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

Cyber³ Conference Okinawa 2015

Crafting Security in a Less Secure World

Okinawa, Japan 7-8 November 2015

INDEX

I. 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 continue to blur.

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 as its components grow more capable and connected. Yet the success of this massive network will not be measured 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 physical-logical-network-applications environment, from device-level authentication and application security, to system-wide assurance, resiliency, and incident 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. Achieving this will require a serious, sustained, high-level commitment by all parties.

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 even more sophisticated digital forms. 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 can be used by terrorist, targeting large groups of people or critical infrastructure (power plants, dams, financial networks, etc.), which can cause everything from severe economic disruption 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 which are used by terrorists 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 attack tool is just a copy/paste away from becoming a teenager's toy. And our interconnected world means a criminal actor or terrorist in one location can leverage the asymmetric characteristics of digital systems to wreak havoc anywhere on the planet.

This document summarizes the discussion in the Cyber³ Conference Okinawa 2015, which does not represent the view of the Government of Japan.
Please refer to the NISC's website in terms of the government's policy on cybersecurity in Japan.
http://www.nisc.go.jp/
http://www.nisc.go.jp/eng/index.html

II. Executive Summary
A) Cyber Connection

Education

There is a vital need to educate industry stakeholders, governments, and consumers about the IoT – both its opportunities and risks. Currently, there is a widespread lack of public trust regarding new technology paradigms. We must accept (and explain) that there is an unavoidable risk-benefit balance: As benefits increase, so does risk.

Artificial Intelligence (AI) and automation technologies can make the public's lives safer and more comfortable – but companies must earn trust and foster understanding. By 2020, 15-20 billion devices will be connected to the Internet through a seamless cloud. No one, not even technologists, fully grasps the enormity of that coming reality. How do we educate the public in a meaningful way? Humans interface with technology without thinking about it, and the amount and nature of personal data is constantly changing, so even user education aims at a moving target. As consumers become able to clearly identify and understand the benefits of new technologies, they naturally begin to accept those technologies (e.g. Web mail — no one thought it was safe when it was introduced; now no one can live without it). The same trend will continue with the IoT, and this will generate a new wave of digital data about users.

Creating structure

For this reason, it is essential to determine an architecture for the IoT. The biggest point, from a security standpoint, is to develop resilience in order to prepare for unknown threats. One of the speakers calls this "thinking the unthinkable." It means assuming that some threats are unstoppable, so rather than trying to defend against every possible unknown, we need systems that can sustain intrusion ("be hacked") and keep on functioning with minimal inconvenience.

In the future, network users will no longer be only humans—robots and AI systems are becoming part of the cyber universe. The Internet must be equipped to manage interfacing with IoT devices smoothly, not just the other way around. Autonomous systems can be attacked and compromised, so they must have defense mechanisms that can operate—at least at some level—without human intervention.

The IoT, by definition, implies a massive increase in data being collected and transmitted. With that increase in the volume of data, there is a concomitant increase in vulnerabilities. Hence, the IoT will usher in a new era of multifaceted vulnerabilities.

How can multi-stakeholder dialogue create processes that will foster genuine cooperation, deal with national regulatory regimes encumbered by problematic relationships, and ultimately, deepen public trust? It is essential to establish a shared-goal-driven, multi-stakeholder network to develop regulations and security standards for the IoT; we need to find a

workable balance between unfettered access and extremely limited innovation. This can only be achieved through the active cooperation of a body of diverse stakeholders.
Furthermore, the IoT can maximize and optimize device functionality, benefitting people by providing contextual experience and enabling mass customization. At the same time, we have to address the necessity of building security into every element of these future networks. The "hyper-connected" world also means that closed/protected innovation will give way to open innovation. Data is becoming the new currency in the age of the IoT. More data is being produced than ever before; analyzing and leveraging that data is a key challenge for the future.
For industrial IoT security, the security of a whole chain must be ensured by a group of diverse stakeholders. Resilience is key to preparing a secure IoT future; anything that can be hacked will be hacked. Even non-networked systems (e.g. voting machines) are at risk. Back-up systems must be in place to mitigate this. Barrier-based (purely defensive) protection is already becoming obsolete. The best security model is something like the human body's immune system: a complex system that sustains myriad attacks daily, but manages these attacks through flexible responses so as to preserve functionality with minimal impact at the day-to-day level. Like the body, a healthy (resiliently secure) system should function for many years without sustaining any serious damage despite constant malware intrusions.

