Executive Summary
Backgrounder
Published by The Heritage Foundation
No. 2300
July 20, 2009

All a Twitter: How Social Networking Shaped Iran's Election Protests

James Jay Carafano, Ph.D.

Disputed results for the election of the Iranian president triggered a wave of public protests in Iran. Extensive media coverage highlighted the role of social networking, both in helping organize activities and sharing the progress of events. The use of e-mail, Facebook, MySpace, Wikipedia, YouTube, Flickr, Digg, LinkedIn, Twitter, and other social-networking tools (often collectively called Web 2.0) to facilitate discussion, debate, and the exchange of ideas and information on a worldwide scale is a well-established phenomenon. Nevertheless, the cyber activism surrounding the Iranian protests was unprecedented, driving the global debate while governments and the established media struggled to keep pace. Though the confluence of events in Iran, including the courage of tens of thousands of Iranian citizens defying the regime of Mahmoud Ahmadinejad, certainly accounts for the dramatic events that played out in the streets of Tehran, there is little doubt that social-networking technologies proved themselves a prominent component of "main street" communications.

The ways in which protesters and others employed social-networking tools illustrate both the opportunities and obstacles of Web 2.0. On the one hand, "citizen reporters" found they could share stories with people around the world in a matter of minutes. On the other hand, "trolls," "vandals," "rats," "sock puppets," and other malicious online actors sought to spread false reports. The war in the streets spread to an online war of words. Internet warriors battled for information supremacy as well as combating the Iranian government's efforts to both limit access to the World Wide Web and spread disinformation. The battle of blogs, tweets, and posts illuminates the key challenge of employing social networking: information assurance—ensuring the right information gets to the right person at the right time, while making sure that the information provided is credible, understandable, and actionable.

The American government should pay close attention to the Iranian experience. Web 2.0 technologies have a potentially important role to play in a range of endeavors related to U.S. national security, from public diplomacy to communicating with citizens during catastrophic disasters. Government must become practiced in effectively employing these technologies, battling malicious actors online, and ensuring the resiliency of the global open network of free debate made possible by social-networking tools. Accomplishing this three-fold mission demands that the U.S. government place

This paper, in its entirety, can be found at:
www.heritage.org/research/Technology/bg2300.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

more emphasis on the professional development of its workforce, the roles and responsibilities of federal agencies for turning Web 2.0 into Government 2.0, and implementing more robust public–private partnerships.

Twitter Turmoil. Iran's national election on June 12 was, according to Heritage Foundation Middle East expert Jim Phillips, "essentially a referendum on President Mahmoud Ahmadinejad's embattled leadership, which has produced economic discontent, international isolation, and greater restrictions on personal freedom." Claims of irregularities emerged even before the vote, Phillips reported, including reports that the Iranian government "distributed 400,000 tons of free potatoes to the poor in a blatant effort to bribe voters. This led supporters of rival candidates to chant 'death to potatoes' at their campaign rallies." Ahmadinejad claimed victory only hours after the polls closed. Despite an endorsement of the election results by Iranian Supreme Leader Ayatollah Ali Khamenei, large street demonstrations escalated in the days following, including clashes with security forces, as well as numerous reports of acts of violence and intimidation after dark and the detention and arrests of political dissidents.

According to press reports, the Iranian government moved quickly to control the flow of public information. This included blocking or interfering with access to mobile networks, the Internet, and satellite television, as well as restricting access to foreign and domestic members of the media. Since the government of Iran, by constitutional fiat, owns and operates radio and television outlets, and by law all newspapers and publications must be supervised by the government, the regime holds a decisive advantage in managing public information. Even after protests subsided, the crackdown on news coverage continued. On June 20, the Iranian government shuttered the Tehran bureau of Al Arabiya, the Dubai-based Arab satellite news station. The next day, the BBC reported, "Jon Leyne, the BBC's permanent correspondent in Tehran, has been asked to leave by the Iranian authorities." In addition to expelling journalists, denying visas to journalists outside the country, and restricting access, Reporters Without Borders stated that as of June 20, the government had arrested at least 24 reporters.

Denied traditional sources of public information, the world turned to social-networking tools that provided services ranging from conventional news reports to a means for organizing protests worldwide. People used Web 2.0 technologies in support of at least four kinds of activities: (1) street journalism, (2) mobilizing the Iranian diaspora, (3) organizing the activists, and (4) information warfare. Though the government attempted to limit access to the Web, it was unable to prevent global activism in response to the Iranian election crisis.

Conclusion. The Iran protests may or may not prove to be a model for sweeping political change and activism in the new century. The lessons of the crisis do illustrate, however, the challenges of operating in a Web 2.0-enabled world. The lessons also suggest that Washington is not ready for prime time. The U.S. government needs to focus more on the professional development of its workforce, the roles and responsibilities of federal agencies for turning Web 2.0 into Government 2.0, and implementing more robust public–private partnerships.

The clock is ticking. Already half the world's population (more than three billion people) has access to a cellular phone. Within a dozen years, a majority of the people on earth will own one. More and more social-networking applications are being developed for cell phones every day. It is not unlikely that some not-too-distant future crisis will spur a global conversation that sweeps across America and around the world at cellular speed. When that happens, the U.S. government must be ready to play its part in the conversation—or its voice will be lost.

—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.

Backgrounder

Published by The Heritage Foundation

No. 2300
July 20, 2009

All a Twitter: How Social Networking Shaped Iran's Election Protests

James Jay Carafano, Ph.D.

