Statement of Edward Amoroso, Ph.D.

Senior Vice President & Chief Security Officer
AT&T

Hearing: Cybersecurity: Threats to Communications Networks and Private-Sector Responses

United States House of Representatives

Committee on Energy & Commerce
Subcommittee on Communications and Technology

March 7, 2012

Chairman Walden and Ranking Member Eshoo, I would like to thank you and all the members of the Subcommittee for this invitation to address the significant challenges facing communications networks in particular, and the private sector in general, with regard to effectively defending against cyber threats. In this statement, I briefly describe cyber threats and cybersecurity, and discuss generally how federal legislation under consideration in this Congress could be fashioned to both enhance the private sector's cybersecurity practices and facilitate greater coordination between the cybersecurity capabilities of the federal government and the private sector.

My Background

I am Senior Vice President and Chief Security Officer, AT&T, where I have worked in the area of cybersecurity for the past twenty-seven years.[1] With the help of my team, I design and operate the security systems and processes that protect AT&T's domestic and international

[1] I hold a Bachelors degree in Physics from Dickinson College, both a Masters degree and the PhD in Computer Science from Stevens Institute of Technology, and have served as an adjunct professor of computer science at Stevens for the past twenty-three years. I am a graduate of the Columbia Business School, and the author of numerous articles and books on cybersecurity, including "Cyber Attacks: Protecting National Infrastructure" (Butterworth-Heinemann, 2011).

wired and wireless network infrastructure. This network infrastructure is the core asset that permits AT&T to provide an array of advanced communications services to many millions of customers around the world, ranging from the largest global business and government enterprises to small businesses and individual consumers. The technologies provisioned and employed by AT&T and the other communications network providers represented here today are a key part of the national infrastructure – the complex delivery and support systems for the large-scale services that are essential to the commercial security of our nation.

What is cybersecurity, and what are today's cyber threats?

National infrastructure, including the communications infrastructure, have always been vulnerable to direct physical attacks such as cable cuts, asset theft, equipment tampering and even more violent forms of sabotage. As elements of this infrastructure became increasingly reliant on software, computers, networks, and access to the Internet for their control systems, they became correspondingly vulnerable to indirect "cyber" attacks by adversaries[2] intruding these computerized control systems. Cybersecurity is the term we use to describe an entity's ability to protect its critical systems from these intrusions by monitoring its systems in order to detect cyber threats and then engage in "active defenses" to mitigate those threats. In addition, the forensic results of this activity might be usefully shared with others, within appropriate parameters, so that others might leverage the experience and knowledge acquired in order to further protect their infrastructure from intrusion.

The methods and forms of cyber attack threats are continuously evolving, and this dynamism enables such threats to bypass standard preventive measures such as the application of

[2] Sources of cyber threats include (but are not limited to) disgruntled individuals, criminal elements, transnational enterprises, and sophisticated and well-resourced nation states. These sources are motivated by a range of purposes, from mischief to deliberate acts of hostility attempted through sabotage and terrorism.

firewalls and intrusion detection systems strategically placed between the critical system and the Internet at large. One form of evolving cyber attack uses "botnets" – which are run by adversaries who are increasingly adept at harnessing the power of dispersed personal computers and other smart devices attached to the national infrastructure and using them to attack unsuspecting victims. Other cyber threats include worms, viruses, and leaks, which can similarly target national infrastructure through their associated automated controls systems. All of these threats can be employed by adversaries to engage in a range of conduct from Distributed Denial of Service Attacks (DDOS) to Advanced Persistent Threats (APT), which are at present the most sophisticated and pernicious forms of cyber attack.

What needs to be done?

