Backgrounder

Published by The Heritage Foundation

No. 2273
May 18, 2009

Social Networking and National Security: How to Harness Web 2.0 to Protect the Country

James Jay Carafano, Ph.D.

Computers have changed how Americans do almost everything. Soon they may alter national security. There is much more on the information superhighway these days than information. There is a traffic jam of conversation facilitated by e-mail, Facebook, MySpace, YouTube, Flickr, Digg, Wikipedia, LinkedIn, Twitter, and other social networking tools (often collectively called Web 2.0) that facilitate discussion, debate, and the exchange of ideas on a global scale.[1] This unprecedented capacity to listen and respond is inexorably restructuring the ways in which information is created and used.

Social networking has already profoundly redefined business practices—think eBay and Craigslist. During the 2008 presidential election, the Obama campaign mobilized social networking in revolutionary ways to garner popular support and raise money. The impact of social networking will not end with business and politics. National security is next.

Washington is well behind in its willingness and capacity to adapt to the world of Web 2.0. Even the new Administration, with a well-earned reputation as "web savvy," has its troubles. A panel of experts assembled by *The Washington Post* gave the new WhiteHouse.gov Web site an averaged grade of C plus.[2] While the White House as well as many federal agencies are experimenting with social networking tools, their efforts are unguided by sound research or clear and coherent policies that encourage innovation while protecting individual liberties and privacy. The hierarchical practices of traditional government

Talking Points

- Computers have changed how Americans do almost everything. Soon they may alter national security.
- Social networking has already profoundly redefined business practices and politics. National security is next.
- Washington is well behind in its willingness and capacity to adapt to the world of Web 2.0. Even the new Administration, with a well-earned reputation as "web savvy," has its troubles.
- Congress and the Administration need to lay the foundation for the broad and effective adaptation of social networking by facilitating early and rapid adaptation of new technologies.
- A 21st-century government must be able to adapt 21st-century instruments to keep the nation safe, free, and prosperous. Steps are needed now to make government a leader rather, than a follower, in using these new technologies to both strengthen and safeguard American society.

This paper, in its entirety, can be found at:
www.heritage.org/Research/NationalSecurity/bg2273.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

are not keeping up; they are inadequate for exploiting the explosion of social networking systems.

Fundamental reforms will be required for conducting national security in a world driven by global listening. Washington cannot fully adopt and exploit social networking systems without profoundly changing the process of governance. Advocating such change, however, is premature. First, the government must understand and develop the means to interact in the new world in which it lives. The Administration should:

- Restructure the government's means for conducting strategic communications;
- Create human capital programs to prepare national security professionals and decision makers with new skills, knowledge, and attributes; and
- Direct national security agencies to establish research and development programs focused on threats and competitive advantages of social networking tools.

These measures are a prerequisite for adapting the practices of national security to future challenges.

The New Net

Social networking involves linking individuals together as part of a voluntary group. People join groups because they share common attributes, interests, activities, or causes. Within the group, they exchange information, goods, services, and opinions. As the group grows, it develops into a network.

A social network is a complex system. When systems become complex, their behavior cannot be easily predicted by traditional methods of analysis—breaking a system down into its component parts and analyzing the elements in detail.[3] As physicist Philip Anderson observed, "aggregations of anything from atoms to people exhibit complex behavior that cannot be predicted by observing the component parts. Chemistry isn't just applied physics—you cannot understand all the properties of water from studying its constituent atoms in isolation."[4] Likewise, social networking is more than simply the sum of the attitudes or activities of its members. The system's complexity creates outcomes that are different than the sum of the group.

Furthermore, outcomes can be dramatically different from those that might emerge from a more rigid system, such as a government bureaucracy. That is because they are usually "nonlinear," often described as "disorganized" systems. Unlike hierarchical organizations, the outputs of a social network are less predictable and controllable. They are subjected to fewer rules and controls.

While social networks are not limited to the Internet, computer technology has greatly expanded the capacity and speed for establishing networks of people. Informal online networks have existed since the inception of the World Wide Web in the 1990s, but they have proliferated remarkably since 2003. This was in part due to the dramatic expansion of data-storage capacity and the exponential decline in the cost of information storage and retrieval. New software created programs that could store and share user profiles and preferences, allowing individuals to post information in form of blogs, video clips, photographs, and audio files.

