Cybersecurity: The New Frontier

KUFM Commentary: November 14, 2012
By Dan Smith, Interim Director of the Maureen and Mike Mansfield Center

About four years ago, I was checking my e-mail while on vacation. As often happens, I was rapidly moving through the dozens of e-mails lodged in my inbox, when I hit on an important message from Hotmail. It said that my e-mail account was in danger of being compromised because of my weak password. The advice – change my password immediately. After requesting specific information, there was a seemingly innocuous question: “Current password?” Foolishly, I filled in my current password – and, then, it hit me! My e-mail had indeed been compromised - my internet identity stolen. I felt personally violated. All of my credit cards had to be cancelled and re-issued. Every one of my contacts received an e-mail within minutes requesting that each send $3,500 to Kuala Lumpur, Malaysia, as I was ostensibly stranded in the airport where my wallet and passport had been stolen and I had no way of returning to Montana without an infusion of cash from my friends. How profoundly embarrassing!

Perhaps you or one of your friends or family members have experienced something similar – identity theft in cyberspace. Through simple inattention, you have bypassed the security software and firewalls intended to protect your identity.

Now project that insecurity on a world-wide screen that could affect the identity – life and livelihood of more than seven billion people, indeed the welfare of the planet through manipulation of cyberspace. Cyberspace is the domain of global digital electronic communications. It is far broader than the internet. It includes the entire spectrum of networked information and communications systems world-wide. Cyberspace permeates all aspects of human society, virtually every aspect of political, economic, cultural and social life is premised on the flow of information through cyberspace.
Ronald Deibert, a professor of political science at the University of Toronto and Director of the OpenNet Initiative, has written extensively on cybersecurity. In a recent article on “Cybersecurity: the New Frontier” in the foreign policy journal, Great Decisions, he outlines key issues we need to consider.

According to Deibert “Cyberspace is entering a period of intense contestation and potential chaos, as a multitude of different actors (states, civil society, businesses, militant and organized criminal groups ) struggle to shape the domain to their strategic interests. Many governments are now grappling with a wide range of new threats that have emerged including cybercrime, espionage and warfare.” Indeed “The transformation of the domain of cyberspace into a matter of national security is perhaps the most important force shaping global communications today.” Today’s news sources are replete with instances of critical disruptions of global transportation, finance, defense, telecommunications and social media systems that affect the lives of multi-millions of people.

At its core is the global challenge to find a way out of the chaos of cyber insecurity. Deibert raises the following suggestions: “In the formulation of cyberspace policy two major issues collide: the practical necessity of securing cyberspace to preserve public confidence (which extends to policing, commercial viability, and national security), and the preservation of openness as a global public good that is in line with the norms of liberal democratic societies. How should these competing challenges be balanced?

Further, “Who should govern cyberspace? Should international efforts be conducted by governments in a centralized, multilateral body – possible under the auspices of the UN? What are the barriers to international cooperation on efforts to combat cybercrime and to regulate other activity in cyberspace?”
Beyond the immediate concern for the security of our own identity in cyberspace, we need to stay tuned to the unfolding answers to these questions which might affect the common future of the human race.