IEEE EXPERTS IN TECHNOLOGY AND POLICY (ETAP) FORUM ON INTERNET GOVERNANCE, CYBERSECURITY AND PRIVACY

BEIJING, CHINA
17 MAY 2016

Version: 29 June 2016

IEEE

Contents

Executive Summary

More than 50 individuals participated in the IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, and Privacy on 17 May 2016—themed "Closing the Cyberspace Policy-Technology Divide to Drive the Future of the Internet"—at the China World Hotel in Beijing. The invitation-only event attracted technology developers seeking a better understanding of the Internet public-policy landscape to help drive proactive technology design, as well as policy experts seeking reliable technical guidance to make informed Internet public-policy decisions. The fifth in a series of regionally oriented gatherings hosted by the IEEE Internet Initiative since last year, the Beijing event was co-sponsored by the China Internet Network Information Center (CNNIC).

Focus areas for this IEEE ETAP Forum included assessing technology and policy factors and actors that affect the development and management of the Internet; global acceptance of technology protocols and standards versus policy localization; and building an environment that enables the interaction of technologists and policymakers. Attendees in Beijing heard keynote presentations and panel discussions on challenges and opportunities in technology and policy, discussed their technology and policy concerns, and convened breakout sessions for in-depth conversation around three topics:

- Cyber-threats to critical infrastructure, including eGovernment/eCommerce
- Transparency as a source of obtaining data for evidence-based decision making
- Biodiversity in the Internet ecosystem

The next regional IEEE ETAP Forum gathering is scheduled for Tel Aviv, Israel, on 22 June 2016.

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

Along with exciting opportunities in areas such as revolutionary services and user experiences, improved productivity and efficiency, real-time decision-making, and fundamentally new business models, the drive toward universal connectivity, proliferation of the Internet of Things (IoT), and adaptation of information and communications technologies (ICT) in new industries are bringing to the fore a complex set of new issues to be solved, as well. Collaboration across traditional professional, technological, and geographic borders is crucial in an environment that is so interconnected and so complex, in order to successfully solve the emerging issues in cybersecurity, privacy, and Internet governance without blunting the historic promise of Internet innovation, in terms of encouraging sustainable development, spurring economic growth, enhancing public safety and security, etc.

Out of this awareness has grown the IEEE Internet Initiative. The initiative facilitates two-way dialogue between the historically separate worlds of technology and policy. In the same way that ongoing Internet innovation, sustainability, and market growth are intimately linked with informed Internet policy, it is also true that effective Internet public policy is reliant on sound, unbiased technical guidance. The IEEE Internet Initiative serves as a neutral platform across which engineers, scientists, industry leaders, and others engaged in disparate technology, policy, and industry domains globally collaborate—within context of advancing technology for the benefit of humanity.

Organized by the IEEE Internet Initiative, the IEEE ETAP Forums on Internet Governance, Cybersecurity, and Privacy have emerged as an integral venue for this conversation. As event co-moderator Oleg Logvinov explained to the attendees in Beijing, the IEEE ETAP Forums are staged "around the world in order to create a fabric of connectivity" and create "a cohesive crosspollination" among technology and policy developers globally.

The first IEEE ETAP Forum occurred in May 2015 in San Jose, California, in the United States (http://sites.ieee.org/etap-sanjose/). As Jared Bielby, co-chair of the International Center for Information Ethics, told the participants in Beijing, "Our initial idea was to try to identify the key issues—what are they regionally, and what are they internationally, and what would a community look like to address these collaboratively?"

IEEE ETAP Forum events subsequently took place in Tel Aviv, Israel, in August 2015 (http://sites.ieee.org/etap-israel1/); in Washington, D.C., USA, in February 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-washington-dc), and in Delhi, India, in March 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-delhi-india). Mr. Bielby said an integrated online community, the IEEE Collabratec™ forum, facilitates follow through on common issues identified across the IEEE ETAP Forums.

"We would really love your further participation," Mr. Bielby said. "There are a number of ways you can get involved."

Beijing IEEE ETAP Forum Invited Speakers

After event co-moderator and IEEE Internet Initiative chair Oleg Logvinov thanked CNNIC for its assistance in the organization of the day's agenda, the Beijing IEEE ETAP Forum opened with welcoming remarks from three speakers:

- Shilong Zhong represented the Bureau of IT Development, Cyberspace Administration of China. He discussed the urgency surrounding concerns in Internet governance, cybersecurity, and privacy as China pursues its "Internet+" strategy to drive economic growth by more fully integrating ICT throughout manufacturing and business. "As we know, a rapid development could not be realized without support for an orderly situation and the harmony between policy and technology," he said. "It is important to find coherent interests of policy and technology—this is also the main mission of the ETAP."

- Bruce Kraemer, president of the IEEE Standards Association (IEEE-SA) and a member of the IEEE Board of Directors, stressed the need for an open and accessible Internet, while building trustworthiness and maintaining security, as the world stands at the point today of roughly half of humanity connected and half unconnected. "IEEE can help bridge geographical differences of opinion that exist as to what the Internet is and how it should be maintained and managed going into the future," he said. "Promoting universal Internet access is inherent in IEEE mission of fostering innovation for benefit of humanity … To this end, IEEE calls upon the worldwide community of engineers and scientists who are responsible for building the Internet, along with the policymakers and other stakeholders in the Internet, to apply their skills and solutions that are needed to extend the success of the Internet moving forward."

- Xiaodong Lee, chief executive officer (CEO) and chief technical officer (CTO) of CNNIC and CEO of NATlab, spoke about China's exploding Internet penetration—700 million users, and over 90 percent of them are mobile users. "We have another 700 million people who do not connect to the Internet," he said. "It's a very big challenge for us to connect them, as they don't have the education to use the Latin characters on the keyboard. It's a big barrier; it's also a big opportunity for us. … How prepared are we for the changes of today and tomorrow? I want to ask all of the experts here to bear these questions in mind during today's discussion."

Following the welcoming remarks, the Beijing event moved on to an opening chat, a series of keynote presentations and a panel discussion.

