation is access to the solution for the users whether through the world-wide web or the use of mobile phone networks or other means.

A Secure Network - HARMONIEWeb[5]

HARMONIEWeb allows DoD to collaborate with U.S. departments and agencies, foreign governments and security forces, international organizations (IOs), non-governmental organizations (NGOs), local organizations including civil groups, community assistance organizations and members of the private sector. It allows users to define meeting sites as open or access restricted as required.

HARMONIEWeb tools include virtual workspaces and event sites as collaboration areas for a group of people or organizations. These spaces can be tailored to meet the specific communication needs of the group. Another tool is Adobe Connect which allows users to conduct virtual meetings in real time using voice and video. Microsoft Office Communicator is a third tool; essentially an Instant Messenger that offers real-time communication and allows collaboration. The platform’s suite also includes Microsoft Virtual Earth Platform, an integrated set of services that combines unique bird’s-eye, aerial, and satellite imagery with mapping, location and search functionality; a Wiki site to provide a low-maintenance way to record knowledge; and Blogs designed to help share information.

HARMONIEWeb uses industry standard information security techniques to provide data encryption, authentication, and security groups and file level access control. It has a relatively robust security firewall in contrast to other environments.

Access to HARMONIEWeb is through a secure server. The Microsoft Internet Security and Acceleration (ISA) Server is a software firewall that limits internet traffic to specific ports for specific domains. All requests to the HARMONIEWeb server go through ISA first, and if the request does not meet the defined criteria for validity, the request is rejected. All users must authenticate successfully before they can access the private HARMONIEWeb site. The application then uses 128 bit Secure Sockets Layer (SSL) to encrypt incoming and outgoing server requests with a 128-bit public/private key algorithm. The SSL allows internet browsers to confirm that the responses returned from requests are coming from the correct source. The HARMONIEWeb server sits outside the firewall allowing it to be visible to internet users. However, all critical and system data sits safely behind a firewall to reduce the risk of malicious users infiltrating the server directly. The SharePoint security model uses an active directory and limits access to pages, navigation items, and actions. It is role-based security, meaning a user must either be given permission directly to perform a single specific action, or the user must be added to a predefined group (or role) that has specific permissions defined. An active directory manages all HARMONIEWeb users. Users have an active directory account created when they are approved. Active Directory is also role based security, ensuring that users are only given the permissions they need to use the HARMONIEWeb site and not any control over the physical machine.

HARMONIEWeb is produced and maintained by US Joint Forces Command (USJFCOM), though this link and support is not easily discerned on the web site itself. For example, in the user guide, USJFCOM is never mentioned and the word military appears only once in the twenty-three page document. The military link is relatively easily discerned by using the colleague search function and noting the ".mil" addresses of the majority of users or using a simple search function.[6] Within the NGO community, HARMONIEWeb's provenance is well-known and its existence is not a secret as it is frequently described in the open press[7]. This is a possible explanation for the slow adoption of HARMONIEWeb outside of the US Government.

Ease of Use

HARMONIEWeb is the most difficult of the solutions to initially access. An on-line registration process requires some time for the request to be validated and processed. Once established with a HARMONIEWeb account, users encounter a document based tutorial that walks them through some of the features on HARMONIEWeb and discusses tools available for users to access. The site provides sample worksites as templates for users to establish for their own projects and uses. Included are templates for establishing on-line decision meetings and operational work sites for contingency or other operations.

Navigation throughout the site is relatively uncomplicated. Users can establish "My Site" content tailored to their individual interests and current needs. The on-line collaboration tools provide multiple venues to exchange information.

Security

HARMONIEWeb is undoubtedly the most secure of the suggested solutions. Access is severely restricted and verified prior to admission. However, the security environment is not completely assured. Because the portal operates on the unclassified web with entry from any internet protocol (IP) address, malicious users could gain access by signing on with a legitimate users log-on ID and password. This could allow an unauthorized user the ability view and input potentially sensitive information depending on the access level of the “hijacked” log-on. The system is only as secure as the weakest link. Because the associated applications on the HARMONIEWeb system operate “behind the firewall” it is unlikely that unauthorized users could do little beyond viewing information or adding to an on-going conversation. The internal tools would be safe to all but users with behind the firewall access.

