Translating the U.S. International Cyber Strategy Into Action

Chris Bronk | 19 May 2011

The Stuxnet computer worm, WikiLeaks and the social-media-facilitated revolutions of the Arab Spring have already provided ample reason for a high-level U.S. policy on cyber issues. Now the killing of Osama bin Laden has provided an opening for a broader strategic dialogue in Washington, one that includes cyberspace in its proper context. This policy discussion has been a long time coming, and it has now arrived in the form of the Obama administration's "International Strategy for Cyberspace" (.pdf), which presents concepts and ideals on a cluster of diplomatic, commercial and security issues related to the global information space that the Internet and its environs have become.

It is important to establish what the strategy is not. It is not a cybersecurity plan, but rather a broad set of prescriptions relating to the Internet and information more generally. At its core, the Obama administration has enunciated a policy that places primary emphasis on the Internet as a going, growing and global concern. To borrow from Ronald Deibert and Rafal Rohozinski, the U.S. government has decided to pursue the protection of a global cybercommons. This translates to a trustworthy Internet that remains open for business, embracing innovation and accepting entrepreneurship. This means managing cybercrime, developing international standards and keeping markets open, to the maximum degree possible across sovereign boundaries.

Such objectives are in line with recent contributions to the macro-strategic literature, particularly "A National Strategic Narrative" (.pdf), written under the pseudonym "Mr. Y" by a Navy captain and a Marine colonel, and Joseph Nye's "The Future of Power." The pseudonymous work expresses the valid concern that the United States will not be able to project its military power abroad if its strategic foundation rests upon an economic bed of sand. Regarding the Internet, the message is clear. The United States, which was a key player in creating the technologies of the Information Revolution, must retain a leading role in the stewardship of the global cyber domain if it is to continue to profi from it.

The values espoused by the Obama administration's cyber strategy go beyond economics, spanning freedom of expression, privacy and the free flow of information. These pillars of American exceptionalism do not scale uniformly across the planet, however. Evgeny Morozov -- whose homeland, Belarus, remains under the control of Europe's last great überauthoritarian regime -- notes that the Internet is no panacea for political repression. In the context of the values embraced by the strategy document, it is important to understand that the Internet by itself is not sufficient to bring about the freedoms of expression and information flow. Furthermore, the world's digitally connected population -- best exemplified by the 500 million users of Facebook -- have willingly abandoned a degree of privacy. While the values outlined in the "Information Strategy" are clearly important, we would do well to question whether they are more germane to the U.S. government than to global

cyberspace.

President Barack Obama has enunciated a policy that goes far beyond cybersecurity, extending outside the province of the Pentagon and its legions of information warriors. What the nation's leaders have inherited is a superb, but flawed platform for global interconnection. The problem they now face is how to develop a diplomatic dialogue with the international community on how to deliver on the strategy's lofty goals (.pdf). We know we need Russia to acquiesce to cooperation on cybercrime, and we would like the new regimes of the Middle East to further open their Internet windows to the world's ideas. Perhaps most importantly, the U.S. will need to determine how its cyber policy will be interwoven with the greater statecraft involved in its relationship with China.

How the United States handles the rise of China and its cyber insecurities, especially regarding human rights, will define what is likely the to be most important bilateral relationship for the next several decades. Former Secretary of State Henry Kissinger argues that although the U.S. must affirm "its commitment to human dignity and popular participation in government . . . experience has shown that to seek to impose them by confrontation is likely to be self-defeating -- especially in a country with such a historical vision of itself as China." This speaks to a need for international cyber policy that is nuanced, accepting of complexity and tuned to both political objectives and technical realities.

The U.S. is lucky that so many of the firms that produce the contemporary Web 2.0 cyber experience -- Google, Facebook, Twitter and many others -- are based within its borders. Like the Internet itself, these companies, as globalized and multinational as any on the planet, have built out the contemporary platform of technologies that are such a big part of what we call cyberspace. The U.S. would do well to protect this position, but preserving the cyber ecosystem should be just a starting point for the Washington policy mandarins engaging in the statecraft of information in our digitally connected world.

Chris Bronk is a fellow at the James A. Baker Institute for Public Affairs at Rice University, where he also teaches computer science. He studied Soviet military doctrine at Oxford University and is a former U.S. diplomat.

Photo: Internet Archive servers (photo by Flickr user Oneras, licensed under the Creative Commons Attribution-ShareAlike 2.0 Generic license).