Opening Chat: Rod Beckstrom, The Beckstrom Group, and Xiaodong Lee, CNNIC

Xiaodong Lee introduced Rod Beckstrom, president of The Beckstrom Group and a member of Global Council on Future of Government, World Economic Forum, who delivered a presentation titled, "It's a MAD MAD MAD Cyber World." He discussed his experience on 11 September 2001, and how his thoughts that day—about the smallness and fragility of the world and how no one is safe until everyone is safe—led him to re-orient his career around serving peace and, specifically, cybersecurity.

“How do we make the Internet safe for everyone?” he said. “Because, right now, it is safe for no one.”

He associated today’s innovations and challenges with the advances that allowed humanity to travel the world in the 1500s, such as globes, astrolabes and clocks. Such developments led to advances in ways of living and market creation, but they also led to negative things such as piracy.
He gave examples of Chinese and Dutch pirates and then the creation of privateers who were sanctioned by their governments to be pirates. He pointed out a similarity to Internet hackers of today. “Around the world, there were nation-state pirates, privateers who were working on behalf of states, and simple criminals, working completely independently,” he said. “… So this world of hacking and piracy that we are in is not new.”

Mr. Beckstrom noted that it took 300 to 400 years to get laws to address piracy. With the development of the nuclear threat, he said, it took about 40 years to get an agreement to slow proliferation of weapons. Credit cards were invented in the 1950s; credit-card fraud was invented one year later, and it has been with us ever since. But the fraud is contained and manageable, and credit cards are used globally.

“What is today’s reality?” he asked. “Anything networked can be hacked. Everything is being networked. Everything is vulnerable. These 12 words describe the baseline reality of this magnificent, interconnected, electronic world … Why is it a ‘MAD, MAD, MAD world?’”

- Nuclear mutual assured *destruction*–“There have been no world wars since the invention of nuclear weapons because of deterrence. So it works, and it's relevant to cyber. There are 14 nuclear powers, and there are a handful of true cyber powers, but it’s a stabilizing force … because of mutual deterrence and mutual assured destruction.”

- Cyber mutual assured *disruption*–“It is the capability of multiple nation-states to wreak havoc with other countries … It’s more problematic than nuclear MAD, because we can count missiles; we can count the countries; we can drive nuclear nonproliferation; and we can start to contain the problem. But with cyber MAD we don’t know how many players there are … we don’t know how many weapons there are; there are 200,000 new strains of malware invented every day.”

- Internet mutual assured *dependence*–“What economy in the world today would choose to unplug from the Internet? The reality is all economies today need the Internet. We need it for trade, welfare, transport ... everything.”

These three interdependencies, Mr. Beckstrom said, are why cyberhacking, while certainly a global problem, “has not spun out of control.” Instead, we come up with acceptable risk and loss based on managing cyberrisk. He suggested that wider-scale adoption of technologies from the financial services sector could be a leading edge of innovation. Because of the huge economic stakes of cybersecurity in that industry, it could provide the impetus to tackle cybercrime effectively in other areas of life.

In conversation with Dr. Lee to close the session, Mr. Beckstrom said that collaborative efforts,

systems-level thinking and more game theory will all be key to addressing the situation.

"I think we have to start with the principles first: collaboration, reciprocity, and the highest form of reciprocity, respect … respecting teach other as human beings, cultures, countries. And another of the principles is truth; we have to get to ground truth," he said. "The good news is that this is a problem for every country in the world, every company, and every person … This kind of forum is the perfect place to advance these discussions … There are differences in opinions, perceptions, and national interests. But it's through dialogue and working together that I'm hopeful we can make progress."

Keynote Presentation: Wei Lu, Internet Society of China

Wei Lu, secretary general of the Internet Society of China, offered an overview of coordinated anti-spam/malware efforts and his organization's work with Internet companies and government to address these challenges including ways to track abuses and supporting committees examining the problems. For example, the organization has created a reporting system for end user involvement and regularly releases publications intended to advance cybersecurity.

The Internet Society of China is a national non-profit organization set up in 2001 to support development of the industry and the government. There are more than 600 members, including legal companies, research institutes, academic associations, universities, and telecoms companies. The organization has established 30 working committees on specific fields (e.g., Internet Copyright Working Committee).

Mr. Lu shared statistics on the challenges faced in China for Internet hacking, including spam and malicious mobile applications. For example, when the Internet Society of China launched its anti-spam campaign, China was the world's second largest source of spam, he said. He said the Ministry of Information Industry published its first anti-spam measure in 2006, and, according to a British report, spam originating from China was reduced from 22.3 percent to 4.1 percent.

Smart mobile devices have introduced particular challenges with regard to cybersecurity, he said. Malicious apps with Trojans and viruses spread with developments, resulting in theft of private information and other forms of fraud. China's Ministry of Information Industry, with the help of the Internet Society of China, launched the 12321 Centre to field complaints from users about spam text messages. Since 2013, there have been more than 900 million reports of malicious apps, and 60,000 apps have been removed. The Internet Society of China then organizes third-party testing organizations to validate the efforts to rectify the apps. Similarly, it has recently initiated a collaborative anti-spam campaign around WeChat mobile text and voice messaging.

Mr. Lu said, detailed collaborative work undertaken by the Internet Society of China in other interrelated areas:

- The organization has worked effectively with the nation's three largest telecoms service providers to reinforce short message service (SMS) spam reporting and treatment through a national system.

- The Internet Society of China has cooperated with industry leaders to share anti-cheating information to enhance the industry's detection abilities.

- The organization has cooperated with app stores to reduce information fraud and roll out public mobile Internet security manuals.

Furthermore, the Internet Society of China "has recruited volunteers who are dedicated to social responsibility and a sense of justice. By now we have thousands of users volunteered to join this action of purifying the Internet." Mr. Lu described the Internet Society of China as "a bridge that actively connects policymakers and industries. We encourage collaboration … to create a healthy, orderly and harmonious online network."

Panel Discussion: Building an Environment to Enable the Interaction of Technologists and Policymakers

Next, the Beijing IEEE ETAP Forum moved to a panel discussion that engaged Alain Durand, principal technologist with ICANN; Min Jiang, associate professor of communication with the University of North Carolina Charlotte and affiliate researcher at the Center for Global Communication Studies at the University of Pennsylvania; James Seng, CEO of Beijing Xianyu Shuma Tech. Co. Ltd., and Baoping Yan, chief engineer of CNIC and director of the Chinese Academy of Sciences Informatization Committee of Experts.