Additionally, individual users can restrict interactions with their own or operationally discreet web pages choosing either to publically “make available” their pages to all HARMONIEWeb users or restrict it to specific individuals or groups. Further, the type of access can be restricted even more by granting read only or read, write, edit access.

Suitability

HARMONIEWeb is a viable collaboration tool for organizations and individuals requiring near real-time sharing of information. Because it requires web access, it is limited to those entities that can operate and have access to the web on a continued basis. This limits its utility in less developed areas or areas that are experience disruption in their access to the world-wide web due to natural or man-made disaster or even those experiencing overload of web resources due to high traffic or interest.

Websites similar to HARMONIEWeb have been developed by other combatant commands.[8]

Emerging Social Media—facebook

The social media site facebook is fast becoming a mainstream method for key leaders and influencers to connect with their constituencies and people of interest. In fact, the Commandant of the Coast Guard and the Commanders of NORTHCOM and SOUTHCOM have established their own personal facebook profiles[9]. During the course of the research project, the Commander of Multi-National Forces – Iraq, General Odierno, established a facebook fan page with multiple updates every day. The facebook site has various applications and interoperability with other software programs that allows users to update and personalize their personal web page. It allows for private communication and chat as well as posting of videos, photos, and other material in addition to the ability to link to other web site addresses and blogs. It can be updated from the web, either at a traditional computer or laptop or through web enabled mobile phones. Additionally, other software or other social media sites (i.e. Twitter) can update individual web pages or statuses. Access to web pages is restricted by the user who must allow access to other users by "friending" them. There are options to automatically "friend" a user who requests it, allowing access to a person's web page (including a list of their friends). There are also options to create a group or support a particular cause or operation.

Facebook's navigation gives users access to core site functions and applications. Profile, Friends, Networks and Inbox – the pages core to the user experience on facebook – have a prominent place at the top of the user's profile page. Facebook applications – Photos, Notes, Groups, Events and Posted items – are displayed on the left side bar, along with any third-party applications a user has added to their account.

Facebook is the second most-trafficked hypertext processing site in the world (after Yahoo)[10], and one of the largest structured query language installations, running thousands of databases. Facebook has built a multi-language remote procedure call framework that allows the company to tie together subsystems written in any language and running on multiple platforms. According to its factsheet[11], the company is the largest user in the world of "memcached", an open-source caching system, and has created a search engine serving millions of queries a day, completely distributed and entirely in-memory, with real-time updates.

Facebook has tools to control the information sharing flow and users determine who they want to share. Users have the ability to share and restrict information based on specific friends or friend lists.

There are over 150 million active (users who have returned to the site in the last 30 days)[12]

Ease of Use

Facebook is relatively easy to sign-up to and access. It should be noted that many DoD installations and agencies restrict access to social networking sites for a variety of reasons, not the least of which is to preserve band-width. The majority of users on facebook use it for social as opposed to work use and it should be noted that the site caters to their needs as a priority. The site has a wide variety of applications that will have little or no use in the work place environment (other than to distract employees or otherwise draw them off of day-to-day activities) and any "on-duty" use of facebook (or any other social media) would likely have to require a set of operating parameters to reduce the occurrence of misuse of government computer resources. Beyond these caveats, the site is extremely user friendly and a new user can set up a web page easily in less than half an hour. Users select a "home" network (i.e. US Air Force) and can specify additional networks to be affiliated (i.e. Silicon Valley[13], Stanford University). Users can then add "friends" to their web page. The "friend" has to accepting the friend request to authorize the addition. Once "friended[14]" the user can access their friends web pages and receives updates on their status as they occur. Users can choose to be notified (or not) via e-mail to various updates and posting provided by their friends. Facebook requires web access (including mobile phone applications).

