Aol News.

http://www.aolnews.com/opinion/article/opinion-its-a-wikileaks-world-better-get-used-to-it/19581407

Opinion: It's a WikiLeaks World, Get Used to It

(Aug. 5) — No matter where right or wrong lie in the posting of classified military reports on WikiLeaks.org, one lesson should be clear: This is how it's going to be. Technology will continue to undercut secrecy — not just in the military, but in all large organizations.

Government and corporate leaders who aren't ahead of this problem may already have trouble on their hands they don't know about.

When 90,000 pages of documents chronicling the Afghan war went online last week, their potential effects on military planning and security caused the White House to strongly condemn their posting as "irresponsible." Differing more than slightly, Salon commentator Glenn Greenwald praised WikiLeaks.org as "one of the most valuable and important organizations in the world."

While there is universal agreement that over-classification in the U.S. government is a problem, leaking government documents isn't a good way to fix it. Nevertheless, a pair of related technology trends will continue to push this "fix" in a disorderly way if it's not solved methodically.

Technology: First, individuals today have tremendous power to collect, transmit and process information. Average people have hand-held computers and phones, huge-capacity flash memory thumb drives, and so on. The tech-savvy have even more powerful information devices, familiarity with encryption, and anonymization tools. We have overcome the natural conditions that made easy-to-censor hand-written letters a minimal threat to "operational security" in World War II.

Culture: Cultural trends are coming into play as well. Military service-members today live in a culture of information sharing that might baffle their senior officers. They expect to be in touch with the outside world during their tours. Their service is long and difficult enough without quarantining them in a communications bubble for protracted periods. Indeed, doing so would undermine military effectiveness by cutting deeply into the morale of young men and women whose stateside lives are "always connected." This is the generation that knows the value and power of sharing information.

More Opinion on AOL News

- Opinion: You Call This Marriage?
- Opinion: For Same-Sex Marriage Opponents, a Catch-22

- Opinion: Prop 8 Ruling Is an Especially Sweet Victory
- Opinion: It's a WikiLeaks World, Get Used to It
- More Stories »

- **Feedback**
- Send letters to the editor to opinion@aolnews.com. Please include your name and location (city and state), and indicate that you intend the letter for publication.

So what's to be done?

Doubling down on information security is an option, but there are better approaches than to hunker in the secrecy corner.

As Admiral Greer said in Tom Clancy's "The Hunt for Red October": "The likelihood of a secret being blown is proportional to the square of the number of people who're in on it." It's a converse of Metcalfe's law, which describes the increase in value of a network as the number of participants grows.

Computer security has wisdom to share with national security and military security — indeed, with any organization that relies too heavily on secrecy: "You're doing it wrong." Secrecy should be treated as a weakness, to be avoided whenever possible.

Since at least the Vietnam-era controversy over the accuracy of U.S. government "body counts," it's been getting harder to control military information, and the difficulty will only increase. Secrecy is sometimes necessary, and propaganda is a legitimate dimension of war, but as technology and tools of transparency make their way even to remote battlefields, secrecy and propaganda that are at odds with the evidence on the ground will necessarily be less effective.

Organizations of any size should examine what information they have that is not publicly available, and how they would be harmed by its release.

Ultimately, the U.S. military and all organizations, government and corporate, should begin to plan strategy and tactics so that they don't rely on controlling information — at least not for long after it originates.

Information technology is a strong and growing adversary, and it is better to turn its strengths to one's advantage than to waste resources trying to fight against it.

Jim Harper is director of information policy studies at the Cato Institute.

Follow AOL News on Facebook and Twitter.