Facilitating Global Coordination

Alain Durand made the distinction that governance is the process by which global decisions are made—it is *not* governing. He said the Internet has been an enormous success largely because it's one Internet, not many small Internets. But, he said, that benefit comes with a price: the need for global coordination.

Mr. Durand said there is a need for openness, transparency and accountability in this global coordination—and that everyone (across disciplines and geographic regions) should be invited to participate. He particularly emphasized the importance of transparency. "I think this is perhaps the most important thing. There is a saying about quality: 'Say what you do, and do what you say.' But you need, too, to verify what has been done. Every time there is missing or hidden data, we are losing transparency, and we are losing trust."

He noted that ICANN's regional teams are working to address such needs. "At the end of the day, this is about increasing the communication," he said. "When I went to one meeting, the government people were wearing suits with ties, and the IETF (Internet Engineering Task Force) people were wearing T-shirts … These are communities that usually don't talk with each other. Anything that can be done like this forum that can cause crosspollination and enable these communities to talk to each other is very, very important."

Learning to Listen

James Seng discussed his work as a technologist working with governments internationally. “I am here to educate the policymakers. If we as technologists do not educate policymakers, they will come up with bad policy,” he said. “This is not because they are ignorant or incompetent but because they are not given inputs from engineers, the people on the ground. So it is up to us to keep up a constant dialogue.”

Mr. Seng said there exists a tension between the communities of technologists and policymakers. He stressed the need for patience in these discussions to be able to truly listen to one another about needs in each area. “I have seen very good, smart people talking to each other and listening but not really able to understand because they lack the patience to learn about these things they are not familiar with,” he said.

He affirmed the importance of environments such as the IEEE ETAP Forum, at which technology and policy experts can interact. But he also pointed out that it tends to be more difficult to get government decision makers to engage. “We are lucky today to have some policymakers here,” he said. “As engineers, we need to reach out to the policymakers more often.”

Building and Preserving Trust

Min Jiang asked how to bridge the gap between technologists and policymakers and noted the need to also include industry leaders, users, and non-governmental organizations (NGOs) in a discussion underpinned by trust and accountability. She observed that users in particular often lack a voice in decision making.

“Trust is hard to build and very easy to lose,” Dr. Jiang said. “Trust between technologists and policymakers works somewhat differently within China and beyond China. Domestically, technologists and entrepreneurs are given a lot of incentives in China, as policymakers really understand that smart people and smart ideas are the drivers of a thriving economy … This basic understanding between the policymakers and technologists really helps to build trust. But there are also constraints on technologists that their counterparts elsewhere do not face. Some of this is to do with content regulation, but, in addition to that, it’s well recognized that technologists are intricately involved in issues of cybersecurity and national security … It’s unclear how these factors affect trust.”

Dr. Jiang referred to examples of problems in the United States (e.g., Edward Snowden, a former U.S. Central Intelligence Agency employee who leaked classified information illuminating global surveillance programs) and in China (e.g., a student who recently died after experimental cancer treatment based on information of poor credibility that was discovered by Internet search) that have eroded trust because technologists and policymakers. She noted that ethical considerations also need to be part of the discussion.

“For a long time I believe policymakers in China and elsewhere saw the Internet as an engine of innovation and growth,” she said. “But they have paid very little attention to challenges of privacy, security, and accountability, which really now demand some sort of resolution.”

Understanding the Internet's Eco-environment

Baoping Yan discussed how there is an eco-environment for the Internet, just as there is in nature. "We need to examine and build this eco-environment to include information society, as well as technologists and policymakers," she said.

She discussed her work on databases related to China's Qinghai Lake nature reserve, where ICT is being adapted to enhance environmental protection work. "I have witnessed engagement with government, and people and even with the monks and the lama, and the way we have overcome prejudice to work together is really positive," she said. "… The biggest achievement is that we have built a local team of people in Tibet, the Chinese and local Tibetans, where we use the Internet to share information."

Ms. Yan said she believes we are still processing what the convergence of health, technology, and industry on the Internet will mean for humanity. She said that determining how we will use the Internet to protect the eco-environments we all live in will be vitally important. "If today the Internet is the most productive source in society, what can we do to protect this environment?"

Q&A

Oleg Logvinov built on the individual talks in the panel discussion to moderate a larger conversation among the participants about spurring meaningful conversations between policymakers and technologists. He synthesized the panelists' points by saying that the Internet is a "new ecosystem that needs to be protected as a fragile garden that we need to grow" and that tools for doing so are transparency, accountability, openness, and ethics.

"There is a difference in speed between what is happening on the Internet and what regulators are doing," Mr. Durand said. "Anything we can do to reduce this gap and make sure that there can be discussion before things become too much of a problem would certainly help move forward."

Mr. Seng added, "Every government works differently … and some have different comfort zones for what they consider to be a safe dialogue space. I think there are good people in every government; they try to create good, productive policy … I think the Chinese government is being smart in some efforts to combat fake goods, fake news, and propaganda of rankings … However, the way that the Chinese government officials would feel comfortable to engage industry and technology is very different from the U.S. government or Singapore or Japan government. Each works slightly differently, and we as a global community must accept that different governments have different tendencies, and we have to adapt for local environment, as well."

Ms. Jiang noted a challenge in bridging the technology and policy development communities. She described technology developers as "rule breakers," who want to make new things. Policy development, however, is essentially rule making. Bridging this cultural gap between the two worlds is crucial, she said, because the two worlds are inseparable.

Mr. Durand offered a caveat on the questions of regulating the Internet based on ethical considerations. "There is a difference between applications, where you can encode the ethics in a

search engine as a perfect example, and the underlying technology on which the Internet is built," he said. "One of the reasons for the Internet's success is the environment of permission-less innovation. If you try to encode ethics too much into the fundamental building blocks, you run the risk of limiting the innovation that is happening there."

Dr. Jiang offered that she believes, as a teacher, that there is an opportunity to encourage students to take into consideration ethical issues as they are designing systems.