Human factors and the moral dimension

There are undeniably serious questions of privacy, human rights, and legal/moral responsibility with regard to the IoT and AI. We must consider what is the best approach to regulating the IoT. On the one hand, a non-regulated world would be a frightening, unusable "jungle," but on the other hand, we could easily create an over-regulated "nanny state." Liability must be clearly established in the event of an attack or accident involving autonomous devices. In order to make AI effective, we must study human decision-making and interaction and apply these insights to our technology. Ultimately, the solutions to current and future issues are not just technical, but social, political, and economic.
The IoT could provide increased access and freedom to users in emerging markets, but in emerging economies technology tends to be more expensive than human resources, and IT governance is more lax. We must ensure that knowledge creation does not merely replicate the current state of economic and social inequality, and will bring tangible benefits to all, not just those who can afford them. Finally, the IoT must not cause damage when implemented in user-based applications (home, office etc.). The digital Hippocratic Oath of the IoT should be, "First, do no harm."

II. Executive Summary
B) Cyber Security

Cyberspace as the fifth domain of war

Traditional precepts of war, such as proportionality and mutual assured destruction, are less applicable to nation state activities within the realm of cyberspace. While cyber attacks could conceivably cause the same degree of massive destruction as a nuclear or biochemical attack, this is an unlikely scenario. A cyber attack can have a much narrower focus than a nuclear or chemical attack. This helps explain why nation states have been willing to engage in aggressive cyber activities. Nations that have refrained from using tactical nuclear or other weapons of mass destruction may be willing to consider cyber warfare. On the other hand, shared use of Internet infrastructure by military and civilian users makes it difficult to distinguish military from civilian targets and to predict the extent of collateral damage. This problem is compounded by uncertainty over the secondary and tertiary impacts of an attack. Moreover, the technical difficulties in conclusively identifying the source of an online attack make traditional risk calculations hard to apply when evaluating options to deal with a cyber adversary.

Many nation states are actively engaged in cyber espionage as well as limited amounts of more offensive activities. Establishing common “rules of the road” (along the lines of the “Gentleman’s game of espionage” during the Cold War) is an essential step if nations are to avoid an accidental escalation of cyber activities into a full-fledged cyber war. The relative ease with which a cyber attack tool can be developed or deployed by a non-state actor further increases the need for nation states to establish common understandings, whether formal or informal, as to what kind of behavior is acceptable.

Viewed in the most general sense, the idea of nations-in-conflict working out an overarching agreement as to what types of cyber activities are permissible and what types are not seems unlikely. However, when the problem is broken down into discrete issues, specific areas of common concern and common values can be tackled first. Over time, we believe that it is possible to make progress toward establishing a multilateral dialog on nation state cyber activity that will contribute to stability and security for all parties and, equally important, their citizens.

International law makes no distinction between cyber war and other forms of war, so existing laws pertaining to cross-border conflicts can be brought to bear. Attribution is a crucial element of any response, so more effort should be put into developing capabilities that will assist nations in identifying the origin of attacks. There are 3 critical areas where nations can enhance their attribution capabilities: better technology, better threat-data sharing, and shared intelligence assessments of adversaries. Without this, nations will not be able to differentiate between activities by other nations and those by non-state actors, nor will they be able to respond appropriately to either. In fact, identifying threats from non-state actors might be one area where traditionally hostile superpowers could find a level of common interest, and that could facilitate the process of

establishing rules. In the immediate future, these nations should identify mutually agreed-upon sensitive areas — nuclear plants, financial systems, etc.—that all parties will agree are off limits to cyber attack. Agreements not to violate each other's most sensitive infrastructure are only part of a bigger picture that needs more development.

