

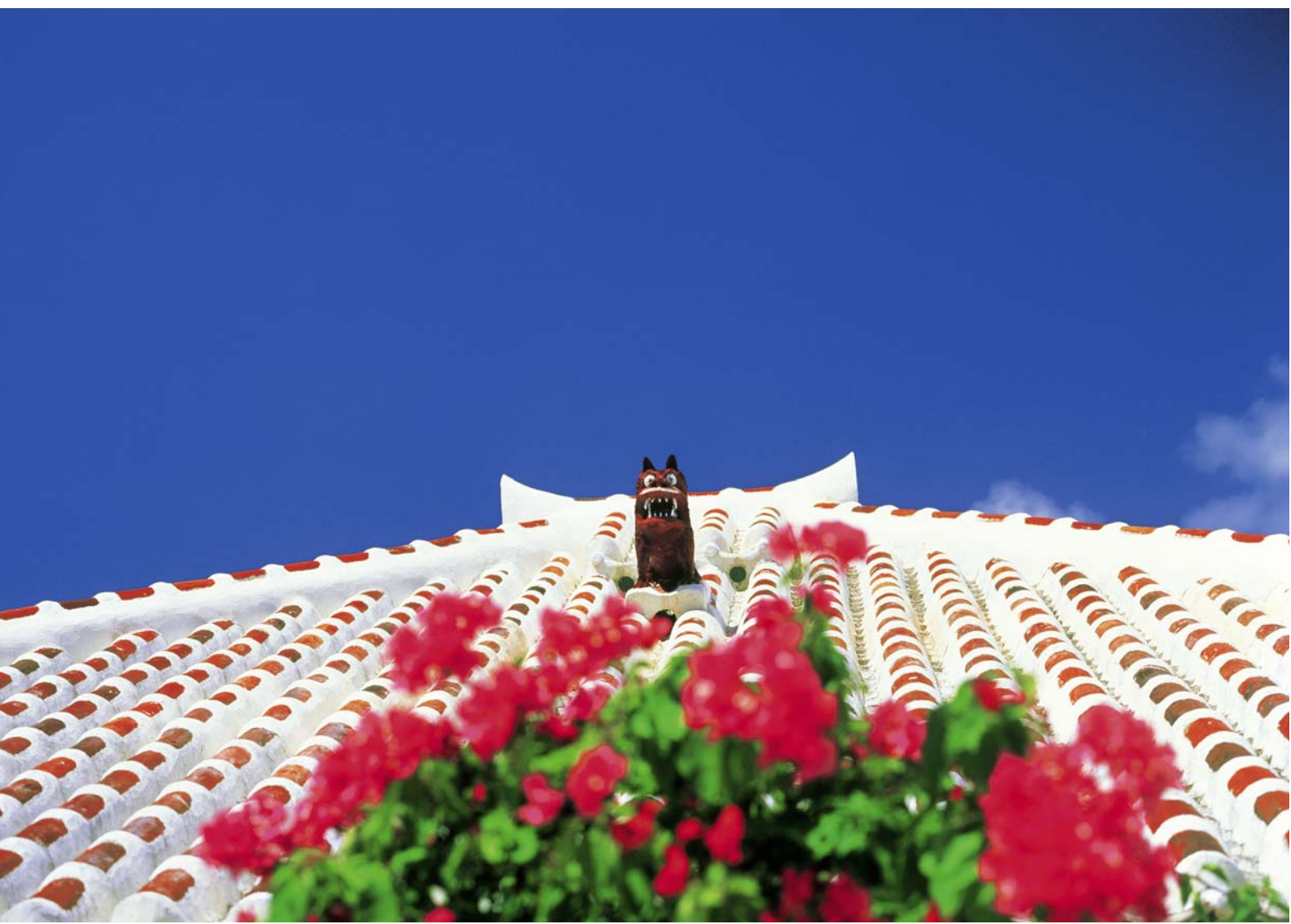


Cabinet Office, Government of Japan
with the support of the World Economic Forum

Cyber³ Conference Okinawa 2015 Program

Crafting Security in a Less Secure World

Okinawa, Japan 7-8 November 2015



INDEX

Greetings	03
Meeting Overview	06
Session Program	14
Speaker's Biographies	38
Venue Map	52
Acknowledgments	55
Useful Information	56

Greeting from Minister Aiko Shimajiri Government of Japan - Conference Organizer

Welcome to Okinawa.

In recent years, Information and Communication Technology (ICT) has been developing rapidly, with both cheap and fast Internet becoming common around the world. Big data analytics has also made great strides, while “things” are now increasingly connected to the Internet.

Cyberspace is full of possibilities and there is no doubt that it is essential for economic activities now and will be so in the future. However, there are also many cases of criminal use of information and property. Therefore, we need to prevent cyber attacks from disrupting society.

In this context, Japan will strive to make the maximum effort to develop a “free, fair and secure cyberspace” for all.

In addition, Japan recognizes cybersecurity as a very important issue from the viewpoint of protecting personal information. This becomes increasingly important as we are now discussing ways to form an international medical data cluster in Okinawa.

Today’s Okinawa has “an overwhelming geographical advantage” thanks to its location in the center of East Asia. More importantly, as the name of this convention center, Bankoku Shinryo (“to bridge the world”), suggests, Okinawa understands and has cherished the value of connecting the world since the 14th century. Therefore, it is an ideal place for discussing how to secure and enhance the global cyber network.

I am happy to say that Okinawa continues to grow, particularly in terms of its excellent business environment, which is well suited to a wide range of IT industries, as evidenced by the IT industry cluster that has already sprung up here.

I hope that all of you will enjoy your stay and have an opportunity to experience the charms and relaxing atmosphere of Okinawa.



Aiko Shimajiri

Minister of State for Okinawa and Northern Territories Affairs
Minister in charge of Information Technology Policy
Minister in charge of “Cool Japan” Strategy
Government of Japan

Letter from Professor Klaus Schwab World Economic Forum - Conference Supporter



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

Professor Klaus Schwab
Founder and Executive Chairman

Greetings and Best Wishes for a Successful Conference

We are on the cusp of a technology revolution unlike anything humankind has experienced before. In this new Industrial Revolution, we are witnessing profound shifts in numerous industries, marked by the emergence of new business models, the disruption of incumbents and the reshaping of production, consumption, transportation and delivery systems. On the societal front, technology is driving paradigm shifts in how we work and how we communicate, as well as how we express, inform and entertain ourselves. Governments and institutions are also being reshaped, as are systems of education, healthcare and transportation, to name a few.

The Cyber³ Conference is at the forefront of this new industrial revolution. I therefore very much welcome the meeting. Such global dialogues are necessary to understand the issues, formulate solutions, and drive actions and impact.

The changes are so profound that, from the perspective of human history, there has never been a time of greater promise, and also of potential peril. While we do not yet know how the transformations driven by this Industrial Revolution will fully unfold, it is clear that all stakeholders of society – governments, business, academia, and civil society – have a responsibility to work together to better understand what is happening and what the possible implications are.

A handwritten signature in blue ink, reading "Klaus Schwab". The signature is fluid and cursive, with a large initial 'K'.

Greeting from William H. Saito

Cabinet Office - Government of Japan Conference Chair

Welcome to Cyber³ 2015

It is no accident that the Japanese Government has decided to organize an international conference on the interconnected topics of cyber security, cybercrime, and the rapidly evolving, hyper-connected “Internet of Things.”

With the fastest aging and fastest shrinking population in the world, Japan is racing towards this new digital frontier in order to respond to the challenges of its changing demographics. New industries have already emerged, while traditional firms have no choice but to embrace ICT and to leverage the power of the Internet to support their global competitiveness.

Furthermore, in just a few years Japan will be hosting the Olympic Games. The 2020 Tokyo Games will be an “all-digital” Olympics, the first with more sensors than spectators. How competently Japan handles this challenge will be on public display 24/7, as the Games will shine the spotlight of global attention on this “high tech” nation and reveal to the world how well it is making the transition from old-style Internet thinking towards the new, hyper-connected Cyber Century.

The enormous promise of this increasingly connected universe and the potential benefits of the Internet of Things (IoT) are staggering, and so is its potential for misuse and abuse. The only sensible way forward is to design a cyber environment that is reliable, usable, affordable, and secure. We are now at a crucial turning point in the history of the Internet, and this task – making it secure – is the most important thing we can do, bar none.

To find the necessary balance to accomplish that requires a multi-stakeholder dialogue that brings together various disciplines to re-think the essence of “security” in terms of varied perspectives, contexts, and goals. Having a wide variety of viewpoints not only helps to articulate the problem, but through the constructive exchange of ideas, will naturally promote mutual respect and cooperation.

My sincere hope is that the Cyber³ Conference will foster real discussion, dialogue, debate, and even arguments. I hope that everyone, speakers and participants alike, will actively contribute to make this shared resource called the “Internet” even more productive than it is today.

I am delighted that the Japanese Government has seen the value in supporting such a landmark event; I am also very grateful to Professor Klaus Schwab for his support, and to the World Economic Forum for contributing both its convening power and its extensive knowledge in this vital area. Thanks to the enormous body of information the Forum has already compiled, we can avoid repeating old discussions and make real progress in these key areas.

Finally, I am personally honored to be here, at this crucial turning point in digital history, to welcome you, one and all, to the first international Cyber³ Conference.



William H. Saito

Special Advisor, Cabinet Office - Government of Japan;
Global Agenda Council - Cyber security, World Economic Forum

Meeting Overview

06

The language of the Conference will be English and simultaneous translations will be provided from English into Japanese.

In principle, all discussions will be open and “on the record.” If a moderator and panel believe that a particular session should not be on the record, that condition will be explicitly stated at the beginning of such a session and it will then be held under the “Chatham House” Rule.

Background

No technology in history has succeeded in connecting both people and things as effectively as the Internet. Yet the changes brought by yesterday's Internet will soon be overshadowed by the growth of a vastly larger, more complex universe of connectivity. As the size, distribution, and functionality of the Internet of Things (IoT) continue to grow, this vast, unseen web of "**Cyber Connection**" will change our world faster than anyone, even experts, can grasp. The IoT is a transformative development that will change the basis of competition, redraw industry boundaries, and create a new wave of fundamentally disruptive companies. Yet most organizations, both public and private, are still struggling to understand its implications.

In theory, the larger the network grows and the smarter its devices become, the more useful and beneficial it will be. Data is the currency of this new economy. By leveraging vast streams of data, users can apply powerful analytics to improve real-time decision-making, and thus create better outcomes for individuals, businesses, and even whole industries. Already, commercial, industrial, medical, governmental, and other applications have taken advantage of this expansion of cyberspace, and the flood of data from connected devices continues to grow. Within the next few years, the IoT will become ubiquitous, and the distinction between online and offline realms will disintegrate.

This hyperconnected world has the potential to be an unprecedented boon for all humankind. However, whether or not it achieves that potential ultimately rests on one essential condition — **Cyber Security**. Especially in the context of IoT devices, cyber security will play an essential role in ensuring the stability and reliability not just of individual systems, but of the entire, interconnected global economy. The IoT will continue to grow exponentially larger and more complex in line with Moore's Law. Yet the success of this massive network will not be measured simply by sheer numbers. It will ultimately be evaluated in terms of the usability, reliability, and trustworthiness that the system generates while providing benefits to society. Creating that trustworthiness is the function of cyber security. Organizations at all levels worldwide need new security frameworks that span the entire cyber physical stack, from device-level authentication and application security, to system-wide assurance, resiliency, and incidence response models. A cooperative global security effort, with shared threat intelligence and rapid dissemination of best practices, will be the necessary foundation for any future built with the IoT.

Without this, there will be a dramatic increase in **Cybercrime** that will effectively undermine that foundation. Cybercriminals are already mimicking real-life criminals, but in an even more sophisticated digital form. We have already seen examples of cross-border blackmail and grand larceny, and it is only a matter of time until they graduate to crimes of violence against individuals. Beyond that level, cybercrime becomes cyber terrorism, targeting large groups of people or critical infrastructure (power plants, dams, financial networks, etc.), which can cause everything from economic collapse to widespread loss of life. This is a particularly frightening aspect of our increasingly connected world. Digital 0s and 1s don't make distinctions among users or targets. Some of the tools of cyber terrorism and high-level cybercrime may require an initial, well-funded genius to develop but little or no intelligence to replicate and execute. One man's million-dollar cyber weapon is just a copy/paste away from becoming a teenager's toy. And our interconnected world means a criminal actor in one location can leverage the asymmetric characteristics of digital systems to wreak havoc anywhere on the planet.

Three Linked Themes

Although the Conference features three apparently separate themes, the three are closely interconnected and interdependent. The inexorable growth of **Cyber Connection** has the potential to become an unequivocal good for society, or it can easily lead to a host of new, quite serious problems. That outcome hinges on a new, globally coordinated approach to **Cyber Security**, for without a new security paradigm involving genuine global co-operation, we will open the door to a new wave of **Cybercrime**.

Some people argue that global standards are impractical, that global coordination is fine in theory but impossible in practice, or that global multi-stakeholder solutions cannot work effectively. And yet, as a multi-national society we have dealt with other, rapidly developing “connection” technologies in the past, e.g., air travel, that demanded nothing less than global standards, global information sharing, and multi-stakeholder co-operation to avoid catastrophe, and the results have been spectacularly successful. Obviously, the world of Cyber³ is growing much, much faster than air travel, telephones, or anything we have known before. This makes it all the more imperative that we become aware of the attendant risks if we do not achieve at least the same level of global co-operation that we have employed in the past to deal with non-cyber challenges.

In summary, the natural logic connecting the three pillars of Cyber³ and the implications arising from that logic are a subject that cries out for immediate attention. For that reason, with the support of the World Economic Forum, the Cyber³ Conference will be held under the auspices of the Government of Japan, as a first step toward understanding and responding to the challenges of the new cyber universe, not only by governments and corporations, but through genuine dialogue with multiple levels of stakeholders. That is one vital element that has not been sufficiently addressed in the past but will be a primary focus of this Conference.

Approach

The Conference will naturally focus on technology, but even more importantly, on practical policy-making and developing cooperative approaches and norms by engaging CEOs, academic experts, and senior government officials from around the world. Internet issues can no longer be separated into “Track 1” (government-related) or “Track 2” (private sector) dialogues, but requires a hybrid “Track 1.5” (multi-stakeholder) approach, which is exactly what we hope to achieve.

Another critical problem is the lack of communication between leadership, management, users, developers, implementers, and engineers in any large organization. Engineers are far removed from considerations about policy, regulations, and financial constraints, while management tends to focus on immediate financial priorities rather than worst-case security scenarios. At the same time, lawyers, academics, and IT vendors are all contributing to the dialogue, but often with very narrow views of the problem. This Conference aims to bridge the gap between political leadership, corporate management, policymakers, researchers, threat intelligence analysts, and engineers. Our goal is to promulgate the essential technical and policy requirements needed to increase security and build a resilient, trusted cyberspace.

Goals

The success of this conference will be measured in part by how well it contributes to achieving meaningful discussion in specific areas such as:

Measures to counter cybercrime — better networking among leading corporations, national governments, and other private-sector entities to fight the explosion of cybercrime

Regional ties — the participation of multiple Asian nations should lead to enhanced dialogue in the region, which is vitally important to regional stability

Multi-stakeholder dialogue — this event will support the development of improved cyber security policies and governance through the co-operation of governmental, civil (but non-governmental), and private sector organizations.

Increasingly secure technology architectures — together with the inexorable increase in the complexity of interconnected systems, it is essential to reduce the vulnerability of new technology so that next three billion people (N3B) who come online will do so in a more secure and trusted environment. This also requires making efforts to patch and improve security for legacy systems, especially those used to serve critical functions.