Disputed results for the election of the Iranian president triggered a wave of public protests in Iran. Extensive media coverage highlighted the role of social networking, both in helping organize activities and sharing the progress of events. The use of e-mail, Facebook, MySpace, Wikipedia, YouTube, Flickr, Digg, LinkedIn, Twitter, and other social-networking tools (often collectively called Web 2.0) to facilitate discussion, debate, and the exchange of ideas and information on a worldwide scale is a well-established phenomenon.[1] Nevertheless, the cyber activism surrounding the Iranian protests was unprecedented, driving the global debate while governments and the established media struggled to keep pace. Though the confluence of events in Iran, including the courage of tens of thousands of Iranian citizens defying the regime of Mahmoud Ahmadinejad, certainly accounts for the dramatic events that played out in the streets of Tehran, there is little doubt that social-networking technologies proved themselves a prominent component of "main street" communications.

The ways in which protesters and others employed social-networking tools illustrate both the opportunities and obstacles of Web 2.0. On the one hand, "citizen reporters" found they could share stories with people around the world in a matter of minutes. On the other hand, "trolls," "vandals," "rats," "sock puppets," and other malicious online actors sought to spread false reports. The war in the streets spread to an online war of words. Internet warriors battled for information supremacy as well as combating the Iranian government's efforts to both limit access to the

Talking Points

- Today's social-networking tools include MySpace, Wikipedia, YouTube, Flickr, Digg, LinkedIn, Twitter, and other online tools (often collectively called Web 2.0) to facilitate discussion, debate, and the exchange of ideas and information on a worldwide scale.
- During the recent Iranian election protests, cyber activists organized via social-networking tools to share information and updates about unfolding events around the world, as well as to engage people within the country.
- The emerging power of social-networking platforms has implications for U.S. national security and foreign policy. In order to understand and harness these tools, the U.S. government must place more emphasis on the professional development of its workforce, the roles and responsibilities of federal agencies for turning Web 2.0 into Government 2.0, and implementing more robust public–private partnerships.
- The U.S. government must prepare itself to take part in future global conversations and information-sharing that takes place online or via cellular phones.

This paper, in its entirety, can be found at:
www.heritage.org/Research/Technology/bg2300.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

World Wide Web and spread disinformation. The battle of blogs, tweets, and posts illuminates the key challenge of employing social networking: information assurance—ensuring the right information gets to the right person at the right time, while making sure that the information provided is credible, understandable, and actionable.

The American government should pay close attention to the Iranian experience. Web 2.0 technologies have a potentially important role to play in a range of endeavors related to U.S. national security, from public diplomacy to communicating with citizens during catastrophic disasters. Government must become practiced in effectively employing these technologies, battling malicious actors online, and ensuring the resiliency of the global open network of free debate made possible by social-networking tools. Accomplishing this three-fold mission demands that the U.S. government place more emphasis on the professional development of its workforce, the roles and responsibilities of federal agencies for turning Web 2.0 into Government 2.0, and implementing more robust public–private partnerships.

Twitter Turmoil

Iran's national election on June 12 was, according to Heritage Foundation Middle East expert Jim Phillips, "essentially a referendum on President Mahmoud Ahmadinejad's embattled leadership, which has produced economic discontent, international isolation, and greater restrictions on personal freedom."[2] Claims of irregularities emerged even before the vote, Phillips reported, including reports that the Iranian government "distributed 400,000 tons of free potatoes to the poor in a blatant effort to bribe voters. This led supporters of rival candidates to chant 'death to potatoes' at their campaign rallies."[3] Ahmadinejad claimed victory only hours after the polls closed. Despite an endorsement of the election results by Iranian Supreme Leader Ayatollah Ali Khamenei, large street demonstrations escalated in the days following, including clashes with security forces, as well as numerous reports of acts of violence and intimidation after dark and the detention and arrests of political dissidents.

According to press reports, the Iranian government moved quickly to control the flow of public information. This included blocking or interfering with access to mobile networks, the Internet, and satellite television, as well as restricting access to foreign and domestic members of the media.[4] Since the government of Iran, by constitutional fiat, owns and operates radio and television outlets, and by law all newspapers and publications must be supervised by the government, the regime holds a decisive advantage in managing public information.[5] Even after protests subsided, the crackdown on news coverage continued. On June 20, the Iranian government shuttered the Tehran bureau of Al Arabiya, the Dubai-based Arab satellite news station. The next day, the BBC reported, "Jon Leyne, the BBC's permanent correspondent in Tehran, has been asked to leave by the Iranian authorities."[6] In addition to expelling journalists, denying visas to journalists outside the country, and restricting access, Reporters Without Borders stated that as of June 20, the government had arrested at least 24 reporters.

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. James Phillips, "Iran's Sham Election: Buying Votes with Potatoes," Heritage Foundation *WebMemo* No. 2480, June 11, 2009, at *http://www.heritage.org/Research/MiddleEast/wm2480.cfm*.
3. *Ibid*.
4. Nahid Siamdoust, "Forbidden Iran: How to Report When You're Banned," *Time*, June 22, 2009, at *http://www.time.com/time/world/article/0,8599,1906069,00.html* (July 13, 2009).
5. Iran CSOs Training and Research Center, "Access is Denied: A Report on the Status of the Internet in Iran," November 2005, p. 7, at *http://www.genderit.org/upload/ad6d215b74e2a8613f0cf5416c9f3865/A_Report_on_Internet_Access_in_Iran_2_.pdf* (July 13, 2009). This organization is a non-governmental organization based in Tehran that promotes an open civil society.
6. "Iran: BBC Journalist Expelled, News Bureau Shut," CNN.com, June 21, 2009, at *http://www.cnn.com/2009/WORLD/meast/06/21/iran.bbc.journalist.expelled* (July 13, 2009).

