Cyber-Security: More Transparency

By Tim Maurer

8 February 2012, Kommersant

One third of the world's population is using the Internet.[1] People's lives in Russia, the U.S., Europe, China, even Africa are permeated by Facebook, Google, Twitter, Baidu, or Skype. When President Medvedev visited the U.S., he met not only with President Obama but also Steve Jobs. What they decide affects most of us.

At the 2011 G8 summit and the London Conference on Cyberspace, cyber-security reached the highest level of government. The Distributed Denial of Server attack against websites in Estonia in 2007 and Georgia in 2008 showed world leaders that threats from cyberspace can rise to the level of a national security risk. The year 2010 provided further proof. The WikiLeaks releases and the Stuxnet virus damaging Iran's nuclear program demonstrated that the Internet can be used to cause significant harm. And the UN Group of Governmental Experts concluded in 2010, "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century".

General Cartwright, former vice chairman of the U.S. Joint Chiefs of Staff, calls for more openness when discussing cyber-security.[2] States must signal their policies and strategies to avoid misperceptions and misunderstandings among each other. The policy documents published by the U.S. government in 2011 are a first step in that direction. Another key question is if all states, particularly China, agree that the established system of rules among states, particularly the law of armed conflict, covers cyberspace or insist on creating new ones.

So what to expect in 2012? James Lewis at the Center for Strategic and International Studies in Washington wrote on December 22, 2011, "This year's theme was Norms. Next year's theme will be Confidence Building Measures." It is a sobering reminder that talking about norms alone will not shape how states behave in cyberspace. It requires the nuts and bolts of classic diplomacy and international cooperation. Harvard University professor Joseph Nye, for example, emphasizes how crucial the involvement of military officials is for international coordination. "The lessons from the nuclear era would suggest the importance of involving People's Liberation Army officers in discussions of cyber cooperation."[3]

The good news is that despite their differences, states also have common interests. The U.S., Russia, and China, for example, are learning that cyber-crime affects them all. The Financial Times quotes cyber-security expert Don Jackson, "Russian cyber-criminals no longer follow hands-off rules when it comes to motherland targets, and Russian authorities are beginning to drop the laissez-faire policy." And computers in the U.S. and China are the world's leading sources of malicious activity.[4]

Cyber-security is now on the agenda of the world's governments. Reducing some of the uncertainty around it is a good start - not only for states to know what they are doing but also for their citizens.

[1] http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf

[2] http://uk.reuters.com/article/2011/11/06/us-cyber-cartwright-idUKTRE7A514C20111106

[3] http://www.au.af.mil/au/ssq/2011/winter/nye.pdf

[4] http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=malicious_activity_by_source