Security

Access to facebook is open to virtually anyone with computer access and an e-mail address. Access to information on individual data or web pages can be restricted to “friends,” “friends of friends,” networks, or everyone. The default settings lend themselves to a wider audience than might be needed for government operations (i.e. friends of friends settings) and would likely need to be adjusted to conform to organizational security parameters. As with HARMONIEWeb, malicious users could gain access by signing on with another users log-on ID and password. This would allow an unauthorized user the ability view and input to that web page as well as interact with friends, friends of friends, and networks. The system is only as secure as the weakest link.

Suitability

Facebook has limited use in the operational area though it has wide spread application in the public affairs arena (outside the scope of this paper). The requirement for robust web access and the significant security concerns limit the utility for dynamic operations. That said, to reach a very wide audience, facebook represents the deepest “pool” of potential information nodes.

Web 2.0 Access--Twitter

Twitter's overriding concept is simplicity and ease of access. Twitter asks one question, "What are you doing?" Answers must be under 140 characters in length and can be sent via mobile texting, instant message, or the web. Twitter's core technology is a message routing system accessible by a variety of devices or inputs tied to rudimentary social networking features. By accepting messages from sms, web, mobile web, instant message, or from third party application programming interface projects, Twitter is the most accessible of the options considered.

In considering the adoption of Twitter as a solution to information sharing requirements, it should be noted that while Twitter has opportunities for generating revenue, they have held off on implementation because they “don't want to distract ourselves from the more important work at hand which is to create a compelling service and great user experience for millions of people around the world.[15]” To date, Twitter has not generated any profit—careful attention to long-term viability will be required if this service is selected as an option.

Twitter is accessed by establishing an on-line account. A person or organization selects a screen name and enters identifying characteristics, typically their real names or the name of the organization, to allow others to find them. Users may then “follow” other users and will be updated every time someone they are following provides an update to their status. Users have the option of allowing anyone to follow them or restricting permission on a case-by-case basis. The update can be provided through the web, by an instant message, or through a mobile phone text message. The updates are limited to 140 characters. There is a special “@” command that allows users to have their replies flagged and held in a separate que and in addition to the stream of other updates (which can be considerable if there are many people or organizations you are a following). Additional special twitter functionality is the support of hashtags[16], designed to accommodate the real-time micro-blogging community. It provides analytic reports and indexing features to allow users to track what's happening in real time. Hashtags are defined by the number symbol (#) immediately prior to a word in a post and are then registered as a hashtag with Hashtags.org. Hashtags can then be tracked through the twitter search function for any relevant input, in reverse chronological order. This functionality allows for rapid dissemination of time sensitive data with a wide access since updates can be received on mobile phone texts as well as on the web.

There is of course significant concern about the security of the data since it is broadcast live and is relatively easy to access by a knowledgeable user. An agency or individual can restrict followers to people or organizations that are known to them. To avail themselves of this increased security, users have to pre-plan access and think through who will be allowed to receive updates. In certain operations or contingencies the security of data may be less critical. Disaster relief, for example, likely has a less need for operational security than a military operation in a non-permissive environment. Each discrete situation will need to be assessed for its security implications.

Government organizations and employees are increasingly accessing twitter. During the course of this research project, the number of U.S. Government and U.S. Military organizations and leaders has increased exponentially. Even the Chairman of the Joint Chiefs of Staff, Admiral Mullen, has a twitter account that is updated several times each day.[17]

Ease of Use

Twitter is easy to sign-up to and access. As with facebook, many DoD installations and agencies restrict access to social networking sites. Users of Twitter are still exploring its uses and the site seeks to serve a wide variety of communities from social (i.e. dating) through news and business applications. The "on-duty" use of Twitter would, like facebook, likely have to require a set of operating parameters to reduce the occurrence of misuse of government computer resources. Twitter is user friendly and a new user can set up and be operating within an hour.

Security

Access to Twitter, like facebook, is open to anyone with computer access and an e-mail address. In addition, twitter can be accessed with a mobile phone with text capability. Access to information on individual twitter web pages can be restricted to followers only or posted on the live stream. The default settings are essentially an open audience to all users of Twitter and are likely not suitable for government operations and would likely need to be restricted to meet organizational security parameters. As with the other solutions, malicious users can gain access by signing on with another users log-on ID and password or utilizing the authorized users mobile phone.[18]. This would allow an unauthorized user the ability to input and receive updates from the Twitter community as well as interact with followers. Again, the system is only as secure as the weakest link.