Denied traditional sources of public information, the world turned to social-networking tools that provided services ranging from conventional news reports to a means for organizing protests worldwide. People used Web 2.0 technologies in support of at least four kinds of activities: (1) street journalism, (2) mobilizing the Iranian diaspora, (3) organizing the activists, and (4) information warfare. Though the government attempted to limit access to the Web, it was unable to prevent global activism in response to the Iranian election crisis.

Street Journalism

Street journalism includes news or opinion from people who are not professional journalists. This form of public journalism takes two forms. Participatory journalists send reports, photos, videos, or information to news sites that are professionally edited. Fox News and MySpace, for instance, manage a Web site called uReport. The site allows MySpace users to upload videos, photos, and stories in various categories including world news. Fox News controls the editorial content of the site and selects which entries will be featured on the Fox News Web site or its cable news programs.

A second form of public journalism is citizen journalism. Citizen journalists develop their own news content and post their unedited products on individual Web sites. These sites may be managed by the user, or individuals may post information to sites hosted by others. For example, according to *Mediaweek*, "[f]rom June 13 to June 17, iReport.com received nearly 1,600 citizen-produced reports from Iran—mostly photos along with some video content. Plus, the site has added over 3,000 new members over that period, more than double its normal rate."[7] iReport.com is managed by CNN, but is headed by a disclaimer that "iReport.com is a user-generated site. That means the stories submitted by users are not edited, fact-checked or screened before they post…." Unlike participatory journalists, who are generally affiliated with official news services, citizen journalism can include everything from private video and photo-journal essays to the 140-character posts on Twitter and be posted virtually anywhere.

The Online Battleground. According to the International Telecommunications Union, a United Nations agency responsible for collecting data on the telecommunications sector, approximately 31 percent of Iranians had access to the Internet (the second highest percentage in the Middle East behind Israel) in 2008.[8] In contrast, approximately 70 percent of Americans have access to the Internet. In Iran, all Internet Service Providers (ISPs) are licensed by the government. Additionally, Internet Connection Providers (ICPs) are subject to government licensing. Both must submit to government restrictions. ISPs, for example, do not have free access to the Internet. The government maintains a list of forbidden Web sites that remain blocked.

Easy access to the Internet for individual users is available in most Iranian cities. Rural areas generally lack access. Availability in urban centers is vital since about 70 percent of Iranians live in cities. Access to high-speed broadband which allows for quickly transmitting large amounts of data, such as video and audio files, is generally limited to government and business use. The majority of individual users are restricted to slow dial-up access, which is expensive.[9]

The Iranian government censors the Internet. In addition to blocking access to specific Web sites, it also bans the search of certain keywords. In 2005, the estimates of the number of sites blocked ranged from 10,000 to 25,000.[10] In addition, according to a survey by the OpenNet Initiative:

> The Islamic Republic of Iran continues to expand and consolidate its technical filter-

7. "Big Jump in CNN's Citizen Journalism Reports From Iran," *Mediaweek*, June 19, 2009, p. 1, at *http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=108301* (July 13 2009).
8. International Telecommunications Union, "Internet," July 15, 2009, at *http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2008&RP_intLanguageID=1* (July 15, 2009).
9. Iran CSOs Training and Research Center, "Access is Denied," pp. 5–6, 11.
10. *Ibid.*, pp. 11–12.

> ing system, which is among the most extensive in the world. A centralized system for Internet filtering has been implemented that augments the filtering conducted at the Internet service provider (ISP) level…. The Revolutionary Guard has begun to play an active role in enforcing Internet content standards. In conjunction with expansive surveillance, this increase in regulatory attention exacerbates an online atmosphere that promotes self-censorship and discourages dissenting views.[11]

According to the survey, approximately 98 percent of all political Web sites in Iran are censored.

Despite the heavy government presence on the Internet, some Iranians trust what they find online more than they trust official media.[12] In addition, "blogging" and the use of social-networking sites have become increasingly popular in recent years. By some estimates, the "Persian blogosphere," includes between 20,000 and 70,000 blogs.[13]

Street journalism through the Internet played a prominent role before and during the post-election protests despite the fact that the government reportedly made some attempts to limit access to social-networking tools. According to a post in the *Los Angles Times* blog from Beirut, Lebanon, "Iranian Internet-service providers had long banned Facebook, making it inaccessible to dial-up and broadband users. Government officials were fearful it could be used by intelligence officials abroad to recruit operatives or by activists to organize anti-government protests. But in January [2009], after watching the way activists were using Facebook to promote opposition to the Israeli offensive in the Gaza Strip, Iranian authorities apparently warmed up to the quirky website and quietly lifted the ban."[14]

As the election loomed, however, there were reports that the site was blocked again. According to the Associated Press, the Facebook ban was lifted a few days later.[15] In addition, "Twitter, another popular and rapidly growing social-networking tool, also has been filtered out, the Iranian daily Abrar reported," the blog added.[16]

In addition to anecdotal reporting that the government attempted to deny service to the Internet, and the slowing effect of many dial-up users trying to access the system simultaneously, there were allegations that representatives of the Iranian government operated online to spread misinformation. Twitspam, a social-networking site that encourages users to identify and block malicious "tweeters" on Twitter, hosted an interactive Web page where users discussed possible "Iranian agents" operating online.[17] Similar claims were made on Facebook and other popular social-networking sites.