Security by design – supporting both industry- and policy-driven promotion of new global standards for security-oriented design — specifically, designing protocols, technology components, platforms and entire systems with security concerns as an essential starting point rather than as an additional feature.

Differentiation

The Cyber³ Conference will NOT be:

A typical academic-style security conference in which participants discuss technical minutiae, algorithms, and unrealistic policy initiatives.

A typical industry-oriented conference where commercially-minded security vendors evangelize their products

A typical law enforcement-oriented conference that analyzes previous crimes and discusses appropriate responses to similar events without addressing how our borderless world poses an unprecedented challenge for traditional law enforcement notions of jurisdiction.

The Cyber³ Conference WILL be:

A multi-stakeholder event focused on multi-stakeholder solutions

A high-level conference driven by practical, productive, and meaningful discussion of urgent issues

One concrete step in a global shift toward future-oriented, cross-border co-operation on all levels

Cyber Security Track

Focus:

We will focus on 3 key areas of Cyber security: national security, global event security (e.g., the Olympic Games), and the regulatory framework for private sector business activities that are affected by cyber risk. The goal is to focus upon how organizations of all sizes and types can develop basic cyber hygiene and become more secure, how disparate organizations around the world can cooperate with each other to defend against and recover from malicious attacks, and how increased sharing of high-quality and timely information can transform inter-connectedness from today's liability into tomorrow's asset.

Examining the National Security implications of the world's dependence on the Internet. One focus of the discussion will be on the rise of Cyber as a fifth domain of war (in addition to land, sea, air, and space). Cyber has become a domain within which nation states define national interests, protect assets, conduct espionage, and wage war.

What are some of the technical and logistical factors required to carry off a successful Olympic event in today's world of Internet feeds, wireless communications, and network-based management of the event itself? Almost all large scale events, from sporting events to global summits, are becoming focal points for protests and attacks, both physical and cyber. We must consider how to protect temporary, but extremely sensitive and visible, events in an ever changing world of cyber threats.

Looking at developments in the regulatory framework of cloud computing, data breach, privacy, and threat data sharing to identify key trends and issues for the private sector. Looking at the rise of civil liability for firms that suffer a data breach caused by either an outside intrusion or insider wrongdoing. Examining calls for better sharing of threat data between private and public sector entities.

Synergies:

Panelists with extensive experience inside the U.S. Department of Defense, the NSA, and the Japanese Self-Defense Forces will interact with legal experts and cyber security experts from other nations to make sense of how cyber affects national security issues. The discussion of global event security will be led by people with hands-on experience doing security for the recent London Olympics, and they will exchange ideas with cyber experts from Australia, Europe, and Japan. The discussion of cyber's new legal paradigm will feature multiple speakers with direct knowledge of European, American, and Japanese thinking on these issues.

Cybercrime Track

Focus:

International Cooperation Today: How do national and international law enforcement agencies cooperate to respond to cybercrime threats?

How do private-sector organizations deal with cybercrime?

The current status and ongoing challenges in public–private-sector cooperation. How do disparate organizations share best-practice information to create effective cooperation?

How digital crime increasingly reflects the full range of traditional crimes, from opportunistic petty theft to brute force physical attacks with collateral damage in the real world

The need for improved attribution. If attribution can be improved, law enforcement agencies can work together to identify and arrest criminals wherever they are located

Recognizing a massive increase in detected cybercrime incidents — most of it masked by victims' reluctance to publicize or even admit to law enforcement that they have been hacked — and the advantages this provides to the criminals

Understanding the full implications of the current situation: Cybercriminals are organized, virtually ignore national borders, and easily exploit outmoded defense systems. Countermeasures are poorly organized, limited by nationalistic mindsets, and complicated by privacy and antitrust concerns, resulting in lots of talk about co-operation, but not enough action with respect to sharing best-practice information about effective and ineffective technologies. Logical conclusion: Crime is on course to expand significantly in the next few years.

The need for global stakeholders at all levels to coordinate efforts, increase their awareness of all forms of cyber threats, and to unreservedly exchange pertinent information and insights

Synergies:

Cybercrime experts from national and international organizations, both public-sector (e.g., law enforcement) and private-sector (corporate security), will engage in a productive interchange focusing on the challenges of international cooperation between public- and private-sector spheres.

Session Program

14

Day-at-a-glance

Friday 6 November

	The Busena Terrace (Hotel)			Bankoku Shinryokan (Conference Venue)			
	Lobby	La Tida	Mahae	Summit Hall	Ocean Hall A	Ocean Hall B	Sunset Lounge
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00	14:00-23:00 Registration						
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							

Friday 6 November

14:00

The Busena Terrace - Lobby

Registration Opens

Please pick up your badge at Registration on The Busena Terrace lobby.

Registration opens until 23:00 on 6th and 7:00-20:00 on 7th.

15:45-18:30

OIST Campus

OIST Visit Program

The Okinawa Institute of Science and Technology (OIST) is an interdisciplinary graduate school offering a 5-year Ph.D. program in Science. Over half of the faculty and students are recruited from outside Japan, and all education research is conducted entirely in English. OIST is conducting outstanding education and research in science and technology, which will contribute to the sustainable development of Okinawa, and promote and sustain the advancement of science and technology in Japan and throughout the world. OIST welcomes you to visit!

Day-at-a-glance

Day 1: Saturday 7 November

	The Busena Terrace (Hotel)			Bankoku Shinryokan (Conference Venue)			
	Lobby	La Tida	Mahae	Summit Hall	Ocean Hall A	Ocean Hall B	Sunset Lounge
07:00							
08:00	08:00-21:00 Registration			Conference Venues open at 8:00			
09:00							
10:00				09:00-10:45 Plenary Sessions			
11:00				11:00-12:30 Session 1			11:00-12:30 Session 1
12:00							
13:00							
14:00				14:00-15:30 Session 2			14:00-15:30 Session 2
15:00							
16:00				15:45-17:15 Session 3			15:45-17:15 Session 3
17:00							
18:00				17:25-18:40 Summary Sessions			
19:00	19:00-19:30 Cocktails						
20:00	19:30-21:00 Cool Japan Dinner						
21:00							
22:00							
23:00							

Day 1: Plenary Sessions

**Saturday 7
November 9:00-10:45**

Bankoku Shinryokan - Summit Hall

Introduction 9:00-9:05

Speaker

William H. SAITO

Special Advisor, Cabinet Office - Government of Japan;
Global Agenda Council - Cyber security, World Economic Forum

A brief introduction to the history and purpose of the Conference.

Welcome 9:05-9:25

Video Message

Shinzo ABE

Prime Minister of Japan

Prime Minister Abe has been a big supporter of the Cyber³ event from its inception and continues to express his desire for Japan to play a more active role in promoting a healthy cyber environment. We are pleased and honored to have the Prime Minister open the Conference by welcoming our guests to Japan.

Speaker

Aiko SHIMAJIRI

Minister of State for Okinawa and Northern Territories Affairs; Minister in Charge of Information Technology Policy; Minister in charge of “Cool Japan” Strategy, Government of Japan

Minister Shimajiri will make a few remarks about Japan’s stance vis-a-vis the future of Cyberspace and the role Okinawa can play in both Japan and Asia’s developing IT business.

Speaker

Shunichi YAMAGUCHI

Former Minister of State for Okinawa and Information Technology Policy, Government of Japan

Former Minister Yamaguchi was instrumental in helping to realize the Cyber³ Conference Okinawa. He will say a few words to commemorate the beginning of this event.

Day 1: Plenary Sessions

**Saturday 7
November 9:00-10:45**

Bankoku Shinryokan - Summit Hall

Moderated Panel 9:25-10:10

From Policy Conception to Implementation: Real World Hurdles in Managing the Cyber Universe

Discussants

Michael CHERTOFF

Co-Founder and Executive Chairman, Chertoff Group; Former Secretary of Homeland Security (US)

Brian D. NORDMANN

Senior Advisor, Bureau of Arms Control, Verification and Compliance, U.S. Department of State

Moderator

Nik GOWING

International Broadcaster; Former BBC Main Presenter; Global Agenda Council on Geo-Economics, World Economic Forum; Visiting Professor, Kings College School of Social Science and Public Policy (UK)

Theme

Many ideas sound attractive when they are discussed in the abstract, and even later on, at the point of drafting regulations or legislation. However, when it comes to implementing those concepts, unexpected problems and issues often arise. The panelists have all been through that process innumerable times and can speak from experience about the major hurdles in taking a concept from consensus to implementation and then the challenges of keeping it current and working under real-world conditions.

Key Questions

- What are the unique challenges when a large, slow-moving bureaucratic environment needs to influence a rapidly evolving target such as cyberspace?
- What is the biggest surprise awaiting government officials looking to create and implement new cyber policy?
- What policy hurdles must be overcome in order to bring a good idea to life as new policy?
- What are some important hints or suggestions one can proffer for implementation at the national or global level?

Day 1: Plenary Sessions

**Saturday 7
November 9:00-10:45**

Bankoku Shinryokan - Summit Hall

Speech 10:10-10:35

Speaker

Makita SHIMOKAWA

Deputy Director-General, Foreign Policy Bureau; Ambassador in Charge of Cyber Policy, Government of Japan

Japan's Cyber Ambassador will speak about the nation's stance towards cyber threats and its diplomatic policy on maintaining the openness and interoperability of cyberspace.

Speaker

Yasu TANIWAKI

Deputy Director-General, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

A senior official of NISC will talk about Japan's new "Cyber security Strategy," which was approved by the Cabinet in September.

Chair Introductions 10:35 - 10:45

Speaker

William H. SAITO

Special Advisor, Cabinet Office - Government of Japan;
Global Agenda Council - Cyber security, World Economic Forum

An explanation of the genesis of the three thematic programs or "tracks" and their interconnections, followed by an introduction of the three track chairs who will lead these parallel sessions.

Session 1A1

Our Hyper-Connected World: Problems, Issues, and Implications

**Saturday 7
November 11:00-12:30**

Bankoku Shinryokan - Ocean Hall A

Issues:

- What is the nature of the coming technology, and how can companies make better use of it, building on its opportunities and minimizing risks?
- How are business leaders reacting to the opportunities and threats of hyper-connectivity and shaping their business models? What can they learn from each other?
- Building a better hyperconnected world: How can we collectively better manage the social, political and economic consequences of digital technology?
- As the world becomes increasingly connected, what concerns will or should arise?
- What are the security ramifications of omnipresent, embedded devices?
- How should businesses respond to ensure their own safety and protect the data in their custody?

Speaker

Toshinori KAJIURA

Chair, Cyber Security Working Group,
Japan Business Federation (Keidanren)

Discussants

Ross FOWLER

Vice President, Digital Transformation and
IoE Acceleration
Cisco Asia Pacific and Japan

Soichiro MURATA

Director, Internet of Things/Fourth Industrial
Revolution, SAP Japan K.K.

Noboru KOSHIZUKA

Professor, Interfaculty Initiative in
Information Studies, The University of
Tokyo; Vice Director, YRP Ubiquitous
Networking Laboratory

Giuseppe TARGIA

Vice-President, Security Business Unit,
Nokia

Jun MURAI

Dean and Professor, Faculty of
Environment and Information Studies,
Dean, Environment and Information Studies
Faculty, Keio University

Moderator

Christopher TREMEWAN

Secretary General, Association of Pacific
Rim Universities

Session 1B1

National Security and Cyber as the Fifth Domain of War

Saturday 7
November **11:00-12:30**

Bankoku Shinryokan - Ocean Hall B

Issues:

- Can nation-states reconcile their different views on the legitimate scope of economic and government espionage?
- Establishing understood but not formally agreed parameters for espionage served the interests of both sides in the Cold War and restrained escalation to conflict in the event that a spy or agent was uncovered. Can a similar set of parameters be established for cyber espionage?
- What is the proper remedy or response for a nation that sees its businesses being harmed by economic espionage?
- Is “hacking back” a legitimate official policy?
- How should nations A and B respond to the respective intrusions?

Speaker

Dennis BLAIR

Chairman of the Board and CEO,
Sasakawa Peace Foundation USA; Former
Director of National Intelligence, USA

Discussants

John C. (Chris) INGLIS

Distinguished Visiting Professor in Cyber
Studies, US Naval Academy; Former
Deputy Director, NSA

Nohyoung PARK

Professor of Law; Director, Cyber Law
Centre, Korea University

Miroslaw MAJ

Founder and President, Cybersecurity
Foundation; CEO, ComCERT

Tatsuhiro TANAKA

Research Principal, National Security
Laboratory, Fujitsu System Integration
Laboratories, Ltd.; Former head of JSDF
communications networks

Moderator

Linton WELLS II

Distinguished Senior Research Fellow,
Monterey Cyber Security Initiative
(MCySec) at the Monterey Institute of
International Studies; Former Acting
Assistant Secretary of Defense / Chief
Information Officer (CIO), US Department of
Defense

Session 1C1

Global Law Enforcement Initiatives to Combat Cybercrime

**Saturday 7
November** 11:00-12:30

Bankoku Shinryokan - Sunset Lounge

Issues:

Legal:

- What needs to be changed /added to the Budapest Convention based on your law enforcement agency experience?
- How effective is the MLAT (Mutual Legal Assistance Treaty) in your agency's experience? What needs to be improved?

Operational:

- What is the biggest obstacle to attribution in cybercrime investigation?
- What is your country's national mechanism (if any) to exchange cyber threat information between LEAs and the private sector?
- What is your law enforcement agency's expectation of the role of an international entity (i.e., INTERPOL) and a regional entity (e.g., Europol) in the coordination of a cybercrime investigation?

Technological:

- How does your agency strike a balance between security/attribution and privacy?
- How does your law enforcement agency stay up-to-date with the latest technologies?

Speaker

Alexander SEGER

Executive Secretary Committee of the Parties to the Budapest Convention on Cybercrime, Cybercrime Convention Committee; Head of Cybercrime Program Office (C-PROC), Council of Europe

Discussants

Mike FLYNN

Former Director, Defense Intelligence Agency (USA)

Toshiaki SHIRAI

Director for Cyber Security, National Police Agency, Government of Japan

Glyn LEWIS

Director, National Coordinator, Cyber Crime Operations, Australian Federal Police (AFP)

Paul WARD

Cyber Intelligence Manager, National Crime Agency (UK), currently seconded to INTERPOL Global Complex for Innovation

Moderator

Noboru NAKATANI

Executive Director, INTERPOL Global Complex for Innovation

Session 1A2

Connected Cars, Robots, and More: The Expanding Industrial IoT

Saturday 7 November 14:00-15:30

Bankoku Shinryokan - Ocean Hall A

Issues:

- Why are AI and deep learning important to develop self-driving vehicles?
- What are the risks of smart cars, and what policy considerations are necessary for such vehicles?
- How is our traditional understanding of “robots” changing, and how will robotics evolve in the coming decade?
- How will robotics in a hyper-connected world affect industry and society?
- How is the IIoT changing existing industries and business models?
- What actions should business and government take now to ensure the long-term success of IIoT?

Discussants

Rick HOWARD

Chief Security Officer(CSO), Palo Alto Networks

Noboru KIKUCHI

President, Toyota Central R&D Labs, Inc., Japan; Director, Toyota Research Institute of North America (TRINA)

Erka KOIVUNEN

Cyber Security Advisor, F-Secure Corporation (Finland)

Tsuguo NOBE

Chief Advanced Service Architect and Director, Intel K.K.; Visiting Associate Professor, Nagoya University

Tomotaka TAKAHASHI

Founder and CEO, Robo Garage (Kyoto University); Research Associate Professor, University of Tokyo; Visiting Professor, Osaka Electro-Communication University

Moderator

Jarno LIMNÉLL

Professor, Cybersecurity, Aalto University; Vice President of Cybersecurity, Insta Group Ltd.

