
Developments in the field of information and telecommunications in the context of international security

(Prepared for the Record)

There is now broad recognition among many States, including the United States, that existing international law serves as the appropriate framework applicable to activity in cyberspace in a variety of contexts, including in connection with hostilities. This area of international law involves two related bodies of law. The first one is *jus ad bellum*, which is the framework that addresses the use of force triggering a State’s right of self-defense; and the second one is *jus in bello*, which is the body of law governing the conduct of hostilities in the context of an armed conflict and is sometimes called the international law of armed conflict, the law of war, or international humanitarian law.

While some attributes of information technologies are unique, existing principles of international law serve as the appropriate framework in which to identify and analyze the rules and norms of behavior that should govern the use of cyberspace in connection with hostilities. In this vein, much work has been done over the last year in developing a better understanding of the issues related to information and telecommunications in the context of international security, in particular, by the on-going UN Group of Governmental Experts (GGE) on “Developments in the Field of Information and Telecommunications in the Context of International Security.”

The consensus report of the 2010 GGE included two very important recommendations: further dialogue to discuss norms to reduce collective risk and protect critical national and international infrastructure, and the development of confidence-building measures to reduce the risk of misperception.

The 2012-2013 GGE is taking up this important work where the 2010 GGE left off. It is focusing on discussion of a normative framework, confidence-building
measures and support for capacity building, and intends to make recommendations in these areas.

During last year’s session of the UNFC, the introduction of a draft Code of Conduct for Information Security presented an alternative view that seeks to establish international justification for government control over Internet resources. At its heart, it calls for multilateral governance of the Internet that would replace the multi-stakeholder approach, where all users have a voice, with top down control and regulation by states. It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights.

In addition, the draft Code appears to propose replacing existing international law that governs uses of force and relations among states in armed conflict with new, unclear, and ill-defined rules and concepts. Indeed, one of the primary sponsors of the draft Code has stated repeatedly that long-standing provisions of international law, including elements of jus ad bellum and jus in bello that would provide a legal framework for the way that states could use force in cyberspace, have no applicability. This position is not justified in international law and risks creating instability by wrongly suggesting that the internet is an ungoverned space to which existing law does not apply.

This draft Code advocates voluntary commitments not to proliferate information technology for offensive purposes, which ignores the fact that this technology is a quintessential dual-use technology. It purports to promote cooperation on cybercrime, but the chief sponsors of the draft Code disavow the only international cybercrime instrument in existence and they seem to be reticent to cooperate effectively on cybercrime matters. Moreover, their definition of criminal activities covers the gamut of all views that may not comport with the prevailing view of the government in power.

While a key provision of the draft purports to ensure ICT supply chain security, other provisions seem to acknowledge a lack of respect for intellectual property rights when they claim that states use their technology and critical infrastructure for advantage and in their call for an equitable division of relevant resources.

Proposals along these lines would discourage the international trade in and the development of information and communications technology (ICT) products and services, which have made the Internet what it is today. We fear that these
proposals would also make it easier for governments to suppress free speech, for example through government control over content for the purpose of political domination.

States do not have a monopoly on the ability to innovate, develop technical capacity, or grasp economic opportunities. These activities should be carried out in an appropriate and responsible manner with the participation of all stakeholders. As such, it is unrealistic and undesirable for States to be given the dominant role on Internet operation and development.

The United States favors international engagement to develop a consensus on appropriate cyberspace behavior, based on existing principles of international law, and we cannot support approaches proposed in the draft Code of Conduct for Information Security that would only legitimize repressive state practices.

It is the view of the United States that transparency, confidence-building, and stability measures should be developed as a voluntary, cooperative effort whose ultimate objective is to enhance international stability and thereby reduce the risk of conflict in cyberspace. Many States could contribute to this goal.

States must unite in the common goal of preserving and enhancing the benefits of information technologies by assuring their security and integrity, while also maintaining an environment that promotes efficiency, innovation, economic prosperity, free trade, and respect for human rights.