The Iranian government also extensively used the Internet to distribute official proclamations. Both the Supreme Leader and of the Office of the Presidency, for example, maintain official Web sites.[18] Press TV is the Iranian government's English-language cable news and Web site. The

11. According to OpenNet's Web site: "The OpenNet Initiative is a collaborative partnership of four leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard University; the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge; and the Oxford Internet Institute, Oxford University." See *http://opennet.net/about-oni* (July 14, 2009).
12. Iran CSOs Training and Research Center, "Access is Denied," p. 15.
13. "Ctrl+Alt+Delete: Iran's Response to the Internet," Iran Human Rights Center Documentation Center, May 2009, p. 10, at *http://www.iranhrdc.org/httpdocs/English/pdfs/Reports/Ctr+Alt+Delete%20--%20Iran's%20Response%20to%20the%20Internet.pdf* (July 14, 2009).
14. "IRAN: Authorities Block Facebook Amid Heated Election Campaign," *Los Angeles Times*, May 24, 2009, at *http://latimesblogs.latimes.com/babylonbeyond/2009/05/iran-ahmadinejad-islam-facebook-social-networking-mousavi-tehran.html* (July 14, 2009).
15. "Iran Lifts Block on Facebook," Associated Press, May 26, 2009, at *http://wtop.com/?nid=500&sid=1682109* (July 14, 2009).
16. *Ibid*.
17. Evgeny Morozov, "Iran Elections: A Twitter Revolution?" *The Washington Post*, June 17, 2009.
18. "Ctrl+Alt+Delete: Iran's Response to the Internet," p. 11.

Web site featured extensive coverage of the elections including criticism of Western media and social-networking tools. One report claimed that CNN interviewed an "anonymous" witness at a demonstration, whose claims conflicted with a Press TV reporter at the scene. "It remains unclear," Press TV concluded, "whether CNN—which has resorted to 'unreliable' sources like social network websites in its coverage of Iran—was duped by the 'anonymous' caller or was simply faking the phone call in line with the Western agenda of destabilizing Iran."[19] This story was emblematic of most of the coverage on the Web site, all of it intended to portray the regime in the most positive light possible.

In spite of government efforts to manipulate public perceptions, Iranians quickly took to the Internet as protests over the election results mounted. On the one hand, Iranians had few other options. The regime exerted widespread and effective control of conventional media. On the other hand, because the official press has been controlled by Tehran over the last decade, the Internet has been increasingly used by Iranian citizens for free expression including dissident speech. Even before the elections, many Iranians advocated drastic "social and political change."[20] This use of the Internet persisted despite the fact that some bloggers had been jailed and tortured.[21]

Despite a government crackdown, Iran's social network managed to penetrate the outside world. The Iranian government censors the Internet with software that blocks access to forbidden Web sites or Internet Protocol (IP) address. Social applications like Twitter, however, are not tied to a particular Web site. Even if access to the Twitter site is restricted, users may, for example, access Twitter through other services, such as Twitterfall, which may not have been blocked by the Iranian government. Another means for bypassing government is data routing to a computer that acts as a proxy server. These servers employ IP addresses that are not on the government's forbidden list; the servers then route the information to other Web sites, even those on the government's restricted list.

Through these "work-arounds," such as routing information to alternative servers or using Web services that are not forbidden, information continued to flow through cyberspace. Indeed, the only means that the government could have used to completely stop the flow of information was to ban any and all access to the Internet. This was a step the government never took. Doing so might have risked shutting down vital government and economic services as well.

The street journalism that propelled the Iranian election protests into global headlines began within hours of Ahmadinejad's victory speech. As the protests began, documentation appeared on Web sites, such as YouTube, Facebook, and Flickr, as well as in blogs and e-mails. In turn, mainstream news sources, including cable news outlets, such as CNN and Fox News, relied on this reporting both for content and as guide to their coverage of events. Conventional media alerted the world to the extensive use of social networking, which further heightened the demand for street news. Furthermore, street journalism facilitated the use of social networking to propel social dissent.

Mobilizing the Diaspora

In 2006, the Iranian diaspora was estimated to be between 2 million and 4 million people around the world. According to the U.S.-based Migration Policy Institute, Iran's emigrant population is "extremely heterogeneous with respect to ethnicity, religion, social status, language, gender, political affiliation, education, legal status, and timing and motivation for departure (ranging from political to sociocultural to economic)."[22] The largest concentration of Iranians outside of Iran, the report finds, "reside in

19. "CNN: Fake Reporting or Duped by Caller?" PressTV.com, June 25, 2009, at *http://www.presstv.ir/detail.aspx?id=99003&sectionid=3510212* (July 14, 2009).
20. John Kelly and Bruce Etling, "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere," The Berkman Center for Internet & Society, April 2008, p. 5, at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf* (July 15, 2009).
21. "Crtl+Alt+Delete: Iran's Response to the Internet," pp. 42–44.

the United States, followed by Canada, Germany, Sweden, and Israel (…); the United States is home to more than three times the number of Iranian-born living in Canada, the country with the next-largest Iranian-born population."[23] This population has a well-established presence on the Internet.

