EMBASSY

The cyber samba turns nasty

PAUL MEYER

The Snowden revelations have only served to exacerbate the suspicions of states as to the intentions and capabilities of others in an environment that appears to be becoming rapidly militarized.

UN Photo: Rick Bajornas

Brazilian President Dilma Rousseff at the UN General Assembly on Sept. 24.

Paul Meyer

Published: Wednesday, 10/23/2013 12:00 am EDT

The implications for international co-operation on cyber security from the revelations of Edward Snowden, the former National Security Agency contractor, are just becoming apparent. But to say that they complicate matters would be an understatement.

The international community's efforts to develop some global norms for responsible state behavior in cyberspace are in their infancy, but there is no question that the disclosure of extensive networks of cyber surveillance abroad have cast a pall on early attempts by states at the multilateral level to promote co-operative action.

The Internet and cyberspace more broadly are uniquely global assets and the United Nations have been engaged over a decade to try to forge a consensus over some basic principles for state conduct in this special environment. Different aspects of the cyberspace issue are being addressed by various organs and agencies of the UN system, including the International Telecommunications Union and the Human Rights Council.

Within the UN General Assembly it is that body's First Committee that is dealing

with the international security dimension of cyberspace and the information and communication technologies that are employed therein.

To date, the committee's consideration of the international security dimension has been largely confined to the conduct of two studies by a 15-nation member UN Group of Governmental Experts that has yielded consensus reports in 2010 and again in 2013.

These reports acknowledge the risk posed to national security interests of the use of offensive cyber operations and call for the development of "norms, rules and principles of responsible behavior" to govern state action.

In particular the reports recommend the adoption of confidence-building measures for reducing the risk of cyber conflict. The emphasis on confidence-building is well founded as there is a growing level of mistrust amongst states as countries move unilaterally to develop significant capabilities for cyber operations (offensive as well as defensive) in the military and intelligence realms.

A recent study by the UN's Institute for Disarmament Research indicated that as of August 2012, 114 states had national cyber security programs and 47 of these designated some role within these programs to the armed forces. Obviously, the Snowden revelations have only served to exacerbate the suspicions of states as to the intentions and capabilities of others in an environment that appears to be becoming rapidly militarized.

The first major pushback to this trend in the UN context has come on the part of Brazil. Stung by revelations of NSA and allied partner cyber intelligence collection activities directed at state leaders and government ministries, Brazil has publicly raised the alarm over such action and suggested it will pursue remedial action.

In her address to the General Assembly last month, Brazil's president, Dilma Rousseff, stated that "information and telecommunication technologies cannot be the new battlefield between states." She went on to say that "time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage, and attacks against systems and infrastructure of other countries."

Brazil's UN ambassador, in his Oct. 9 speech to the First Committee, decried "the activities of a global network of electronic espionage" and said that "such unacceptable practices constitute serious threats to national sovereignty and individual rights, besides being incompatible with the democratic coexistence between friendly countries."

The Brazilian representative gave notice that at this session of the General

Assembly his country will engage in initiatives to improve multilateral norms relating to cyberspace and its governance.

Although it is not yet clear what form Brazil's action will take, it is an influential actor in multilateral diplomacy and can count on considerable support from its Latin American partners, as well as members of the Non-aligned Movement. Brazil's vehement protest and call for improving global norms for state action in cyberspace has also provided other major players with an opening to highlight their own proposals for such a set of norms.

China, which along with Russia, submitted two years ago a draft Code of Conduct for Information Security, was quick to exploit Brazil's public concern. In his speech to the committee, the head of the Chinese delegation declared that "cyberspace is neither an enclave without law nor the jungle where the law of the jungle applies."

Drawing attention to the Sino-Russian proposal, the Chinese ambassador said the text of the code was being revised and that China wished to work with other parties "to achieve an early consensus on the Code of Conduct and jointly build a peaceful, secure, open and co-operative cyberspace."
This last phrase deftly echoes a conclusion of the most recent GGE study and highlights the fact that despite the frequent references by Western officials of the need to develop a global consensus on norms for state behavior in cyberspace, the Sino-Russian Code of Conduct remains to date the only elaborated proposal before the UN General Assembly.

The way ahead for the international community on the daunting challenges posed by state-conducted cyber operations is far from clear. Although Brazil's championing of the cause of global norms was prompted by its being the victim of cyber espionage, this field of state activity has historically eluded international agreement.

More feasible in the near term would be some action to address the international security dimension of the problem with a view to precluding or moderating the conduct of cyber warfare. The UN GGE exercise has yielded a useful, if modest, initial menu of confidence building measures. It would be wise for UN member states to take them up seriously if they wish to reverse the current negative trend and preserve the peaceful character of cyberspace.

Paul Meyer is adjunct professor of international studies and a dialogue fellow at Simon Fraser University, as well as a senior fellow at the Simons Foundation. A former Canadian ambassador for disarmament, he writes on issues of international cyber security policy.