Suitability

Twitter is becoming ubiquitous and hardly a day goes by without at least half a dozen references to its use in the media or "blogosphere." Its pervasiveness means a large audience will already be familiar with it and will need little to no training to use it. However, twitters core users are extremely diverse, with a wide set of interests completely separated from the type of information sharing addressed in this paper. Assuming an increase in twitter use, and given the lack (to date) of a viable business plan, there is a danger is selecting it as a long term solution set in that its operating parameter may change (or slow down) or it may go out of business[19]. Twitter may find the most use in disaster scenarios, requiring a wide dissemination of succinct information to a growing audience.

FrontlineSMS – Stand-Alone Simple Messaging for Developing Countries

FontlineSMS is in some ways similar to the previous solution sets in that it uses some social networking architecture with multi-mode update possibilities (i.e Twitter). However, FrontlineSMS is a stand-alone software system specifically tailored to information sharing within and between non-governmental organizations. If used through an indigenous mobile phone carrier or paired with a deployable mobile phone facility (such as Télécoms Sans Frontières, described below) it can provide an intrinsic capability to accommodate information sharing solutions in areas where access to the world-wide web and 3G networks are not ubiquitous. Additionally, because of its narrower focus and limited access, the attendant "distraction" applications[20] found on other social networking sites are significantly less prevalent. It does not require an internet connection except to download and update[21] and it works with existing plan on all GSM phones, modems and networks. FrontlineSMS is laptop-based and can be used on the road or during power outages. The software stores all phone numbers used and records all incoming and outgoing messages and all data lives on a local computer, not on servers controlled elsewhere[22]. A major advantage is its scalability and messages can be sent to individuals or large groups. It enables two-way communication and is relatively easy to install and requires little training to use.

The software can be used to forward messages to other cell phones on the network, run software applications on the laptop, and, if connected to the internet, forward messages as e-mail to another server or anywhere on the world-wide web. The additional features of the software can be "disabled" (actually, just hidden) if desired to reduce the complexity for users who are less "computer savvy" or technologically impaired.[23]"

In areas of limited cell phone coverage, organizations such as Télécoms Sans Frontières (TSF) can play a role in strengthening coordination and communication when they deploys telecommunications centers. TSF maintains they can be operational with a communications center within 48 hours of an emergency[24]. These communication centers offer broadband internet access, voice communications, fax lines and all the information technology equipment needed for a field office. TSF uses portable satellite terminals that are quickly deployable and provide worldwide coverage[25].

Ease of Use

FrontlineSMS is the one of the easiest of all solutions to get operational. Initial set-up requires a laptop and access to the internet (to download the software and get the system up and running). Once operational, the system is stand alone and two-way messaging (limited to 160 characters) is enabled through the local phone system. The software allows phone numbers to be grouped and messaging can be sent individually or out to a group. This capability could be "boxed up" for deployment with the laptop pre-loaded with the software and cell phones (with the proper SIM chips for the country of deployment) delivered to the end user for distribution. The "user group" of FrontlineSMS is still relatively small (less than 400 in mid-February 2009) and they are still developing (and debugging) the software to assure access from a wide variety of mobile devices. To date, a little over 1500 downloads of FrontlineSMS have occurred.[26] Unlike twitter and facebook, the "on-duty" use of FrontlineSMS will not require a set of operating parameters because the system is indigenous to the area deployed and has little utility outside its stated purpose. There is little likelihood of misuse of government computer resources. The FrontlineSMS is user friendly and intutitive and a new user can set up and be operating within fifteen minutes.

Security

Access to individual FrontlineSMS systems, unlike like facebook and twitter, is limited to users with phone numbers entered in the system. Access to information on individual messages are completely controlled at the host laptop and dissemination (or rebroadcast) of the information can be controlled by the user. It is unlikely a malicious users could gain access to the control laptop (though, being an easily pilfered item, security will have to be assessed) although, the loss or compromise of the host laptop would effectively shut down the FrontlineSMS operation for that application. A malicious user could easily gain access to send or receive messages either by stealing a cell phone "known" and authorized by the system or getting a new cell phone number "registered" by "spoofing" whoever is running the host laptop with their cell number. In these cases, unauthorized users would have the ability to input and receive updates from the FrontlineSMS community as well as interact with other users depending on the messaging protocols in place at the host laptop.