The Iranian diaspora is also well represented on social-networking sites. A 2005 study of a popular multinational online community called Orkut reported that the site listed 11.4 million users. Of that number, Iranians made up about 340,000, the third most common nationality on the list. While many users were located in Iran, the service was also a popular way to reach the global Iranian diaspora.[24]

Outside of Iran a number of diaspora Web sites served as portals for accumulating and disseminating information about the election protests. A case in point is the Tehran Bureau which is described on its Web site as "an independent source of news on Iran and the Iranian Diaspora." The site was established as an online news magazine only a few months before the election. Its editor in chief is Kelly Golnoush Niknejad, who was born in Iran and emigrated to the U.S. as a teenager. She and most of the site's editors are professional journalists. During the protests, the site's blog-style format included work from participatory journalists, as well as commentary, photos, and videos.

Organizing the Activists

Social networking outside of Iran was probably key to the explosive reliance on these tools. With restricted access, slow Internet service, and limited knowledge of events inside the country as well as the international response to events, Iranians turned to activists outside the country to help facilitate the transfer of information. Blogs, for example, offered advice on how to set up proxy servers to help shuttle information in and out of the country.[25] The Translation Initiative for Iranian Protestors site recruited translators and solicited English translations of information through e-mails, YouTube videos, Facebook, news stories, and press releases, and began posting material within days. The original Farsi-language material and the English translations were posted on a Wikipedia page (a Web site where software allows multiple users to create and edit a Web page as well as track changes made to the page).[26]

Numerous other Web sites were set up as an information clearinghouse, including funneling details about the location of future protests, posting warnings on government crackdowns, and sharing updates of individuals injured, killed, arrested, or missing. According to the World Security Network, one "example of an Iranian-founded social network group is '100 million Facebook members for Democracy in Iran', which can be found on Facebook. In only a few days this group found 150,000 members that created 108,000 board topics, 1,759 wall posts, 6 videos, 496 photos and 1,098 links. And it is growing as everything is just a mouse click away."[27] In fact, the expansion of information on the protests was remarkable. A Google search on the keywords "Iran election protests," on June 28 returned more than one million results.

22. Shirin Hakimzadeh, "Iran: A Vast Diaspora Abroad and Millions of Refugees at Home," Migration Policy Institute, September 2006, at *http://www.migrationinformation.org/Profiles/display.cfm?ID=424* (July 14, 2009).
23. *Ibid*. See also, Ali Mostashari and Ali Khodamhosseini, "An Overview of Socioeconomic Characteristics of the Iranian–American Community Based on the 2000 U.S. Census," Iranian Studies Group at MIT, February 2004, at *http://www.isgmit.org/projects-storage/census/socioeconomic.pdf* (July 14, 2009).
24. Hazir Rahmandad *et al.*, "Iranians on Orkut: Trends and Characteristics," Iranian Studies Group at MIT, January 2006, pp. 1–2.
25. See, for example, Elizabeth Oppenheimer, "The App World has been a Bit of a Trip," blog post on TheFutureoftheInternet.org, at *http://futureoftheinternet.org/the-app-world-has-been-a-bit-of-a-trip* (July 15. 2009).
26. See, for example, the translation of a June 26, 2009, sermon on the elections by Ayatollah Sayyid Ahmad Khatami, an Iranian cleric and member of the Assembly of Experts on Translation Initiative for Iranian Protestors, at *http://translate4iran.wikispaces.com/Ahmad+Khatami+Friday+sermons* (July 15, 2009).
27. Frauke John and Sabrina Schmitt, "Iran: Six Options to Support the Green Flames of Freedom," World Security Network Newsletter, June 28, 2009, at *http://www.worldsecuritynetwork.com/showArticle3.cfm?article_id=17709&topicID=44* (July 14, 2009).

Information Warfare

In addition to facilitating the distribution of street journalism, and mobilizing and organizing political activities, social-networking tools were also employed to conduct information warfare. While the Internet can be used to spread information, it can also be used to distort or prevent access to knowledge. These activities can range from identifying and blocking certain users, to spreading disinformation and disseminating propaganda, to obstructing use of the Internet. Sometimes these efforts are undertaken by governments, but they can also be the work of groups and individuals. Indeed, malicious actors are an already well-established fixture of the social-networking world.

There is a continuous debate among social-networking leaders about the best way to deal with trolls (users who intentionally post inflammatory, controversial, or offensive information), sock puppets (deceptive online identities), vandals (users who post false, extraneous, or nuisance edits to Wikipedia pages), and rats (users who post malicious software programs), as well as other efforts to subvert online content.[28] Some argue that the great strength of social networking is that it creates "open" systems that allow for self-correction. Individuals can more readily challenge inaccurate information and offer corrections. Recent research finds that Wikipedia maintains a high level of accuracy even though editing of its online entries is open to anyone.[29]

During the Iranian election protests, social-networking sites attempted to address the problem of misinformation. Twitspam set up a Web page titled "Fake Iran election Tweeters." The page contained a list of "possible fakes accounts and may have connections to the Iranian Security apparatus." The site added that, "This post will be updated as fake accounts are received. For those questioning the information here, we place accounts here that a) post multiple comments of the same sort (i.e., spam) and b) accounts that are obviously trying to entrap Twitter users who are tweeting from Iran or c) those who obviously are trying to spread misinformation. If we aren't 100% sure we will put in it the 'Suspected' list."[30] Media sites, such as FoxNews.com and CNN.com, vetted information posting stories to its news portals or used materials in its cable news coverage. *The Huffington Post* has established "citizen journalism publishing standards" on its Web site.[31]

