Thank you, Mr. Chairman.

Our agenda examines some of the most difficult problems of our time, and the challenges we face in the area of cybersecurity rightly take their place among them. Information technology (IT) has become crucial to the development of all States, making an important contribution to the essential functions of daily life, to commerce and the provision of goods and services, to research and innovation. Information technology is promoting economic development by opening access to new markets, facilitating the organizing and delivery of humanitarian assistance and is increasingly supporting the functioning of critical civil, public safety and national security infrastructures. It has also become a key tool in ensuring the free flow of information between individuals, organizations and governments in ways that few of us could have foreseen only a few years ago. It is our expectation that as traditional telecommunications and Internet networks converge, global dependency on information technology will only increase.

We are acutely aware that as our dependency has grown, so too have the risks to our security associated with that dependency. A wide range of primarily man-made activities threaten the reliable functioning of national and global networks and the integrity of the information that travels over them. These threats are increasing in sophistication and
gravity and have many sources. The vast majority are rooted in criminal behavior and target individuals, businesses, and governments alike. Some threats are State-sponsored and involve the extension of traditional forms of state-on-state activities and conflict into cyberspace. Whatever the source of the cyber threat, defending against it is a key priority of President Obama who has stated that we need a strategy for cybersecurity designed to:

"...bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure. ...Only by working with international partners can the United States best address these challenges, enhance cybersecurity, and reap the full benefits of the digital age."

As a consequence, he has directed the implementation of a comprehensive domestic strategy to address our cyber vulnerabilities. He has done so, however, with the clear recognition that whatever national steps the United States may take domestically to defend its information networks, our global interdependence means they are unlikely to be fully successful without effective international collaboration.

It has long been our view that cybersecurity efforts of each nation must proceed on two levels: at the national level, where every government must make cybersecurity a domestic priority, and at the international level, where each nation must collaborate on common, or at least complementary, approaches to transnational cybersecurity issues. Drawing on our own experience, the United States has offered five cybersecurity awareness-raising resolutions in the UN General Assembly over the past decade, culminating last year in UNGA Res
64/211 which provides a roadmap for Member States to use to assess the progress of their domestic efforts. We do not underestimate the difficulty of this task for any State and we are still engaged in trying to find the right solutions for ourselves. We understand that all of us differ in experience and technical sophistication in this area as well as the priority we can assign to cybersecurity nationally. Nevertheless, we view national efforts as a prerequisite for effective international ones.

From our vantage point, international collaboration should focus on a variety of cooperative strategies to address the various transnational threats to information networks. We believe we are making some progress in establishing the foundation for better collaboration in a variety of areas. Of importance to this Committee, this past year, a group of fifteen governmental experts began an important discussion on the difficult issue of the appropriate standard of behavior for States with regard to the use of information technology tools in the political-military arena. In the context of the long-standing, Russian-sponsored UNGA First Committee resolution, this Group of Governmental Experts—ably led by the Russian Chairman—was able to identify some key areas of common ground and it emerged with a short but valuable consensus report that points in a fruitful direction for further collaboration.

From the United States vantage point, key among these recommendations was that there should be further dialogue to discuss norms pertaining to State use of information technology in order to reduce collective risk and protect critical national and international infrastructures and; that further steps include consideration of confidence-building, stability and risk-reduction measures to address the implications of State use of information technology, to include exchanges of national views on its use in the context of conflict. I would note that during the course of these discussions the United States took the significant step of affirming formally its view that existing principles of international law, specifically the Law of Armed Conflict, serve as the
appropriate framework within which to identify and analyze the rules and norms of behavior that should govern the use of cyberspace in connection of hostilities just as it governs the use of kinetic force.

The Russian-proposed resolution on "Development in the field of information technology in the context of information security" takes into account the important work of the GGE and proposes continuing discussion of its recommendations. For this reason, the United States will join the Russian Federation by co-sponsoring this resolution.

Thank you, Mr. Chairman.