Keynote Presentation: Greg Austin, EastWest Institute

Greg Austin, a professorial fellow with the EastWest Institute and professor of cybersecurity, strategy, and diplomacy with the Australian Centre for Cyber Security at University of New South Wales Canberra, presented on "Internet Futures: Closing the Policy-Technology Divide in Research, Education & International Collaboration."

He said that the cyberspace environment keeps shifting with priorities of governments and international relations. So, both positive and negative trends are present, he said. At the same time that states are stepping up the arms race in cyberspace, for example, they also are sharing more information with one another about their challenges.

"Sovereignty in cyberspace remains a highly contested policy priority, but it is undermined and conditioned by realities of entanglement and unrelenting forces that have globalizing, anti-sovereignty effects," he said. "I'm really a fan of the proposition that governments can want for sovereignty in cyberspace all they like; they will never get it."

He described 2015 as a year of "amazing developments in cyberspace history," noting, for example, scientists' considering advanced artificial intelligence's relationship to human existence; China's president and the U.S. president agreeing not to engage in commercial espionage against the other; China and Russia's bilateral agreement, more or less creating a cyber alliance between them; and the United States' publishing a vision document of cyber options for all levels of the armed forces.

Mr. Austin said that education around Internet futures today is struggling to keep up with trends in technology and policy. He said there is a strong need for policy research, research-based education, and international collaboration, and he said that policy research is late in coming and being overtaken by events. There are also substantial gaps to be closed, particularly on the relationships among key countries. In some cases, he said, today's research tends to be biased by the researchers' specific national perspectives. Research coming out of the United States might illuminate U.S.-Chinese relationships but show an ignorance of Chinese-European or Chinese-Russian relations, when, indeed, the contrast is very frequently stark. In other cases, Mr. Austin, said research is simply lacking. For example, he said, the NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, is one of the key research centers in the world, but even it does hardly any research on Russia. Policymakers on the whole, he concluded, are drawing from a very thin pool of useful research.

Mr. Austin said he believes IEEE can play a role beyond mining nuggets of information, such as

through the IEEE ETAP Forums. He recommended that IEEE pursue wider partnership to help set the research agenda, deliver it, and promote/advocate results. “We must do more to harvest the outcomes in a way that can project them forward,” he said, proposing “more research and more collaboration, but finding mechanisms for practical projects, which do involve research, which can be translated into education, and which can set the foundation for more effective international collaboration.”

Keynote Presentation: Yuejin Du, Alibaba

Dr. Yuejin Du, senior researcher and vice president of technology with the Alibaba Group, presented on “Cybersecurity in the New Era of Internet+.”

Dr. Du asked, why have we spent so much time and effort on cybersecurity and the situation is getting worse? The threat stands to grow even worse with the proliferation of the IoT, he said, as virtually anything could be hacked remotely.

Dr. Du noted the convergence that is conveyed in China through Internet+, where the Internet will bring everything together in the future. “So today Internet is no longer and information and communication platform; it’s a platform for everything, a platform for manufacturing, a platform for living,” he said. “We do not have to say ‘eCommerce’ in the future; in the future, eCommerce *is* commerce. In the future, ‘Internet-based finance’ *is* finance. In the future, ‘eGovernment’ *is* government. The traditional working converged with Internet is not only to increase efficiency; it’s changing your working mode.”

However, wherever we can go with the Internet, the hackers can follow, Dr. Du warned. As interconnection expands to more things and users themselves, “this is good for bad guys,” he said. “Bad guys can control your vehicle. Bad guys can kill people. Bad guys can make your society turn into chaos. In the future, the Internet will be a network of living or surviving, so crashing the Internet can crash everything.”

The programmability, ubiquity, and convergence of the systems in the emerging Internet intensify security challenges. “In the past we tried to enhance security by dividing, but today everything is working together,” he said. “This makes defense very difficult.”

He noted that technologists must find ways to explain the security risks in understandable terms and that the traditionally isolated disciplines of physical security and cybersecurity must be integrated. “We have a chance to turn challenges into chances, to avoid data threat,” he said. “We need new technology, new modes, and new mindsets for policymakers to deal with these threats.”

Discussions and Next Steps

The Beijing IEEE ETAP Forum shifted to discussion of the individual concerns identified by attendees during the event registration process, as well as some new topics generated during rapid-fire conversation at the event. Co-moderator Clint Andrews reviewed the topics as synthesized into 18 sets of issues, and then the attendees voted three of them for concentrated discussion within breakout groups:

- Cyber-threats to critical infrastructure, including eGovernment/eCommerce
- Transparency as a source of obtaining data for evidence-based decision making
- Biodiversity in the Internet ecosystem

“We will only focus on three topics so we can have a deep discussion on them,” event co-moderator Oleg Logvinov said. “But the topics that don’t get chosen will be documented, with the potential to collaborate on later.”

Cyber-threats to Critical Infrastructure, Including eGovernment/eCommerce

The group discussed how traditional infrastructure, government, or a cyber system, such as a domain name system (DNS), could be considered “critical infrastructure.” The Internet itself can be considered an infrastructure. Originally viewed strictly as a communications medium, the Internet today is much more than that with crucial subsystems (DNS, routing, wired and wireless communications, etc.), all of which are susceptible to cyber-threats.

Nations today are only now beginning to document threats to critical infrastructure, the group said, and cyber-threats specifically are generally less understood. Motivations for cyber-attack span attaining profit, inflicting damage, or ruining reputations. Weaknesses can be exploited anywhere in the increasingly connected world, the group discussed. Even very small utilities and companies can be targets for large-scale attack, because of the global nature of the Internet.

An additional challenge that the group identified is that, whereas the “good guys” are bound by national rules and norms, the “bad guys” are not. Protection against cyber-threat must somehow bridge national boundaries while still respecting national needs.

The group proposed that threat intelligence standards are needed to define threat terminology, to categorize the various types of threats, and to create methodologies for sharing information about threats. Furthermore, the group said a platform such as IEEE could allow researchers, industry, and authorities to carry out a range of important tasks in combating cyber-threats to critical infrastructure:

- Building and sharing best practices
- Bridging today's nation-by-nation methodologies
- Facilitating more rapid response in a complex and evolving world
- Establishing cybersecurity as another element of physical security
- Prioritizing what needs the most protection
- Promoting the need for a "global Internet police"

Transparency As a Source of Obtaining Data for Evidence-based Decision Making

In this breakout session, IEEE ETAP Forum attendees articulated differences among transparency, openness, and accountability. Transparency, the group said, has to do with access to data, while openness suggests a process in which everyone can participate, and accountability addresses using data to validate decisions.

