



OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role

**Opening Session
Vienna, May 9, 2011**

**Remarks by Christopher M. Painter
U.S. Coordinator for Cyberspace Issues
U.S. Department of State**

Challenges to national and international cyber security increasingly compel Member States to face the daunting challenge of managing a highly varied and complex threat environment. In a variety of international and regional forums including the United Nations, all States have affirmed the necessity of performing domestic due diligence in a variety of areas related to cyber crime and creating a culture of cybersecurity. We have all endorsed State obligations to combat terrorist facilitation and planning, whether or not they take place in cyberspace. Many States have also endorsed the need for transnational cooperation in cyber crime and sharing best practices.

Over the last decade, extensive efforts to combat the threat of cyber crime have been conducted internationally. Extensive international cooperation in the investigation and prosecution of cyber crime has been accomplished through the Convention on Cybercrime, as well as through bilateral efforts between affected countries and continues to be the most effective way of dealing with the threat to information networks by criminal activity.

As this conference signifies, other areas of transnational cybersecurity concern, such as the political-military arena, are only now receiving comparable attention. As we have discussed already, a key challenge we must meet here is how to foster and maintain a system of international cyber stability. By this I mean that we must create incentives for States to coalesce around generally agreed norms of acceptable behavior in cyberspace, by finding economic and other social benefit in a predictable, secure environment, and with a stake in actively opposing those who would destabilize it.

Norms alone will not be sufficient in establishing and maintaining a stable environment. The unique attributes of information technology which render intentions and

capabilities essentially unknowable and even prevent high confidence attribution of identity to attackers require that we cultivate measures to enhance the predictability of state behavior in cyberspace. Risks of misperception may result from a lack of shared understanding regarding the norms governing State behavior in cyberspace and could affect crisis management and escalation in the event of major cyber events. This situation argues for the elaboration of mutually reinforcing and overlapping measures designed to enhance predictability, increase transparency, build confidence – and thereby, reduce risk that misperceptions may inadvertently lead to unintended conflict. This is no small task. While CBMs have long been a staple of bi- and multilateral risk reduction efforts, measures regarding activities in cyberspace must be designed that take into account and effectively address the thorny problems of lack of attribution, of proxy actors, and inability to assess military capabilities. The United States believes that the OSCE has particular competence in the area of CBMs and transparency measures and would like to see that expertise applied to these novel issues.

To stimulate that activity, the United States can reiterate some of the ideas we offered in the Food for Thought paper that we circulated last year.

Transparency Measures

- Exchanges of national views of international legal norms pertaining to the use of cyberspace ☐ Exchanges of information regarding national organizational structures devoted to cybersecurity and points of contact ☐ Exchanges of “White Papers” describing national military organizations involved in cyberspace activities

Stability and Risk Reduction

- Establishing or upgrading crisis communications links and associated protocols to encompass cyber incidents
- Establish procedures and requirements to permit routine exchange of information between Computer Security Incident Response Teams. These procedures would facilitate information-sharing in the event of a major incident