We need to improve the overall cybersecurity posture of the nation by facilitating the widespread and rapid adoption of cyber threat detection and mitigation practices through private sector investment and innovation. Because of the global nature of the threat, we cannot undertake this challenge unilaterally – it is clearly a global issue in all its dimensions. The Administration and the Congress have put forth a variety of ideas and initiatives on how we can begin to tackle this challenge; some are helpful, and some would stifle the innovation and flexibility we need to identify and respond to the ever changing threats. AT&T commends, in particular, the work of the Cyber Security Task Force and the leadership of Congressman Mac Thornberry. The Task Force produced a focused set of recommendations that should be used as the framework for any proposed cyber legislation. Implicit in the Task Force recommendations is the principle that improving our national cyber security posture is a process that will not be solved by simple legislative pronouncements or regulatory dictates. We can, however, begin to establish foundational elements for future progress.

1. <u>Build a Collaborative Active Cyber-Defense Capability</u>.

First and foremost, the United States needs to build a collaborative active cyber-defense capability that builds upon well-established coordination processes that have been developed for assessing cyber threat risks to critical infrastructures and key resources (CIKR). Our experience participating in these processes, as well as in pilot programs such as the Defense Industrial Base (or "DIB") Project, informs our view that more targeted cyber threat information sharing capabilities to support active cyber defense should be the next step in our nations approach to securing its infrastructure.

To this end, the global communications infrastructure is the primary vehicle for delivery of cyber attacks against U.S. interests, yet there is no comprehensive coordination mechanism for rapidly detecting and analyzing emerging threats. Each Tier One communications network operator and service provider monitors its own network to varying degrees, with varying capabilities to mitigate or block attacks. In addition, the multiple government programs which already exist are focused on monitoring traffic to and from multiple government networks – none of which are operationally integrated.

Actionable emerging threat information might be known to the Federal Government, for example, but otherwise unknown to private industry. In the event that a government agency becomes aware of a malicious attack signature that could be deployed into intrusion detection systems to protect industrial, non-government assets, the government should have the confidence that it can be so deployed without further delay or review. A collaborative, active cyber-defense capability to detect, analyze, and mitigate malicious cyber activities in the core networks that make up the Internet itself will enable cyber attacks to be detected and attempts be made to stop them before they reach their target.

This Congress there have been a number of legislative proposals that appear to be an excellent first step toward achieving the end goal of a collaborative active cyber-defense capability by explicitly authorizing cyber threat information sharing between private and public sector participants, as well as the active defenses or countermeasures necessary for entities to engage in so that they can address those threats, either for themselves or on behalf of others. In particular, we note H.R. 3523, the Cyber Intelligence Sharing and Protection Act, introduced by Michigan Congressman Mike Rogers. This proposal has done much to advance the discussion of the appropriate range and scope of cybersecurity activities and threat information sharing among all stakeholders.

An important component of these more recent proposals is statutory clarity with regard to an entity's lawful authority to monitor, use and disclose cyber threat information for cybersecurity purposes in the first instance, as well as corresponding market incentives, such as liability protection, for entities that engage in active cyber defense. I cannot overstate the importance of such clarity to speeding the more rapid adoption of effective cybersecurity practices, and the significance of the paradigm shift that we see taking place. Until stakeholders, including lawmakers, fully appreciate and understand that the monitoring, use and disclosure activities engaged in by cybersecurity providers are largely limited to non-content metadata, and are undertaken solely to defend network systems and assets against cyber attacks, then terms like "monitor," "use," and "disclose" – will continue to be viewed with apprehension even in the context of legitimate cybersecurity.

This apprehension, we believe, is manifested in the current, complicated legal and regulatory environment in which cybersecurity is practiced. This environment necessarily compels significant lawyer involvement in various aspects of the provision of cybersecurity

services. This need for near-continuous legal consultation necessarily inhibits the more rapid and widespread adoption of robust cybersecurity practices by private sector firms. However, if carefully circumscribed cybersecurity activities were to be clearly defined in functional, non-legalistic terms in a federal statute for which cybersecurity professionals need not resort to legal consultation and interpretation as a matter of course, then we believe entities will more readily adopt cybersecurity practices and more-readily share cyber threat information.

