Commentaries on Albert-László Barabási's books

Networks101Link9.2 Cybersecurity and Democracy ©frederick david abraham, 12 May 2013

Cybersecurity against the collapse of system control from malicious and natural disasters is essential to protect vital infrastructure, such as civil, economic, information, energy, goods, and military systems. Here is a famous example of internet susceptibility:

From http://en.wikipedia.org/wiki/Eligible_Receiver_97**,** retrieved 12 May 2013**:**

Eligible Receiver 97 was a U.S. government exercise conducted under what is known as the No-Notice Interoperability Exercise Program. The exercises were held June 9–13, 1997 and included participants such as the National Security Agency (which acted as the Red Team), Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation,National Reconnaissance Office, Defense Information Systems Agency, Department of State, Department of Justice, as well as critical civilian infrastructure providers such as power and communication companies.

The NSA Red Team used hacker techniques and software that was freely available on the Internet at that time. The Red Team was able to crack networks and do things such as deny services; change and manipulate emails to make them appear to come from a legitimate source; disrupt communications between the National Command Authority, intelligence agencies, and military commands. Common vulnerabilities were exploited which allowed the Red Team to gain root access to over 36 government networks which allowed them to change/add user accounts and reformat server hard drives.

National Security Agency Red Team had no inside information to work with, but by engaging in extensive preliminary electronic reconnaissance of target agencies and sites prior to the attacks, they were able to inflict considerable simulated damage. Although many aspects of Eligible Receiver remain classified, it is known that the Red Team was able to infiltrate and take control of U.S. Pacific Command computer systems as well as power grids and 911 systems in nine major U.S. Cities.

From http://deibert.citizenlab.org/bio/ and http://en.wikipedia.org/wiki/Ronald_Deibert

Ronald J. Deibert, OOnt (PhD, University of British Columbia) is professor of Political Science, and Director of the Canada Centre for Global Security Studies[1] and the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The Citizen Lab is an interdisciplinary research and development "hothouse" working at the intersection of the Internet, global security, and human rights.[2] He is a co-founder and a principal investigator of the OpenNet Initiative and Information Warfare Monitor projects.[3]

Not only is Deibert a leading expert on cybersecurity, cyberespionage, and cyberwarfare, fields that have developed largely since Barabàsi's *Linked*, but he is a also leading exponent of the OpenNet democracy and individual rights. These goals can be both competitive and synergetic. He first caught my attention with his great book, *Parchment, printing, and hypermedia* which tells how large corporations and government use the IT so subvert governmental controls over global businesses, and thus corrupt the democratic processes that Hiltz and Turoff (1978, 1994) tout in their book *Network nation*, and John Perry Barlow's expressed in his

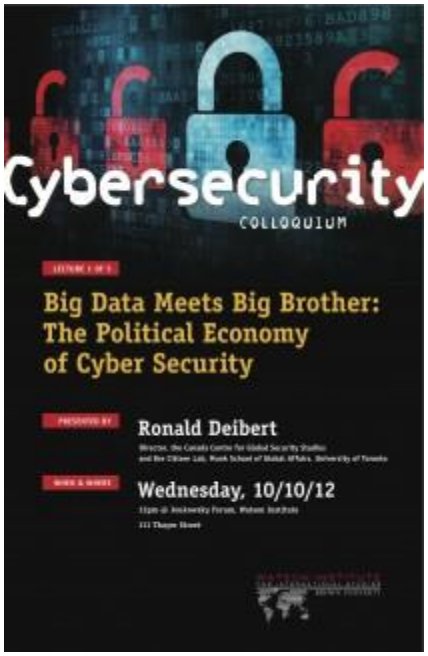
Declaration of the Independence of Cyberspace In *Parchment*, Deibert used an informal systems theoretical point of view.

From http://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace

The Declaration sets out, in sixteen short paragraphs, a rebuttal to government of the Internet by any outside force, specifically the United States. It states that the United States did not have the consent of the governed to apply laws to the Internet, and that the Internet was outside any country's borders. Instead, the Internet was developing its own social contracts to determine how to handle its problems, based on the golden rule. It does this in language evocative of the United States Declaration of Independence and obliquely cites it in its final paragraphs. Although the paper mentions the Telecommunications Act, it also accuses China, Germany, France, Russia, Singapore, and Italy of stifling the Internet.[1]

From: http://www.watsoninstitute.org/events_detail.cfm?id=1904

As policy makers are given the products and services to do things that they never before even imagined, an epistemic shift occurs around the framework for rights and governance. What was inconceivable is increasingly considered routine. Lawmakers now justify radical changes to basic checks and balances on state surveillance as part of a supposed necessity of the digital age. Not too long ago, Internet pundits mocked slow-footed authoritarian regimes and predicted their demise. Today, they are prime customers for the tradecraft of cyberspace controls. Big Data meets Big Brother. [read the whole thing, it is short.]



See also:

Deibert's forthcoming (2013) book, Black Code: Inside the Battle for Cyberspace

Also in the new book, *Liberation Technology: Social Media and the Struggle for Democracy*, edited by Larry Diamond and Marc F. Plattner, Canada Centre for Global Security Studies and Citizen Lab Director Ron Deibert authored the chapter on "International Mechanisms of Cyberspace Controls".