**STATEMENT OF EDWARD AMOROSO**
**SENIOR VICE PRESIDENT & CHIEF SECURITY OFFICER**
**AT&T INC.**

**BEFORE:**

**UNITED STATES SENATE**
**COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION**

**HEARING ON IMPROVING CYBERSECURITY**

**MARCH 19, 2009**

Good morning, my name is Edward Amoroso. I currently serve as Senior Vice President and Chief Security Officer of AT&T. I have worked in the area of cyber-security for the past twenty-four years, starting at Bell Labs. My current responsibilities include design and operation of the security systems and processes that protect AT&T's vast domestic and international wired and wireless infrastructure. This infrastructure supports AT&T's voice and data networks, and permits AT&T to provide the Internet access, telephony, video entertainment, data transmission and managed services that AT&T offers to its many millions of customers around the globe.

My educational background includes a Bachelor's degree in physics from Dickinson College, as well as Masters and PhD degrees in computer science, both from the Stevens Institute of Technology, where I have also served as an adjunct professor of computer science for the past twenty years. I am a graduate of the Columbia Business School, and have written four books and many articles on the topic of cyber-security.

On behalf of AT&T, I would like to thank the Committee for this invitation to comment on the cyber-security challenges facing my company, this nation and the rest of the world. My

comments include a professional perspective on how and why cyber-security threats have increased significantly over the past five years, as well as suggestions on how these threats should be addressed.

I believe most citizens equate the issue of cyber-security with viruses that find their way onto computers, or with the stories they hear about so-called "security breaches" resulting from laptops being lost or stolen. These are certainly problems, but from the perspective of protecting the nation's critical infrastructure, these issues are not severe. Cyber-security is more about protecting the infrastructure from intrusion by individuals or forces determined to disrupt the flow of data and the storage of information. Motives might be mere mischief, making a political statement, gaining business advantage, making pecuniary gain, exposing a vulnerability or something more sinister.

In the mid-1990s, attacks on the infrastructure sometimes were clumsy, or so sophisticated as to be admired, but they did not cause lasting damage. But just as computing has advanced and evolved, so too has the frequency and form of attacks. For a time, those determined to intrude (call them hackers for simplicity-sake) were able to take advantage of the fact that most consumers, businesses and government agencies had not done a good job maintaining the security of their operating systems and common applications (such as browsers and email applications) by applying security patches and running system security programs. "Patching" has improved dramatically across the global infrastructure, and anti-malware applications have become common place. Thus, attackers now use "phishing" or "pharming" approaches, whereby an unsuspecting victim is tricked into giving away passwords or personal information, or

allowing malware to be dropped onto machines – even those that are properly patched. Last year the FBI announced that revenues from cyber-crime, for the first time ever, exceeded drug trafficking as the most lucrative illegal global business, estimated at reaping more than $1 trillion annually in illicit profits.

Evolving and more lethal type of cyber-attacks can devastate infrastructure. One form of attack uses "botnets," which work by harnessing the power of unprotected PCs from homes and businesses. Malicious intruders, hackers and even terrorists are getting very good at harnessing the power of PCs and aiming them at unsuspecting victims. It has become so easy and rampant that the risk has grown exponentially. The result is a laser-like cyber-attack on an unsuspecting business or government system. Estonia, for example, was the subject of a botnet attack two years ago, and the results were catastrophic: The entire country was disconnected from the Internet, and the event has come to be known as "WWI" for "Web War I."

For AT&T, cyber-security is the collective set of capabilities, procedures and practices that protect our customers and the services we offer them from the full spectrum of cyber-threats, including botnets. This assures that the information, applications, and services our customers want are secure, accurate, reliable and available wherever and whenever they are desired. Cyber-security is a leading corporate priority, and we are investing significant resources in making our network and our customers more secure. To this end, strong cyber-security is essential to maintaining the integrity and reliability of the network, and well as protecting privacy of personal customer information.