Session 1B2

The Olympics: Preparing for PyeongChang 2018 and Tokyo 2020

Saturday 7
November 14:00-15:30

Bankoku Shinryokan - Ocean Hall B

Issues:

- What do Japan and Korea need to learn from past Olympics?
- What are the expected changes in the Cyber world for 2018-2020 compared to 2012?
- What sort of technical platforms need to be in place to monitor for activities or events that suggest an attack is imminent or that one has already occurred and that Incident Response Plans need to be initiated immediately?
- Should an international police task force be present at the Olympics to facilitate the lawful request of IP addresses and other evidence to support law enforcement activities arising from malicious attacks against Olympic operations?
- Does lax press security represent a special threat?
- Should public Wi-Fi be completely open, with the high potential for MiTM attacks, or closed but with some kind of very easy sign-on/registration system?
- Who typically attacks sporting events such as the Olympics, and why?
- Who has ultimate responsibility to perform overall cyber-security for the Olympics—the government, the local OCOG, or the sponsors?
- How is the profile of cyber-security different between the build-up phase (i.e. planning and construction of the venues) versus the operational phase?

Discussants

Mark HUGHES

CEO, BT Security

Reinhard POSCH

Chief Information Officer, Government of Austria; Professor, Graz University of Technology

Steve INGRAM

Partner and National Cyber Leader, PwC Australia

Jun TAKEI

Director of Global Internet Policy and Standards, Intel Japan Corporation; Visiting Professor, Keio University

Moderator

Phillip MORRIS

CTO, BT Japan

Session 1C2

Industry Effort to Tackle Cyber Threats

**Saturday 7
November** 14:00-15:30

Bankoku Shinryokan - Sunset Lounge

Issues:

New legal paradigm for security – at the country level

- There has been a significant increase in cybersecurity rules and legislative proposals: from critical infrastructure protection to cybercrime over the past two years. What are the new trends?
- How do you effectively protect critical infrastructure?
- How should countries at various levels of development balance their investments in this area?

Company responsibility for cybersecurity

- What responsibilities do companies have for protecting their intellectual property and customers' personal information in their networks?
- What is the best way to ensure that companies increase the security of their systems?
- How do you ensure there is sufficient expertise to understand what needs to be done?

International cybersecurity norms and the future

- How can international cybersecurity cooperation improve the overall cybersecurity environment?
- Are there any proposed norms on the table? Are they useful?
- What will drive cybersecurity concerns in the next 10 years?

Speaker

Jeff MOSS

President and Founder, DEF CON
Communications; Member, U.S.
Department of Homeland Security Advisory
Council

Discussants

Jerry HOFF

Principal Security Strategist, Vice
President, Static Code Analysis Division,
WhiteHat Security

Christophe NICOLAS

Senior Vice-President and Head of Cyber
Services and Technologies, Kudelski
Security, Kudelski Group

Carlos MOREIRA

Chairman, Chief Executive Officer and
Founder, WISeKey SA

Howard A. SCHMIDT

Partner, Ridge-Schmidt Cyber; Former
Cyber-Security Coordinator, Executive
Office of the President of the United States

Moderator

Angela MCKAY

Director of Cybersecurity, Policy and
Strategy, Global Security Strategy and
Diplomacy (GSSD) team, Microsoft
Corporation

Session 1A3

Tomorrow's IoT: A New Global Vision of Cyber Connectivity

Saturday 7 November 15:45-17:15

Bankoku Shinryokan - Ocean Hall A

Issues:

- What lessons were learned from Industries 4.0?
- What is the Industrial Internet Consortium (IIC) achieving and what more needs to be done?
- What are the Japanese government and industry doing in terms of IoT?
- How can countries take advantage of global standardization to boost competitiveness, scalability, and speed?
- Will emerging nations take advantage of the Industrial IoT to leapfrog developed countries in building out digital infrastructure?
- Is the very rapid evolution of IoT technologies actually limiting their adoption? (Companies are reluctant to make large investments in technologies that may soon be outmoded.)
- A fully functional digital ecosystem will require seamless data sharing between machines and other physical systems from many different manufacturers. Any lack of interoperability among existing systems will significantly increase complexity and cost in Industrial Internet deployments. How can we overcome the current silo-like structure of so many of today's technology systems and promote interoperability?
- Both C-level executives and public policy-makers are poorly informed about even the current state of the IoT. How can we educate them most effectively to grasp the pros and cons of tomorrow's IoT?
- What policies/regulations will need to be discussed? What are the top priorities for policy & regulation formation (e.g., spur innovation; be responsive to change)?

Speaker

Jazi Eko ISTIYANTO

Chairman, Nuclear Energy Regulatory Agency(BAPETEN), Republic of Indonesia; Professor of Electronics and Instrumentation, Gadjah Mada University

Discussants

Raman Jit Singh CHIMA

Policy Director, Access Now

Yoshihiro KAWAHARA

Associate Professor, Department of Information and Communication Engineering, University of Tokyo

Yu-chuang KUEK

Vice-president, Stakeholder Engagement - Asia, Internet Corporation for Assigned Names and Numbers (ICANN)

Joseph Lorenzo HALL

Chief Technologist, Director, Internet Architecture project, Center for Democracy & Technology

Makiko YAMADA

Director-General, Global ICT Strategy Bureau, Ministry of Internal Affairs and Communications (MIC), Government of Japan

Moderator

Rod BECKSTROM

Former President and CEO of Internet Corporation for Assigned Names and Numbers (ICANN); Former Director of U.S. National Cybersecurity Center

Session 1B3

Developing a New Legal and Regulatory Paradigm for Security Intrusion

Saturday 7
November 15:45-17:15

Bankoku Shinryokan - Ocean Hall B

Issues:

- What responsibilities do companies have for protecting their intellectual property and customers' personal information in their networks?
- Should there be a regulatory framework to require a level of cyber-security, and if that level is satisfied, should a company be protected from lawsuits or regulatory fines in case of successful hacking of their databases?
- Should companies be required to report data breaches?
- Are there different expectations and standards in different countries?
- How do multinational companies deal with compliance in the various jurisdictions within which they operate?
- How far should healthcare institutions be required to go to protect personal medical data?

Speaker

Francisco García MORÁN

Chief IT Advisor, European Commission

Discussants

John Michael FOLEY

President, CEO and Founder of Danish Centre of IT and Cybersecurity (COPITS)

Harry D. RADUEGE, Jr.

Senior Advisor and Director for Cyber Risk, Deloitte & Touche LLP; CEO, Network Centric Operations Industry Consortium (NCOIC); Chairman, Deloitte Center for Cyber Innovation; Former Director, Defense Information System Agency (DISA),

Jim PENROSE

Senior Vice-president for Cyber Intelligence, Darktrace Limited; Former Technical Director of Intelligence Operations, National Security Agency, USA

Yoshihiro SATOH

Asia Regional Chief Privacy Officer, HP, Inc.; Former Assistant Councillor, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

Moderator

Jim FOSTER

Professor, Graduate School of Media and Governance, Keio University

Session 1C3

Building a Framework to Share Information and Threat Intelligence

**Saturday 7
November** 15:45-17:15

Bankoku Shinryokan - Sunset Lounge

Issues:

- How should concerns of liability be addressed, from participants and regulatory bodies, for those providing intelligence and those utilizing the information?
- What governance models may be the most effective for different industries and company profiles?
- How can ISAOs build membership and increase efficacy while maintaining trust among new and existing members?
- What roles should governmental and law enforcement bodies be expected to play, and how can their intelligence capabilities inform ISAOs?
- How should concerns of liability be addressed in information sharing, from participants and regulatory bodies, for those providing intelligence and those utilizing the information?
- What is the benefit to share a victim organization's incident information with competitors or other organizations?

Discussants

Clive LINES

Coordinator, Australia Cyber Security Centre; Deputy Director, Cyber & Information Security; Deputy Director, Australian Signals Directorate

Toshio NAWA

Executive Director, Senior Security Analyst, Cyber Defense Institute, Inc. (Japan)

Cheri MCGUIRE

Vice-President, Global Government Affairs and Cyber Security Policy, Symantec Corporation

Stein SCHJOLBERG

Chair of The International Think Tank on Justice, Peace and Security in Cyberspace

Moderator

David BURG

Principal, PwC Global and U.S. Cybersecurity Leader, PricewaterhouseCoopers LLP

Day 1: Summary Sessions

**Saturday 7
November** 17:25-18:40

Bankoku Shinryokan - Summit Hall

Summary Session 17:25-17:55

In a brief, lively, and interactive discussion, the moderator and panelists will summarize the key points raised during the day's three sessions. Beyond simply presenting an objective reiteration of what they see as the most important points brought out in the day's discussions, this session will explain why certain ideas stood out and why they are important for further discussion in the following day's plenary sessions.

Key questions

- Were there common issues between the tracks?
- Are there similar issues that keep coming up year after year without apparent resolution?
- What new challenges were presented here?
- What do we most need to focus on in tomorrow's Summary Presentation?

Discussants

Rex B. HUGHES

Co-Director, Cyber Innovation Network, The Computer Laboratory, Cambridge University

Hideyuki TOKUDA

Dean, Graduate SCHOOL OF MEDIA AND GOVERNANCE; Director, Ubiquitous Computing and Communications Laboratory, Keio University

Moderator

Nik GOWING

International Broadcaster; Former BBC Main Presenter; Global Agenda Council on Geo-Economics, World Economic Forum; Visiting Professor, Kings College School of Social Science and Public Policy (UK)

Speech 17:55-18:25

Japan's "My Number" System

An introduction to Japan's new Social Security and Tax Number System – commonly known as "My Number." My Number is an all-encompassing national identification system due to begin on Jan. 1, 2016. It will assign a unique number to every permanent resident of Japan, with individual implementation at the local level and data management at the central government level. This session will explain the background and goals of the system.

Speaker

Akira AMARI

Minister in Charge of Economic Revitalization,
Minister of State for Economic and Fiscal Policy,
Government of Japan

Speech 18:25-18:40

Countermeasures against threats in cyberspace

From his position as Chairperson of the National Public Safety Commission, which administers the National Police Agency (NPA), Mr. Kono will speak about Japan's "Countermeasures against threats in cyberspace."

Speaker

Taro KONO

Chairperson of the National Public Safety Commission, Government of Japan

Day-at-a-glance

Day 2: Sunday 8 November

	The Busena Terrace (Hotel)			Bankoku Shinryokan (Conference Venue)			
	Lobby	La Tida	Mahae	Summit Hall	Ocean Hall A	Ocean Hall B	Sunset Lounge
07:00	Conference Venues open at 8:00						
08:00							
09:00				09:00-09:35 Plenary Sessions			
10:00				09:45-11:15 Summary			
11:00				11:45-13:00 Summary Sessions			
12:00							
13:00	13:15-14:45 Lunch		13:15-14:45 Lunch				
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							

Day 2: Plenary Sessions

**Sunday 8
November 9:00-9:35**

Bankoku Shinryokan - Summit Hall

Welcome Address 9:00-9:05

Speaker

William H. SAITO

Special Advisor, Cabinet Office - Government of Japan;
Global Agenda Council - Cyber security, World Economic Forum

A brief greeting to open and explain the goals of the second day of the Conference.

In-depth Conversation 9:05-9:35

Interviewee

Eugene KASPERSKY

Chairman and CEO, Kaspersky Lab

Interviewer

Maoko KOTANI

Chief News Anchor, "Nikkei Plus 10" on TV Tokyo BS (satellite) Network

A "conversation" with Eugene Kaspersky, the founder of one of the world's best-known and most widely installed security products. No stranger to controversy, Kaspersky and his firm have been making headlines recently.

Session 2A1

Summary

**Sunday 8
November 9:45-11:15**

Bankoku Shinryokan - Ocean Hall A

An initial review session that brings together the key presenters from the Cyber Connection track to sum up, analyze, and discuss the main ideas from the previous day. This is a first step toward the final Summary Session that follows. Its principal goal is to clarify the most important points that came out of the three previous sessions by allowing the track leaders to discuss them objectively.

Discussants

Rod BECKSTROM

Former President and CEO of Internet Corporation for Assigned Names and Numbers (ICANN); Former Director of U.S. National Cybersecurity Center

Christopher TREMEWAN

Secretary General, Association of Pacific Rim Universities

Jarno LIMNÉLL

Professor, Cybersecurity, Aalto University; Vice President of Cybersecurity, Insta Group Ltd.

Moderator

Toshiyuki SHIGA

Chairman and CEO, Member of the Board, Innovation Network Corporation Vice Chairman, Member of the Board of Directors, Nissan Motor Co., Ltd.

Session 2B1

Summary

**Sunday 8
November** 9:45-11:15

Bankoku Shinryokan - Ocean Hall B

An initial review session that brings together the key presenters from the Cyber Security track to sum up, analyze, and discuss the main ideas from the previous day. This is a first step toward the final Summary Session that follows. Its principal goal is to clarify the most important points that came out of the three previous sessions by allowing the track leaders to discuss them objectively.

Discussants

Phillip MORRIS

CTO, BT Japan

Jun TAKEI

Director of Global Internet Policy and Standards, Intel Japan Corporation; Visiting Professor, Keio University

Linton WELLS II

Distinguished Senior Research Fellow, Monterey Cyber Security Initiative (MCySec) at the Monterey Institute of International Studies; Former Acting Assistant Secretary of Defense / Chief Information Officer (CIO), US Department of Defense

Moderator

Dennis BLAIR

Chairman of the Board and CEO, Sasakawa Peace Foundation USA; Former Director of National Intelligence, USA

Session 2C1

Summary

**Sunday 8
November** **9:45-11:15**

Bankoku Shinryokan - Sunset Lounge

An initial review session that brings together the key presenters from the Cybercrime track to sum up, analyze, and discuss the main ideas from the previous day. This is a first step toward the final Summary Session that follows. Its principal goal is to clarify the most important points that came out of the three previous sessions by allowing the track leaders to discuss them objectively.

Discussants

David BURG

Principal, PwC Global and U.S.
Cybersecurity Leader,
PricewaterhouseCoopers LLP

Angela MCKAY

Director of Cybersecurity, Policy and
Strategy, Global Security Strategy and
Diplomacy (GSSD) team, Microsoft
Corporation

Alan COHN

Of Counsel, Steptoe & Johnson LLP;
Former Assistant Secretary, U.S.
Department of Homeland Security

Moderator

Noboru NAKATANI

Executive Director, INTERPOL Global
Complex for Innovation

Day 2: Summary Sessions

**Sunday 8
November** 11:45-13:05

Bankoku Shinryokan - Summit Hall

Day 2: Summary Session 11:45-12:45

Discussants

Dennis BLAIR

Chairman of the Board and CEO,
Sasakawa Peace Foundation USA; Former
Director of National Intelligence, USA

Toshiyuki SHIGA

Chairman and CEO, Member of the Board,
Innovation Network Corporation Vice
Chairman, Member of the Board of
Directors, Nissan Motor Co., Ltd.

Noboru NAKATANI

Executive Director
INTERPOL Global Complex for Innovation

Moderator

Richard SAMANS

Head of the Centre for the Global Agenda,
Member of the Managing Board, World
Economic Forum

The three track chairs speak on behalf of the thematic tracks they have overseen during the past day and a half.

This session will summarize what their respective teams have accomplished, highlight key ideas and insights that emerged from the discussions of the previous day, and also present important suggestions from their tracks about how best to move forward in these three areas.

The moderator will facilitate the discussion by trying to draw parallels between the tracks and looking to connect dissimilar concepts in an effort to create a cohesive summary and conclusion.