In addition to combating suspected Iranian government disinformation, social-networking tools have also been used to organize attacks on the regime Web sites and databases. These attacks, often referred as "Hacktivism," include denial-of-service attacks, disrupting Web sites and databases, and distributing disruptive software.[32] According to the Associated Press, one team of hackers developed and distributed software to bypass Iranian government censorship software.[33]

Lessons Learned

Claims about the revolutionary power of social-networking tools began within days of the protests. Well-known blogger and veteran journalist Andrew Sullivan wrote that, "[y]ou cannot stop people any longer. You cannot control them any longer. They can bypass your established media; they can broadcast to one another; they can organize as never before."[34] While it is premature to forecast a global

28. Andrew Lih, *The Wikipeida Revolution: How a Bunch of Nobodies Created the World's Greatest Encyclopedia* (New York: Hyperion, 2009), pp. 169–182.
29. 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* (July 14, 2009).
30. "Fake Iran election Tweeters," Twitspam.com, June 17, 2009, at *http://twitspam.org/?p=1403* (July 14, 2009).
31. "Citizen Journalism Publishing Standards," *The Huffington Post*, April 14, 2009, at *http://www.huffingtonpost.com/2009/04/07/citizen-journalism-publis_n_184075.html* (July 14, 2009).
32. For an introduction to the origins and development of these activities, see Athina Karatogianni, *The Politics of Cyberconflict* (New York: Routledge, 2006), pp. 121–126.
33. Shaya Tayefe Mohajer, "'Hacktivists' Take up Iran Fight as Streets Quiet," Associated Press, June 28, 2009.

changing political order based on the anecdotal and unstudied events from the days following the Iranian election, available data does suggest some tentative conclusions:

Geography Matters. It is probably wrong to assume that the trends and impacts of social networking will map out equally well across the globe. The availability of the Internet in Iran (though significant by standards in the Middle East) trails the U.S., Europe, and parts of Asia significantly. Additionally, Iranian infrastructure, while rapidly growing, does not provide most Iranians with access to broadband. Yet, through the Iranian diaspora, Iran's citizens achieved a global reach out of proportion to the nation's infrastructure. This phenomenon suggests that other nations with large diaspora populations, such as "labor frontier" countries including Morocco, Egypt, Turkey, Mexico, and the Philippines (which provide much of the world's mobile work force), could also well exhibit online social-networking behaviors more similar to nations with high levels of Internet penetration.

Another factor that perhaps made Iran unique was the character of its civil society. Since government controls state media, Iranians increasingly looked to social-networking tools to create a private sphere where they could discuss issues of politics, culture, sports, and religion. Even though government censorship also existed online, Iranians had fewer inhibitions to employing these tools during crisis, since they were comfortable with them in everyday life.

In short, it appears that the character of the society—from culture to physical infrastructure—is an important factor in determining how social-networking systems will function as an instrument of crisis response.

The Internet is Neutral. No party can count on a decisive and unassailable advantage in cyberspace. Much of the debate over the impact of social networking centered over whether these tools offered a decisive advantage to the protestors or the government. Writing in *The Washington Post*, John Palfrey, Bruce Etling, and Robert Faris offered several counterpoints to those who had concluded that the force of online political activism is irreversible. They argued that there are, "sharp limits on what Twitter and other Web tools such as Facebook and blogs can do for citizens in authoritarian societies." Government, they noted, "jealous of their power can push back on cyberspace when they feel threatened." They also noted that the "freedom to scream" online may actually help regimes by providing a "political release valve." Repressive regimes can also employ social networking for their own ends, hawking propaganda and spreading disinformation.[35] Indeed, during the crisis, the Iranian government exploited all these advantages and in the end was able to largely stifle overt social unrest.

Technology is continuously evolving, as are the practices of how the Internet is used. For example, the Iranian government thought it could maintain permanent dominance of the Web by only allowing slow, expensive dial-up service. That assumption proved wrong. Social-networking tools helped dissidents overcome the limitations of the nation's technological infrastructure.

It is probably incorrect to look at cyberspace as a static contest. Addressing cyber issues begins with the premise that challenges are a series of actions and counteractions between competitors, and inquiring how these competitions might progress in the future. Looking for single "silver-bullet" solutions will not work. There is no technology, government policy, law, treaty, or program that can stop the acceleration of competition in the cyber universe.

The Web Can Take It. The World Wide Web may be more resilient than commonly assumed. Despite Iran's limited infrastructure, denial-of-service attacks on both sides, and the insatiable global demand for information, the Internet held up well. That perhaps should be surprising. A National Academies study that surveyed the capacity of the Web to operate in the wake of 9/11 concluded that

34. Andrew Sullivan, "The Revolution will be Twittered," *The Daily Dish*, June 13, 2009, at *http://andrewsullivan.theatlantic.com/the_daily_dish/2009/06/the-revolution-will-be-twittered-1.html* (July 14, 2009).
35. John Palfrey, Bruce Etling, and Robert Faris, "Reading Twitter in Tehran?" *The Washington Post*, June 21, 2009, at *http://www.washingtonpost.com/wp-dyn/content/article/2009/06/19/AR2009061901598.html* (July 14, 2009).

the Web proved fairly resilient despite the destruction to telecommunications in Manhattan and surge in Internet traffic.[36] While the number of social-networking users online has grown dramatically since 9/11, so has the capacity to respond to the demand. ISPs and social-networking sites have both come to expect "unexpected" changes in demand. This was witnessed recently in the wake of the death of Michael Jackson. Google experienced a dramatic surge in searches for the King of Pop's name. Initially, this surge was believed to be a denial-of-service attack by hackers. Wikipedia shut down its "Michael Jackson" page for six hours when hundreds of people tried to edit it at the same time.