Additionally, the developer of FrontlineSMS advises there is an encrypted version of the software available to protect the information[27]. While in most of the secure applications the purpose of the encryption is to provide secure banking or credit card payments to the latest international banking security standards, they would be just as applicable for information exchange.

Suitability

When utilized in a environment with at least some cell phone coverage, or utilized in conjunction with Télécoms Sans Frontières or similar contingency capability, the use of FrontlineSMS seems ideal for the sharing of unclassified information with a wide-variety of participants. The deployment capability of FrontlineSMS seems ideal for small to medium, targeted operations. Frontline SMS is not infinitely scalable however, and the single point of failure limitation on the host laptop and the requirement to "program" in the cell phone numbers of all users limits the practical size of the capability.

The benefit of coupling with distributed systems like FrontlineSMS, and the low-specification phone support of FrontlineForms (the downloadable forms client for old and new phones) is that expensive smartphones are not needed, and the system can work from anywhere an SMS can be sent. The distributed system architecture allows safe information exchange between parties via SMS where the central server, mobile network systems and any relaying systems are not a party to the data exchanged, and the vulnerabilities of the GSM A5 encryption algorithms are not an issue to data security, and the system can cope with the disappearance of the central servers and operate islanded (quite key in most FrontlineSMS deployments)[28].

Notes

[1] Joint Forces Command Briefing by Rear Admiral Wachendorf, JFCOM Chief of Staff, at Industry Symposium 2007 National Defense Industry Association Greater Hampton Roads Chapter on July 30, 2007, briefing available at: http://www.ndia-ghrc.org/Symposium_2007/briefs/02.pdf

[2] Information from the facebook fact sheet available at: http://facebook.com/

[3] Non-Technical is subjectively defined as requiring basic computer knowledge but no in-depth programming or troubleshooting expertise.

[4] i.e. the SIPRnet; however, there are some architectures that could use these tools on the "high" side; that discussion is outside the scope of this paper.

[5] *A Basic User Handbook for HARMONIEWeb, "Back pocket" Tactics, Techniques, and Procedures (TTP),* (draft) version 2.0, available through www.HARMONIEweb.org (registration required)

[6] As an example the HARMONIEWeb search for "JFCOM" returned 27,000+ "hits" on the site

[7] Donna Miles, 'Strong Angel III' Tests Military-Civil Disaster Response, American Forces Press Service, August 25, 2006, accessed at http://www.usmilitary.com/modules.php?name=HeadlineNews&story=20060824 as an example

[8] For example, USSOUTHCOM established a similar information sharing portal on the unclassified portion of Intelink

[9] Gordon Lubold, "Military Brass Joins Wired Troops," Christian Science Monitor, Tuesday, January 20, 2009, http://features.csmonitor.com/innovation/2009/01/20/military-brass-joins-wired-troops/

[10] facebook fact sheet. http://facebook.com

[11] Ibid.

[12] Ibid.

[13] Only one regional network is allowed under facebook rules

Notes

[14] "Friended" and "Friending" while not actual words, are common in the social media vernacular as is "twittering" and "tweets" (see below).

[15] Twitter Official Web Site, www.twitter.com, http://twitter.com/about#about

[16] Information provided by Hashtags.org available at: http://hashtags.org/

[17] The author "follows the CJCS on twitter: http://twitter.com/thejointstaff

[18] The technology for "spoofing" or cloning a particular cell phone number is available though the later generation cell phones are harder (but not impossible) to clone. Info from tech-faq.com accessible at: http://www.tech-faq.com/cell-phone-cloning.shtml

[19] Though this seems very unlikely given its explosive growth and generally positive press.

[20] For example, dating, gift giving, birthday tracking, etc.

