COUNCIL on FOREIGN RELATIONS

International Institutions and Global Governance Program

POLICY INNOVATION MEMORANDUM NO. 2

Date: Monday, November 14, 2011

From: Adam Segal

Re: Cyberspace Governance: The Next Step

After years of dismissing the utility of international negotiations on cyberspace, U.S. officials now say that they will participate in talks to develop rules for the virtual world. But which norms should be pursued first and through which venues? As a start, the United States should issue two "cyber declaratory statements," one about the thresholds of attacks that constitute an act of war and a second that promotes "digital safe havens"—civilian targets that the United States will consider off-limits when it conducts offensive operations. These substantive statements should emerge from a process of informal multilateralism rather than formal negotiations. Washington should engage allies and close partners such as India first and then reach out to other powers such as China and Russia with the goal that they also issue similar statements. Washington should also reach out to the private corporations that operate the Internet and nongovernmental organizations responsible for its maintenance and security.

Declaratory statements play an important role in the definition, diffusion, and adoption of international norms. The discussions that precede the statements encourage actors to identify desirable and realistically attainable norms; the statements themselves set the behaviors that states will be held to. They are also likely to increase strategic stability. Explicit statements give potential attackers a more concrete picture of what type of attacks the United States will respond to and how, making signaling easier and improving stability.

THE PROBLEM

Increased U.S. receptivity to international negotiations reflects a growing sense that domestic efforts to secure cyberspace are inadequate and that the United States has hurt itself by sitting on the sidelines. There is real fear that a cyberattack—the use of computer power to attack computer, communication, transportation, and energy networks—could disrupt the economy, destroy critical infrastructure, or degrade military capabilities. The Internet was originally designed for the use and convenience of a small group of researchers in the United States; security was an afterthought. Now the network is global and there has been a proliferation of devices from laptops to smartphones connecting to it. No one agency, either national or multilateral, exerts authority over all parts of the Web.

As the United States has focused on domestic efforts to make cyberspace more secure—appointing a cyber coordinator, standing up Cyber Command, and deploying Einstein 2, an intrusion detection system—other states have challenged the U.S. conception of the web as a global commons open to commerce and the free exchange of information. Moreover, the United States' refusal to enter into negotiations reinforced the sense that it intended to dominate cyberspace and limit the ability of other countries to maneuver in this new domain.

The Obama administration's May 2009 Cyberspace Policy Review revealed a shift in U.S. attitudes. "International norms are critical to establishing a secure and thriving digital infrastructure," the report concluded. In December 2009 the United States agreed to talk with Russia and a United Nations arms control committee about Internet security.

International cooperation is necessary, but some fundamental characteristics of cyberspace make traditional arms control agreements unlikely. The technologies used in most attacks are commercial and widely available. Attacks can be masked and routed across several networks, obscuring whether they are the work of independently operating "patriotic hackers," criminal groups, an official security agency, bored teenagers, or some combination of all four. This problem of attribution undermines verification; signatories to any agreement would have little confidence they could identify violators.

Moreover, there is no consensus about what constitutes a cyberattack. The United States talks primarily about defending critical infrastructure like the power grid or financial systems; China, Russia, and others worry about these vulnerabilities but also see the free flow of information as a threat to domestic stability. As a result, in any negotiations, Beijing and Moscow are likely to demand that the United States limit its support for "digital activists" in return for China and Russia controlling "patriotic hackers," a requirement Washington is unlikely to meet.

THE RULES OF CYBERSPACE

While a more formal agreement may never be reachable, the United States has a clear interest in defining the rules of interstate behavior in cyberspace. It has a particular interest in identifying the point at which a cyberattack becomes the equivalent of an "armed attack" in international law as well as in defining what constitutes a legitimate target of cyberattack. In the physical world, for example, states are expected to abide by the principle of distinction which requires attacks only be made on legitimate military targets and permits attacks on civilian targets only when "demanded by the necessities of war." This norm was developed through several centuries of war and formalized after World War II in the Geneva Protocols.

