The New York Times
The Opinion Pages

Arms Control in Cyberspace

Ron Deibert *is the director of the Citizen Lab at the Munk Centre for International Studies at the University of Toronto. He is the co-founder of the Information Warfare Monitor report, and one of the principal investigators and a co-author of the GhostNet study investigating alleged Chinese cyberespionage.*

President Obama's announcement of his administration's commitment to cyber security caps months of speculation and intense bureaucratic maneuvering. But the most intriguing part concerns the lingering devils in the policy details, and not just about whom will fill the Office of Cybersecurity coordinator.

The president's announcement and report affirms his commitment to the protection of civil liberties and privacy and makes a strong endorsement of net neutrality that will please many. But his policy record on surveillance is considerably more hawkish, and there was no detail given that resolves the controversial role in cybersecurity of the National Security Agency.

Although the agency has digital expertise, it is among the nation's most secretive organs with connections to incidences of extra-legal domestic surveillance. The success of private-sector sharing arrangements, and protections for civil liberties, laid out by the President depends on the now ambiguous role of this agency. Also left unaddressed is what, if any, international mechanisms will be developed to address cybersecurity.

> Obama's announcement will unleash more attack strategies from adversaries, including Russia and China, who will see the U.S. policy as a legitimization of such tactics.

The president acknowledges the globally interconnected character of cyberspace in detail. But curiously there is not even a strategic vision, much less a blueprint, for how the United States will work to protect global networks as part of its own security.

Indeed, the biggest black hole — likely to remain as such — concerns U.S. offensive operations in cyberspace, which presumably include everything from denial of service attacks to targeted malware to Web 2.0 psychological operations.

I rather naively hoped today would have been President Obama's Eisenhower moment, an opportunity to lay out a grand strategic vision for "Bits for Peace" (or maybe an "Open Net Initiative"?) and take leadership in swiftly controlling weapons in cyberspace worldwide. Instead, it is almost certain (and it is among the worst kept secrets) that a stamp of approval is forthcoming for the Pentagon's plans to fight and win wars in cyberspace.

Undoubtedly the move will trigger an escalation of attack strategies and incidences from adversaries, including Russia and China, who will see the U.S. policy as a ratcheting of threats and a legitimization of such tactics. And we can expect more debilitating attacks on Websites and services, contracted out to third parties to muddy attribution issues and allow for plausible deniability.

Today's announcement does nothing to explain how to secure against the chaos unleashed by that threat. Ultimately the assurance of security for every nation's critical infrastructure must include an international dimension that preserves the openness of global cyberspace.