International Law as a Framework for Peace and Security in Cyberspace

A presentation at the EastWest Institute 7th Worldwide Security Conference
Special Consultation "International Pathways to Cybersecurity"
February 17, 2010

by

Stein Schjolberg
Chief Judge
Moss tingrett Court
Norway
steins@mosstingrett.no
stein.schjolberg@cybercrimelaw.net
www.cybercrimelaw.net

Introduction

The rapid growth of cyberspace has created new opportunities for criminals in perpetrating crime on a global level. These cyberthreats are global problems and they need a global solution, involving all stakeholders. International Law should be the framework for peace and security in cyberspace.

I have four topics I shall introduce to you for our discussions:

1. A Global Convention or Protocol on Cybersecurity and Cybercrime
2. Regional Organizations Forum
3. The International Criminal Court
4. The International Law Commission

1. A Global Convention or Protocol on Cybersecurity and Cybercrime

In order to reach for a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, a Convention or a Protocol at the United Nations level should be established that includes solutions aimed at addressing the global challenges. Crimes against peace and security of cyberspace should be protected under international law. Serious crimes in cyberspace, such as massive and coordinated cyber attacks against the critical information infrastructures, should be recognized under international law, whether or not they are punishable under national law.

A proposal for a global Convention or a Protocol on the United Nations level on cybersecurity and cybercrime may be based on a potential for consensus.

As a follow-up of the High Level Experts Group (HLEG) output I presented a paper " A Global Protocol on Cybersecurity and Cybercrime" at the Internet Governance Forum (IGF) in Sharm El Sheikh, Egypt, in November 2009.

With regard to the development of a model cybercrime legislation, this proposal for a Protocol is based on a kind of "Council of Europe Cybercrime Convention light model" with some additional provisions due to the development after 2001.

2. Regional organizations forum

The individual countries in each region around the world are members of the United Nations. In addition, most of the countries are also members of regional organizations within their region. But there is no "umbrella" organization or institution only for the regional organizations.

Another recommendation from the HLEG was that a global conference for international or regional organizations and relevant private industry should be established.

With regard to cybersecurity and cybercrime, the purpose for such a forum would be to discuss, exchange information and approach a common understanding or coordination on principles and standards for the global combat against cyberthreats. That includes massive and coordinated cyber attacks against countries critical information infrastructure, and against terrorist use of Internet. The regional organizations may then be able to assist and make guidelines for their member countries within the regional traditions.

Several regional organizations have been identified, and at least 12 organizations are of relevance for reaching a common understanding and coordination on principles and standards for the global combat against cybercrime.

The strategy for solutions may unite the existing regional initiatives, and bring the organizations together with the goal of proposing global solutions.

3. The International Criminal Court

The International Criminal Court (ICC) is the first ever permanent, treaty based, fully independent, international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished whether or not they are punishable under national law.

The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute, is unwilling or unable to prosecute. These States are obliged to cooperate fully in the investigation and prosecution.

Article 5 limits the jurisdiction to the most serious crimes of concern to the international community as a whole.
In the final diplomatic conference in Rome in 1998,[1] other serious crimes such as terrorism was discussed, but the conference regretted that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of concern to the international community, and recommended that a review conference consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court.

Serious cybercrime, such as massive and coordinated cyber attacks against critical information infrastructure and cyberterrorism, may be serious crimes of concern to the international community. Such crimes should also be included in the Statute and be a part of international law and prosecuted at the International Criminal Court, whether or not they are punishable under national law.

The review conference is held in Kampala, Uganda, in April and May this year.

4. The International Law Commission

I have on January 29, 2010, sent the following letter to the United Nations International Law Commission titled: **"A United Nations Convention or Protocol on Cybersecurity and Cybercrime."**

I will read to you the main parts of this letter:

"In order to reach for a global agreement on cybersecurity and cybercrime among countries at all stages of economic development, the International Law Commission should consider a draft code of a Convention or a Protocol. Peace and security of cyberspace should be a part of the progressive development of international law.

It is now in my opinion, necessary to make the International Law Commission aware of the need for a global response to the urgent cyberthreats and cyber attacks. These are new developments in international law and pressing concerns of the international community as a whole.
……

In addition, the progressive developments of cyberthreats and transnational cyber attacks against sovereign States, such as massive and coordinated attacks against critical information infrastructures, will necessitate an urgent response for a global legal framework.

…….
I recommend that the Commission due to the urgency of the global challenges establish a working group to handle this topic. This group may undertake preliminary work or help to define the scope and direction."

Thank you for your attention.

---

[1] Final Act of the United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court, Rome July 17, 1998 (U.N. Doc. A/CONF.183/10)