WISIS Forum 2010
10-14 May 2010 Geneva

High-Level Debate on Cybersecurity and Cyberspace

Need for a United Nations Cyberspace Treaty

Prof. Solange Ghernaouti-Hélie
University of Lausanne - Switzerland
12 May 2010

Summary

As already presented by Judge Stein Schjolberg, HLEG Chairman, at IGF 2009, and based on the document « A Global Protocol on cybersecurity and cybercrime: an initiative for peace and security in cyberspace » – Cybercrimedata – 2009, this speech aims to reinforce the idea that the international community needs to set up a United Nations Cyberspace treaty.
Nowadays, there is a real and urgent need for an international agreement, for a coherent and global approach to deal with cybersecurity and cybercrime issues. Organisations, businesses and states face significant risks in relation to the inappropriate disclosure, misappropriation and destruction of data and information and such incidents, when viewed at a macroscopic level, can be viewed as posing a potential threat not just to the competitiveness or reputation of a business but also at a national level to public safety, national security or democracy itself.

These issues cannot be addressed effectively on a purely local level. In the same way as the Kyoto Protocol is an international agreement linked to the United Nations Framework Convention on Climate Change, a Global Protocol on Cybersecurity and Cybercrime should be seen as a truly global approach to reducing risks and threats in cyberspace. It should provide the essential architecture to set up effective national and international measures to combat cybercrime and terrorist uses or misuses of the Internet, and include the clear definition of acceptable and unacceptable behaviours, of the reality and severity of risks, and of the frameworks necessary for control.

A Global Protocol will contribute to:

- Better understanding of all aspects of cybersecurity;
- Facilitating the development and deployment of measures that can help to increase resilience to the impacts of cyberthreats and increase the effectiveness of international cooperation;
- Defining an appropriate cybersecurity culture and developing efficient measures for raising awareness among the population;
- Assisting developed and less developed countries to develop an inclusive information society by reducing the security digital divide;
- Developing capacities to enforce and enhance peace and security in cyberspace and in real life.

Nowadays there is only one world, the one we live in that is dominated by the intensive use of ICT devices, infrastructures and services. Nowadays citizens, organisations and states are dependent on ICT infrastructures for everything they need. It is a complex dependency with multiple interdependencies involving several types of actors distributed all over the world.

But the digital world is fragile. Organisational, managerial, legal and technical vulnerabilities exist at several levels.

Moreover, some business models, such as those relying upon personal data, consumer profiles and the commercialization of behaviour, can constitute at the same time a potential threat for data protection and a source of profits for licit or illicit entities that know how to exploit these models.

Nothing in Cyberspace is free of charge and for a so-called "free service" users pay in kind, by giving personal data. Information given by the end-users, collected with or without their knowledge or consent, could easily be misused. In any case, personal data should not be considered as vulgar merchandize!

For public or private organisations, the risks of the inappropriate disclosure or misuse of information, of the unfair appropriation, exploitation or destruction of resources, including massive and coordinated attacks against critical information infrastructures, are important. These risks should be considered at a macroscopic level, as a potential threat to organisations' competitiveness or reputation, or as potential threats to state sovereignty, which could even, for example, impact public safety, national security or democracy.

Cyberwarfare, information warfare, defence or offensive computer warfare, whichever name is used, is related to issues of economic and/or military conflict, and raises, among others, the question of individual, national, global and international responsibilities, the question of international collaboration and the question of private and public partnerships.

At the same time reliable and complete statistics related to cyberattacks or cybercrime are rare. That could lead to over- or underestimating the real needs for cybersecurity. All of this contributes to generating insecurity and fear.

But if we believe that cyberspace can be increasingly considered as a global economic and military battleground, where all kind of cyberconflicts can arise, reflecting all kind of political and economic competition, it is time to frame what is acceptable or not on a common and well approved basis and to set up an effective international instrument for controlling it.

Nevertheless, because cyberspace is the fifth common space, after land, sea, air and outer space, in the same way as these other domains, it requires coordination, cooperation and legal measures among all nations to function smoothly. And when it comes to constructing an effective system of deterrence against cyber threats, the best means to that end would be the construction and utilization of a global United Nations framework. The ultimate goal would be to establish a Cyberspace Treaty, which would spell out what constitutes acceptable and unacceptable behaviour.