Cyber defense is really the first concern of nation states in the cyber realm. Threat-data-sharing mechanisms (both government-to-government and two-way public-private) can contribute to a nation's ability to fend off attacks. To be useful, however, these mechanisms must allow for the collection and sharing of meaningful data upon which groups can act. Otherwise, the data sharing becomes of little value. While destructive retaliation should remain a tool of sovereign powers only, there is also room for the private sector to assist in responding to attacks through tool development and network management.

Firms that are hacked have a right to self-defense, but it is unclear whether that right extends to hacking back, particularly when that involves destroying or disabling the hacker's assets. While there have been maritime privateers in the past who had permission to hunt down and destroy an adversary's ships, it is not clear that such behavior is possible, much less desirable today in the cyber realm. There are other steps that must be taken as well. Building resilient systems that move the most sensitive or volatile elements behind multi-tiered defenses is essential.

The issue of economic espionage is particularly difficult because it requires nation states to reach agreements in an area where normative values are not shared among major powers. Indeed, the scope of economic espionage itself can be called into question. For example, the use of state-sponsored economic espionage by a nation engaged in trade negotiations could prove beneficial to companies based in that nation if it succeeds in gaining privileged access and insight into a rival's negotiating position. These difficult issues can only be solved if countries are willing to engage each other in bilateral and multilateral forums and begin the process of finding common ground.

Olympic security

The security team for the London Organising Committee of the Olympic and Paralympic Games (LOCOG) dealt with five distinct networks, each of which required its own security architecture:

– the LOCOG operator's corporate Local Area Network (LAN)
– the scoring network that transmitted scores and game data
– the press network
– the broadcast network
– a public access WiFi network

The network operators installed the usual firewalls, IDS, and anti-virus defenses, but in addition, they created a big data analytical machine that sampled traffic and looked for less obvious signs of ongoing intrusions. The number of attacks registered—11,000 per second—required a huge amount of processing power. More importantly, it required planning, practice, and a firm grasp of the full nature of the risks faced—by the Olympic village, by its sponsors, the visiting dignitaries, and the nation as a whole. The London Olympic security team engaged in a massive planning effort, which included prioritizing what needed protection. It also required a deep look at governance and an understanding of the roles and responsibilities of the various local actors—venue security, network security, police, etc. It also meant identifying the populations of visitors, contractors, press, and others that use Olympic network assets and the problems and risks that they bring. For example, logs showed malware activity emanating from devices brought onsite not only by visitors, but by press as well. Understanding these risks and dealing with them by such things as network segmentation is critical.

LOCOG and the UK Government initiated a number of new efforts that facilitated their ability to respond rapidly and effectively to emerging threats. They established solid partnerships with the security services of nations expected to participate in the Olympics, not only leveraging best practices across the collective brain trust and expanding capabilities beyond the norms of UK security and police forces, but also creating a sense of common cause among the coalition participating in the Olympics. These relationships paid huge dividends during the Games, in that intelligence feeds, real-time analysis, and course-of-action formulation were supported broadly across the Olympic coalition. The host government should provide an onsite fusion center where other governments and stakeholders can set up operations and share threat data as problems develop.

LOCOG also engaged in a series of technology freezes with the

goal of minimizing the threat of new vulnerabilities being introduced by new technology. Unfortunately, this principle must give way to the technological needs of users. In London's case, the explosion in WiFi devices led to a late decision to add a public access WiFi network. Again, governance must be worked out. The roles and responsibilities of security teams—everyone from the police to private security—must be understood, and personal relationships must be established so that groups know who to turn to for help. Once the initial planning is done, security staff must be trained and drilled extensively. Red teaming (simulated opposition players) and attack scenarios must be used to test and refine responses. Physical and cyber security must be coordinated. Physical access enables access to IT assets and IT assets enable physical access. Adversaries understand this. Security teams must be able to coordinate across multiple attack vectors—from physical ingress/egress points to authentication fraud to DDoS, etc. This is what teaches them the kinds of real problems they will face and puts them in touch with the counterparts with whom they must work to resolve incidents. Unlike the military, the Olympic committee does not control all of the security assets involved. Therefore, outside groups, whether police or foreign security teams, must share a unity of purpose. Establishing trusting, personal relationships can substitute for a chain of command and ensure that teams coordinate on developing issues quickly. Rio de Janeiro used the recent World Cup games to train its security teams for the upcoming 2016 Olympics. Tokyo should make sure the security assets deployed for the 2019 World Rugby Cup are the same assets that will be deployed in 2020.