The civil cyber war in Iran also demonstrated the limits of intentionally blocking service or access to Web sites. The ISPs that manage social networks also carry on government business as well as the instruments of commerce. If the government had elected a "nuclear option," it might well have shut down its industrial, energy production, and financial sectors as well as crippling its capacity to control public media. Likewise, in a global economy, states or groups that conduct massive cyber attacks could do as much damage to themselves as to their enemy. Thus, a kind "mutual assured destruction" deterrent policy appears to be evolving in the cyber world.

Furthermore, since competitors seemed deterred from conducting all-out cyber war, it appears that many loopholes remain to allow Internet services to recover. This was demonstrated during the Russian cyber attacks on Estonia in 2007 and Georgia in 2008.[37] In both instances, despite massive attacks and disruption of government sites, both nations were able to re-establish the instruments of governance within hours. In the case of the attack on Georgia, other countries, including Estonia, established proxy servers to host Georgian government Web sites.

While the Internet may be tough enough in the face of cyber competition, it is still at risk to both natural and manmade physical disruptions. In the wake of Hurricane Katrina, for example, the city of New Orleans lost almost complete access to the Internet. There were no adequate contingency plans to restore service. The problem in the wake of Katrina was not the lack of interoperable communications; it was the lack of virtually any kind of communications.

Rather than merely focusing on protecting systems, the national priority should be ensuring resiliency—the capacity to maintain continuity of activities even in the face of threats.[38] Resiliency ensures real security—both physical and economic; a dual approach of protecting against attack and ensuring that if we are attacked, society will continue. Thus, ensuring the resiliency of the global online community against man-made and natural threats remains a subject of concern.

The Rules Work. In his seminal book *Here Comes Everybody*, Clay Shirky outlines the principles for effective adoption of social-networking tools. Shirky's rules address the nature of the technology, the structure of the social interaction, and the value assigned to social-networking transactions.

- **Technologies should be well established.** As Shirky points out, "new tools are not always better. New tools, in fact, start with a huge social disadvantage, which is that most people don't use them, and whenever you have a limited pool from which potential members can be drawn, you limit the social effects."[39] The preference in social networking is to adopt proven and widely available software and systems.
- **Systems should seem simple.** Shirky notes as an example that, "the basic bargain [Wikipedia] offers is that you can edit anyone else's writings and anyone else can edit yours."[40] Simple rules

36. Computer Science and Telecommunications Board, *The Internet Under Crisis Conditions: Learning from September 11* (Washington, D.C., The National Academies Press, 2003).
37. See, for example, Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 29, 2007, at *http://www.nytimes.com/2007/05/29/technology/29estonia.html* (July 14, 2009).
38. James Jay Carafano, "Resiliency and Public–Private Partnerships to Enhance Homeland Security," Heritage Foundation *Backgrounder* No. 2150, June 24, 2008, at *http://www.heritage.org/Research/HomelandDefense/bg2150.cfm.*
39. Clay Shirky, *Here Comes Everybody* (New York: Penguin, 2008), p. 269.

and simple operational routines are the hallmark of widespread adoption of social-networking tools.

- **There has to be something in it for the user.** "[S]ocial tools don't create new motivations so much as amplify existing ones," says Shirky.[41] Users are drawn to social networks because they believe participation will bring them a benefit that they want.

The Iranian case appears to validate Shirky's rule set. Even Twitter, among the newest of the social-networking tools widely used during the protests is two years old. Additionally, Twitter is among the simplest of online communities to participate in. Finally, Twitter and other social-networking sites were popular in Iran because they provided something people wanted—a "space" where they could share ideas with friends and family inside the country and around the world.

Crisis Mis-Management is a Grave Danger. Information assurance—knowing that data are precise and reliable—remains the most serious concern regarding social-networking tools. The global debate around the election protests demonstrated that 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. 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.[42]

In social networks, the group itself assumes responsibly for culling out bad data. This includes everything from battling trolls to debating aspects of *sharia* law on a religious blog. While this method of adjudicating information may be suitable during normal social-networking interactions, there is a real question over whether it is appropriate for crisis communications. An effective crisis communication must be credible, understandable, and actionable. Under great stress and limited time, as well as limited information, it is unrealistic to hold that negotiated online interactions are an effective mechanism for determining factual and dependable information.

Twitspam offers a case in point. It recommends shutting off suspected trolls, but is not always clear how the decision is made that a particular tweeter is a malicious actor. In its rush to safeguard the site from bad users, Twitspam could inadvertently be subverting the opportunity for individual free expression it is trying to safeguard.

For Web 2.0 to be used effectively *during* a crisis, trusted actors and trusted networks must be established *before* a crisis. Only these can serve as an effective backbone for turning a social network into an effective crisis management and risk communication tool.