As already presented by Judge Stein Schjolberg, HLEG Chairman, during the Internet Governance Forum last November in Sharm Al Sheik (1) and during the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, in Salvador in April (2), I would like to reinforce the idea that the international community needs to set up a United Nations Cyberspace Treaty. Because regional or bilateral agreements will not be enough, a broader view of international law is needed.

An international agreement should facilitate the development of a global strategy to deter cyber threats from any direction.

The process of working towards a United Nations Cyberspace Treaty should help develop a common understanding of all aspects of cybersecurity among countries at various stages of economic development.

All stakeholders need to come to a common understanding on what constitutes cyber crime, cyber terrorism and other forms of cyber threats. That is a prerequisite for developing national and international solutions that harmonize cybersecurity measures. These kinds of common understandings will also help reduce the divide between developed and developing country perceptions of cybersecurity.

Because criminal conduct in cyberspace is global by nature it requires global harmonization of cyber crime legislation, it requires effective international justice and police cooperation and a real will to do this.

A Cyberspace Treaty on the United Nations level should establish serious crimes against peace and security perpetrated through the Internet as crimes under international law, whether or not they were punishable under national law.

It is proposed that the United Nations International Law Commission should consider drafting a Cyberspace Treaty – a convention or a protocol, as mentioned in the document « A Cyberspace Treaty – a United Nations convention or protocol on cybersecurity and cybercrime », copies of which are available in this room.

National and international strategies should exist not only to respond to cyberattacks, thus defining reactive measures to be undertaken after an attack, but should also consider proactive measures in order to avoid security breaches and to prevent unsolicited incidents. This could be done, for example through developing an appropriate cybersecurity culture, by reducing vulnerabilities that could be exploited to attack systems; in fact, by taking into consideration in a holistic way all those factors that can lead to deviant behaviours, crises, acts of retaliation or crimes, and by enhancing complementary and coherent measures in a holistic way.

In fact, as has already been outlined well in ITU – GCA HLEG Global strategic report (3), relevant measures are related to legal, technical and procedural dimensions that rely upon organizational structures, on effective capacities and on international cooperation. A Global Protocol on Cybersecurity and Cyber Crime can be seen as a follow-up to the HLEG reports. It constitutes a step forward within the ITU's Global Cybersecurity Agenda initiative that encourages countries to develop national cybersecurity program and to promote international cooperation. A "Global Protocol" should commit them to do so. It should provide the essential architecture to set up effective national and international measures to fight against cybercrime or misuses of the Internet and constitute a reference basis for any future international agreement on cybersecurity issues.

A Global Protocol on Cybersecurity and Cyber Crime should answer a strong political and economic willingness and a real commitment of each involved actor to enforce the robustness and resilience of reliable ICT infrastructures for the benefit of a durable and inclusive information society.

To conclude, a common international and well-accepted agreement could be an incentive to reduce vulnerabilities, threats and risks to an acceptable level.

References

(1) « A global protocol on cybersecurity and Cybercrime: An initiative for peace and security in cyberspace ». Stein Schjolberg & S. Ghernaouti-Hélie - Cybercrime data, Oslo 2009.
www.cybercrimelaw.net/

(2) « A Cyberspace treaty – a United Nations convention or protocol on cybersecurity and cybercrime » Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador - April 2010
www.un.org/en/conf/crimecongress2010/
www.cybercrimelaw.net/

(3) ITU Global Cybersecurity Agenda, Hight-Level Experts Group Global Strategic Report
www.itu.int/osg/csd/cybersecurity/gca/index.html

Short biography: Professor Solange Ghernaouti–Hélie, President of the Social Commission, President of the Equal Opportunities Commission - University of Lausanne (Faculty of Business and Economics). She is active as an ICT security expert, possessing extensive experience of security governance, security strategies and the evaluation of security policies. She was a member of the High Level Expert Group within the ITU Global Cybersecurity Agenda and co-leader of the working groups on "Capacity Building" and "Organizational Structures". Professor Ghernaouti-Hélie is the author of more than twenty books including the ITU reference guide "Cybersecurity for developing countries" (an enlarged 2009 edition is available on the ITU-D website). She is also the best-selling author of the book "*La cybercriminalité: le visible et l'invisible*" (Le savoir Suisse, 2009).

Contact: sgh@unil.ch - *Web site* : www.hec.unil.ch/sgh/