Confidence Building Measures in Cyberspace
Presentation to the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States
James A. Lewis, Center for Strategic and International Studies
February 26, 2016

I would like to thank the organizers of this conference for inviting me to speak on one of the most important problems we face for growth and security. The OAS has been a leader in cybersecurity and it has a real opportunity to make further progress.

In the last five years, a robust international discussion on cybersecurity has developed as nations respond to disturbing trends that threaten stability and security. The international cybersecurity agenda is focused on developing norms for responsible state behavior, capacity building, the application of international law to cyberspace, and confidence building measures. Drawing on this dialogue, we can identify four general principles that guide the international discussion of cybersecurity:

- First, the central importance of national sovereignty as the basis for State responsibility in cyberspace. National sovereignty firmly embeds cybersecurity in the existing framework of state relations under the Charter of the United Nations.

- Second, the applicability of existing international commitments and law to cyberspace.

- Third, acceptance by states of their responsibility for actions in cyberspace emanating from their territory.

- Last, the need for a commitment by states to cooperate with other nations and assist them in the event of a crisis.

This last point is crucial for our discussion today. Calling this confidence building measures is misleading in some ways for what we want to talk about. It sounds like another relic of the Cold War, something from arms control negotiations. A person could reasonably say, my country does not face the threat of war, we have no enemies, so why do I need arms control or confidence building measures.

This is where the connotations of the term confidence building measures are unhelpful. There are of course regions where arms control measures are needed to deal with the potential for military conflict, but the Americas, fortunately, are not one of them. It is more helpful to think of our topic as building areas of common understandings and practical cooperation among nations, including preparations for crisis management. To understand how confidence building measures are essential in this hemisphere, we need to move beyond the context of traditional disarmament and arms control and look at broader issue of public safety.

Some might also say, my country does not face great risk or potential crises in cyberspace, so why do I need confidence building measures. This is a very positive, optimistic, attitude, perhaps too positive and optimistic. Our economic life is now shaped by the internet, critical services are increasingly delivered over the internet, the interconnections among companies and countries grow more robust every day, and the skills and tools needed to disrupt these beneficial activities are now widely available. You do not need a war for a cyber crisis. The whole idea of a crisis is that it is unexpected, it comes upon you suddenly, and that your daily routines and procedures will be inadequate to deal with it.

This is why cyber confidence building measures are essential.

Bear in mind that any cyber crisis will most likely be transnational, originating from outside your country and perhaps having consequences that affect several neighbouring countries simultaneously. Cybercrime is transnational. Cybercrime is endemic. It costs the hemisphere tens of billions of dollars every year. This creates risks for financial stability, especially since banks are a primary target for cybercrime. We do not want to overstate risk, but we also do not want to ignore it. No country has perfect cyber defenses and no country can say this will never happen to me. There is risk in cyberspace, and few governments would wish to be found unprepared if a crisis should occur.

Cooperation among countries is absolutely essential for dealing with such cyber crises. Effective cooperation, as you know, does not occur spontaneously, even when there is the best will in world and complete amity. So the measures we are talking about are how to build a network of support and cooperation in the hemisphere so countries can be prepared for any eventuality.

The OAS's already has significant experience with confidence building measures. The Committee on Hemispheric Security released a "Consolidated List of Confidence and Security Building Measures" that includes the voluntary exchanges of information on organization and structure, of government cyber entities, the exchange of policy and doctrine papers, and the establishment of national points of contact regarding critical infrastructure protection and the exchange of research between member states. This is a good precedent, but we now need specific measures designed for cybersecurity

The OAS should extend its work on confidence building measures to cover cyber security issues. It is time to think about a formal approach and agreement on specific measures to build collaborative networks, strengthen cooperation on critical infrastructure protection and share information on best practices and policies. Specific steps that should be considered include:

- The identification of points of contact at policy and technical levels and the creation of a directory of national cybersecurity contacts. This could include the development of focal points for the exchange of information on cybersecurity and for the provision of assistance in investigations;

- The development of permanent consultative mechanisms. This should include permanent processes and points of contact for communication at the senior policymaker level. In a real cyber incident, senior policymakers and heads of state would be directly involved in decision making, and there is a need for contacts who can facilitate communication at senior levels

- The sharing among members of national views and information on cyber threats and best practices for responding to them, including processes to allow for information exchange on vulnerabilities and attacks.

- The exchange of national views on critical infrastructure protection, including information on national laws and policies for critical infrastructure protection. These national views policies and laws for cybersecurity could be organized into a central repository open to all member and managed by the OAS;

- The creation of exchange programs for cybersecurity and law enforcement personnel, along with programs for exchanges between research and academic institutions.

- The OAS could host regular exercises to strengthen regional cooperation in cybersecurity;

- There should be formal agreement to respond to requests from other States in investigating and mitigating cybercrime or malicious cyber activity.

One issue that always comes up in discussions of confidence building measure is whether they should be voluntary or not. In the UN and in the OSCE, confidence building measures are voluntary. This is appropriate for these groups, since they are marked by tension and even conflict among their members. Conflict and distrust create a preference for voluntary measures.

But this is not the case, fortunately, in the western hemisphere. That means the OAS should go beyond a voluntary approach. The challenge for the OAS is therefore to define and adopt binding commitments among members to prepare them to better manage cyber risk and crisis. It is an ambitious step, but action by the OAS could set the standard for the rest of the world and make the hemisphere a safer place.

The OAS plays a prominent role in international cooperation on cyber security. Its work on capacity building is a model for other nations. Its efforts to facilitate the development of national capabilities has made the Americas a global leader. It should now turn its attention to cybersecurity confidence building measures. Cybersecurity depends on cooperative relations among states. No nation can succeed by itself. It takes a network to defend a network - a network, not of computers, but of among people, agencies, and governments, and a network created by formal agreement.