Information Technology Industry Council

As prepared for delivery, April 9, 2013

# "Getting the Innovation Equation Right for Internet Governance and Cybersecurity"

Keynote Remarks by Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

At the 7th Annual U.S.-China Internet Industry Forum

I want to thank the organizers of this august forum first for the vision and leadership to hold these annual gatherings and second for inviting me to speak at today's event. The Information Technology Industry Council (ITI) is a global trade association representing 48 of the world's most innovative, forward-thinking technology companies.

In spite of the fact that I ended up missing my country's college basketball championship, I am really excited to be here in China. We have something far more important to discuss: The integrated nature of the Chinese and U.S. Innovation Ecosystem. In fact, it is my firm view that the United States technology sector will not be successful without China, and that China will not be successful in achieving the goals outlined in its12th Five-Year Plan without the United States. Innovation is the common key driver for energizing both of our economies, sustaining our environment, and ensuring the health of both of our populations as we live longer.

The continued forward progress of innovation in both of our countries is intimately interconnected. Both of our countries are major hubs in globally integrated supply chains. The power of the Internet intertwines our futures whether we like it or not.

The fundamental question is what does that future look like. Is it a future of antagonistic accommodation where every gain for China is a loss for the United States, and vice-versa? Or is it competitive collaboration, where we challenge each other, but fairly, while seizing the opportunities to collaborate for our collective good?

If given a choice between antagonistic accommodation or competitive collaboration, I would hope the choice is obvious. So today, I would like to highlight two related challenges we believe must be addressed together in order to strengthen and deepen that potential future of successful competitive collaboration. The first is global Internet governance and how we must collaborate to ensure the Internet continues to grow, thrive and fulfill its enormous potential of providing more and unimagined benefits to our economies and societies. The second challenge is ensuring we get the cybersecurity equation right. Both of these fundamentally intertwined issues are likely to continue to define and hopefully not disrupt our mutual ability to find greater success in the China-U.S. ICT industry relationship.

These are enormously challenging times for our two countries and our industries. Tensions are higher than they should be. Frankly, there is too much finger pointing. Perhaps these words

are blunt, but they should not come as a shock to anyone. Yet, we are here because we believe there is an opportunity for dialogue, and an even greater opportunity to work together toward mutual good that benefits the world. We at ITI are about bridging communities, bridging differences. Our membership is comprised of global companies that compete aggressively but also work together to create an environment in which innovation can flourish. We recognize and seek to preserve common values and address the common obstacles facing our sector no matter which continent we call home. It is with these thoughts in mind that I make my remarks this afternoon.

## Global Internet Governance

The global Internet is an amazing innovation that is both powerful and fragile. With 2.5 billion users, 46 percent of whom are in China, the Internet is perhaps the most disruptive development of the last century. The surge in Internet usage in China alone in the last decade has been nothing short of amazing, going from 22 million users to 528 million. Think of it: There are more netizens here in China than citizens in the U.S, and almost as many as the online population of North America and Europe combined. Also impressive is the growth of new Internet companies like Sohu, Baidu, Sina, and Tencent. Indeed, Tencent's new app WeChat, and social media generally, is significantly accelerating the positive power of the Internet for economic and social good.

It is critical that we get the governance of this technological marvel right. With the Internet's present and future seemingly riddled with complex challenges, the solution is perhaps easier than it appears: don't fix what is not fundamentally broken. Instead, we should embrace and improve the current multi-stakeholder process to help sustain the Internet's continued flexibility, growth and catalytic power to spur new generations of ICT innovation. Failure to do so smartly and effectively could endanger the ability of the Internet to drive economic and societal progress.

The Internet is the lifeblood of astounding new technologies related to cloud computing, sweeping innovations in big data, and new wireless technologies rapidly entering the marketplace, including more than a billion smartphones sold in 2012 alone. As impressive as this seems, the global technology revolution is still in its early stages. Worldwide smartphone penetration was only at 27 percent at the end of 2011. This year, for the first time, smartphone sales are projected to exceed sales of standard mobile technology, bringing the Internet within reach of millions of more new users every day.

According to a World Bank report, these technologies are "offering major opportunities to advance human development -- from providing basic access to education or health information to making cash payments." All of us are reaping countless social and economic benefits associated with these Internet-related technologies.