In-depth Conversation 12:45-13:00

A Look Backward, A Look Forwards

Speaker

William H. SAITO

Special Advisor, Cabinet Office -
Government of Japan;
Global Agenda Council - Cyber security,
World Economic Forum

Richard SAMANS

Head of the Centre for the Global Agenda,
Member of the Managing Board, World
Economic Forum

The closing session will summarize, what was answered, what was not, and what to look forward to in the discussion of these themes next year at World Economic Forum Annual Meeting 2016 in Davos, Switzerland.

Closing Address 13:00-13:05

Speaker

Aiko SHIMAJIRI

Minister of State for Okinawa and Northern Territories Affairs; Minister in Charge of Information
Technology Policy; Minister in charge of "Cool Japan" Strategy, Government of Japan

Speaker's Biographies

38

Speaker's Biographies



Aiko SHIMAJIRI

Minister of State for Okinawa and Northern Territories Affairs; Minister in Charge of Information Technology Policy; Minister in charge of "Cool Japan" Strategy, Government of Japan

Ms. Shimajiri is a former director of the Women's Affairs Division of Japan's ruling Liberal Democratic Party. She also served as Parliamentary Vice-Minister of the Cabinet Office, Chairperson of the Committee on Environment of the House of Councillors (upper house of the national legislature), and other significant roles in government. She was appointed to her current posts in October 2015 when Prime Minister Abe created his third cabinet. Ms. Shimajiri studied in the faculty of humanities at Tokyo's Sophia University.



William H. SAITO

Special Advisor, Cabinet Office - Government of Japan; Global Agenda Council - Cyber security, World Economic Forum

An authority on encryption, authentication, and biometric technologies, Saito is Japan's leading advisor on cyber security. While still in university in the U.S., he founded a software firm and built it into a global leader in information security, earning him recognition as Entrepreneur of the Year in 1998. He later sold the firm to Microsoft, moved to Japan, and founded InT Secur, a global consultancy focused on technology-driven issues. He became a venture capitalist; a popular university lecturer; a Global Shapers Foundation Board Member, Young Global Leader, and Global Agenda Council Member of the World Economic Forum; a successful author; and an adviser to G-8 governments. Following the earthquake of 2011, he served as CTO of the Fukushima Nuclear Accident Independent Investigation Commission, which ultimately led to his current role as a policy advisor to the Cabinet Office of Japan.



Richard SAMANS

Head of the Centre for the Global Agenda, Member of the Managing Board, World Economic Forum

Mr. Samans leads the World Economic Forum's action and policy oriented multi-stakeholder initiatives on major global challenges. He is also responsible for the Forum's relations with international organizations and coordinates its portfolio of public-private partnership projects. From 2011 to 2013, he served as Director-General of the Global Green Growth Institute, a new international organization headquartered in Seoul, Republic of Korea. He led the organization's transformation from a start-up non-governmental entity to a treaty-based intergovernmental institution active in over 20 countries. Before joining the World Economic Forum, Samans served in the White House as Special Assistant for International Economic Policy to President Bill Clinton and Senior Director for International Economic Affairs at the National Security Council. Prior to that, he was Economic Policy Adviser to the Senate Democratic Leader and served in a range of roles in other public, private, and research institutions. Since 2007, he has also served as Chairman of the Climate Disclosure Standards Board, a consortium of business and environmental organizations that has established a common framework for reporting of carbon-related corporate performance and risks in mainstream reports to the investment community.

Cyber Connection Track

Track Chair



Toshiyuki SHIGA

Chairman and CEO, Member of the Board, Innovation Network Corporation
Vice Chairman, Member of the Board of Directors, Nissan Motor Co., Ltd.

Before assuming his current position as Vice Chairman of Nissan in November 2013, Shiga held several key positions in the company. After joining Nissan in 1976, he served in a number of positions in Corporate Planning and Sales operations in Asia. From 1991 to 1997, he was General Manager of Nissan's Jakarta office, responsible for much of Asia and Oceania. From 2000 to 2005, he served as Senior Vice President in charge of the general overseas market (GOM) Sales & Marketing division, and from 2005 to 2013 he served as Chief Operating Officer. In addition, he has served as Chairman, CEO, and Member of the board of Innovation Network Corporation of Japan since June 2015. Mr. Shiga holds a degree from the faculty of economics of Osaka Prefecture University.

Policy Lead



Rod BECKSTROM

Former President and CEO of Internet Corporation for Assigned Names and Numbers (ICANN); Former Director of U.S. National Cybersecurity Center

Mr. Beckstrom is an authority on cybersecurity who currently serves as an advisor to multinational companies, governments, and international institutions. He was the founding Director of the U.S. National Cybersecurity Center, the office entrusted with coordinating the Federal Government's cybersecurity efforts, and a former President and CEO of ICANN, the multi-stakeholder organization that helps keep the global Internet secure, stable, and unified. As a graduate student, he helped to create CAT•S Software, a public risk management company, in his Stanford, CA garage apartment. As CEO, he grew it into a global enterprise and took it public before successfully merging it into another global organization. He has helped in founding or funding numerous high-tech ventures, including database company Mergent Systems, Privada Inc., eMotion Inc., SV2, Kiva.org, and American Legal Net. Beckstrom is co-author of *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*, has an MBA from Stanford University, and was a Fulbright Scholar in economics at the University of St. Gallen, Switzerland.

Technology Lead



Jarno LIMNÉLL

Professor, Cybersecurity, Aalto University; Vice President of Cybersecurity, Insta Group Ltd.

Mr. Limnéll has been working with security issues for more than 20 years. He holds a Doctor of Military Science degree in Strategy from the National Defense University in Finland; a Master of Social Science degree from Helsinki University; and an Officer's degree from the National Defense University. He has published a comprehensive list of works on security issues, and his most recent book is *Cybersecurity for Decision-makers*. Limnéll served a long career as an officer in the Finnish Defense Forces and worked as Director of Cybersecurity in McAfee.

Academic Lead



Christopher TREMEWAN

Secretary General, Association of Pacific Rim Universities

Mr. Tremewan was most recently the Vice-President/Pro Vice-Chancellor (International) of the University of Auckland. He was a visiting professor at Peking University in 2007 - 2008, and a visiting fellow at Georgetown University in Washington, D.C. in 2003. He was elected a senior associate member of St. Antony's College, Oxford University, in September 1991. In 1995 he became the founding director of the New Zealand Asia Institute, which he led until 1999. Previously, he held positions as a senior consultant, executive secretary, and research director for international development organizations based in Hong Kong, Singapore, and Tokyo, respectively. Mr. Tremewan holds bachelor's and master's degrees in social anthropology from the University of Auckland, a Ph.D. in political science from the University of Canterbury, and a master's degree in public administration from Harvard University.

Secretariat



James KENDALL

Fellow for the Common Challenges Program, Executive Director, Japan-US Military Program (JUMP), Sasakawa Peace Foundation USA

Mr. Kendall's expertise includes defense and aerospace, Asia-Pacific affairs, project management, and strategic planning. A career Marine Corps officer, Kendall's last military assignment was as Senior Japan Program Analyst at U.S. Marine Corps Headquarters. He also served as the East Asia & Pacific Affairs Bureau Military Advisor at the State Department; Strategic Analyst with the Marine Corps' Strategic Initiatives Group (SIG) at the Pentagon; exchange officer at the Japan Defense Agency, Tokyo and commander of several Marine artillery units in addition to multiple staff jobs. Kendall served three overseas assignments in Japan and deployments to Somalia, Kuwait, and Iraq. During Operation Tomodachi, following the 2011 earthquake and tsunami, he was the Marine liaison to the Japanese Self Defense Forces providing disaster relief.

Prior to joining Sasakawa USA, Kendall founded Red Fox Consulting, LLC, providing analysis, advice, and insights on Asia to clients in private industry, government, and the not-for-profit sphere. He holds a master's degree in National Security Affairs from the Naval Postgraduate School in Monterey, California. He studied at St Anne's College, Oxford, and is a Distinguished Graduate of the Japan National Institute for Defense Studies, Tokyo.

Cyber Security Track

Track Chair



Dennis BLAIR

Chairman of the Board and CEO, Sasakawa Peace Foundation USA; Former Director of National Intelligence, USA

During his 34-year Navy career, Blair served in both the Atlantic and Pacific fleets and commanded the Kitty Hawk Battle Group. Among many other positions, he served as Director of the Joint Staff and also on the National Security Council. Prior to retiring from the Navy in 2002, Blair served as Commander in Chief of the U.S. Pacific Command. From January 2009 to May 2010, as Director of National Intelligence, Blair led 16 national intelligence agencies, managed a budget of \$50 billion, and provided integrated intelligence support to the President, Congress, and operations in the field.

From 2003 to 2006, Blair was president and CEO of the Institute for Defense Analyses (IDA), a federally funded research and development center that supports the Department of Defense, the Department of Homeland Security, and the intelligence community.

He has served as a director of several corporations, both public and private. He resigned from all board positions when he re-entered government in 2009. He is currently a consultant for Lockheed Martin Space Systems and the European Aeronautic Defense and Space Company, North America. Blair co-chaired the Commission on the Theft of American Intellectual Property. He is the author of *Military Engagement: Influencing Armed Forces Worldwide to Support Democratic Transitions*, published in 2013.

A renowned expert on Asia Pacific policy and issues, Admiral Blair is also on the boards of the National Bureau of Asian Research, and the National Committee on US-China Relations. He has been awarded four Defense Distinguished Service medals, three National Intelligence Distinguished Service medals, and has received decorations from the governments of Japan, Thailand, Korea, Australia, the Philippines and Taiwan.

Policy Lead



Linton WELLS II

Distinguished Senior Research Fellow, Monterey Cyber Security Initiative (MCySec) at the Monterey Institute of International Studies; Former Acting Assistant Secretary of Defense / Chief Information Officer (CIO), US Department of Defense

During his 51 years with the U.S. Department of Defense, Mr. Wells held various positions, including chief information officer (CIO) and acting assistant secretary of defense for networks and information integration. In these roles he oversaw the Department of Defense's \$30 billion budget for information technology and related areas and was responsible for enhancing the DOD's networked capabilities and support structures. From 2010 to 2014 he was a distinguished research professor at U.S. National Defense University where he also directed the Center for Technology and National Security Policy. There he initiated the Transformative Innovation for Development and Emergency Support (TIDES) that promotes sustainable assistance to impoverished, post-disaster or post-war populations worldwide. In June 2014 he left government service. At MCySec, his current research efforts focus on the relationships between cyberspace issues and Command, Control, Communications, and Computers (C4), as well as how cyberspace issues may impact, assist, or thwart humanitarian assistance or disaster relief efforts. He is a three-time recipient of the U.S. Department of Defense Medal for Distinguished Public Service. Mr. Wells is currently the Managing Partner of Wells Analytics LLC.

Technology Lead

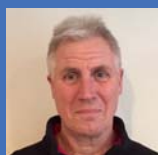


Phillip MORRIS

CTO, BT Japan

Morris is responsible for the design and delivery of large-scale, complex solutions throughout Asia, the Middle East, and Africa. His areas of specialty include cloud computing, big data analytics, IoT / Smart projects, high-performance computing, and cyber-security architecture. He has 30 years' experience in ICT and has been a recognized leader with technical expertise in security, systems & data center architecture, cloud computing, big data analytics, high-performance computing (HPC), design for efficiency (at the application, VM, ICT, and DC infrastructure levels), data center infrastructure design (1st LEED Platinum data center in Japan), and O&M (operations and maintenance). He is also a highly sought-after speaker for conferences, executive briefings, and webinars. Prior to joining BT, Morris was the CTO at Platform Computing, helping to drive them from pure HPC cluster management into cloud computing automation and management as well as an enterprise-ready version of Hadoop, providing higher availability and faster processing.

Academic Lead



Jim FOSTER

Professor of Political Economy, Graduate School of Media and Governance, Keio University

Mr. Foster also serves as Executive Director of the Keio University International Center for the Internet & Society (KICIS). He is a former Vice President of the American Chamber of Commerce in Japan (ACCJ) and a founder of that Chamber's Internet Economy Task Force. He served as a US diplomat for 25 years, with postings in Tokyo and in Brussels, and was director of corporate and regulatory affairs at Microsoft Japan before joining the faculty of Keio University. He is a graduate of the University of Notre Dame and received his Ph.D. in government from the University of Washington in Seattle.

Secretariat



William "Bud" ROTH

Senior Manager, Cyber & National Security of Public Sector, Deloitte Tohmatsu Consulting LLP

Mr. Roth brings a combination of investigative, legal, and cyber security skills to his engagements. He recently finished a 2.5-year stint with Deloitte's Tokyo practice, where he supported the defense and cyber risk teams. In Washington, D.C., he managed a cross-functional research team that investigated subjects of interest for the Department of Defense. Prior to Deloitte, Mr. Roth deployed in support of Special Forces GWOT activities in Iraq and the Horn of Africa. As an attorney, he was a founding member of the SEC Office of Internet Enforcement, investigating Internet-based securities fraud. He conducted a number of joint investigations with DoJ/FBI and was the sole SEC member on one of the 9/11 Financial Crimes Task Forces.

Cybercrime Track

Track Chair



Noboru NAKATANI

Executive Director, INTERPOL Global Complex for Innovation

Mr. Nakatani has served as Executive Director of the INTERPOL Global Complex for Innovation (IGCI) in Singapore since April 2012. The IGCI is a research and development facility for the identification of crimes and criminals, and it provides innovative training and operational support for law enforcement agencies across the globe, especially in the field of technology-enabled crime. Prior to his current post, he served as Director of Information Systems and Technology at INTERPOL's General Secretariat headquarters, overseeing the development of innovative IT services for the global law enforcement community. He also served as Assistant Director of INTERPOL's Financial and High Tech Crime unit, where he specialized in cybercrime and cyber security issues. Mr. Nakatani holds the rank of Commissioner in the National Police Agency (NPA) of Japan. Prior to being seconded to INTERPOL, he was Special Advisor to the Commissioner General of the NPA and Director of the Transnational Organized Crime Office. He was also the Senior Assistant Director for the NPA's Cyber Crime Division, with responsibility for national policy and planning in the area of cybercrime. He was the National Police Agency representative for the G8 Rome/Lyon High Tech Crime Sub-Group.

Policy Lead



Angela MCKAY

Director of Cybersecurity Policy and Strategy, Global Security Strategy and Diplomacy (GSSD) team, Microsoft Corporation

In her role with the GSSD team, she leverages her 15+ years of experience to address complex global challenges and drive strategic change, both within Microsoft and externally, to advance trust in the computing ecosystem. Ms. McKay engages internationally with industry, governments, and civil society to improve security and stability of the computing ecosystem for users around the world.

Prior to joining Microsoft, she served in several key roles at Booz Allen Hamilton supporting the Department of Homeland Security's Office of Cybersecurity and Communications. From 1999 through 2003, she worked for BellSouth Telecommunications. Ms. McKay holds a Bachelor's of Industrial and Systems Engineering from the Georgia Institute of Technology.

Technology Lead



David BURG

Principal, PwC Global and U.S. Cybersecurity Leader, PricewaterhouseCoopers LLP

Based in PwC's office in McLean, VA., Mr. Burg leads a variety of engagements around the world, including work in connection with a number of significant sensitive data breaches and intellectual property thefts, hacking events, forensic investigations, and security and vulnerability assessments for clients in a wide range of industries. In this role, he leads a team of cyber security professionals who assist multi-national businesses, private organizations, and governments to understand, plan for, and mitigate the risk of global cyber threats.

Secretariat



Lena RYUJI

External & Community Affairs Manager, Microsoft Japan

Ms. Ryuji joined Microsoft in 2007 after working first at a Japanese automotive company and later setting up Asia Pacific Academic relations and CSR operations for SAS, the world's largest private software company. Since joining Microsoft she has worked on projects such as helping to rebuild Tohoku after the East Japan Great Earthquake, supporting women in difficult societal circumstances, helping unemployed youth, and NGO/NPO capacity-building. She is multi-lingual and remains deeply interested in international relations.