The popularity of new Web tools and services is remarkable. MySpace, for example, established in 2003, had 80 million members and hosted more than 6 million Web pages within three years.[5] In

1. Josef Kolbitsch and Hermann Maurer, "The Transformation of the Web: How Emerging Communities Shape the Information We Consume," *Journal of Universal Computer Science*, Vol. 2, No. 2 (2006), pp. 187–207.
2. Jose Antonio Vargas, "Grading WhiteHouse.gov," *The Washington Post*, March 24, 2009, at *http://voices.washingtonpost.com/44/2009/03/24/grading_whitehousegov.html* (May 12, 2009).
3. L. A. N. Amaral and J. M. Ottino, "Complex Networks: Augmenting the Framework for the Study of Complex Systems," *The European Physical Journal* (May 14, 2004), pp. 147–162, at *http://amaral.northwestern.edu/Publications/Papers/Amaral-2004-Eur.Phys.J.B-38-147.pdf* (May 12, 2009).
4. Cited in Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin Books, 2008), p. 28.
5. E. Barsky and M. Purdon, "Introducing Web 2.0: Social Networking and Social Bookmarking for Health Librarians," *Journal of Canadian Health Librarian Association,* Vol. 27 (2006), p. 65, at *http://pubs.nrc-cnrc.gc.ca/jchla/jchla27/c06-024.pdf* (May 12, 2009).

The Heritage Foundation LEADERSHIP FOR AMERICA

less than eight years Wikipedia, an online encyclopedia that allows users to post and adjust entries, has grown to four million individual pages, all created, edited, and monitored by users who volunteer their expertise and time. By 2009, the number of messages transmitted on Facebook exceeded those sent by e-mail.

Additionally, digital networking is not tied to a specific platform. More and more social networking applications are being developed for cell phones. Already half the world's population (more three billion people) has access to a cellular phone. Other new and different social networking is likely to emerge in the future as nanotechnology and new materials are developed that could greatly reduce the weight, cost, and power requirements for information-sharing technologies.[6]

Networks and National Security

The growth of Web 2.0, its expanding global reach, and potential new technologies to further its use and adoption argue that today's social networking is a change in the form of human communication that cannot be ignored. Online social networks have impacted every field of human endeavor from education to health care. National security is no exception.

In February 2000, a handful of officers teaching at West Point created CompanyCommand.com, a Web portal that allows junior Army officers to share experiences and lessons learned. By 2005, the site had more than 10,000 members. It was officially adopted by the Army as a professional development tool in 2002.[7] GovLoop, an online information-sharing network that facilitates collaboration between government employees and contractors was created by a Department of Homeland Security employee in his spare time. It now has more than 7,000 users across federal, state, and local governments as well as the private sector and academia.

Not only have some government agencies developed or adapted Web 2.0 systems, some have exploited existing public social networking tools. There is no consolidated list of all the on-going government initiatives, though a cursory search of the Internet reveals many examples. During the 2008 terrorist attacks in Mumbai, for example, people on the scene sent Twitter updates (limited to 140 characters), including the emergency contact number for the U.S. State Department's consular call center. Colleen Graffy, the State Department's Deputy Assistant Secretary for Public Diplomacy, used Twitter postings to provide updates on her personal experiences.

The FBI also recently established a Twitter account under FBIpressoffice. The former Secretary of the Department of Homeland Security (DHS) Michael Chertoff had his own blog. The Office of the Director of National Intelligence maintains its own e-mail list-serve, which includes updates from the FBI and DHS. Clearly, many agencies are experimenting with social networking initiatives.

Applications for defense-related social networking are not limited to military tactics, intelligence, law enforcement, or other operational activities. National Defense University researchers Mark Drapeau and Linton Wells argue that the "proliferation of social software has ramifications for U.S. national security, spanning future operational challenges of a traditional, irregular, catastrophic, and disruptive nature. Failure to adopt these tools may reduce an organization's relative capabilities over time.... Governments that harness its potential power can interact better with citizens and anticipate emerging issues."[8] Social networking has the potential to affect every aspect of national security:

6. James Jay Carafano and Andrew Gudgel, "Nanotechnology and National Security: Small Changes, Big Impact," Heritage Foundation *Backgrounder* No. 2071, September 21, 2007, at *http://www.heritage.org/Research/NationalSecurity/bg2071.cfm*.
7. Nancy M. Dixon *et al.*, *CompanyCommand: Unleashing the Power of the Army Profession* (West Point, New York: Center for the Advancement of Leader Development & Organizational Learning, 2005).
8. Mark Drapeau and Linton Wells II, "Social Software and National Security: An Initial Assessment," Center for Technology and National Security, National Defense University, April 2009, p. v, at *http://www.ndu.edu/ctnsp/Def_Tech/DTP61_SocialSoftwareandNationalSecurity.pdf* (May 13, 2009).