While the Internet's rapid evolution as a central change agent in global economics and society is well known, the Internet's governance structure is not. Relatively few outside of this room know anything about the many stakeholders that make up the institutions and bodies that are enabling its growth. Although government stakeholders had a hand in the creation of some of these organizations, namely the Internet Engineering Task Force, or IETF, and ICANN, these organizations are governed through collective input from technicians, academics, innovators, governments, and civil society.

They and other related organizations are part of a "multi-stakeholder" model that, while at times seemingly complex and arcane, is widely recognized as the stabilizing force that ensures that open and transparent rules, standards and protocols are in place to make network interconnection easy and reliable. The continuing engagement and viability of these organizations is critical to sustaining the Internet's role as an engine of ICT innovation.

Of course, the Internet is linked to a global telecommunications infrastructure that has been regulated by national governments since the days of the telegraph. The International Telecommunication Union (ITU), a United Nations "special agency," has been the legacy multilateral telecommunications oversight agency since 1934. An important discussion was convened last December in Dubai by the ITU at the World Conference on International Telecommunications, or WCIT.

But was this telecommunications treaty conference the proper place for determining whether the ITU should have a role in Internet governance? After all, only Member State government representatives attending the WCIT meeting were permitted to vote on proposed changes to the telecommunication regulations. The private civil society stakeholders that have helped enable the Internet explosion were relegated to advisors at best, and mere spectators at worst. The ITU continues to have an important role in the tradition telecom space. But the ITU was not created, nor is it currently designed, to respond to the very non-government stakeholders that are chiefly responsible for the Internet governance framework that has benefitted us all.

We are pleased to see positive demonstrations that China's own Internet and ICT industry is increasingly aligned with and contributing to the multi-stakeholder approach. Innovative Chinese companies such as Lenovo, Huawei, and ZTE actively participate at the IETF. Moreover, China this week is hosting the 47th ICANN Stakeholders Conference in Beijing. Deeper Chinese participation and leadership in these collaborative bodies will not only be good for China, but also essential for the global community, as China is of course a critical stakeholder in this realm.

At the same time, we hope China can move to create more effective policies at home that leverage the flexibility and catalytic power of the Internet by reducing regulatory and other barriers that may hinder rather than foster it. As I mentioned, the Internet is a powerful technology, but even minor regulatory restrictions, if they are not well thought through, can cripple this still nascent technology.

## Getting Cybersecurity Right

A second major challenge is getting cybersecurity policies in the right place and aligned. This is a critical priority for all governments, including China. The ICT sector is of course deeply committed to protecting against cyber threats. A collaborative, innovative cybersecurity structure is central to safeguarding public safety, national security, and economic stability. The interests of industry and governments in securing and facilitating cyber-based activities must be fundamentally aligned. All global companies, regardless of their location or origin, want a secure digital infrastructure for commercial translations.

China's e-commerce industry giants, such as Alibaba and Taobao, could not have evolved to build one of the world's largest online marketplaces without access to the most innovative global

security technologies. To ensure continued viability of the infrastructure and growth of our sector, global technology companies are deeply committed to designing and building strong security into the DNA of their products and systems.

Robust cybersecurity is, of course, not just about effective private-sector practice, but sound public policy. That's why cybersecurity is at the forefront of extensive policy discussions from Beijing to Brussels. As a leading public policy advocate for the world's most innovative companies, ITI has been at the heart of these discussions. We believe efforts to improve cybersecurity should follow six key tenets:

1. Leverage public-private partnerships that build upon existing initiatives and resource commitments;
2. Reflect the borderless, interconnected, and global nature of today's cyber environment;
3. Adapt rapidly to emerging threats, technologies, and business models;
4. Be based on effective risk management;
5. Raise public awareness; and
6. More directly focus on bad actors and their threats.

What does this look like in reality? Recently, the United States and other governments have taken concrete steps to embrace these principles, and have begun to tackle the challenging task of protecting citizens, critical assets, and infrastructures from ever-evolving cyber threats around the world. More specifically, the United States recently issued a Presidential Executive Order designed to advance critical infrastructure cybersecurity.

I want to stress the executive order set a framework for the public and private sector to work collaboratively to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting security, business and individual privacy, and civil liberties.

We fully support this emphasis on creating a cybersecurity framework based on existing, voluntary, consensus-based standards and best practices – one that allows critical infrastructure owners and operators to identify, assess, and manage their cyber risks, and is technologically neutral. We also support the effort to establish a framework that is risk-based, seeking to identify critical infrastructure where a cybersecurity incident could have catastrophic effects on public health or safety, economic security, or national security. Similarly, we welcome efforts to ensure that trade secret and intellectual property protections are a key component of cybersecurity.