Speakers / Discussants



Akira AMARI

Minister in charge of Economic Revitalization; Minister in charge of Total Reform of Social Security and Tax; Minister of State for Economic and Fiscal Policy, Government of Japan

Mr. Amari is a prominent member of the LDP, currently the ruling party of Japan. After graduating from Keio University's Department of Law, where he majored in Politics, he went to work for Sony Corporation. He later ran for political office and won a seat in the National Diet in 1983. Since then he has served as Minister of Labor, Minister of Economy, Trade and Industry, and Minister of State for Regulatory Reform. In 2012 he was appointed to multiple concurrent posts in the Cabinet of Prime Minister Shinzo Abe.



Michael CHERTOFF

Co-Founder and Executive Chairman, Chertoff Group; Former Secretary of Homeland Security (USA)

Mr. Chertoff was the second United States Secretary of Homeland Security, serving primarily under President George W. Bush, and co-author of the USA PATRIOT Act. After graduating from Harvard Law School, he clerked for a Supreme Court justice, then began working as a federal prosecutor, investigating cases of political corruption, organized crime, and corporate fraud. From 2001 to 2003, he headed the criminal division of the Department of Justice, working on several high-profile cases, including helping to trace the 9/11 terrorist attacks to Al-Qaida. He served as a judge on the U.S. Court of Appeals for the Third Circuit just prior to his work for the Department of Homeland Security. Upon leaving government service, he formed the Chertoff Group, which handles crisis and risk management. Mr. Chertoff is a graduate of Harvard College and Harvard Law School.



Raman Jit Singh CHIMA

Policy Director, Access Now

Raman Jit Singh Chima leads Access Now's team of global public policy staff in protecting an open Internet and advancing the rights of users at risk across the world. Prior to his current assignment, he served from 2010-2014 as Policy Counsel and Government Affairs Manager with Google based in Delhi and advised government, lawmakers, industry bodies, and academia on technology policy issues. He has studied Internet regulation as an independent research fellow with the Sarai program of the Centre for the Study of Developing Societies, and contributed to Freedom House's inaugural Freedom on the Internet report in 2009. He holds a Bachelors in Arts and Law from the National Law School of India University, Bangalore, where he was Chief Editor of the Indian Journal of Law and Technology.



Alan COHN

Of Counsel, Steptoe & Johnson LLP; Former Assistant Secretary, U.S. Department of Homeland Security

For the past nine years, Mr. Cohn served in senior policy and management positions at the US Department of Homeland Security (DHS). His most recent post was Assistant Secretary responsible for strategy and risk assessment, and second-in-charge overall of the DHS Office of Policy. He is currently of counsel at Steptoe & Johnson LLP, an international law firm, where he focuses on legal issues associated with cybersecurity, cybercrime, and cyber risk management issues, as well as emerging financial technology issues involving virtual currencies and the use of the blockchain. He is also president and principal of adc/strategy.works, where he provides insight and knowledge concerning complex governance and risk management challenges.



Mike FLYNN

Former Director, Defense Intelligence Agency (USA)

Gen. Flynn, an expert in national security and cyber security, is a 33-year veteran of the U.S. Army, with a long career in intelligence. He was the top intelligence advisor to General Stanley McChrystal in Iraq and Afghanistan and also served as the assistant director of National Intelligence for Partner Engagement; the director of intelligence for the Joint Special Operations Command; and was the senior intelligence advisor to the Chairman of the Joint Chiefs. He also headed the Defense Intelligence Agency, which functions as the main foreign military espionage organ in the United States. There, he pushed for greater information sharing across agencies, strengthening the cooperation between the Army, the FBI, and the CIA. Gen. Flynn holds three masters degrees and two honorary doctorates, along with numerous other awards and honors.



John Michael FOLEY

President, CEO and Founder of Danish Centre of IT and Cybersecurity (COPITS)

Mr. Foley has an academic and military background and was the key author and writer of the first Cyber Security Strategy for the Danish Armed Forces. He also assisted in establishing the first Danish National Cyber Security Center in 2012. The sharing of threat and hacking information among its member states is high on the EU's priority list, and Mr. Foley is the Danish representative at the EU's Network and Information Security Platform (NISIP), where he works with private-public partnership issues.



Ross FOWLER

Vice President, Digital Transformation and IoT Acceleration, Cisco Asia Pacific and Japan

Mr. Fowler leads Cisco's Digital Transformation and Internet of Everything (IoT) initiatives across the Asia Pacific region, leveraging his more than 40 years of technical, business, and sales leadership experience in the ICT industry. Fowler joined Cisco in 2003 from Alcatel, where he was the CEO for its Australia and New Zealand operations. In the dozen years since he joined Cisco he has held several key leadership roles, most recently as Executive Sponsor for the firm's Lend Lease relationship and the leader of Cisco's Asia Pacific, Japan and Greater China Enterprise Segment. Prior to that, he was the worldwide sales leader for the company's San Jose (US)-based Enterprise Networking and Security business, its London-based European Service Provider segment leader, and Sydney-based leader for Australia and New Zealand.



Nik GOWING

International Broadcaster; Former BBC Main Presenter; Global Agenda Council on Geo-Economics, World Economic Forum; Visiting Professor, Kings College School of Social Science and Public Policy (UK)

Mr. Gowing was a main news presenter for the BBC's international 24-hour news channel BBC World News from 1996-2014. He presented The Hub with Nik Gowing, BBC World Debates, Dateline London as well as award-winning location coverage of major global stories.

Prior to that he worked for 18 years at ITN where he was bureau chief in Rome and Warsaw, and Diplomatic Editor for Channel Four News (1988-1996). He has been a member of the councils of Chatham House, the Royal United Services Institute, the Overseas Development Institute, the board of the Westminster Foundation for Democracy, and the advisory council at Wilton Park. In 1994 he was a fellow at the Shorenstein Center of the Kennedy School of Government, Harvard University. Mr. Gowing has over three decades of reporting experience in diplomacy, defense, and international security, with analytical expertise on the failures to manage information in the new transparent environments of conflicts, crises, and times of tension. His peer-reviewed study at Oxford University, Skyful of Lies and Black Swans, which follows an earlier study undertaken at the Kennedy School, predicts and identifies the new vulnerability of institutional power in the new, all-pervasive public information space. In 2014 he was appointed a Visiting Professor at Kings College, London. Gowing was awarded Honorary Doctorates by Exeter University in 2012 and Bristol University in 2015.



Joseph Lorenzo HALL

Chief Technologist, Director, Internet Architecture project, Center for Democracy & Technology

Hall received his Ph.D. in information systems from the UC Berkeley School of Information. In his postdoctoral work (including NYU, Princeton, and UC Berkeley), he developed techniques to improve accountability mechanisms in electronic elections. Hall holds master's degrees in astrophysics and information systems and has served as an expert on independent teams retained to analyze legal, privacy, security, usability, and economic aspects of voting systems in three U.S. states. He is the Vice-Chairman of the Board of the California Voter Foundation, a director of the Verified Voting Foundation, and a member of the Federal Communications Commission's Computer Security, Reliability, and Interoperability Council (CSRIC) IV.

Hall currently works for a Washington, DC-based non-profit advocacy organization dedicated to ensuring the Internet remains open, innovative, and free. His work focuses on the intersection of technology, law, and policy, working to ensure that technical considerations are appropriately embedded into legal and policy instruments. Hall leads CDT's Internet Architecture project, which focuses on embedding human rights values into core Internet standards and infrastructure, engaging technologists in policy work, and producing accessible technical material for policymakers.



Jerry HOFF

Principal Security Strategist, Vice President, Static Code Analysis Division, WhiteHat Security

In his current role, Mr. Hoff oversees the development of WhiteHat's cloud-based static application security testing (SAST) service. Prior to joining WhiteHat, Mr. Hoff was co-founder and managing partner of Infrared Security, a leading application security professional services firm. He is an experienced application security consultant with years of professional development and training delivery. He taught for many years at Washington University's CAIT program and also in the microcomputer program at the University of Missouri in St. Louis. He is also the lead of the OWASP Appsec Tutorial Series.



Rick HOWARD

Chief Security Officer (CSO), Palo Alto Networks

Mr. Howard currently oversees Palo Alto Networks' internal security program, leads its Threat Intelligence Team (Unit 42), directs the company's efforts on the Cyber Threat Alliance Information Sharing Group, and hosts the Cybersecurity Canon Project. Prior to joining the firm he served as the CISO for TASC, the GM of iDefense, the SOC Director at Counterpane, and Commander of the U.S. Army's Computer Emergency Response Team. Rick holds a Master of Computer Science degree from the Naval Postgraduate School and an engineering degree from the US Military Academy.



Mark HUGHES

CEO, BT Security

Mr. Hughes is the person responsible for all elements of BT's global security activities. It is his responsibility to see that the company's assets – physical, logical, and information-based – are secure from attack. His security team is also charged with minimizing disruption to BT's national, regional, and global operations in the event of an incident. One of his jobs is to ensure a high level of reliability and user experience for the BT Assure portfolio, which is designed to protect customers' data and assets. He joined BT in 2002, running projects such as a partnership with the UK Government for the Criminal Records Bureau in Scotland. Prior to joining BT he was commercial director of MWB Business Exchange, and before that he was in the Army for seven years, serving in both the Falklands and Bosnia and retiring with the rank of captain. Mr. Hughes is a member of the Senior Strategic Steering Group of the Centre for the Protection of National Infrastructure (CPNI).



Rex B. HUGHES

Co-Director, Cyber Innovation Network, The Computer Laboratory, Cambridge University

In addition to co-directing the Cyber Innovation Network at the University of Cambridge Computer Laboratory, Dr. Hughes is a Visiting Professor at the University of Toronto Munk School of Global Affairs. His research examines the impact of the cyber revolution on national security and financial services. Since 2008, Hughes has advised senior NATO officials on the development of a common cyber defense policy and contributed to the cyber defense sections of the 2010 NATO Strategic Concept. At the University of Washington, he founded the first university-based Center for Internet Studies, and with IBM sponsorship, Hughes led the development of iEnvoy™, the first secure Internet communications platform for diplomats licensed by U.S. Department of State to APEC and ASEAN. Hughes holds a Ph.D. from the University of Cambridge.



John C. (Chris) INGLIS

Distinguished Visiting Professor in Cyber Studies, US Naval Academy; Former Deputy Director, NSA

Mr. Inglis was formerly Deputy Director of the National Security Agency (NSA). He holds degrees in engineering and computer science from the United States Air Force Academy, Columbia University, the Johns Hopkins University, and George Washington University. He is the recipient of three U.S. Presidential Rank Awards, the USAF Distinguished Service Medal, the Director of National Intelligence Distinguished Service Medal, and The President's National Security Medal. Mr. Inglis is currently a Venture Partner with the Paladin Capital Group in Washington, D.C



Steve INGRAM

Partner and National Cyber Leader, PwC Australia

Prior to joining PwC in 2004, Mr. Ingram was a General Manager with the Commonwealth Bank of Australia (CBA), where he was responsible for fraud- and security-related intelligence and risk management. Before that, he was the lead fraud and integrity risk consulting partner at Anderson Consulting (Australia). He has extensive experience helping corporations to manage their financial crime and corruption prevention programs, conduct investigations, and integrate risk management systems into their operations. Ingram worked on fraud and corruption prevention for the Sydney 2000 Olympics and was involved with security for the G20 Australia summit. He has authored a number of papers and presented at venues such as the 2007 APEC summit.



Jazi Eko ISTIYANTO

Chairman, Nuclear Energy Regulatory Agency (BAPETEN), Republic of Indonesia; Professor of Electronics and Instrumentation, Gadjah Mada University

Mr. Istiyanto currently serves as Chairman of BAPETEN, Indonesia's nuclear energy regulatory agency. At various times he has served as Head of the Departments of Computer Science and Electronics; Physics; and Electronics and Instrumentations at Gadjah Mada University. He also currently serves as a professor in the department of Electronics and Instrumentation and continues to supervise a number of Ph.D students. His research interests cover information security, electronic systems optimization, and embedded and cyber-physical systems. Mr. Istiyanto is a member of IET (Institution of Engineering and Technology), the Indonesian Physical Society, and the Indonesia Engineers Association. He serves as one of the Deputies (computational physics) at the Indonesia Physical Society (HFI) and also as an Honorary Board Member of the Indonesian Association of Computer Science Universities (APTİKOM). received a B.Sc in Physics from Gadjah Mada University, Yogyakarta, Indonesia, then pursued higher degrees at the the University of Essex (UK), where he received a Postgraduate Diploma in Computer Programming and Microprocessor Applications, an M.Sc in Computer Science, and a Ph.D in Electronic Systems Engineering.



Toshinori KAJIURA

Chair, Cyber Security Working Group, Japan Business Federation (Keidanren)

Mr. Kajiura joined Hitachi, Ltd. in 1981 and engaged in the development of the engineering work-station. He also developed several commercial products, including a tablet PC, the Japan postal automation system, and the domestic banking system. In 2001, he became Director of the Business Incubation Division, and later, in 2003, became involved in ICT Policy. Since 13 years ago, he has participated in KEIDANREN meetings, and now chairs the "Internet Economy Working Group" and "Cyber Security Working Group" in that organization. Mr. Kajiura earned a Master of Science degree in Computer Engineering from Nagoya University in 1981.



Eugene KASPERSKY

Chairman and CEO, Kaspersky Lab

Mr. Kaspersky is a world-renowned cybersecurity expert and successful entrepreneur. He runs Kaspersky Lab, the world's largest privately-held vendor of endpoint protection and cybersecurity solutions. He began his career in cyber security accidentally in 1989 when his computer became infected with the 'Cascade' virus. His specialized education in cryptography helped him to analyze the encrypted virus, understand its behavior, and then develop a tool to remove it. In 1997 he and a group of associates founded Kaspersky Lab, which now has more than 3000 employees and operates worldwide. Today he is well known not only as the head of one of the world's premier cyber security firms, but also as a speaker at high-profile international conferences. Kaspersky has received awards from both the Russian Federation and the People's Republic of China.



Yoshihiro KAWAHARA

Associate Professor, Department of Information and Communication Engineering, University of Tokyo

Mr. Kalahari is a founder and technical advisor of two start-up companies: AgIC, Inc and SenSprout, Inc. Among other things, he is known for inventing a new digital circuit fabrication technology titled Instant Inkjet Circuit. His particular research interests are in the areas of ubiquitous computing and the Internet of Things. He received his Ph.D. in Information Communication Engineering from the University of Tokyo in 2005 and went on to work as a visiting assistant professor at Georgia Institute of Technology and later at the MIT Media Lab.



Noboru KIKUCHI

President, Toyota Central R&D Labs, Inc., Japan; Director, Toyota Research Institute of North America (TRINA)

Mr. Kikuchi's engineering specialty is digital engineering including CAD/CAM/CAE for mechanical, aerospace, and civil engineering as well as medical applications. He is a pioneer of the Topology Optimization Method for lightweight structural design using multi-scale multi-Physics CAE in computational science and engineering. Further, he is a leading researcher for computer-aided industrial manufacturing technologies including CT scan and 3D printing. Kikuchi is the Roger L. McCarthy Professor Emeritus of Mechanical Engineering, University of Michigan, Ann Arbor. He graduated from Tokyo Institute of Technology (BS, Civil Engineering) and the University of Texas, Austin (MS and Ph.D., Aerospace Engineering).



Erka KOIVUNEN

Cyber Security Advisor, F-Secure Corporation

Mr. Koivunen's former positions include Deputy Director of the National Cyber Security Centre Finland, Head of CERT Finland, and Chief Information Security Officer and head of Elisa CERT. He holds a Master of Science (Tech) from Aalto University in Finland. He is particularly interested in how and why carefully constructed security controls fail and let attackers operate with little resistance and often without detection. Mr. Koivunen's whole professional career has been an exercise in incident-related information sharing and vulnerability coordination.