[21] FrontlineSMS hopes to field a USB memory stick version negating the need for internet access, Presentation to Stanford university Students by Ken Banks, CEO of Frontline SMS, February 19, 2009, Stanford CA

[22] However, a server based version is being developed, Interview by the author with Ken Banks, CEO of Frontline SMS, February 19, 2009, Stanford CA

[23] Ken Banks presentation, February 19, 2009

[24] TSF website accessible at: http://www.tsfi.org/tsfispip/rubrique.php

[25] Ibid.

[26] Ken Banks presentation, February 19, 2009

[27] The encrypted version is available at: http://www.masabi.com/tech_encryptME.html

[28] On-line post from Ben Whittaker, software developer for FrontlineSMS, April 13, 2009, available at: http://frontlinesms.ning.com/profile/BenWhitaker

Chapter 5

Conclusions and Recommendations

Conclusions

The leveraging of technology and social networks appears to be an inevitable course of action in the day-to-day interaction of any government agency, non-governmental organization or private organization. Both systematic and ad-hoc adaption of these “tools” occurs with regularity, particularly within the strategic communications and public affairs arenas. In the 5 months or so researching this paper, daily news items appear reporting on the adoption or adapting of social networking tools or other technology in businesses, government agencies and other organizations. The case for use of these tools in the operational planning and execution areas is less evident. However, given the success in utilizing the tools across a wide variety of venues, test use and adoption of them is likely a prudent course of action. Failure to do so will forfeit opportunities for more effective and efficient information sharing across a wide venue. As previously noted, security considerations must be at the forefront of factors considered before embarking on the selection of a solution set. The emergence of more secure software solutions enhances this paradigm.

On the assumption that security concerns are properly addressed and mitigated and a risk assessment confirms appropriate selection of a solution set is warranted, the use of a non-web based only solution has the best applicability across the environment. If any solution (such as HARMONIEWeb and facebook) is tied to constant access to the world-wide web, it will limit the applicability in those areas and regions that lack the capability for 24/7 web access. There may be many cases where 24/7 access is assured and if that condition exists, those web-based solutions may be applicable. However, for planning purposes it is likely better to select and become proficient and experienced using solutions that don't require constant web connectivity.

In addition, as noted in the various solution explorations, there are many facets to the solution sets that are not applicable to the use in day-to-day government operations, particularly in the social media arena. A robust protocol will have to be devised to assure government resources, including duty time, are not misused or wasted. This will be a particular challenge for operating in social media using advertising as a business model to generate revenue. These ventures increase profitability by drawing users to various web sites and links, the majority of which have no governmental use or application. The utilization protocols should address the limits of use on government computer systems. Finally, consistent oversight and inspection regimes should be employed.

Recommendations

Organizations with an operational planning and execution mission of non-combat operations should select a social networking system accessible by a variety of devices or inputs (i.e. Twitter) and establish an on-line presence and network with interested collaborators. The organization should limit the audience in the social network to known partners and players in the planning and execution.[1] A strict assessment of security vulnerabilities should be made and protocols should be developed to frame what types of information or operations will be "worked" in the environment. Additionally, access protocols and responsibilities should be addressed and constantly evaluated and updated as information flow matures. This will help assure positive utilization of the technology and minimize the prospect for misuse.

It would be advisable for organizations taking this course of action to establish an on-line presence well in advance of actual need for operational planning or execution. This will allow users to develop an expertise with the software and will allow the organization to begin working and collaborating with other organizations prior to a “real world” operation. This will also allow other organizations, possibly those not initially considered or visible, to seek out collaborative ties. If limiting protocols are in place (as described above), security can be maintained at the same time allowing for an expansion of potential cooperative partners.

Additionally, organizations that require information sharing and communications in a stand-alone (or technologically isolated) environment should consider adopting a software system specifically tailored to facilitating communication within and between non-governmental organizations using indigenous mobile phone carriers or pairing with a deployable mobile phone facility (i.e. FrontlineSMS). Strong consideration should be given to a pre-packaged capability available on short notice. For example, a laptop pre-loaded with Frontline SMS and 100 text capable cellular phones with SIM cards installed for a specific country or region could be sent in with an advance team to distribute to on-the-ground partners including individuals, non-governmental organizations or host country government officials.

