Security Policy Briefing

Can't we all just get along? A view of the United Nations General Assembly hall during Security Council elections this month. *UN Photo: Amanda Voisard*

The Wild West of governments in cyberspace

We need a set of global norms for responsible cyber conduct.

PAUL MEYER

Threats to our cyber security are now ubiquitous and a matter for almost daily media reporting. The magnitude of the breaches can still provoke shock: 80 million accounts compromised at Target, contact data on 76 million clients exfiltrated at JPMorgan. Internet users have grown accustomed to the reality that malevolent actors will exploit cyber vulnerabilities (software or human) to further criminal ends.

More complicated is the question of state-conducted cyber operations that may intrude on the systems of others in the pursuit of national security aims.

To date most of this state activity has involved the murky world of cyber espionage, a realm in which governments were inclined to lick their cyber wounds in private rather than go public with news of their victimization. This attitude has changed as states have escalated their previously confidential diplomatic protests into the public arena.

The sharp response of the Canadian government to alleged Chinese cyber espionage conducted against the National Research Council this summer is a case in point. This response followed American official action this spring against a Chinese military unit in which five individual People's Liberation Army officers were indicted by the Department of Justice for cyber espionage against United States private sector firms. Rather predictably, this prompted a series of official denials by the Chinese authorities. More significantly, it led to the suspension by Beijing of a promising bilateral Sino-US cyber-security consultation that had just gotten underway in 2013.

Talking to each other

Given the levels of mistrust and conflicting security perspectives amongst major powers, initiating and sustaining dialogue processes is a crucial element of promoting international cyber security.

Complicating the prospects for international co-operation is the fact that militaries as well as intelligence agencies are investing heavily into cyber-security capabilities. Although much of this interest relates to defence of their own systems, there is also a focus on offensive operations, actions that could inflict damage or destruction on the computer systems or cyber-enabled operations of an adversary. Given the limited transparency of this military dimension of cyber security, it is difficult to judge what type of action is being conducted and under what doctrinal or policy control.

While the current reality belies the more extreme scenarios of unrestrained cyber warfare, there is a distinct danger that absent some collective efforts at prevention, cyberspace could become yet another battleground for warring states. As the vast majority of the owners and users of the Internet and its supporting infrastructure are civilians, there is a clear public interest in avoiding becoming collateral damage in some future cyber clash.

Ensuring a special status for cyberspace to prohibit destructive cyber activity and agreeing to some rules for state conduct is a logical point of departure. There is a need to assert a global public interest in preserving cyberspace for peaceful purposes. As an expert cited in a recent Economist article exclaimed: "The Internet is the most transformative innovation since Gutenberg and the printing press. Yet we're treating it as a war zone."

Bits and pieces

Establishing a set of global norms for responsible state behaviour in cyberspace would also constitute an important objective. Indeed in May 2011 the Obama administration in the United States issued an International Strategy for Cyberspace that called for an urgent international dialogue to achieve such norms.

Regrettably, there has been scant follow-up to this goal on the part of the US. Its own credibility to lead such an exercise has been undermined by the revelations of former National Security Agency contractor Edward Snowden.

Other states, notably China and Russia, have entered the diplomatic arena with their own version of what should constitute norms for responsible state action in cyber space. In September 2011 at the United Nations General Assembly, these countries introduced a Code of Conduct on Information Security that sets out a series of voluntary measures for states to adopt. Although problematic in several aspects, the purported goals of the code in building a "peaceful, secure, open and co-operative cyberspace" will have general appeal.

Last year a UN Group of Governmental Experts managed to produce a consensus report calling for international co-operation to "reduce risk and enhance security" in cyberspace. The report recommended that states consider adopting confidence-building measures for cyber security, such as information exchange, establishing consultative mechanisms and promoting co-operation amongst cyber-incident response teams.

This represented an initial if modest menu for international co-operation but there has been little pick-up by states. The General Assembly's chief response to the 2013 GGE report was to commission a further study by another GGE with a deadline of 2015 to submit its findings. Studies are relatively easy to undertake. Hammering out a consensus on a set of guiding principles is a more difficult, if far more important, exercise.

There has been more substantive action taken by some regional organizations, notably the Organization for Security and Cooperation in Europe, which actually agreed on a set of cyber-security confidence-building measures in December 2013. The degree of state implementation of these measures is not clear, however and the deterioration of East-West relations in the wake of the Ukraine crisis is not conducive to building confidence on the cyber-security file or any other.

Other regional organizations such as the Organization of American States, ASEAN Regional Forum and the African Union are also addressing cyber security although the emphasis has been on fighting cyber criminals rather than moderating inter-state behaviour.

The pace of multilateral action on cyber security has been slow overall and military developments have outstripped diplomatic ones. The stakeholders of cyberspace can ill afford having their operations disrupted by irresponsible action by agents of the state. The international community cannot rely indefinitely on state self-restraint in the cyber sphere.

We need to initiate a more purposeful, multilateral process to establish some key norms for responsible state conduct in the vital, if fragile environment of cyberspace. Canada can, and should, play a role, in concert with like-minded states and civil society actors, in getting such a diplomatic enterprise underway.

Paul Meyer is adjunct professor of international studies and fellow in international security at Simon Fraser University and a senior fellow with the Simons Foundation.
editor@embassynews.ca