Taro KONO

Chairperson of the National Public Safety Commission, Government of Japan

Mr. Kono is a Japanese politician belonging to the Liberal Democratic Party, and a member of the House of Representatives. After working at Fuji Xerox and Nippon Tanshi, he was first elected to the House of Representatives in October 1996. He served as Parliamentary Secretary for Public Management (2002) and Senior Vice Minister of Justice (2005). In 2015 he was appointed as the present post in the third Abe Cabinet. Mr. Kono graduated from Georgetown University with the Bachelor of Science in Foreign Service.



Noboru KOSHIZUKA

Professor, Interfaculty Initiative in Information Studies, University of Tokyo; Vice Director, YRP Ubiquitous Networking Laboratory

For the past two decades, Prof. Koshizuka has been researching ubiquitous computing, Internet of Things (IoT), embedded systems, human interface technologies, and computer networks. His main research interests include IoT, linked open data, embedded real-time systems, and operating systems. Since 1990, he has been participating the now-famous TRON (The Realtime Operating system Nucleus) Project. He earned a Ph.D in computer science from the University of Tokyo, Japan.



Maoko KOTANI

Chief News Anchor, "Nikkei Plus 10" on TV Tokyo BS (satellite) Network

Ms. Kotani is one of the most familiar faces on serious Japanese television, having been a prominent newscaster on three networks during a span of more than 20 years. She holds the title as the longest-running TV anchor on any business news program for her 16-year stint as host of TV Tokyo's "World Business Satellite." She has traveled extensively and interviewed numerous top business leaders.



Yu-chuang KUEK

Vice-president, Stakeholder Engagement - Asia, Internet Corporation for Assigned Names and Numbers (ICANN)

Mr. Kuek is ICANN's vice president and managing director for its Asia Pacific hub and oversees ICANN's expansion and operations in the region. A Singapore native, he received his B.A. from Peking University (PRC), where he studied International Politics, then went to Harvard University for his M.A. Before joining ICANN in August 2013, he served as a Senior Director for Yahoo! Inc., where he led the company's public policy efforts in the Asia Pacific and Latin American regions. Mr. Kuek also has extensive government experience. Prior to joining Yahoo!, he worked for the Singaporean government. He helped with intellectual property policy development at the Ministry of Law, worked on the China Desk for the Ministry of Foreign Affairs, and served at the Singapore Embassy in Washington, D.C., where he helped to plan and implement outreach to the U.S. Congress and the White House.



Glyn LEWIS

Director, National Coordinator, Cyber Crime Operations, Australian Federal Police (AFP)

Prior to his current position, Mr. Lewis was seconded by the AFP to INTERPOL for three years. At INTERPOL he performed a number of leadership roles including that of Executive Director, Strategy & Governance; Director of Specialized Crime & Analysis; and Assistant Director of Public Safety and Terrorism. In his work for the AFP, Mr. Lewis has taken up several overseas posts, including Tonga, the U.K., India, and Kuala Lumpur, and served with the United Nations Police in Cyprus, Timor Leste, and Sudan. He also took a one-year sabbatical as a Forensic Fraud Manager at KPMG. Lewis holds a Masters of International Law, postgraduate finance, leadership and development effectiveness qualifications, and a Bachelor of Business in Management.



Clive LINES

Coordinator, Australia Cyber Security Centre; Deputy Director, Cyber & Information Security; Deputy Director, Australian Signals Directorate

Mr. Lines was appointed Deputy Director, Australian Signals Directorate in 2013. In 2015 he was appointed Deputy Director, Cyber & Information Security. He is now the Coordinator for the Australian Cyber Security Centre, and holds all three posts concurrently. Prior to these appointments, he was first assistant secretary of ICT Reform in the Department of Defence's CIO Group, and was responsible for the development and support of the Department's enterprise IT systems in the finance, logistics, military, intelligence, and corporate domains.



Miroslaw MAJ

Founder and President, Cybersecurity Foundation; CEO, ComCERT

Mr. Maj is a former leader of the CERT Polska team and was an Initiator of the Polish Civic Cyberdefence organization. Leveraging his nearly 20 years of experience in ICT security, he cooperates with the Polish Government in the field of cybersecurity and CIIP. He is a member of the Trusted Introducer team responsible for accreditation and certification of CERTs and co-author of many ENISA publications, including papers on improving CERT coordination. Mr. Maj organized cyber exercises in Poland and Georgia for the energy, banking, and telecommunication sectors. He appears frequently as a speaker at international conferences including the FIRST conferences.



Cheri MCGUIRE

Vice-President, Global Government Affairs and Cyber Security Policy, Symantec Corporation

Ms. McGuire currently leads global public policy agenda and government engagement strategy at Symantec, which includes cybersecurity, data integrity, critical infrastructure protection, and privacy. She works extensively with industry and multiple governments. She was formerly chaired the US IT Sector Coordinating Council, and is a Member of the Board of the IT Industry Council, the US IT Office in China, and the National Cyber Security Alliance. Ms. McGuire formerly held senior positions at the U.S. Department of Homeland Security, Microsoft Corporation, and Booz Allen Hamilton. She is a frequent presenter at international cyber conferences and has testified repeatedly before the US Congress.



Francisco García MORÁN

Chief IT Advisor, European Commission

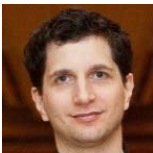
Since 1986, Mr. Morán has been working with the European Commission, and is now its Chief IT Advisor working on Digital Policies/Services and IT Security. From 2012-2013 he supervised the CERT-EU, and prior to that, served as a representative of the European Commission on the Management Board of ENISA (European Network and Information Security Agency). In 2004, he helped to create the European Commission's Directorate General for Informatics, and from 2005-2013 served as Director General of IT. He was previously the head of the IT Unit in the Corporate Data Centre of Spain's Ministry of Education and Science.



Carlos MOREIRA

Chairman, Chief Executive Officer, and Founder, WISeKey SA

Mr. Moreira began his career as a United Nations expert on IT, e-security, and trust models. From 1983-98, he worked for ILO, the UN, UNCTAD, ITC/WTO, the World Bank, UNDP, and ESCAP. He was an early pioneer in the field of digital identity. From 1995-99, he worked as Adjunct Professor and Head of the Trade Efficiency Lab, Graduate School of Engineering, Royal Melbourne Institute of Technology. In 1999, he founded WISeKey, a global specialist in online security and identity management solutions. He is a member of the World Economic Forum, where he has founded, managed, or worked on numerous projects. He is a founder of the Geneva Security Forum and Geneva Philanthropy Forum, and was named one of the 300 most influential people in Switzerland for 2013.



Jeff MOSS

President and Founder, DEF CON Communications; Member, U.S. Department of Homeland Security Advisory Council

Mr. Moss is the founder and creator of both the Black Hat Briefings and DEF CON, two of the most influential information security conferences in the world. He was previously the Chief Security Officer for ICANN. Prior to creating Black Hat Briefings, Jeff was a director at Secure Computing Corporation, where his primary work was security assessments of large multi-national corporations. However, he also helped to establish the firm's Professional Services Department in the United States, Asia, and Australia. Prior to that, Jeff worked for Ernst & Young, LLP in their Information System Security division. He is currently a member of the Council on Foreign Relations, a Senior Fellow at the Atlantic Council, and serves on the Georgetown University School of Law Cybersecurity Advisory Committee.



Jun MURAI

Dean and Professor, Faculty of Environment and Information Studies, Dean, Environment and Information Studies Faculty, Keio University

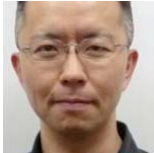
Mr. Murai has been called "the father of the Internet in Japan" and the "Internet samurai" for his pioneering work in developing Japanese networks. In 1984, three years before receiving his Ph.D. in Computer Science from Keio University, he developed the Japan University UNIX Network (JUNET). In 1988 he founded the WIDE Project, aiming to further research and develop computer networks. He is a member of the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters), chairs and serves on many other governmental committees, and is active in numerous international scientific associations. He was a Member of Internet Architecture Board (IAB) from 1993-1995, Board of trustee of Internet Society (ISOC) from 1997-2000, and a Director of the Internet Corporation for Assigned Names and Numbers (ICANN) from 1998-2000. Murai was inducted into The Internet Hall of Fame in 2013 and won the 2011 IEEE Internet Award and the 2005 Jonathan B. Postel Service Award.



Soichiro MURATA

Director, Internet of Things/Fourth Industrial Revolution, SAP Japan K.K.

Mr. Murata leads SAP Japan's Internet of Things (IoT) and Industrie 4.0 business development as a part of SAP's global IoT/Industrie 4.0 team. Most recently, he was appointed to head the Internet of Things/Fourth Industrial Revolution, an internal SAP Japan organization to facilitate customers' digital transformation. Murata has more than 20 years of professional experience in IT and business consultancy. Prior to joining SAP, he was in an IT startup for nine years, leading its business consulting division. Before that, he was in Compaq/Hewlett Packard in sales and business development roles for 10 years, including 3 years located in its then-headquarters in Houston, Texas. He joined SAP in 2011, taking various positions in the business development of SAP HANA, the in-memory computing technology that now powers more than 7,200 companies worldwide, and SAP Cloud, which now powers more than 1.7 million companies. He was the principal author of SAP - The Simple Innovator of Companies, Societies and the World, a Japanese-language book sponsored by SAP Japan (Nikkei BP Publishing, 2014). He holds an MBA from Rice University in Houston, Texas.



Toshio NAWA

Executive Director, Senior Security Analyst, Cyber Defense Institute, Inc. (Japan)

Mr. Nawa is a specialist on cyber security incident coordination/management. He has considerable experience in the development of CSIRT and Security Teams and is an expert on cyber security exercises (both discussion-based and operation-based). He is a frequent speaker in IT/Security seminars and workshops. Prior to joining the Cyber Defense Institute, he worked with the Japan Air Self-Defense Force and was the executive in charge of security in message coding/transmission. He was also responsible for liaison and coordination with U.S. Air Force in Japan, the air defense command system, etc. Later in his career, he served as a security/training division manager for a venture company.



Christophe NICOLAS

Senior Vice-President and Head of Cyber Services and Technologies, Kudelski Security, Kudelski Group

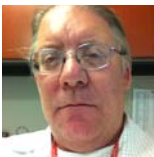
Mr. Nicolas has been with the Kudelski Group since 1996. He previously served as Chief Technology Officer (CTO) and continues to oversee Corporate IT for the Group, which offers security services and solutions to clients in Government, Financial Services, Media, and Telecommunications. He is also a member of the Management Board for the Digital TV Unit, which is in charge of security-related aspects of business and product strategy. Prior to his current positions, Mr. Nicolas held executive roles, including CTO and Chief Security Officer (CSO), at Nagracard and Nagravision. He holds a Master's degree in Computer Science from the Swiss Federal Institute of Technology, Lausanne and an MBA from IMD, Lausanne. He is a member of the IEEE Computer Group.



Tsuguo NOBE

Chief Advanced Service Architect and Director, Intel K.K.; Visiting Associate Professor, Nagoya University

Mr. Nobe joined NEC Corporation in 1983 and helped to establish the firm's global standard PC business in the U.S. and Europe, and later also in Japan. In 2001, he started the Japan subsidiary of an online gaming company. That firm's online MMORPG technology was thought to be applicable for auto-use telematics, and so, in 2004, he joined Nissan Motor Co., Ltd. At Nissan, he managed the integration of ICT for vehicles and received the Best Mobile Innovation for Automotive and Transport award at the GSM Association Mobile World Congress 2011. In 2012, Mr. Nobe joined Intel to promote the global standard Vehicle IoT architecture, with emphasis on Connected Cars and Autonomous Driving with Deep Learning. In 2014, he also took up a position as Visiting Associate Professor at Nagoya University.



Brian D. NORDMANN

Senior Advisor, Bureau of Arms Control, Verification and Compliance, U.S. Department of State

Mr. Norman is responsible for STEM policy and inter-agency integration. He has researched and spoken on the subject of the Internet of Things and Arms Control throughout the world, including at South by Southwest in Austin, as well as at Stanford University and Imperial College in London. Formerly head of the Department of State's Office of Verification and Transparency Technologies, he was responsible for administering the Key Verification Assets Fund, seeking innovative technical solutions to some of the country's most pressing national security needs.



Nohyoung PARK

Professor of Law; Director, Cyber Law Centre, Korea University

Prof. Nohyoung Park is currently Director of the Cyber Law Centre at Korea University. He graduated from the College of Law, Korea University, the Graduate School, Korea University, Harvard Law School, and the University of Cambridge (Ph.D. in International Law, 1990). His main research interests cover international economic law, negotiation, and mediation, and cyber security and privacy.



Jim PENROSE

Senior Vice-president for Cyber Intelligence, Darktrace Limited; Former Technical Director of Intelligence Operations, National Security Agency (USA)

Mr. Penrose spent 17 years at the NSA, where he achieved the rank of Defense Intelligence Senior Level, and founded the NSA Operational Discovery Center. He was the first mission manager in the NSA/CSS Threat Operations Center, served as the Technical Director for Counterterrorism in the Signals Intelligence Directorate, and was tapped to become a Technical Director in the Office of Information Operations. Jim holds a Master's in Computer Science from George Washington University and a graduate certificate in Computer Security and Information Assurance. In both 2013 and 2014, Jim was nominated for the Presidential Rank award.



Reinhard POSCH

Chief Information Officer, Government of Austria; Professor, Graz University of Technology

As CIO for the Austrian government, Mr. Posch is primarily concerned with the strategic coordination of ICT-related activities that concern multiple ministries. The CIO is the chair of the eGovernment platform "DIGITAL:AUSTRIA" that includes all levels of government. He also serves as scientific director of the Austrian Secure Information Technology Centre (A-SIT), where he is mainly concerned with cyber security, cryptography, and eGovernment. He holds the title of Full Professor for Applied Information Processing and Communications and heads the Institute of Applied Information Processing and Communications Technology (IAIK) at Graz University of Technology in Austria. In addition, Posch is chairman of the board of trustees of a non-profit foundation, the Stiftung Secure Information and Communication Technologies SIC. From 2007 to 2011 he served as Chairman of the Board of the European Network and Information Security Agency (ENISA). He has been awarded the Grand Decoration of Honor in Silver for Services to the Republic of Austria.



Harry D. RADUEGE, Jr.

Senior Advisor and Director for Cyber Risk, Deloitte & Touche LLP; CEO, Network Centric Operations Industry Consortium (NCOIC); Chairman, Deloitte Center for Cyber Innovation; Former Director, Defense Information System Agency (DISA),

Gen. Raduege works globally with clients across government and industry in reducing risk to their business and mission operations due to cyber-attacks and other unauthorized intrusions. He served for 35 years in the U.S. military in technology-related areas, including telecommunications, space, information, and network operations. His career included positions as Commander of the Joint Task Force for Global Network Operations, and Deputy Commander for Global Network Operations and Defense for the US Strategic Command. In these roles, he was the first commander assigned responsibility for directing the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across the entire Department. Prior to his last assignments, General Raduege directed command and control systems for North American Aerospace Defense Command, US Space Command, and Air Force Space Command. He also served as the Chief Information Officer for all three commands and was the architect for computer network defense and attack capabilities within the Department of Defense. He is now Senior Counselor for the Cohen Group.