The technology within our network is rapidly evolving to support new applications and services. This year alone, AT&T is investing more than $18 billion in expanding the capabilities of our network and infrastructure to meet the rapid global expansion of advanced information technology and services, and to enhance reliability and security. The size and scope of AT&T's global network, coupled with our industry-leading cyber-security capabilities, gives us a unique perspective into malicious cyber-activity. Our advanced network technology currently transports more than 17 Petabytes a day of IP data traffic, and we expect that to double every 18 months for the foreseeable future. Our network technologies give us the capability to analyze traffic flows to detect malicious cyber-activities, and, in many cases, get very early indicators of attacks before they have the opportunity to become major events. For example, we have implemented the capability within our network to automatically detect and mitigate most Distributed Denial of Service Attacks within our network infrastructure before they affect service to our customers. Indeed, part of the investment I described above is targeted to advancing our attack mitigation capabilities. We doubled, and are now redoubling, our ability to provide global coverage to scrub for denial-of-service attacks. We went from one domestic scrubbing complex to multiple locations across the United States, as well as nodes in Europe and Asia. This gives us the ability to filter out attack traffic as close to the source of the threat as possible.

To address the growing cyber threat to our nation, and in particular the threat of botnets, three actions are recommended. First, our federal procurement process needs to be upgraded to implement sufficient security protections to deal with large-scale cyber-attack. The denial-of-service threat, for example, is largely overlooked in most civilian agency networks. On the other hand, private sector companies like AT&T offer advanced services that can mitigate the threat of

a denial-of-service attacks before they arrive on an agency's doorstep. Without a strategic emphasis to build strong cyber-security protections into the federal requirements development process, however, those protections are unlikely to find their way into systems procurement requirements.

A second recommended action involves international partnership during a cyber-attack. When a botnet is aimed at some critical asset, the servers controlling the attack might be scattered to the farthest reaches of the globe. The local service provider is thus in the best position to take suitable security action. But this requires international cooperation that has been so far inadequate. Such a course would be consistent with the recent recommendations by the National Security Telecommunications Advisory Committee (NSTAC) that international coordination receive prioritized attention. Specifically, NSTAC recommended that the federal government pursue development of international cyber-incident warning and responsible capabilities since network attacks or incidents originating outside of the United States raise increasing concerns about the security and availability of domestic national security and emergency preparedness communications. In many ways, the international paradigm reflects the flaws in the current, domestic security paradigm – international coordination on incident response remains largely ad hoc. The continuing absence of a coordinated, scalable, international structure for response that includes all relevant stakeholders undercuts efforts to develop systemic solutions and responses.

Finally, our government should rethink its own relationship with its network service providers. As attacks become more mobile and network-based, the service provider has the best vantage point to mitigate the threat. Too often, in our work at AT&T, we see government and business

systems designed with the service provider at arms-length. This practice must be discouraged. In fact, agencies that run their own cyber-security operation should be ready to justify such decision. They cannot stop network threats such as botnets on their own.

To this end, we endorse the several NSTAC recommendations that encourage such relationship rethinking. We believe that the public and private sectors can and should create structures for timely and secure sharing of cyber-security threat and response information between government and industry, and between and among critical infrastructures in a trusted, collaborative environment. In partnership with the private sector, the government can and should create a secure and responsive identity management framework to support cyber-based identity processes and applications, thereby ensuring emergency response access to critical infrastructure in support of disaster recovery. In collaboration with industry, the government can and should create a comprehensive incident-response architecture embracing critical infrastructure facilities and core infrastructure services. Perhaps most importantly, the government should collaborate with industry on research and development efforts in pursuit of critical cyber-security capabilities, and in furtherance of interoperable identity management processes between government and the private sector.

To conclude, I am pleased that this Committee is focusing on cyber-security, and looking forward to working with you to develop practical steps to ensure that cyber security does not threaten our nation's present and future well-being.