As to those proposals that bear on the establishment of a national, collaborative active cyber-defense capability, we believe that many of the "information sharing proposals" under consideration in Congress have made a sound start in this regard by establishing a basis for the Federal Government to more routinely share classified threat warning information with appropriate private sector entities as well as to permit such private entities to share threat information with each other. In our own case, AT&T leverages the intelligence of its advanced global network, coupled with sophisticated behavioral analysis techniques, to detect attacks while they are still in the development stage, and to rapidly implement protective measures for ourselves and our customers. By joining these capabilities with those of the other carriers/service providers, along with those of the security and software companies, we can create a capability to identify cyber threats as they emerge, and to rapidly mitigate them. This leveraging of existing private sector capabilities and "fusing" them with the classified threat warnings that only the Government can provide should be central to any legislative proposal on cyber threat information sharing. We look forward to working with stakeholders on ways to ensure that federal cybersecurity legislation will enable this end.

2. <u>Government Leadership</u>.

The United States government must lead by example in cyber security. The federal government is the largest single purchaser of information technology and network services in the United States, and its leadership and buying power can have great influence on the cyber security marketplace. Several worthwhile federal initiatives are in place to improve cyber security for the ".gov" domain, such as the Trusted Internet Connection effort by the Office of Management and Budget (OMB) and the advanced security service carriers offer Federal agencies through the General Service Administration/Department of Homeland Security joint initiative on Managed Trusted Internet Protection Service (MTIPS), but they are being applied inconsistently throughout the government. These initiatives could be expanded throughout the Federal Government in order to provide better cyber security at lower cost. By integrating MTIPS and like-managed cyber security services with the advanced cyber threat detection capability discussed above, our entire critical infrastructure can be more effectively and efficiently protected against the full range of cyber threats.

The Department of Defense also has its own effort to protect ".mil", separate from the ".gov" efforts. These initiatives do not yet take full advantage of the portfolio of managed security services offered by many private sector network service providers, such as network-based protection against DDOS attacks. The federal government needs a clear and comprehensive strategy for cyber security of all Federal systems that make up ".gov" and ".mil" - one which effectively leverages existing cyber security capabilities offered by the network service providers.

Further, the current roles and authorities of the various federal agencies overlap and are unclear with respect to cyber security for federal government infrastructure. Congress can lead

by establishing discrete, definitive roles and authorities of the various Executive Branch elements involved in all aspects of cyber security – including the National Security Council and the Cyber Policy Coordinator, the Office of Management and Budget, the Office of Science and Technology Policy, the Department of Homeland Security, the Department of Commerce including the National Institute of Standards and Technology and the National Telecommunications and Information Administration, the Department of Defense including U.S. Cyber Command and the National Security Agency, and the Department of State. The United States needs a unified Federal government effort on cyber security with a clear understanding of the roles involved – not the confusion that currently exists.

Happily, a number of the pending legislative proposals seek to address the problem of duplicative or redundant roles and authorities, and seek to establish other government cyber reform, particularly with regard to reforming the Federal Information Security Management Act of 2002, or FISMA. A number of proposals are properly focused on cyber awareness and cyber education, as well as work force development and cybersecurity R&D. The federal government can help to improve overall cybersecurity by promoting the creation and adoption of cybersecurity-oriented curriculum in schools, as well as work with the private sector to facilitate cybersecurity education and research.

Indeed, we all must redouble our efforts in cyber security education and awareness across the full spectrum of the Internet user base – from the boardrooms of our largest companies to the millions of individuals who surf the 'net. Current efforts in cyber security education and awareness are fragmented and the messaging is often confusing. The ultimate key to improving our national cyber security is technology innovation driven by market demand from informed users and purchasers of all kinds. By creating market demand for cyber security through

heightened consumer awareness, we can spur fundamental security innovation at all levels of the Internet eco-system, and allow the United States to continue as a leader in Internet development.

To that end, Congress should consider designating a lead Agency on cyber security education, and support that designation with an appropriate level of funding to make it effective. The roles of other Federal Agencies in supporting this effort should also be clarified. One of the key struggles in cybersecurity at the individual consumer level is the low rate of user adoption of proven protection mechanisms. This is one area where the government could positively influence the trajectory of cybersecurity by engaging in a comprehensive education and outreach campaign to inform consumers about security best practices and how to protect themselves and their sensitive information.[3]

3. <u>Global Strategy</u>.