The group looked at reasons why transparency is not present in some instances of decision making:

- Business needs
- Localization issues (such as cybersecurity and cross-border coordination)
- Privacy
- Cost and capability hurdles (not all companies have the resources)
- Political concerns (organizations might hide or doctor unfavorable data)

Finally, the group explored potential solutions such as encouraging best practices, building user trust, fostering competition and diversity, and separating the tasks of data collection, analysis, and usage in order to avert potential conflicts of interest. The group affirmed the need for a standardized benchmark for transparency that could address questions such as how to measure and track transparency over time. The group, furthermore, asked whether too much transparency as a means toward evidence-based decision making could end up having bad effect, in terms of saturating decision makers with information that is not meaningful, relevant, and/or navigable.

Biodiversity in the Internet Ecosystem

This breakout group applied the biodiversity analogy to the Internet and explored its explanatory power and limitations.

The Internet is a natural system that we literally cannot control but maybe can steer/manage/police, the group said. The biodiversity of the Internet ecology is reflected in its diverse elements (e.g.,

humans, systems, and protocols), diverse growth paths (the Internet takes on different forms in different countries), diverse economies (anything from commercial to free), and diverse governing bodies and working communities (e.g., ICANN, ISO, and IEEE). At the same time, analogizing has its limits. Fundamentally, companies and organizations are distinct from individual human beings, animals, and other organisms and are guided by different assumptions and behavioral patterns.

A nurturing and open environment was deemed crucial to the growth of the Internet in both the United States and China. While the U.S. government provided initial funding, the group said, development of the Internet in the United States gained momentum from a vibrant "techno-culture" of tinkering and experimentation. In China, the group said, the nation's opening and reform, which started in the late 1970s, provided a more open economic and intellectual environment for growing the Chinese Internet since the mid 1990s. Besides a decentralized technical infrastructure, the exponential growth of the Internet ecosystem also benefited from various economic incentives, the group said. In addition, a "survival-of-the-fittest" mode of competition fueled innovations and adaptations in various food chains and lifecycles in the Internet ecology.

Over time, the group discussed, predators and monopolists (i.e., dominant industry players) have emerged to pose threat to the biodiversity of the Internet ecology. This has demanded intervention for the biodiversity to be sustained. In this process, both policymakers and technologists can play a role as conscientious gardeners to ensure diversity, resilience, and sustainability of the Internet ecology, the group said. While diversity in certain areas (e.g., technical standards) may pose challenges to the overall system's efficiency, competition as a result of choices and alternatives, especially in areas of products and services, is beneficial. For example, the group suggested, there should not be just one DNS clearinghouse, and an Internet that is good for all of humanity needs support from all directions and should not be strictly top-down regulated.

Conclusion

Event co-moderator Oleg Logvinov concluded the Beijing IEEE ETAP Forum by encouraging attendees to stay involved and engaged in the conversations sparked at the meeting. “This is not just a one-off discussion,” he said. “The purpose is for you to become part of the community, part of the movement that propels humanity forward.”

The next regional IEEE ETAP Forum gathering is scheduled for Tel Aviv, Israel, on 22 June 2016. Mr. Logvinov said, too, that he hopes to organize a panel at the Internet Governance Forum in Guadalajara, Mexico, on 6-9 December 2016 that would engage participants from each IEEE ETAP Forum, in order to provide perspective on the full spectrum of the regional events.

Join the Conversation

The IEEE Internet Initiative is a cross-organizational, multi-domain community that connects technologists and policymakers from around the world to foster a better understanding of, and to improve decisions and advance solutions affecting, Internet governance, cybersecurity, and privacy issues. There are many ways to engage through the IEEE Internet Initiative. Please visit http://internetinitiative.ieee.org or email internetinitiative@ieee.org for more information.

Appendix I: Program

The IEEE Experts in Technology and Policy (ETAP) Forum in Beijing, China, on 17 May 2016 was the fifth in a series of regional meetings to advance a global-scale discussion about top public-policy issues in cybersecurity, privacy, and multi-stakeholder Internet governance. Diverse stakeholders from around the world—government and industry representatives, legal practitioners, and academics—gathered for the one-day event organized by the IEEE Internet Initiative and technical co-sponsor China Internet Network Information Center (CNNIC).

Location: China World Hotel, Beijing

Moderators: Clint Andrews and Oleg Logvinov

Clint Andrews

Clint Andrews is a professor in the Bloustein School of Planning and Public Policy at Rutgers University, and was previously director of the Urban Planning program. His expertise is in the substance and processes of energy and environmental planning and policy. He was educated at Brown and MIT as an engineer and planner. He is a member of the American Institute of Certified Planners, a LEED Accredited Professional, and a licensed Professional Engineer. Previous experience includes working in the private sector on energy issues, helping to launch an energy policy project at MIT, and helping to found a science policy program at Princeton. Andrews currently serves on the Board of Governors of the American Collegiate Schools of Planning, and is a past member of the Board of Directors of the Institute for Electrical and Electronics Engineers (IEEE) and the International Society for Industrial Ecology, and a winner of the IEEE's 3rd Millennium Medal. His books include Industrial Ecology and Global Change, Regulating Regional Power Systems, and Humble Analysis: The Practice of Joint Fact Finding.

Oleg Logvinov

Oleg Logvinov is the President and CEO of IoTecha Corporation, an industrial IoT solutions provider.

In March 2016, Mr. Logvinov co-founded IoTecha Corporation. Prior to joining IoTecha, Mr. Logvinov was a director of special assignments in STMicroelectronics' Industrial & Power Conversion Division, where he was deeply engaged in market and technology development activities in the area of industrial IoT, including the applications of IEEE 1901 powerline communication technology in harsh environments of industrial IoT. During the last 25 years Mr. Logvinov has held various senior technical and executive management positions in the telecommunications and semiconductor industry. After graduating from the Technical University of Ukraine (KPI) with the equivalent of a master's degree in electrical engineering, Mr. Logvinov began his carrier as a senior researcher at the R&D Laboratory of the Ukraine Department of Energy at the KPI.