- Gathering and vetting intelligence and information;
- Gauging and influencing public opinion;
- Distributing "risk communications" (such as how to respond to a pandemic threat);
- Conducting research and analysis;
- Developing policies;
- Planning and implementing programs and field activities; and
- Conducting information operations.

Washington's approach to adapting Web 2.0 to national security has not been coherent, comprehensive, or integrated. While certain government organizations have recognized and adopted some tools, such as CompanyCommand and GovLoop, others have been more cautious. Some agencies ban on-the-job use of Facebook and other social networking tools.

The Federal Web Managers Council details a list of government obstacles to the effective adoption of social networking technologies.[9] These include:

- Institutional barriers, such as cultural issues and lack of a strategy for using new tools;
- Lack of access to online tools;
- Security and privacy concerns;
- Resources and budget limitations; and
- Legal concerns and terms-of-service restrictions.

These impediments make it difficult for traditional government bureaucracies to adopt social networking practices. While the Federal Web Managers Council offers some potential solutions to overcome these obstacles, such initiatives have not been uniformly applied. Nor is it clear that all the major impediments can be overcome even with more significant changes in government programs and policies.

Obstacles and Opportunities

Even if the organizational and institutional government barriers to Web 2.0 could be overcome, there are legitimate concerns over making Government 2.0 a national security instrument. The most widely voiced concern is information assurance—knowing that the data are precise and reliable. Rumors, perfidy, or inaccurate information can be dispersed at least as fast as facts.

Web 2.0 can also create "information overload," burdening the network with irrelevant data that could complicate, instead of facilitate, analysis and decision making. For example, while the White House allows outside users to post comments on WhiteHouse.gov, and maintains MySpace, Twitter, and Facebook accounts, the amount of information the White House staff receives makes it physically impossible to read, let alone assess, all the data.

In addition, while social networking facilitates conversation, it does not necessarily promote effective knowledge creation. The information age has empowered the scientific as well as the narrative cultures. Information technology allows researchers to conduct more and better analysis, but it also allows opinion makers to spin better, more compelling stories faster and proliferate them more widely.[10]

Others argue that the great strength of social networking is that it creates "open" systems that allow self-correction. Individuals can more readily challenge inaccurate information and offer corrections. Recent research finds, for example, that Wikipedia maintains a high level of accuracy even though editing of its online entries is open to anyone.[11]

Indeed, Wikipedia and other online social tools have developed their own rules and procedures for addressing both innocent and malevolent efforts to distort or manipulate information. There is a continuous debate among social networking leaders

9. Bev Godwin, Sheila Campbell, Jeffrey Levy, Joyce Bounds, "Social Media and the Federal Government: Perceived and Real Barriers and Potential Solutions," Federal Web Managers Council, December 23, 2008, at *http://www.usa.gov/webcontent/documents/SocialMediaFed%20Govt_BarriersPotentialSolutions.pdf* (May 12, 2009).
10. Alex Wright, *Glut: Mastering Information Through the Ages* (Washington, D.C.: National Academies Press, 2007), pp. 231–232.
11. Paper presented by Besiki Stvilia *et al.*, "Information Quality Discussions in Wikipedia," Graduate School of Library and Information Science, University of Illinois at Urbana–Champaign, at *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.3912&rep=rep1&type=pdf* (May 12, 2009).

The Heritage Foundation LEADERSHIP FOR AMERICA

about the most efficacious manner for dealing with trolls (people who intentionally post inflammatory or irrelevant information) and other efforts to subvert online content.

Some argue that the benefits that result from the enormous number and diversity of individuals that can engage in global listening far exceeds the risks. Michael Tanji, a proponent of adapting Web 2.0 to national security decision making, argues that "in terms of intellectual capital, a virtual think tank can be at least an order of magnitude larger than any current think tank 1.0 in existence today…. [T]he more minds working on a given problem the better the solution. It is unlikely that a policymaker would care one way or another if a good idea was generated by an individual or a group, but as a friend who was an early adopter of the 2.0 approach explains: 'None of us is as smart as all of us.'"[12]

Research suggests that Tanji's observation is overly simplistic. Who interacts and how they interact can have a significant impact on the character of the ideas created. For example, Ronald Burt, a researcher at the University of Chicago, studied an online social network set up for participants in the supply chain of a major electronics manufacturer. Burt found that managers who had a broader perspective, who worked with and interacted with employees and individuals outside their department, provided better recommendations on how to improve business practices. He called this "bridging structural holes."[13] Thus, in terms of using social networking to improve national security policy and programs, Government 2.0 needs to do more than simply "tweeting" (the action of sending a message using Twitter) in broadcast mode or trying to solicit millions of opinions. Social networking structures need to be designed and implemented to achieve specific measurable outcomes based on knowledge about how networks actually work.

