Iran, Disintermediation, and Cyberwar

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

With some justification, skeptics have questioned whether cyberwar is a realistic scenario for concern or merely a scary story to earn funding for security companies and writers. Unfortunately, there are many cases in which journalists and others have leaped to the conclusion that security breaches are examples of cyberwar; recent examples include the Estonian “cyberwar” of 2007 and the attacks on the Church of Scientology in early 2009. <http://www.newscientist.com/blog/technology/2008/01/scientology-hacks-cyberwar-or-street.html>

We may be seeing an illustration of one kind of cyberwar in June 2009 as many readers follow news of the post-election events in Iran with interest and concern. Following a vigorous election campaign in which Mir Hossein Mousavi appeared to have a majority of the voters’ support but not a majority of the reported votes <http://www.independent.co.uk/news/world/middle-east/mousavis-aides-fear-dirty-tricks-could-swing-result-1703226.html>, the situation after the balloting quickly degenerated into claims and counterclaims of ballot-rigging <http://www.cnn.com/2009/WORLD/meast/06/15/iran.elections.qa/index.html> and demonstrations that turned into violent confrontations.<http://www.boston.com/bigpicture/2009/06/irans_disputed_election.html>

Throughout the conflict, electronic communications have been central to the organization of protests and to the attempts of the dictatorial regime to suppress dissent. In particular, the tiny-message network Twitter <http://twitter.com/> has been central to the coordination of mass action. Canadian writer Brett Anningson has a summary of Twitter’s role in the protests <http://timestranscript.canadacanews.com/opinion/article/706779> in which he comments, “Iranian Twitterers, many writing in English, posted photos of huge demonstrations and bloodied protesters throughout the weekend, detailing crackdowns on students at Tehran University and giving out proxy web addresses that let users bypass the Islamic Republic’s censors. | By Monday evening, it had become such a movement that Twitter postponed maintenance scheduled for the wee hours of the morning, California time -- midday Tuesday in Iran. | The maintenance was rescheduled to be between 2-3 p.m. in California which happens to be 1:30 a.m. in Iran. | A couple of Twitter feeds have become virtual media offices for the supporters of Moussavi. One feed, mousavi1388 (1388 is the year in the Persian calendar), is filled with news of protests and exhortations to keep up the fight, in Persian and in English. It has more than 15,000 followers.” He adds that the social networking site Facebook <http://www.facebook.com/> has over 50,000 members in the Moussavi fan group.

The government has been fighting back: “Access to networking sites such as Facebook and Twitter and the photography site Flickr have been blocked in Iran, where the government has also been accused of blocking text-messaging, launching denial of service attacks and spreading misinformation to protest communities online.” <http://english.aljazeera.net/programmes/rizkhan/2009/06/200962281940160238.html>

Iranians have been bypassing these attempts to shut down their communications; countermeasures include using proxy servers to evade Iranian government Internet blocks.<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/06/17/MN75188C6K.DTL> Supporters
of the protests have posted lists of suggested countermeasures <http://boingboing.net/2009/06/16/cyberwar-guide-for-i.html>; e.g., they advise Twitter users not to publicize the location of proxy servers, not to rebroadcast information without verifying its origin and authenticity (to circumvent Iranian government propaganda), and to switch Twitter settings to match the geographical location of Tehran and thus make it harder for the government agents to identify local protesters (the “I AM SPARTACUS” defense<http://www.imdb.com/title/tt0054331/>).

So it seems that Professor Phil Agre’s emphasis on the importance of disintermediation<http://www.mekabay.com/opinion/critical_thinking.pdf> – the removal of institutional barriers to mass communications – and the widespread availability of electronic networks really has brought the world of cyberwar to reality.

And I don’t think that this is as far as cyberwar will go. Keep your attention focused on that screen / cell phone / neural implant . . .

* * *

On another note: join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” (July 18-23)<http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php> “Management of IA,” (Aug 1-6)<http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php> and “Cyberlaw for IA Professionals.”(Aug 8-13)<http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php> Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.