Washington is Not So Hot. The U.S. government is not well prepared to exploit social-network tools during a crisis. Washington is well behind in its willingness and capacity to adapt to the world of Web 2.0. Even the Obama Administration, with a reputation as "Web savvy," has its troubles. A panel of experts assembled by *The Washington Post* gave the new WhiteHouse.gov site an average grade of C+.[43] That grade seemed to track well with the Administration's response to the Iranian election protests. Despite the flood of information driving the global debate as the protests grew, the President remained equivocal until several days into the crisis. Yet despite subdued rhetoric from the White House, the Administration found itself pummeled by Iranian government accusations of interference, including a charge that an innocent bystander had been shot by the CIA to foment a riot.[44]

40. *Ibid.*, p. 271.
41. *Ibid.*, p. 294.
42. Alex Wright, *Glut: Mastering Information Through the Ages* (Washington, D.C.: National Academies Press, 2007), pp. 231–232.
43. Jose Antonio Vargas, "Grading WhiteHouse.gov," *The Washington Post*, March 24, 2009.
44. See, for example, "Iranian Envoy: CIA Involved in Neda's Shooting?" CNN.com, June 25, 2009, at *http://www.cnn.com/2009/WORLD/meast/06/25/iran.ambassador* (July 25, 2009).

The government's online engagement proved equally unfocused and ineffective. Heritage analyst Helle Dale noted that initially most government outreach was limited to the "State Department's revelation that it requested that the social Web site Twitter postpone its scheduled maintenance operation in the days after the election as protesting Iranians were relying heavily on its service to communicate—causing some to suggest that these protests could end up being called the Twitter Revolution. Undoubtedly, this action was important, but given the resources of the U.S. government, it was hardly proactive."[45] The lack of effective Web 2.0 engagement represented a lost opportunity for the White House to demonstrate global leadership during the crisis.

The disappointing results are not surprising. 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 are not keeping pace; they are inadequate for exploiting the explosion of social-networking systems.[46]

Next Steps

The preliminary list of lessons learned offers a starting place for a national agenda to make the federal government better prepared to employ Web 2.0 technologies during a national crisis.

Start with Strategic Communications. The United States requires the rudimentary backbone for conducting strategic communications in the information age. The White House cannot assemble a better Web 2.0 tool kit without a solid foundation. Of all the institutions engaged in national security, foreign policy, and public diplomacy, 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.[47]

Build a Network Savvy Workforce. Washington needs a proactive professional leadership development plan and research agenda. The lessons of the Iranian election protests illustrate the many complex factors that drive competition in the Web 2.0 world, from understanding culture to providing information assurance. To overcome these obstacles, much of the innovation in the social-networking environment is based on intuition, guessing, trial and error, and blind luck. That is not good enough for matters of state. Unless the government develops leaders imbued with the skills, knowledge, and attributes to operate in a network world, it will never master the challenges of social-networking technology.

Likewise, Washington must 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 of the science behind social networking 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-

45. Helle C. Dale, "The Iranian Elections and Public Diplomacy 2.0: A Tale of Untapped Potential," Heritage Foundation *WebMemo* No. 2497, June 19, 2009, at *http://www.heritage.org/Research/PublicDiplomacy/wm2497.cfm*.

46. James Jay Carafano, "Social Networking and National Security: How to Harness Web 2.0 to Protect the Country," Heritage Foundation *Backgrounder* No. 2273, May 18, 2009, at *http://www.heritage.org/Research/NationalSecurity/bg2273.cfm#_ftn2*).

47. 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*.

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.

Public–Private Partnerships Are Essential. Trusted space and relationships as well as resilient infrastructure can only be established with effective cooperation between government and the private sector. These partnerships must focus both on mastering the challenges of effective risk communications as well as ensuring the resiliency of national and vital global infrastructure. These partnerships should not be "corporatist" collusion between government and big business. The best way to achieve resiliency in infrastructure is through the free market. The private sector can—and should—play a role in the development of resilient infrastructure. Developing 21st-century infrastructure requires the private sector, whose members are generally well informed on current infrastructure needs because of the need to stay competitive.

The U.S. government should look at models such as Pacific Northwest Economic Region (PNWER). PNWER facilitates cooperation through regional issue action plans developed by fourteen working groups corresponding to the region's key priorities. Each group is co-chaired by an industry leader and legislator. The organization has a statutory basis but all its operations are conducted on a voluntary, non-profit, non-partisan basis. The PNWER models work because participants have trust and confidence in the mechanisms used to develop and implement action plans and commonly value the outputs of the organization.

Conclusion

The Iran protests may or may not prove to be a model for sweeping political change and activism in the new century. The lessons of the crisis do illustrate, however, the challenges of operating in a Web 2.0–enabled world. The lessons also suggest that Washington is not ready for prime time. The U.S. government needs to focus more on the professional development of its workforce, the role and responsibilities of federal agencies for turning Web 2.0 into Government 2.0, and implementing more robust public–private partnerships.

The clock is ticking. Already half the world's population (more than three billion people) has access to a cellular phone. Within a dozen years, a majority of the people on earth will own one. More and more social-networking applications are being developed for cell phones every day. It is not unlikely that some not-too-distant future crisis will spur a global conversation that sweeps across America and around the world at cellular speed. When that happens, the U.S. government must be ready to play its part in the conversation—or its voice will be lost.

—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.