The debate over how great ideas can be created and disseminated through Web 2.0 is far from over. Research in the field of social networking is hard pressed to keep up with the rapid pace of change in how information technologies are fielded and employed. Understanding social networking requires a multi-disciplinary approach to research that combines the techniques of the social sciences with "hard science" disciplines.

This mix of disciplines is often called "network science." Network science examines how networks function.[14] It studies diverse physical, informational, biological, cognitive, and social networks searching for common principles, algorithms and tools that drive network behavior. The gained understanding of networks can be applied to a range of challenges from combating terrorist organizations to organizing disaster responses. This science will be particularly fruitful for understanding how online social networks function as well as how they can exploited, disrupted, manipulated, or improved.

Joining the Brave New World

Given Washington's difficulty in adopting new information technologies and the rapid expansion and evolution of the tools of social networking, it is premature to promote specific programs for establishing Web 2.0 as the basis for National Security 2.0. Congress and the Administration need to first lay the foundation for the broader and effective adaptation of social networking.

Congress should direct the National Academies to conduct a study on national security and social networking and make recommendations to the Administration and Congress in three broad areas: research and development, professional development, and strategic communications. The study should examine lessons learned from ongoing initiatives, such as GovLoop and CompanyCommand; forecast future developments in social networking and national security applications; and propose alternative strategies for exploitation.

12. Michael Tanji, "The Think Tank Is Dead: Long Live the Think Tank," unpublished paper, at *http://haftofthespear.com/The%20Think%20Tank%20is%20Dead%20Final%20Print.pdf* (May 12, 2009).
13. Ronald S. Burt, "The Social Origins of Good Ideas," unpublished paper, January 2003, at *http://web.mit.edu/sorensen/www/SOGI.pdf* (May 12, 2009).
14. See, for example, Committee on Network Science for Future Army Applications, *Network Science* (Washington, D.C.: The National Academies, 2005).

The Administration should lay the groundwork for exploitation of social networking by developing the key enablers for facilitating early and rapid adaptation of new technologies. The Administration should:

- Establish requirements for research and development in social networking. While individual initiative, creativity, and experimentation will likely remain the basis for most Web 2.0 applications, Washington requires a sound knowledge in order to adopt responsible policies and programs that facilitate making the best use of innovation. This foundation of research can be built by conducting cutting-edge network science. The government must develop better capacities to undertake multi-disciplinary research of complex networks. Specifically in regard to Web 2.0, government research should ensure the protection of individual privacies and liberties; exploit commercial off-the-shelf technologies; develop metrics to measure the effectiveness of Web 2.0 tools; create information assurance and security procedures, software, and hardware; and develop cutting-edge platforms and software.
- Embed the knowledge, skills, and attributes for exploiting Web 2.0 in national security professional development programs.[15] An educated workforce and capable, competent leaders are the greatest competitive advantage for dealing with the challenges of rapidly changing technology.
- Restructure U.S. strategic communications. Of all the institutions engaged in national security, those engaged in strategic communications face the greatest challenges. Government institutions tasked with strategic communications lack the leadership and resources necessary to do their jobs well in today's ever-changing technology climate and operate with virtually no interagency coordination, let alone the capacity to effectively exploit Web 2.0 capabilities. A new institutional framework and strategy, including the establishment of an Agency for Strategic Communications, are prerequisites for the effective employment of social networking.[16]

A 21st-century government must be able to adapt 21st-century instruments to keep the nation safe, free, and prosperous. Concerning Web 2.0, Washington's best efforts are lagging. Steps are needed now to make government a leader, rather than a follower, in using these new technologies to both strengthen and safeguard American society.

—James Jay Carafano, Ph.D., is Assistant Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.

15. See, for example, James Jay Carafano, "Missing Pieces in Homeland Security: Interagency Education, Assignments, and Professional Accreditation," Heritage Foundation *Executive Memorandum* No. 1013, October 16, 2006, at *http://www.heritage.org/Research/HomelandSecurity/em1013.cfm*.
16. Tony Blankley, Helle C. Dale, and Oliver Horn, "Reforming U.S. Public Diplomacy for the 21st Century," Heritage Foundation *Backgrounder* No.2211, November 20, 2008, at *http://www.heritage.org/Research/PublicDiplomacy/bg2211.cfm*.

The Heritage Foundation LEADERSHIP FOR AMERICA