Yoshihiro SATOH

Asia Regional Chief Privacy Officer, HP, Inc.; Former Assistant Councillor, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

Mr. Satoh started his career as an R&D engineer working in both software and hardware at Apollo Computer Inc. Following Apollo's 1989 acquisition by Hewlett-Packard, he did technical marketing and IT consulting for new technologies such as OSF/1, DCE, HA, and others. In the past 20 years, he has mainly focused on information security, not only from the viewpoint of technology, but also in light of IT strategy, such as enterprise architecture. Through his consulting for Japanese manufacturing, financial, telecommunications, media and other sectors, as well as for government, he has worked to establish a culture wherein organizations appreciate the critical need for an overall security policy.

As one of the original members of the National Information Security Center (NISC), he helped to design and launch an information security management system for the Japanese Government, developing comprehensive standards for information security measures. For the past decade he has also been involved in HP's own privacy protection measures. In addition, he developed METI's safeguard guidelines for Japan's personal information protection law and joined the Cabinet secretariat working group for the revision of that law.



Stein SCHJOLBERG

Chair of The International Think Tank on Justice, Peace and Security in Cyberspace

Stein Schjolberg was a prosecutor and an Assistant Commissioner of Police in Oslo, Norway. In 1984 he was appointed to serve as a judge, and in 1994 as a Chief Judge of Moss District Court, where he served until 2010. He then served as an extraordinary Court of Appeals Judge until August 1, 2013, when he retired. Judge Schjolberg is an international expert on cybercrime, and one of the original promoters of the movement for the global harmonization of computer crime legislation. He helped to organize the First INTERPOL Training Seminar for Investigators of Computer Crime in Paris in 1981. Judge Schjolberg has served as an expert on cybercrime for several international institutions and has published widely on computer crime and cybercrime legislation in addition to court technology issues. In 2007 he was appointed Chairman of the global High-Level Experts Group (HLEG) on cybersecurity by the International Telecommunication Union (ITU) in Geneva and was awarded the ITU Silver Medal in recognition of his contributions to the HLEG. He also served as Chair of the EastWest Institute (EWI) Cybercrime Legal Working Group (2010-2013) and as a member of World Economic Forum's Partnering for Cyber Resilience (PCR) project (2012-2013).



Howard A. SCHMIDT

Partner, Ridge-Schmidt Cyber; Former Cyber-Security Coordinator, Executive Office of the President of the United States

Mr. Schmidt has broad-based expertise in business, defense, intelligence, law enforcement, privacy, academia, and international relations, gained from a distinguished career spanning 40 years. Today he serves as a partner in Ridge-Schmidt Cyber, a strategic advisory firm that helps leaders in business and government navigate the increasing demands of cybersecurity. Prior to joining Ridge-Schmidt, he was the Cyber-Security Coordinator in the Obama Administration, operating in the Executive Office of the President of the United States. He also served as President of the Information Security Forum and President and CEO of R & H Security Consulting LLC.



Alexander SEGER

Executive Secretary, Committee of the Parties to the Budapest Convention on Cybercrime, Head of Cybercrime Program Office (C-PROC), Council of Europe

Mr. Seger has been with the Council of Europe (Strasbourg, France) since 1999. In addition to his role as Executive Secretary of the Committee of the Parties to the Budapest Convention on Cybercrime, he heads the Cybercrime Program Office of the Council of Europe (C-PROC) in Bucharest, Romania, which is responsible for global capacity-building on cybercrime. Before 1999, he was with what is now the United Nations Office on Drugs and Crime in Austria, Laos, and Pakistan. Seger is from Germany and holds a Ph.D. in political science, law, and social anthropology after studies in Heidelberg, Bordeaux, and Bonn.



Makita SHIMOKAWA

Deputy Director-General, Foreign Policy Bureau; Ambassador in Charge of Cyber Policy, Government of Japan

Immediately after graduating from the University of Tokyo in 1984, Mr. Shimokawa joined the Ministry of Foreign Affairs, and soon he was working in MOFA's international divisions. In 1998 he served as Counsellor of the Japanese embassy in France. In 2007 he was named Chief of Staff to the Minister for Foreign Affairs, and the following year he became Director of the National Security Policy Division. After serving as DCM at the Japanese Embassy in Indonesia, and Deputy Director-General of the Asia and Oceanic Bureau, he took up his current post in July of this year.



Toshiaki SHIRAI

Director for Cyber Security, National Police Agency, Government of Japan

Mr. Shirai is the head of cyber security at Japan's National Police Agency (NPA), which he joined directly after graduating from Tokyo University in 1991. During his career, he has worked as Director of Second Investigation Division (Hokkaido Prefectural Police), First Secretary of the Embassy of Japan in the U.K., Principal Director of International Affairs (NPA), Principal Director of Personnel Division (NPA), Director of First Security Division (Tokyo Metropolitan Police Department), Director of Public Relations Office (NPA), and Counsellor (National Security Secretariat). He was appointed to his current position in March of this year.



Tomotaka TAKAHASHI

Founder and CEO, Robo Garage (Kyoto University); Research Associate Professor, University of Tokyo; Visiting Professor, Osaka Electro-Communication University

Mr. Takahashi is widely known for single-handedly researching, developing, designing, and manufacturing humanoid robots from scratch. His designs include Kirobo (the first communication robot in space), Ropid, Chroino, FT, and many more. Evolta (featured in a TV commercial for Panasonic batteries of the same name) climbed a 1,500 foot rope to scale a cliff in the Grand Canyon, and RoBoHoN (Robo Phone), which just debuted last month, is a small personal robot that can walk, dance, and recognize faces, yet also functions as a smartphone. Takahashi leads a robot development collaboration called Team Osaka, which includes Osaka City, Osaka University, Robo Garage, and a number of private companies. Team Osaka competes in international competitions such as the RoboCup soccer tournament, and famously won the Louis Vuitton Humanoid Cup three years in a row. TIME magazine highlighted one of his creations in its "Coolest Inventions of 2004" article, and he holds multiple Guinness records for his robotic achievements.



Jun TAKEI

Director of Global Internet Policy and Standards, Intel Japan Corporation; Visiting Professor, Keio University

Mr. Takei is responsible for Internet technology, which includes cybersecurity and privacy. He served as executive officer on public policy at Intel Japan from 2011 to 2014. Based on his experience in the communications industry and as an Internet researcher, his responsibilities cover a broad scope of ICT-related policies at the company. From 2009 to 2014 he was a visiting professor at Keio University, where he taught a course in the interaction between technology advancement and policies. He has been a board member of the WIDE Project since 2004.



Tatsuhiko TANAKA

Research Principal, National Security Laboratory, Fujitsu System Integration Laboratories, Ltd.; Former head of JSDF communications networks

Prior to joining Fujitsu, Major General Tanaka served on the Japan Self-Defense Forces (JSDF) joint staff for international matters such as military exchange programs and arms control. He gained considerable experience working on bilateral matters, including planning for the first-ever US-Japan command post exercise in 1989. In the field of C4ISR, he was the first commander for the Defense Information Infrastructure (DII) Management Office, and a commanding general of the JSDF Signal School. Gen. Tanaka studied at the US Marine Corps Command and Staff College during the Gulf War, and later at the JSDF's Joint War College. He was a Fellow Researcher at the Henry L. Stimson Center and a Senior Fellow at the Harvard University Asia Center.



Yasu TANIWAKI

Deputy Director-General, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

After graduating from Hitotsubashi University in Tokyo, Mr. Taniwaki joined the Ministry of Post and Telecommunications (now Ministry of Internal Affairs and Communications (MIC)) in 1984. From 2002-2005 he served as Economic Counsellor for ICT and Telecommunications Attaché at the Embassy of Japan in the United States. He returned to MIC, where he served as Director of Competition Policy Division (2005-2007), Director of Telecommunications Policy Division (2007-2008), Director of Information Policy Division (2008-2011), Director of Policy Planning Division, Minister's Secretariat (2011-2012) and Deputy Director-General, Information and Communications Bureau (2012-2013). He has served in his capacity since June 2013.



Giuseppe TARGIA

Vice-President, Security Business Unit, Nokia

After starting his career in 1995 in Telecom Italia as an IP system engineer, Mr. Targia joined Marconi plc (now Ericsson) as System Engineer Manager in 1999, and then went to Siemens in 2002. He served as Business Development Director of the IP Architecture and Solution Department in Siemens Italy, then as Vice President of the same unit. Later, he moved to Nokia, where he became Head of Product and Partner Management of the Nokia Business Line, which covers the product & solution portfolio built around IP routing products of partner companies. In 2013 he started a special program called "End to End Security" and created the Security Business Unit that he is now heading. Mr. Targia holds a Master's degree in electrical engineering and a Ph.D in engineering from the University of Palermo and a Master in Telecommunication from Scuola Superiore Guglielmo Reiss Romoli. He completed an intensive 4-week executive program at London Business School.



Hideyuki TOKUDA

Dean, Graduate SCHOOL OF MEDIA AND GOVERNANCE; Director, Ubiquitous Computing and Communications Laboratory, Keio University

Mr. Tokuda is a professor of the Faculty of Environmental Information at Keio University.

After he completed his Ph.D. in 1983, he joined the School of Computer Science at Carnegie Mellon University and worked on distributed real-time operating systems such as Real-Time Mach and the ARTS Kernel. In 1990, he returned to his alma mater, Keio University, where his research and teaching interests include ubiquitous computing systems, decentralized autonomous systems, embedded systems, sensor networks, and smart spaces. His current research field is Information Appliances and Smart Space for the Ubiquitous Computing Environment. His research lab is working on applications, middleware, network, and hardware to realize this concept of "Smart Space." The significance of his research was recognized by the Motorola Foundation Award (1989), IBM Faculty Award (2002), Ministry of Economy, Trade and Industry Award (2004) and Ministry of Internal Affairs and Communication Award (2005) in Japan. He obtained his B.S. and M.S. from Keio University and Ph.D. (Computer Science) from the University of Waterloo, Canada.



Paul WARD

Cyber Intelligence Manager, National Crime Agency (UK), currently seconded to INTERPOL Global Complex for Innovation

Mr. Ward is a veteran of 27 years UK law enforcement, predominately in investigative roles leading pro-active national and international investigations against organized crime groups. In 2005 he joined the UK's Serious Organised Crime Agency's (SOCA) Cyber Department. During his tenure he led major cyber investigations before moving to a cyber intelligence role. He was promoted to Head of Cyber Intelligence for SOCA, and on commencement of the National Crime Agency, he developed and led the NCA's proactive Cyber Intelligence function. Mr. Ward is currently on secondment from the National Crime Agency to INTERPOL.



Makiko YAMADA

Director-General, Global ICT Strategy Bureau, Ministry of Internal Affairs and Communications (MIC), Government of Japan

Ms. Yamada joined the Ministry of Internal Affairs and Communications (MIC) in 1984. She has served in both regional and national government, holding several positions, including Deputy Mayor of Setagaya City, Tokyo (2004-2007), Director, International Policy Division (2007-2009), Director, Accounts Division, Minister's Secretariat (2010-2011), Counselor of Global ICT Strategy Bureau (2011-2013), and Executive Assistant to the Prime Minister (2013-2015). She has served in her current capacity since August 2015.



Shunichi YAMAGUCHI

Former Minister for Okinawa Affairs and Information Technology Policy, Government of Japan

Mr. Yamaguchi is a member of the House of Representatives. After graduating from Aoyama Gakuin University in Tokyo, he went to Paris to study at the University of Paris (Paris IV). He was elected to four terms in his prefectural assembly and then, in 1990, to the House of Representatives of the National Diet. In September 2014, when Prime Minister Abe reshuffled his Cabinet, Mr. Yamaguchi was appointed Minister for Okinawa Affairs and Information Technology Policy. During his term he vigorously promoted Okinawa, reformed the "Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure," and launched the Cybersecurity Strategic Headquarters, becoming its Vice Director-General. As Minister, he played a key role in supporting and realizing the Cyber³ Conference Okinawa 2015. It is largely due to his influence that the Conference became a reality.



Ichita YAMAMOTO

Member, House of Councillors; Former Minister for Okinawa Affairs and Minister for Science and Technology Policy, Government of Japan

Mr. Yamamoto studied in the Foreign Service program at Georgetown University in Washington, D.C. Upon graduation, he returned to Japan and worked for the Asahi newspaper and then for the Japan International Cooperation Agency, a government agency that coordinates development aid (ODA) for developing countries. He later transferred to the United Nations in New York. In 1995, he ran for his deceased father's seat in the House of Councillors and won. In 2012 he was appointed Minister of State for Okinawa and Northern Territory Affairs in Prime Minister Abe's Second Cabinet. It was actually Minister Yamamoto who proposed an international conference on cyber security. Without his vision and impetus there would not be a Cyber³ Conference Okinawa 2015.

Venue Map

52

Venue : Bankoku Shinryokan

Summit Hall

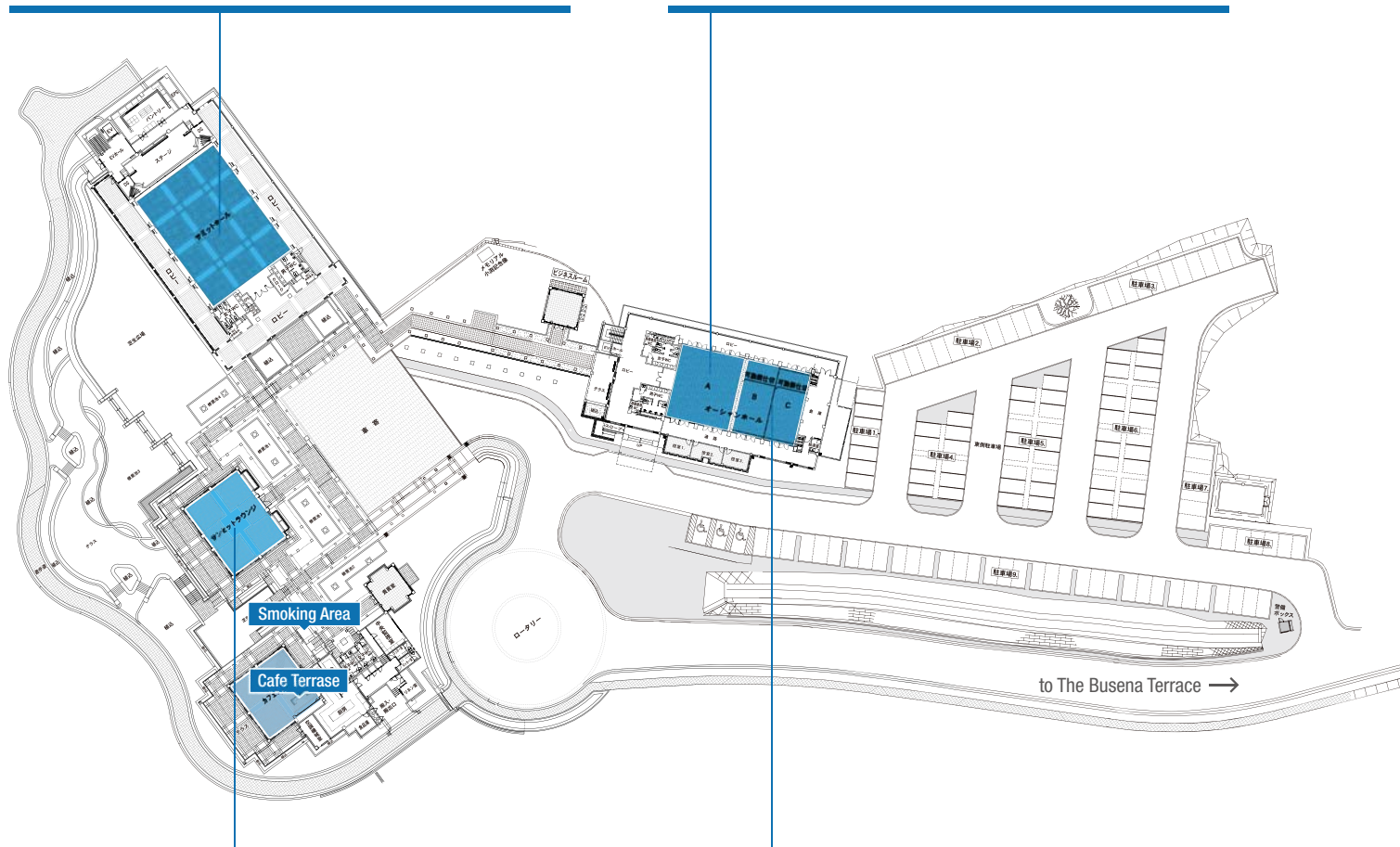
7 November 9:00-10:45 Day 1: Plenary Sessions
17:25-18:40 Day 1: Summary Sessions