In January 2015, Mr. Logvinov was appointed as the chair of the IEEE Internet Initiative. The IEEE Internet Initiative connects engineers, scientists, industry leaders, and others engaged in an array of

technology and industry domains globally with policy experts to help improve the understanding of technology and its implications and impact on Internet governance issues. In addition, the Initiative focuses on raising awareness of public policy issues and processes in the global technical community. He is also a past member of the IEEE Standards Association (IEEE-SA) Corporate Advisory Group and the IEEE-SA Standards Board. Mr. Logvinov also chairs the industry engagement track of the IEEE IoT Initiative and has created a series of worldwide IoT startup competition events.

Mr. Logvinov actively participates in several IEEE standards development working groups that focus on IoT and communications technologies. Mr. Logvinov is chair of the IEEE P2413 "Standard for an Architectural Framework for the Internet of Things" Working Group. He helped found the HomePlug Powerline Alliance and is the past president and CTO of the Alliance. Mr. Logvinov has 24 patents to his credit and has been an invited speaker on multiple occasions.

Start Time	**End Time**	**Tentative Program**
8:15 am	9:00 am	Network and Continental Breakfast
9:00 am	9:10 am	Introductions Oleg Logvinov, Chair, IEEE Internet Initiative; President and CEO, IoTecha Corporation; Moderator
9:10 am	9:30 am	Welcoming remarks Shilong Zhong, Deputy Director General, Bureau of IT Development, Cyberspace Administration of China Bruce Kraemer, President, IEEE Standards Association and Member, IEEE Board of Directors Xiaodong Lee, CEO and CTO of CNNIC; CEO of NATlab Bruce Kraemer, IEEE Standards President, 2016. He has 30 years of experience in high-tech research, development, and strategic marketing with companies including Foxboro, Harris, Intersil, and Conexant. He is currently with Marvell Semiconductor in Strategic Marketing. Mr. Kraemer has 13 years of standards development experience in ETSI, IEEE 802.11, and IEEE 802.15, serving as chair of numerous activities. He has been chair of the IEEE 802.11n Task Group for six years, which in September 2009 completed its standards development work for a new high-throughput MAC and PHY. Dr. Xiaodong Lee is the CEO and CTO of CNNIC and CEO of National Engineering Laboratory of Naming and Addressing Technologies (NATLab). He is a Research Professor at the Chinese Academy of Sciences, a board member of the Internet Society of China, and the former vice-president for Asia-Pacific of ICANN. Dr. Lee is a member of the Global Agenda Council on Cybersecurity of World Economic Forum, a member of the Multi-Stakeholder Advisory Group of Internet Governance Forum (IGF), a member of the IANA Stewardship Function Transition Coordination Group (ICG), and a member of the ICANN Security and Stability Advisory Committee. Dr. Lee has been previously honored as one of the "Ten Outstanding Youth" in China's software industry as well as a Young Global Leader of The World Economic Forum in 2014. He received the "Outstanding Youth Medal of China" in 2009, and is currently a member of the All-China Youth Federation.

Start Time	End Time	Tentative Program
9:30 am	10:10 am	Opening Chat Rod Beckstrom, Member, Global Council on Future of Government, World Economic Forum Xiaodong Lee, CEO and CTO of CNNIC; CEO of NATlab Mr. Beckstrom is a well-known cybersecurity authority, Internet leader, and expert on organizational leadership. He is the former President and CEO of ICANN, founding Director of the US government's National Cybersecurity Center in the Department of Homeland Security, and co-author of the critically acclaimed book, The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. He is President of the Beckstrom Group, which invests in and builds high-technology companies. The group also advises multinational companies and international institutions. He is a member of the core team on the Future of the Internet at the Swiss-based World Economic Forum. He is an advisor to the Stanford University Cybersecurity Policy Program. He graduated from Stanford University with a BA (with Honors and Distinction) and an MBA, and he was a Fulbright Scholar in economics at the University of St. Gallen, Switzerland.
10:10 am	10:30 am	Keynote Presentation Wei Lu, Secretary General, Internet Society of China; Senior Engineer Wei Lu is Secretary General of Internet Society of China, Senior Engineer. With vast management experience in the industry, he has long been engaged in management of ICT programs and Internet- related fields.
10:30 am	10:45 am	Break