Development of this framework will be led by the U.S. National Institute of Standards and Technology, or NIST, which does not write security standards for industry. As the envisioned cybersecurity framework takes shape, NIST's role is only as a convener to compile standards over the next year through a multi-stakeholder process that is participatory and consensus-based. It's important that the development of such a completely voluntary framework will be built on consensus-based global standards and rely on agile, cutting-edge security technologies.

In China, we see and welcome some helpful developments related to strengthening cyber crime laws. This includes strengthening of penalties for cyber crime and new protections for data. At the same time, we are concerned that Chinese approaches towards critical information infrastructure protection, encryption, mobile smartphone security, and information security standards can diverge from the global best practices for increasing security.

This has sometimes manifested here in the mandating of country-specific approaches, standards, and technologies. Some of these policies also require the use of local intellectual property and domestic content. We feel very strongly that such approaches will not lead to effective cybersecurity protection for China's networks and consumers. Innovation simply cannot thrive in such a siloed environment, where obsolete technologies tend to get locked in.

Effective cybersecurity in China is, of course, important to our industry, but it's also critical to China. We count on China's success. We trade here. We invest here. We operate here. And because of the interconnected nature of the Internet, we rely on both the United States and China to have secure, robust, and flexible digital ecosystems.

Critical to ensuring success in information security and cybersecurity are effective global ICT standards that are voluntary, consensus-based, and driven by the companies that produce and understand the technologies. Global ICT standards together represent the foundation that undergirds our global supply chains and enables companies around the world to build complex and competitive products.

It is also important for all of our governments to stay focused and clear-headed, and not let rhetoric lead us astray. There is, as you all know, an ongoing and often colorful debate in capitols around the world from DC to Beijing on supply chain security and cyber trust. It is important to recognize that rhetoric does not necessarily translate into law and policy, though we cherish heated discussion and the free exchange of ideas.

But when the dust settles, we must ensure that the policies put in place embrace the reality that product security is a function of how a product is made, used, and maintained, not by whom or where it is made. Good security, like good ideas, knows no national boundaries. We do not believe that discriminating based on national origin is an effective means of achieving security assurance. We advocate these same positions with all governments – including in China and in the United States.

Good bilateral cooperation in related areas is real and happening in concrete ways. Take, for instance, our joint work on the ambitious initiative to expand the Information Technology Agreement (ITA). This is an important undertaking to the tech sector and we very much welcome China's recent ramping up of participation to advance this work. If people cannot get access to innovative, affordable tech products that ITA expansion would facilitate through tariff elimination, we limit our ability to grow the Internet and ensure we get the strongest cybersecurity. We also hamstring global economic growth and job creation. The U.S. tech industry looks forward to continuing our close cooperation with China to ensure we obtain a commercially significant outcome this year on ITA expansion.

## The Critical Need for Global Collaboration

It is no secret the ICT industry is one that is relentlessly competitive. The constant, never-ending push for innovation is the manifestation of that competitive spirit. Yet, there are a few select issues where aggressive competition takes a back seat to thoughtful collaboration -- and cybersecurity is one of them. Governments, too, have their own motivations to compete with one another, but as we have seen from the growth of multinational bodies focused on advancing best practices in cybersecurity and good global Internet governance, effective collaboration is happening and growing.

We at ITI seek to be an enabler of both industry and government collaboration. In fact, at ITI, we have over the past two years begun deep dialogues with Chinese stakeholders on issues relating to cyber norms, security, standards, and innovation. We certainly can't expect to solve all of our challenges through these dialogues. But we are now two years into such exchanges with key Chinese stakeholders. And our experience has shown that experts simply agreeing to sit down together for sober discussion has led to a better understanding of the commonalities and differences the United States and China take in approaching these complex issues. Our strong belief is that mutual understanding will lead to mutually agreed approaches.

To be sure, we have myriad common challenges in the Internet and cyber arenas. In our interconnected, globally integrated world, the answers lie in competitive collaboration, which can result in solutions that make sense for the United States, China, and the world. We know the formula for success, and it is not built on suspicion. It is built on cooperation and understanding, on a willingness to find solutions in partnership. We are the two largest economies in the world. It is our responsibility to work out our complex challenges. While sometimes daunting, too much is at stake to do otherwise. Thank you.

-30-