8 November 9:00- 9:35 Day 2: Plenary Sessions
11:45-13:00 Day 2: Summary Sessions

Ocean Hall A

7 November 11:00-12:30 Cyber Connection 1A1
14:00-15:30 Cyber Connection 1A2
15:45-17:15 Cyber Connection 1A3

8 November 9:45-11:15 Summary



Sunset Lounge

7 November 11:00-12:30 Cybercrime 1C1
14:00-15:30 Cybercrime 1C2
15:45-17:15 Cybercrime 1C3

8 November 9:45-11:15 Summary

Ocean Hall B

7 November 11:00-12:30 Cyber Security 1B1
14:00-15:30 Cyber Security 1B2
15:45-17:15 Cyber Security 1B3

8 November 9:45-11:15 Summary

Venue : The Busena Terrace

2F



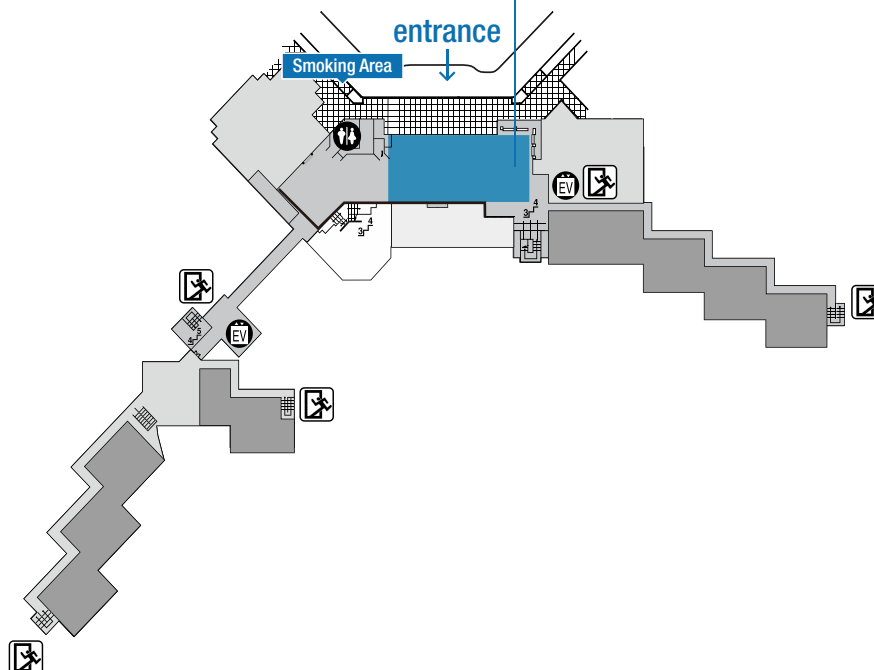
2F La Tida

7 November
19:00-19:30 Cocktails
19:30-21:00 Cool Japan Dinner

4F Lobby

6 November
14:00-23:00 Registration

4F



Acknowledgments

The Cyber³ Conference 2015 Okinawa was the first time that this kind of event has been hosted by the Japanese Government. As such, it was an enormously complex undertaking, and it could not have happened without the dedicated efforts of many people.

I would like to thank all the volunteers who worked tirelessly to share their ideas, wisdom, experience, personal connections, and enormous amounts of their time to make Cyber³ a reality. Unfortunately, we cannot possibly thank everyone who deserves it, but I do want to extend my personal gratitude first to people within the Japanese government including Shinzo Abe, Yoshihide Suga, Hiroshige Seko and Ichita Yamamoto. Furthermore, in helping plan, program and prepare this conference in tandem with the World Economic Forum, Klaus Schwab, Daniel Bob, Jim Foster, Mariko Miya, Mihoko Matsubara, Phillip Morris, Bud Roth, Lena Ryuji and Kenji Uesugi for their very special and invaluable contributions.

There are so many more names I would like to list here if I had the space – people who went above and beyond the call of duty to help make Cyber³ such a success. Instead, to each and every one of you, I will say a heartfelt Thank You.

Sincerely,

William H. Saito

Conference Chair

Useful Information

56

General Information

Conference Outline

Cyber³ Conference Okinawa 2015
-Crafting Security in a Less Secure World-

Host: Cabinet Office, Government Of Japan

Date: Saturday-Sunday, November 7 and 8, 2015

Venues:

Bankoku Shinryokan
1792 Kise, Nago City,
Okinawa 905-0026, Japan

The Busena Terrace
1808 Kise, Nago City,
Okinawa 905-0026, Japan

Participants:

Approx. 300 people including policymakers, CEOs of major companies, and leading academics from around the world.

Location Information (Okinawa Prefecture)



Okinawa consists of 160 islands stretching 400 kilometers from north to south and 1,000 kilometers from east to west, between the Pacific Ocean and the East China Sea. Naha City, the prefectural capital, is located approximately 1,500 kilometers away from Tokyo, the capital of Japan. The average flight duration from Tokyo to Okinawa is around three hours.

*Okinawa Tour Guide from Okinawa Convention & Visitors Bureau

*Okinawa-Distinctive Beauty & Culture from Okinawa Prefectural Government

Temperature

In November, Okinawa is surrounded by deeper signs of autumn with sugarcanes in bloom. It may become cloudy after a monsoon, but overall the weather is very nice.

The average lowest temperature of Naha, Okinawa, in November, is 19.9 , while the average highest temperature is 24.6 . The average humidity is 69%



Dress Code

Participation to the conference with casual style is acceptable. The traditional "Kariyushi Shirt," Okinawa's business style, is also recommended

Time

Okinawa is 9 hours ahead of GMT/UTC.

Currency (Japanese yen ¥)

as of 09 September 2015

€1	=	¥134.48
¥100	=	€0.742
\$1	=	¥120.30
¥100	=	\$0.830

Tipping

In Japan, a service charge will be included in the payment. Tipping individually to housekeeping staff and others are not required.

Electricity

100 volts and 60 hertz. A step-up transformer is required to convert the voltage.

The standard socket has two flat pins, and it is therefore advised to prepare a plug adapter beforehand.



Mobile Phone

Japan uses both the UMTS and CDMA standards for mobile telecommunications. Foreign visitors can use their mobile phones outside the national network under the international roaming system.

The Japanese country code is +81.

Travel and Transport

Visa

Regardless of your visa status, please make sure that you have a valid passport in advance. For visa requirements, please contact the nearest embassy or consulate of Japan. For contact information of Japanese embassies and consulates, please visit: http://www.mofa.go.jp/about/emb_cons/mofaserv.html

A letter for visa application can be issued upon request. Please contact Cyber³ Administration Office (*1).

Air Travel

Please confirm the procedure on “My page” of the registration website (<https://reg.cyber3conf-okinawa2015.jp>). If you have any questions, please contact Cyber³ Administration Office (*1).

Cyber³ Administration Office (*1)

Tel: +81 (0)3-3591-0731

Fax: +81 (0)3-3591-0732

Email: info@cyber3conf-okinawa2015.jp

*Hours: 9:30am to 5:30pm on weekdays (Japan time)

Flight Schedule (November 2015)

Tokyo → Naha

Haneda to Naha		Flight No.	ANA 461	JAL 901	ANA 993	ANA 463	JAL 903	JAL 905	ANA 467	JAL 907	ANA 995	ANA 469	ANA 471	JAL 909
Haneda Airport	Dep.		06:10	06:20	06:40	07:50	07:55	08:25	08:40	08:50	09:10	10:30	11:05	11:05
Naha Airport	Arr.		09:00	09:05	09:25	10:35	10:40	11:10	11:25	11:35	12:00	13:20	13:55	13:50
		Flight No.	JAL 913	JAL 915	JAL 917	ANA 473	ANA 475	JAL 919	ANA 477	JAL 921	JAL 923	JAL 925	ANA 479	
Haneda Airport	Dep.		11:35	12:20	12:55	13:05	14:35	14:55	15:50	16:25	17:25	19:50	20:00	
Naha Airport	Arr.		14:20	15:05	15:40	15:55	17:20	17:40	18:35	19:10	20:10	22:35	22:40	
Narita to Naha		Flight No.	ANA 2159											
Narita Airport	Dep.		17:55											
Naha Airport	Arr.		21:05											

Naha → Tokyo

Naha to Haneda		Flight No.	JAL 900	ANA 460	JAL 902	ANA 994	ANA 462	JAL 904	ANA 464	ANA 996	JAL 906	JAL 908	ANA 468	ANA 470
Naha Airport	Dep.		07:40	08:00	10:05	10:15	11:30	11:45	12:20	12:45	12:45	13:40	14:10	14:40
Haneda Airport	Arr.		09:50	10:15	12:15	12:30	13:45	13:55	14:40	15:05	14:55	15:50	16:30	17:00
		Flight No.	JAL 910	JAL 912	JAL 914	JAL 916	ANA 472	ANA 474	JAL 918	ANA 476	JAL 920	ANA 478	JAL 922	
Naha Airport	Dep.		14:40	15:05	15:55	16:35	16:45	18:10	18:40	19:25	20:15	20:45	21:20	
Haneda Airport	Arr.		16:50	17:15	18:05	18:45	19:00	20:25	20:50	21:40	22:25	23:00	23:30	
Naha to Narita		Flight No.	ANA 2158											
Naha Airport	Dep.		12:00											
Narita Airport	Arr.		14:30											

*Arrival and departure time, flight number, model, equipment, and operating company are subject to change without prior notification.

*If you prefer other flight schedule than the above, please contact Cyber³ Administration Office.

Cyber³ Administration Office

JTB Travel Desk

Tel: +81 (0)3-6737-9272

Fax: +81 (0)3-6737-9266

Email: C3_2015@bwt.jtb.jp

*Hours: 9:30am to 5:30pm on weekdays (Japan time)

Access to the Conference Venues

Complimentary transportation (shuttle bus) will be provided from Naha Airport to Bankoku Shinryokan and The Busena Terrace during the conference.

Naha Airport → The Busena Terrace

6 November	Naha Airport	Dep.	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00
	The Busena Terrace	Arr.	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
7 November	Naha Airport	Dep.	10:00	11:00	12:00	13:00	14:00	15:00				
	The Busena Terrace	Arr.	12:00	13:00	14:00	15:00	16:00	17:00				

The Busena Terrace → Naha Airport

8 November	The Busena Terrace	Dep.	09:00	13:00	14:00	14:30	15:00					
	Naha Airport	Arr.	11:00	15:00	16:00	16:30	17:00					
9 November	The Busena Terrace	Dep.	08:00	09:00	10:00	11:00	12:00					
	Naha Airport	Arr.	10:00	11:00	12:00	13:00	14:00					

*Arrival time may vary depending on the traffic conditions.

Access Map for Conference Venues



By Taxi

90 minutes from Naha Airport via National Route 58.
75 minutes via Okinawa Expressway.

Accommodation

Cyber³ Administration Office, the official logistics and production provider of the Cyber³ Conference, is committed to provide the most professional service to participants by securing the best available rooms and rates. If you do not yet have accommodation, please contact Cyber³ Administration Office. If the hotel of your choice is fully booked, every effort will be made to find a suitable alternative.

Cyber³ Administration Office

JTB Travel Desk

Tel: +81 (0)3-6737-9272

Fax: +81 (0)3-6737-9266

Email: C3_2015@bwt.jtb.jp

*Hours: 9:30am to 5:30pm on weekdays (Japan time)

The Busena Terrace (Cyber³ Official Hotel)

1808 Kise, Nago, Okinawa 905-0026 Japan

<http://www.terrace.co.jp/en/busena/>

Connectivity

Internet Access

Free Wi-Fi is available throughout the conference venue area.

Activities

Tours are scheduled on a first come, first served basis.
All tours are free of charge.

OIST Visit Program

Date : Friday 6 November

Time : 16:00-18:00

The Okinawa Institute of Science and Technology (OIST) is an interdisciplinary graduate school offering a 5-year Ph.D. program in Science. Over half of the faculty and students are recruited from outside Japan, and all education research is conducted entirely in English. OIST is conducting outstanding education and research in science and technology, which will contribute to the sustainable development of Okinawa, and promote and sustain the advancement of science and technology in Japan and throughout the world. OIST welcomes you to the visit!

15:45 Busena Terrace Lobby

↓  Approx. 30 min.

16:30 - 17:45

OIST (Okinawa Institute of Science and Technology)

Its objective is to contribute Okinawa's independent development and improvement in science technology worldwide, by providing education and research of an excellent global science technology.



↓  Approx. 30 min.

18:30 Busena Terrace

Churaumi Aquarium Tour

Date : Saturday 7 November

Time : 9:30-14:15

Okinawa Churaumi Aquarium is a Japan's aquarium frontier, in which the world's largest aquarium, "The Kuroshio Sea" of 7,500m³ is installed. It is a must see popular exhibition of whale sharks and manta rays, which succeeded in the world's first long term breeding.

9:30 Busena Terrace Lobby

↓  Approx. 45 min.

10:15 - 12:45

Okinawa Churaumi Aquarium

Enjoy the never-seen group swimming of whale sharks and manta rays in the world's largest aquarium, "The Kuroshio Sea."



↓  Approx. 20 min.

13:05 - 13:45

Shopping at Okashi Goten, in Nago.

Okashi Goten, is famous for variety of sweets and tarts made by "Okinawan sweet potato /purple yam." Including the main sweets by "Okinawan sweet potato," they provide various kinds of souvenirs of Okinawa.



↓  Approx. 30 min.

14:15 Busena Terrace

Shuri Castle Tour

Date : Sunday 8 November

Time : 9:00-13:30

It was registered as a world heritage in December, 2000. Its original Ryukyu architecture to fit the climate of Okinawa is a mixture of Chinese and Japanese architecture, which is the largest wooden building in Okinawa. It was a residential castle of the king of Ryukyu Kingdom. It is a must see sight to understand its continuously flourished history of politics, foreign diplomacy, and culture.

9:00 Busena Terrace Lobby

↓  Approx. 60 min.

10:00 - 11:00

Shuri Castle

Center of Shuri Kingdom Government and residence castle of the King and the family, which governed Ryukyu Islands and developed foreign diplomacy and trades among Asian countries.



↓  Approx. 30 min.

11:30 - 13:00

Kokusai Street

Street which lies 1.6 km from the front of Okinawa prefectural government. Various shops of Okinawa style, such as t-shirts, Kariyushi wear, Awamori, and sweets stand aside on both side of the street.



↓  Approx. 30 min.

13:30 Naha Airport

Please contact JTB Travel Desk for a tour request.

Cyber³ Administration Office
JTB Travel Desk

Tel: +81 (0)3-6737-9272

Fax: +81 (0)3-6737-9266

Email: C3_2015@bwt.jtb.jp



Cyber³ Administration Office

Tel: +81 (0)3-3591-0731

Fax: +81 (0)3-3591-0732

Email: info@cyber3conf-okinawa2015.jp

*Hours: 9:30am to 5:30pm on weekdays
(Japan time)

*Your inquiry may be answered the
following day, depending on the time it
is received.

*Inquiries will be accepted until Mon. 30
November 2015.