An advance draft (not yet published) of “Social Software and Security: An Initial ‘Net Assessment[2]’” by Mark Drapeau and Linton Wells II amplifies these analyses and the subsequent recommendations. In assessing social media and other technology, Dr Drapeau notes “It's still important to be aware of the power and reach of these tools. If you work in national security some of these things happening in other countries may affect your job or mission. What's happening over the past couple years is people in other countries are using Facebook, Twitter and blogs to organize[3]." Clearly, leveraging social media and technology is an imperative

Notes

[1] In Twitter, this is accomplished by protecting updates and adjusting preferences to only allow followers who are known

[2] Mark Drapeau and Linton Wells II, "Social Software and Security: An Initial 'Net Assessment '" Center for Technology and National Security Policy, National Defense University, Washington DC, Draft dated April 2009

[3] Gautham Nagesh "Researchers Say Social Media Essential for National Security" NextGov.com, April 15, 2009, http://www.nextgov.com/nextgov/ng_20090415_8127.php

Bibliography

Associated Press "Vatican launches Pope YouTube Channel", January 23, 2009, http://tech.yahoo.com/news/ap/20090123/ap_on_hi_te/eu_vatican_youtube (accessed 24 January 2009)

————. "Obama Asks For Review Of Online Security," Washington Post, February 10, 2009

Beckstrom, Rod, Director, National Cybersecurity Center. To Secretary Janet Napolitano, Department of Homeland Security (DHS), memorandum, March 5, 2009, http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf (accessed 7 March 2009)

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *The Report to the President of the United States on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington D.C. http://www.wmd.gov/report/index.html (accessed 24 January 2009)

Drapeau, Mark and Linton Wells II, "Social Software and Security: An Initial 'Net Assessment '" Center for Technology and National Security Policy, National Defense University, Washington DC, Draft dated April 2009

Environmental Protection Agency. *Web 2.0 Whitepaper*, Washington DC, February 2008, available on-line at http://www.collaborationproject.org/download/attachments/11206698/ EPA+Web+2.0+White+Paper.pdf (accessed 15 January 2009)

Esser, Victoria. "Can Social Networking Fix U.S. Image?" Politico.com, February 4, 2009, http://www.politico.com/news/stories/0209/18353.html (accessed 6 February 2009)

HARMONIEWeb.org. *A Basic User Handbook for HARMONIEWeb, "Back pocket" Tactics, Techniques, and Procedures (TTP), (draft) version 2.0.* www.HARMONIEweb.org (registration required) (accessed 15 January 2009)

International Committee of the Red Cross (ICRC). *Mission Statement*, www.redcross.org (accessed 15 January 2009)

Lubold, Gordon. "Military Brass Joins Wired Troops," Christian Science Monitor, January 20, 2009. http://features.csmonitor.com/innovation/2009/01/20/military-brass-joins-wired-troops (accessed 24 January 2009)

Miles, Donna. "'Strong Angel III' Tests Military-Civil Disaster Response." American Forces Press. http://www.usmilitary.com/modules.php?name=HeadlineNews&story=20060824 (accessed 24 January 2009)

Nagesh, Gautham. "Researchers Say Social Media Essential for National Security" NextGov.com. April 15, 2009. http://www.nextgov.com/nextgov/ng_20090415_8127.php (accessed 16 April 2009)

Project on National Security Reform. *Forging a New Shield*, 2008, Washington DC www.pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf (accessed 15 January 2009)

Shachtman, Noah. “Air Force Blocking the Military's Own Video Site,” Wired.Com Danger Room Blog, March 27, 2009, http://blog.wired.com/defense/2009/03/air-force-were.html (accessed 1 April 2009)

Wachendorf, Miles B. "Ben," Rear Admiral, US Navy. “Joint Forces Command Briefing” Industry Symposium, 2007 National Defense Industry Association Greater Hampton Roads Chapter. July 30, 2007. http://www.ndia-ghrc.org/Symposium_2007/briefs/02.pdf (accessed 6 February 2009)