Start Time	End Time	Tentative Program
10:45 am	11:30 am	Panel: Building an environment to enable the interaction of technologists and policymakers Oleg Logvinov, Moderator Alain Durand, Principal Technologist, ICANN Min Jiang, Associate Professor of Communication, UNC Charlotte; Affiliate Researcher at the Center for Global Communication Studies, University of Pennsylvania James Seng, CEO of Beijing Xianyu Shuma Tech. Co. Ltd. Professor Baoping Yan, Chief Engineer of CNIC and Director of Informatization Committee of Experts, Chinese Academy of Sciences Alain Durand is a Principal Technologist in the Office of the CTO at ICANN. His responsibilities include applying expert technical knowledge and experience to improve ICANN's technical capabilities and stature. Prior to ICANN, Alain was a distinguished engineer at Juniper networks, a large Internet equipment vendor. Prior to Juniper networks, Alain worked at Comcast, a very large cable service provider. He served Comcast as director of IPv6 and Internet governance. While developing the first IPv6 deployment plan for a service provider of this size, Alain represented Comcast in various Internet governance forums. Alain has been part of the Internet technical community for over 20 years, being a pioneer in IPv6 standardization and deployment. In particular, he has served as working group chair for several working groups at IETF and authored over 14 RFCs. Min Jiang, PhD, is Associate Professor of Communication at UNC Charlotte and an Affiliate Researcher at the Center for Global Communication Studies, University of Pennsylvania. Her research focuses on Chinese Internet technologies, politics, and policies. Highly interdisciplinary, her work blends new media studies, political communication, international communication, legal studies, and information science. She has written on Chinese digital technologies (search engine, social media), business, policies, and digital diplomacy. She has published over 25 journal articles, book chapters and conference proceedings. Her research has appeared in Journal of Communication, New Media & Society, Information, Communication & Society, Social Science Computer Review, Policy & Internet, Electronic Journal of Communication, and Information Visualization among others. A recipient of over two dozen research grants, she has received funding from and presented her work at various institutions including Social Science Research Council (SSRC), National Committee on US-China Relations (NCUSCR), Oxford University, Harvard University, University of Pennsylvania, Johns Hopkins University and French Institute of International Relations (IFRI). Prior to pursing her doctor's degree in the US, she worked at China Central Television and Kill Bill I in her native country China. Mr. James Seng is now the CEO of Beijing Xianyu Shuma Tech. Co. Ltd. James is a well-known international expert on the Internet. He is also known as the "father of internationalized domain names." He started his career in 1993 with Technet, the first ISP in Singapore (the precursor to Pacific Internet). He was involved in a number of pioneering Internet projects in the early days of the Internet, including the development and standardization of internationalized domain names. Previously James was with Infocomm Development Authority of Singapore, responsible for the Next Generational Internet. He was also the advisor and consultant to MiTV that rolled out U-Mobile in Malaysia. He also advises family offices about their TMT investments in China. In 2008, James joined PPTV as CTO of a company that became one of the largest video streaming services in China. In 2010, he founded a video platform company that was acquired by HiSense. In 2014, James joined 21Vianet Group as the Vice President responsible for the technology strategy for its New Business division. Professor Baoping Yan is Chief Engineer of CNIC and Director of Informatization Committee of Experts, Chinese Academy of Sciences. She graduated from Xi'an Jiaotong University and the Institute of Computing Technology (ICT), CAS with her bachelor's, master's and doctorate degrees, and she accomplished her postdoctoral research at ICT, CAS. Since 2006, Professor Yan has been the Chief Engineer of CNIC and director of the Informatization Committee of Experts, CAS. She is standing deputy director of the Committee of Experts for Scientific Database of CAS, deputy director of the Internet Society, China Computer Federation, as well as the standing trustee of the China Computer User Association and trustee-general of Beijing Computer User Association. She is a member of the National Technology & Science Infrastructure Committee of Experts, Ministry of Science & Technology of China and China's Next-Generation Internet Committee of Experts, National Development and Reform Commission, also a member of the Tibet Development and Advisory Committee and the supervisor of the Information Group. Professor Yan is a trustee of the Chinese ISOC Council, AC member of W3C Committee, and a member of the International Council for Science (ISCU), World Data Scientific Committee (WDS-SC).

Start Time	End Time	Tentative Program
11:30 am	11:55 p.m.	Rapid-fire identification of issues Clint Andrews
11:55 am	12:15 pm	Review and comparison of previous ETAP Forum outputs and discoveries Jared Bielby, Co-Chair, International Center for Information Ethics Jared Bielby received a double master's degree at the University of Alberta, Canada, in information science and digital humanities with a thesis route in the field of information ethics. He works as an independent consultant in information ethics and internet governance. He currently serves as co-chair for the International Center for Information Ethics and editor for the International Review of Information Ethics. He is moderator and content writer for the Institute of Electrical and Electronics Engineers' (IEEE) Collabratec Internet Technology Policy Forum (IEEE-ETAP) and is founder and editor-in-chief of The Freelance Netizen. His research and writing looks at the interdisciplinary connections between information & communication technologies (ICTs) and information ethics, digital citizenship and culture. Bielby has written and spoken internationally on subjects of information ethics, internet governance and global citizenship in a digital era.
12:15 pm	1:15 pm	Lunch
1:15 pm	1:35 pm	Keynote Presentation Greg Austin, EastWest Institute Dr. Greg Austin is a Professor in the Australian Centre for Cyber Security in the University of New South Wales. He also serves as a Professorial Fellow at the East West Institute, where as vice-president from 2006-2011 he helped set up and lead its Worldwide Cyber Security Initiative. Greg is a co-chair of the EastWest working group on Measures of Restraint in Cyber Armaments. He has held senior posts in the International Crisis Group and the Foreign Policy Centre (London). Other assignments include service in government, defense intelligence, academia, and journalism. He is the author of several books on China's strategic policy, including China's Ocean Frontier (1998) and his most recent book, Cyber Policy in China (Wiley 2014). The latest book offers the first comprehensive analysis (military, economic and political) of China's leadership responses to the information society. It explores the dilemmas facing Chinese politicians as they try to marry the development of an information economy with old ways of governing their people and conducting international relations. Greg has a PhD in international relations and a master's degree in international law. He is an Australian citizen.

Start Time	End Time	Tentative Program
1:35 pm	1:55 pm	Keynote Presentation Yuejin Du, Senior Researcher and VP of Technology, Alibaba Group Dr. Yuejin Du is currently working as Senior Researcher and VP of Technology at Alibaba Group, focusing on data security, threat intelligence, standards, and outside cooperation on cybersecurity. He is a famous expert on cybersecurity in China. He was one of the founders of Chinese national computer emergency response team (CNCERT/CC) and the Asia-Pacific cooperation group of CSIRTS (APCERT). Before he joined Alibaba, he was the founder and director of National Engineering Laboratory for Cybersecurity Emergency Response Technology, the director of the National Institute of Network and Information Security, and deputy CTO of CNCERT/CC. Dr. Du has more than 15 years of experience in Internet security. He contributed greatly to national Internet security capacity building, leading the development of a Chinese national Internet intrusion monitoring and warning platform, playing a key role on setting up a Chinese national incident response cooperation framework, and raising public awareness Dr. Du has also played and active role in international cooperation. He proposed a China-ASEAN cooperation framework on network security, lead an APEC-TEL project on botnet countermeasures, and has made presentations at various international conferences.
1:55 pm	2:15 pm	Synthesize and refine selection of highest priority issues Clint Andrews, Professor, Rutgers University
2:15 pm	3:15 pm	Breakout Session — Delve deeper into highest priority issues Volunteer breakout leads
3:15 pm	3:30 pm	Break
3:30 pm	4:15 pm	Report-outs from breakout teams Volunteer breakout leads
4:15 pm	4:30 pm	Next steps, action plan and wrap up Clint Andrews

Appendix II: Participants

The following individuals attended the Beijing IEEE ETAP Forum:

Sandesh Acharya, Student

Clint Andrews, Rutgers, The State University of New Jersey, Professor and Associate Dean, Planning and Public Policy

Greg Austin, EastWest Institute, Professorial Fellow; Australian Centre for Cyber Security at University of New South Wales Canberra, Professor

Rod Beckstrom, The Beckstrom Group, President; Global Council on Future of Government, World, Member

Jared Bielby, International Center for Information Ethics, Co-Chair

Udo Chima, Schlumberger Oilfield Services Nigeria Limited, Maintenance Technician Electronics

Nan Chu, CNNIC, Policy Advisor

Julie Cong Zhu, CNNIC, Policy Liaison

Lucian Cristache, LucommTechnologies, IOT Architect

Shefali Dash, National Informatics Centre, Govt. of India (Retd.), Former Director General

Dr. Yuejin Du, Alibaba Group, Senior Researcher and Vice President of Technology

Alain Durand, ICANN, Principal Technologist

Mark Epstein, Qualcomm Inc., Senior Vice President

Jean-Philippe Faure, member IEEE Standards Association Board of Governors; Progilon

Samah Ghanem, Huawei R&D Labs, Senior Research Scientist

Shuyi Guo, CNNIC, Policy Liaison

Dr. Braham Deo Gupta, Jiwaji University

Liyun Han, CNNIC, Policy Executive

Yanjun Hu, BII Group, Executive Assistant

Ning Hua, IEEE, Senior Director, Asia Operations

Min Jiang, University of North Carolina Charlotte, Associate Professor of Communication; Center for Global Communication Studies at the University of Pennsylvania, Affiliate Researcher

Konstantinos Karachalios, IEEE Standards Association (IEEE-SA), Managing Director

Karen Kenney, IEEE Standards Association Senior Director, Business Operations and Administration

Ning Kong, CNNIC, Director of International Department

Bruce Kraemer, IEEE-SA, President; IEEE Board of Directors, Member

Xiaodong Lee, CNNIC, CEO and CTO; NATlab, CEO

Conglun Liu, Internet Society of China, Secretary of Foreign Affair

Dong Liu, IEEE-SA, Board Member

Oleg Logvinov, IEEE Internet Initiative, Chair; IEEE P2413 Internet of Things (IoT) Architecture Working Group, Chair; IoTecha Corporation, President and CEO

Wei Lu, Internet Society of China, Secretary General

Cong Ma, IEEE, Meeting and Conference Manager

Jay Merja, MUVR.in, Founder Director

Andrew Myles, member, IEEE Standards Association Board of Governors; Cisco

Mary Lynne Nielsen, IEEE, Global Operations and Outreach Program Director, Standards

Paul Nikolich, IEEE 802 LMSC chair

Glenn Parsons, Ericsson, Standards Advisor

Trish Rafferty, IEEE, Associate Manager, EMS

James Seng, Beijing Xianyu Shuma Tech. Co. Ltd., CEO

Jessica Shen, CNNIC, Head of IP Operations

Linjian Song, Beijing Internet Institute, BII Lab Director

Zheng Song, Internet Corporation for Assigned Names and Numbers, Head of China

Yatin Trivedi, Synopsys, Director, Standards and Interoperability

Lan Wang, IEEE China office, Project Manager

Selin Wang, CNNIC, Cooperation Executive

Zhimin Wang, SUNWODA Electronics Co., Ltd.

Ping Wu, Internet Society of China, Coordinator

Xiucheng Wu, Coremail Information Tech. (Beijing) Co. Ltd., VP

Hong Xue, Beijing Normal University Institute for Internet Policy & Law, Director

Baoping Yan, CNIC, Chief Engineer; Chinese Academy of Sciences Informatization Committee of Experts, Director

Jiankang Yao, CNNIC, Senior Engineer

Tianxue Zhai, CNNIC, PR Supervisor

Tianyu Zhang, Beijing Jiaotong Univ, Student

Meng Zhao, IEEE China office, Standard Program Manager

Shilong Zhong, Deputy Director General, Bureau of IT Development, Cyberspace Administration of China

Linlin Zhou, CNNIC, Standardization Researcher

Mengqi Zhou, IEEE China Council, Past Chairman

Judy Zhu, Alibaba, Standardization Director

Appendix III: Top Issues

From topics suggested during registration and at the Beijing IEEE ETAP Forum, the following 18 key issues were considered for targeted breakout sessions:

- Finding more effective forums to bring together technologists, market decision makers, and public policymakers
- IoT and cybersecurity
- Internet governance
- Identity management
- Diplomacy
- Connectivity and rural telecomm management
- What kinds of cyber-threats does the Internet- critical infrastructure bring to a country and how that relates to eGovernment strategies
- Privacy, information security, business development
- Net neutrality and its implications
- NTIA IANA functions' stewardship transition
- IEEE role in current transition scenario
- Policy segmentation: how fine-grained can it be in order to be representative of a substantial majority of the affected community?
- Need for information systems to allow common representation of knowledge and information sharing between computer emergency response teams (CERTs) and between countries
- Internet biodiversity
- Cross-border data flow
- Biometrics
- Transparency as a source to get data for evidence-based decision making
- Balancing valued of share data and privacy

Appendix IV: Combined Issues List, Beijing/Delhi/Washington/Tel Aviv/San Jose IEEE ETAP Forums

Beijing

- Cyber-threats to critical infrastructure, including eGovernment/eCommerce
- Transparency as a source of obtaining data for evidence-based decision making
- Biodiversity in the Internet ecosystem

Delhi

- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Multi-stakeholder Internet governance
- Options and challenges in providing universal access for social and economic inclusion

Washington

- Data localization
- Education and ethics
- End-to-end security/privacy by design
- Technology-policy development process

Tel Aviv

- User assessment of trustworthiness of devices, enterprises, and governments
- Educating users about characteristics of information society
- Machine-readable privacy agreements and who enforces them?

San Jose

- Threats and opportunities in data analytics
- Multi-stakeholder Internet governance
- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Fragmentation of the Internet due to local policies and how to avoid it
- Algorithmic decision making that exacerbates existing power balances and ethical concerns
- How to best engage IEEE as a platform for contributing to the resolution of these and related issues