ROD BECKSTROM
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)
The London Conference on Cyberspace
2 November 2011
As prepared for delivery

The cyberworld is a brave new world. Now that we have opened this Pandora's box of incredible technology and connectivity, society is changed forever. And we cannot go back. The Internet is not unlike man's discovery or taming of fire - once he experienced its benefits, he chose never to do without them. And so it is with the benefits we derive from the Internet, which connects billions of people and devices, and within decades might connect trillions of devices, sensors and other electronic tools.

I stand before you as a fellow student of this incredible world of change, striving to understand this system holistically. Like those of you attending this conference, I seek to contribute to the Internet's stabilization and evolution for the benefit of mankind. Over the course of my career, I have had the opportunity to observe this phenomenon from a number of very unique vantage points: from the perspective of a high-tech entrepreneur, as an officer in private and public companies, as a contributor to the world's largest national cybersecurity architecture, and as the head of ICANN, a critical global body that works to assure that the Internet remains open, unified and global. ICANN works with 242 countries and territories in supporting the daily operation of the Internet, as the global coordinator of the Domain Name System, or "DNS". This system is used more than one trillion times per day by humans and our machines, and yet most of us don't give it a second thought.

I mentioned my early career path because I find experience has a way of revealing patterns. Our current discussion of the Internet, and the challenges of cybersecurity, remind me of my very first job, here in London when I worked as a derivatives trader. Even then, derivatives were highly complex, and it was clear that to manage them we had to develop new models and clear insights into their elusive structure in order to model, price, and manage their risk successfully. Unfortunately, the recent meltdown in the financial sector demonstrates what can happen when risk mitigation efforts do not keep pace with the growing scale and complexity of systems.

Cybersecurity is no different.

While this is a radically different and new hyper-networked world, with new realities and virtualities, we can begin to understand some of the structural

concepts of security in cyberspace. And we can see how some approaches to the problem may fail and how some may succeed.

Before I comment on how we should organize to protect society from the darker side of cyberworld, I'd like to highlight three key principles that apply to the Internet:

1) Anything connected to the Internet can be hacked.
2) Everything is being connected to the Internet.
3) So everything is becoming vulnerable and a new dynamic of cyber crimes countered by security measures, countered by new criminal efforts, and so forth, is now unleashed

Thus cybersecurity is a question of the struggle between offensive and defensive measures. And in this context, remember that offense is considered by many experts to be a thousand times easier than defense. The offender needs to find only one way out of millions to break into a machine or system, whereas the defender is in a constant state of high alert, guarding entire massive, complex systems.

So is the goal of your conference hopeless, Minister Vaizey?

No. I think not. For inasmuch as the cyberworld is driven by quantum science and the weirdness of its subtleties and complexities, some patterns do emerge. Some solutions do suggest themselves.

The last time we had a quantum shift was the invention of the nuclear bomb. We thought it might end the world. It didn't. It changed our *strategies for handling war between nation-states*. From massive full-force wars between superpowers, we retreated to proxy wars at the periphery of our system with stability amongst the most powerful nations.

That's because to fight directly with a threat of nuclear escalation was too risky – no one wanted Mutual Assured Destruction or MAD. Fear of MAD led to more substantive negotiations, treaties and agreements among nations and, in the main, it stabilized world affairs. Let us hope it remains so.

Cybersecurity is the next quantum shift, but it too can lead to a new global political equilibrium. We simply have a new type of MAD to deal with – namely "Mutually Assured *Disruption*." Now, even small groups of cyber mercenaries can threaten national electrical grids or other key infrastructure, should they choose to. Massive disruptions could occur. And the only way out is what?

Collaboration. What will be necessary is a higher level of collaboration among public entities and private entities than ever before. We need good networks to counter bad networks. More fluid and faster. And we will get through this collaboration, not with antiquated governmental bureaucratic structures, but rather with new networks of centers of excellence, centers of security, new CERTS and with thousands or millions of young people learning how to participate and contribute. And in that process, top-down, centralized solutions will fail, and will be humbled by the decentralized forces arrayed against them.

So in matters of developing norms for cybersecurity, and for Internet governance generally, here are three assertions to consider.

Assertion 1: The best way forward is a decentralized, multistakeholder model. We know the multistakeholder model works. Why? Because the Internet works. The model has led to performance, innovation, and evolution on many levels. It has led to an open and unified DNS that has now scaled to more than a trillion transactions per day. It has led to internationalized domain names or IDNs. We have seen the addition of 30 IDNs from 20 countries and territories in the DNS root zone, with nine more to come. It has driven the cost of registration down from US $35 per year to about US $7 per year. It has facilitated greater online innovation through the introduction of new top-level domains (TLDs) such as .asia, .biz, .info, .mobi, and many more. It is supporting the successful transition from IPv4 addresses to IPv6 addresses.

So think decentralized. Top-down just does not work in a system that connects millions of networks, with most owned by the private sector. As the Foreign Secretary said yesterday, "Nothing would be more fatal or self-defeating than the heavy hand of State control on the Internet, which only thrives because of the talent of individuals and of industry within an open market for ideas and innovation…"

Assertion 2: we must re-architect the Internet for security. The network was designed for openness and flexibility. Now we need to make investments to enhance the security of the Internet itself. We need to do a few simple things, such as deploying DNSSEC universally. DNSSEC is the technology that assures you, the user, that you are really receiving information from the website you request, and not from a hijacker who has corrupted a web page. It prevents what we call "man-in-the-middle" attacks. Last July, we signed the root of the Internet with DNSSEC. Now most major top-level domains such as .com, .net or .uk have signed their zones with DNSSEC. Now we need you to sign your organizations' domain names, and to ask your Internet service providers to turn on DNSSEC validation. This is one concrete action that each and every person can take back to their organizations. Regardless of the function of your organization, go back and see your CIO tomorrow, and ask him or her to sign your domain name. Implementing DNSSEC helps plug a fundamental weakness of the Internet as it is today.

Assertion 3: Please improve the Internet by joining us. If you are not already directly involved in a multistakeholder Internet body, please join one. We certainly invite you to join the ICANN community and I'm sure the other groups would be pleased to have your involvement as well. We have dozens of different stakeholder groups, constituencies, review teams and working groups. And it is in this same spirit that I would like to invite all of you present here today to build more inclusiveness into the system, by participating in the next ICANN Public Meeting, in San Jose, Costa Rica next March. Next June, we will meet here in Europe in Prague. Please join us. While we already have many active accountability and transparency measures, programs and reviews, your direct participation can only enhance these, as well as help move important policy efforts forward.

Working together, we can prevail and we can even succeed in a noble endeavor of achieving one world, one Internet." Thank you.