This is the second of two parts looking at the implications for information warfare of disintermediation coupled with a lack of critical thinking.

Disintermediation in general is defined by the Webopedia as “Removing the middleman. The term is a popular buzzword used to describe many Internet-based businesses that use the World Wide Web to sell products directly to customers rather than going through traditional retail channels. By eliminating the middlemen, companies can sell their products cheaper and faster. Many people believe that the Internet will revolutionize the way products are bought and sold, and disintermediation is the driving force behind this revolution.”

Disintermediation in the distribution of news is the phenomenon of reducing gate-keepers in the flow of information from provider to user. For example, Matt Drudge is free to spread unsubstantiated rumors to a huge audience without having to bother with the fact-checking that is customary in responsible news media such as reputable newspapers or magazines and some television or radio programs.

Critical thinking is the ability to analyze information skeptically rather than gullibly. For example, people who open unexpected attachments in e-mail from friends are failing to distinguish among different targets of trust:

* Trust in the authenticity of the FROM line of an e-mail message (which may not, in fact, correctly identify the source);

* Trust in the technical competence of the sender to evaluate the quality of the attachment (which may not, in fact, correlate with how loveable and friendly Aunt Gladys is);

* Trust in the authenticity of the labeling of the attachment (which may not, in fact, really be a document at all but may be an executable);

* Trust in the description and safety of an attachment (which may not, in fact, be a screen saver with frogs).

Now couple disintermediation with a lack of critical thinking. Consider the likely effects of a concerted campaign to, say, spread a number of rumors about major publicly-traded companies. We know that pump ‘n’ dump schemes have successfully manipulated stock values to the benefit of criminals; why not expect terrorists to apply the same techniques to manipulating the entire stock market? If people are willing to believe and act upon stock tips e-mailed to them by total strangers using spam (even though tiny print clearly states that the junk mailer has been paid to distribute the information), why wouldn’t uncritical thinkers cheerfully act on “advice” spread by enemies of the nation?

Similarly, the phenomenon of flash crowds worries me: training people to assemble on command in large numbers at, say, shoe stores, piano showrooms or restaurants for no good
reason other than the fun of being part of a huge crowd is a perfect setup for creating an army of
willing, mindless drones who will congregate on command at the site of a terrorist attack or at
places where their presence will interfere with response to criminal or terrorist activities. Want
to rob a bank in peace and quiet? Set up a conflict between two instant crowds to draw the
police to an instant riot.

I think that all of us in the IT, network and security fields are used to critical thinking. We have
to be to keep up with the flood of technical information and distinguish marketing exaggerations
from realistic information. We are used to writing and reading product comparisons, strategy
evaluations and management recommendations as part of our work. Let’s use our skills to foster
critical thinking throughout the educational system. Let’s work as volunteers on school boards,
in the classroom and in social organizations to introduce critical thinking to children and adults
who haven’t learned how to distinguish reality from propaganda. Push for curriculum changes to
accompany lessons on how to use the Internet with lessons on how to weigh the information
found through e-mail and on the Web.

Let’s make sure that we’re not patsies for an information warfare attack rooted in
disintermediated propaganda.

* * *

For Further Reading


* * *

Come to the e-ProtectIT Infrastructure Protection Conference at Norwich University 23-25

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information
Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 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.