As I mentioned at the outset, cybersecurity is a global issue in all its dimensions. The United States must move forward aggressively to create a comprehensive strategy for addressing global cooperation in cyber security. We must reinforce the leadership of the United States in shaping the future of the Internet, and assuring its stable, reliable, and secure operation, as U.S. enterprise expands in the global Internet marketplace. In particular, all members and participants of the global Internet community must achieve consensus on the fundamental point that malicious cyber activities of any sort will simply not be tolerated. Federal legislation should at least attempt to address the global context of cybersecurity by establishing a framework for international cooperation in this regard, particularly in the establishment of international

[3] AT&T is itself actively engaged in the provision of cyber security information and protective tools to our customers, and actively participates in pan-industry cyber awareness education efforts such as "Stop.Think.Connect," the coordinated messaging effort spearheaded by the Anti-Phishing Working Group and the National Cyber Security Alliance and comprised of government agencies, private sector entities, and not-for-profit corporations.

agreements that will enable real-time global coordination in addressing cyber attacks. Concurrent with these efforts, Congress should also expand incentives for investment by the private sector to help invigorate U.S. technology leadership in cyber security and the Internet.

When legislation has the potential to hinder, rather than help

1. <u>Unintended Consequences of Regulation</u>

Some cybersecurity legislative proposals include a variety of regulatory schemes, ranging from standardized certification regimes to processes that could result in the imposition of regulatory performance standards on some critical infrastructure sectors, including the communications sector. Such proposals, while undoubtedly well-intentioned, are the antithesis of innovation – such requirements could have an unintended stifling effect on making real cyber security improvements. Cyber adversaries are dynamic and increasingly sophisticated, and do not operate under a laboriously defined set of rules or processes. The challenges we face in cyber security simply cannot be solved by imposing slow moving, bureaucratic processes on those who build, operate in, and use cyber space. Overbroad regulation and certification requirements will likely have unintended consequences, such as emphasizing the status quo by focusing on yesterday's challenges. An overly prescriptive approach can only serve to stifle Internet innovation and the technology leadership of the United States in the global information infrastructure. Quite simply, innovation is inconsistent with standardization.

I have heard it observed that federal cyber regulation is needed because no one firm in the private sector has the financial incentive to invest in capabilities to address a cyber incident that affects more than the value of the assets of that firm. Even if this were true, the answer is not for government to prescribe regulatory patches on discrete elements of the various critical infrastructure sectors in the hopes that these patches will effectively deter ever-evolving

intrusions by cyber adversaries. Rather, the answer is for government to facilitate the creation of the most effective cybersecurity tools possible and to permit the private sector to respond to emerging threats in diverse and innovative ways.

Conclusion

Private sector investment and innovation has made the Internet ecosystem the success it is today, and drives the dynamics of the technology and how it is used in global business and the operation of our critical infrastructure. AT&T invests in our network and leads innovation in cyber security because it is in our customers' interests to do so. We want to be a leader in cyber security, as well as all the other aspects of our business, because we understand the competitive advantage such leadership provides in a highly competitive global marketplace. We strongly believe that the most effective way to move forward on cyber security is to broadly spur investment and innovation, based on increased awareness of cybersecurity by the CEOs of the largest companies to the individual consumers that drive market demand.

The Internet itself was created through innovation. Some key early investments by the government helped spur that innovation. Congress and the Administration have leadership rolls to play in assuring that the United States continues to focus on technology innovation. Burdening the private sector with the cost of unnecessary and ineffective regulations and processes is contrary to that objective, and will only slow advances in cyber security. Congress must insist on and support initiatives that provide the flexibility needed to deal with the dynamics of the threat and the technology, while creating innovation and investment through market demand.

I thank the Subcommittee for its timely and focused attention on cybersecurity, and I look forward to providing on-going guidance, assistance, and recommendations as we collectively work to reduce the cybersecurity threat to our nation and our critical infrastructure.