

AMBASSADOR'S REMARKS FOR  
CYBER SECURITY CONFERENCE ("NATIONAL SECURITY IN THE INFORMATION AGE")  
AZERBAIJAN DIPLOMATIC ACADEMY (ADA) UNIVERSITY  
APRIL 13, 2015 AT 9:30AM

Thank you for your very kind introduction.

Mr.Mammadov, your Excellencies, ladies and gentlemen, good morning. Let me first of all thank the Ministry of Foreign Affairs, the Organization for Security and Cooperation in Europe, the other contributing partners, and ADA for organizing and hosting this important and highly topical event. It is a pleasure to be here with you today.

Over the past 30 years the information revolution has had a tremendous impact on people's lives around the globe – in how we live, in how we do business, and in how our systems and our very economics operate.

But as President Obama said, "It is one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm ... We only have to think of real-life examples -- an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness -- to imagine what a set of systematic cyber attacks might do."

Even on an individual level, cyber security is vital. We have probably all received emails from friends or family members apologizing for the spam sent from their accounts after they were hacked. And we are all familiar with the high profile cases such as the outlandish hacking of Sony Pictures Entertainment by North Korea in November and its release of confidential business and personal information.

Yet, while cyber security is clearly a national security issue, much of our computer networks and critical infrastructure are in the private sector, which means government cannot do what is needed by acting on its own. This wish has to be a shared mission.

At the national level, cyber security policies, effectively planned and implemented, protect critical infrastructure, our economies, and people from those who seek to exploit them for political, military, financial or other illicit gain.

In recent years, the United States has weathered a significant number of attacks on its governmental and private-sector information networks. Officials at the U.S. National Nuclear Security Administration, for example, have reported they are hit with millions of cyber-attacks per day from a “full spectrum” of sources.

I know the United States is not alone in facing this level of threat – just ask my Estonian colleague here who knows all too well what the threats are – and like other governments, private corporations, and even individuals, we are acting to defend cyber systems and critical infrastructure.

Less than two weeks ago, on April 2, President Obama signed an Executive Order to strengthen U.S. government cyber security measures.

This Executive Order provides the U.S. Government with the authority to impose sanctions on individuals or entities who engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health of the United States.

Equally important, President Obama has also sought to bring the private sector and government together to deal with this challenge.

For example, President Obama hosted a White House Summit on Cybersecurity and Consumer Protection this past February, which focused on four principles for confronting cyber threats: 1) cyber security is a shared mission between government and industry; 2) constantly, government and industry should focus on and complement their respective strengths; 3) we need to evolve our defenses, and 4) we must protect people's privacy and civil liberties.

Stronger international cooperation in cyber security is essential. It strengthened cooperation among our governments, businesses, and citizens will help forge stronger economic links, facilitate a growing segment of global commerce, ensure the reliability of electrical utilities and other infrastructure, protect our citizen's personal data and personal safety, and build a more prosperous and secure future.

Azerbaijan is making a real contribution to that more secure future by hosting this conference.

In a number of my initial meetings with Azerbaijani leaders, business people, and private citizens, they have flagged the need for increased economic ties not only between Azerbaijan and the United States, but between Azerbaijan and the rest of the world as well.

Azerbaijan seeks to become a regional hub for information and telecommunications technology, as well as for transportation and globally-needed energy supplies, and the United States strongly, strongly supports these aspirations.

Yet as Azerbaijan becomes a more heavily networked society, its inter-dependencies will increase. And so the security of its increasingly interconnected communications infrastructure will only become more important.

Before I conclude, I would like to note that the U.S. Embassy is very pleased to support this conference by sponsoring two speakers to share their experiences and expertise with you.

Ms. Melissa Hathaway is a senior advisor at the Kennedy School's Belfer Center for Science and International Affairs at Harvard University, and a former cyber security adviser to U.S. Presidents George W. Bush and Barack Obama. Ms. Hathaway will join you via a digital video conference.

The other speaker is Dr. James D. Cannady, a professor in the Graduate School of Computer and Information Sciences at Nova Southeastern University. Dr. Cannady traveled to Baku to be with us for the conference and will be a panelist.

So, in closing, let me thank you for all that you do in this challenging and dynamic field. I look forward to our countries continuing this work together.