At this point, most countries would accept that a cyberattack with "kinetic effects" equivalent to those of a conventional armed attack should be treated in the same manner, allowing for individual and collective self-defense as well as cyber and kinetic responses. But what about attacks below this threshold that nonetheless threaten critical interests, say, by destroying public data or disrupting financial markets? After consulting with its allies and friends, the United States should issue a public "cyber declaratory statement" that reserves the right to respond either through a conventional or computer network attack, but leaves some room for maneuver. Attacks on data and financial markets could both be covered by this statement as long as the consequences of an attack resulted in real suffering, not simply inconvenience.

The United States will not renounce the development and use of offensive weapons, but it should still work to develop "digital safe havens" and then in a separate initiative declare these targets off limits. Again, there is likely to be relatively easy consensus around some areas—hospitals and medical data—and much less agreement around others such as financial systems, power grids, and Internet infrastructure.

The United States should also develop methods to mark its digital safe havens. It may have to separate its own network and data systems—data, for example, from the Department of Health and Human Services and the Pentagon should not sit on the same servers. U.S. policy makers should also work with companies and NGOs to address what are likely to be significant technical challenges in disentangling protected and non-protected spaces.

BUILDING INTERNATIONAL SUPPORT

Since communication networks are global and primarily in private hands, an informal multilateralism is a more appropriate approach than a more formal multilateralism. U.S. officials should continue to show flexibility about venue, engaging through bilateral and multilateral meetings such as the United Nations, the G20, and regional groupings. There have been several moves to limit the role of nongovernmental groups in Internet governance—most recently in a December 2010 decision to involve only member states and exclude the Internet Governance Caucus and other organizations from a UN working group. By insisting on their participation in the relevant forum, the United States can continue to strengthen the authority of these groups.

In the case of thresholds and digital safe havens, the United States should conduct discussions with close allies, friends, private companies, and NGOs over a twelve-to-eighteen month period. The discussions about thresholds are particularly important for the United States to have with its allies; the large scale distributed denial of service attacks on Estonia in 2007 raised the question of whether the country should, or could, have invoked Article 5 of the NATO charter, in which members agree that an "armed attack against one or more of them . . . shall be considered an attack against them all." At the time and as is still the case today, NATO and international law lacked an accepted definition of what constitutes a cyberattack. These discussions should then be expanded to include other partners such as India and then to potential adversaries. After all of these consultations, the United States should issue substantive statements about thresholds and response. Although these statements will be unilateral, the goal of the consultative process should be to spur others to issue similar commitments.

This decentralized strategy is particularly important after Stuxnet, the malware that appears to target the Iranian nuclear program. It is now widely assumed that the United States, along with Israel, was behind the code. As a result, many countries will remain skeptical about Washington's intentions. Rules that appear to be the work of the United States alone will have little chance of gaining international support. But building a coalition of states who will gain from and are willing to push for new rules may give these norms greater legitimacy.

There has been in the United States' international engagement, however, a tendency to substitute process for strategy. While the decentralized approach to cyberconflict is the right one, it does not help in identifying strategic goals. The White House will have to become actively involved in order to push the process forward. The National Security Council's Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC) subcommittee on international cyberspace policy efforts should drive action, not just coordinate and share information about what other agencies are doing.

An informal multilateralism is best suited to cyberspace, and by focusing on some of the norms of interstate cyberconflict, and on thresholds and legitimate targets in particular, the United States will be better able to begin shaping international norms.

Adam Segal is Ira A. Lipman senior fellow for counterterrorism and national security studies at the Council on Foreign Relations.

This publication is part of CFR's International Institutions and Global Governance program and has been made possible by the generous support of the Robina Foundation.

The Council on Foreign Relations (CFR) is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries.

The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained in its publications are the sole responsibility of the author or authors.

Policy Innovation Memoranda target critical global problems where new, creative thinking is needed. Written for policymakers and opinion leaders, the memos aim to shape the foreign policy debate through rigorous analysis and specific recommendations.

The International Institutions and Global Governance program aims to identify the institutional requirements for effective multilateral cooperation in the twenty-first century.

For further information about CFR or this paper, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10065, or call Communications at 212.434.9888. Visit CFR's website, www.cfr.org.