The next Olympics will surely face almost every sort of cyber threat. It is therefore crucial to assess and plan for a wide array of threats—hacktivists, organized crime, insiders, state-sponsored hackers, and terrorists. Each adversary's psyche must be profiled and, to the extent possible, potential attack vectors must be identified and neutralized. As we saw with the Germanwings plane crash earlier this year, safeguards (in this case, locks on cabin doors) designed to thwart the attack can open up new and deadly attack vectors. We still need to make best-guess predictions about what an adversary will do and then take appropriate countermeasures, but we must not become complacent: we must assume that new and unexpected attack vectors will appear, and we must plan as best we can to deal with those events as they happen or as they are discovered. The Olympic Games dramatically raise a nation's profile on the world stage, so security teams must be prepared for attacks against a variety of targets—the energy grid and other infrastructure targets, sponsors' assets, government sites, etc.—and not just the Olympic website and Olympic Village network. Simulated attack exercises and "red team" can improve response effectiveness.

An interesting example of getting one step ahead of an adversary's thinking was the real-world problem of how to deal with hooligans at the last European football championship. The event sponsors cleverly invited police from various EU nations that had a history of game-related hooligan violence to appear at the championships wearing their local uniforms. Surprisingly, the plan worked. Hooligans were much more reluctant to misbehave when police from their home countries were visible. It would be worth considering the benefits of allowing host nation police and police from neighboring countries to share threat data in real time. By planning, practicing, and working together, event managers can minimize the threat to their events, and ensure that the upcoming Olympics are safe and enjoyable for all.

Cyber regulation

Cyber regulation is the middleware that ties big picture concepts such as nation state security goals to tactical day-to-day issues such as managing a large-scale sporting event. Japan is positioned to be a showcase for cyber regulation as a positive contributor to Internet safety. Japan is committed to Internet access for its citizens, but wants to ensure that this access is safe and contributes to the welfare of society. The key to successfully navigating the Internet, in the eyes of many EU counterparts, is to establish regulatory guidelines that embody the normative values and priorities of the member states. This includes building resilience, employing cross-border collaboration mechanisms, protecting infrastructure, and managing risk. At the same time, citizen privacy and convenience must be respected. For this reason, issues such as net neutrality and data breach notification must be addressed as well. The goal is to strike the best balance between competing needs and interests in accord with established values and legal processes.

While the United States and EU attempt to address the recent High Court decision to nullify the Safe Harbor provisions used by US companies for storing EU citizen data, the EU must define its own internal rules in a way that fosters and does not inhibit innovation. Although there remains a vital role for government, private sector firms must be actively involved as well. Governments must rely on the private sector to lead the way in a variety of areas, from initial threat response to new security tool developments. Privacy is a paramount concern, but it cannot be the only concern. Access to threat data and the ability to share data between government and private parties must be enshrined as well.

There is a tendency for media to seize on worst case scenarios in dealing with cyber news, which contributes to misunderstanding and hysteria. Cyber regulation designed only to deal with worst case scenarios will be far off the mark. Regulatory action must reflect a more measured, reasonable assessment of threats. In cases where certain threats are known, it is possible for government bodies to require that steps be taken to prevent or mitigate these known threats. Addressing Advanced Persistent Threats (APTs) and zero-day threats is more difficult, but this fact alone does not justify a failure to act where threats are known and countermeasures are available.

The situation is analogous to the laws of the roads. Every nation has its own rules, but there are many commonalities. Complete harmonization is not required in order for countries to issue and honor international drivers licenses. The international driver must modify some driving practices to abide by the laws of a particular nation, but the process works quite well, allowing countries to manage road safety in accord with local norms and international travelers to take advantage of the roadways in many countries. A similar approach should be considered for the legal and regulatory framework for cyberspace, particularly as it pertains to the private sector. Each nation is free to implement its own rules, but there are certain core concepts (defense in depth) and basic realities (such as threat vectors) that will ultimately play out, with some variations, just about everywhere. Businesses, particularly multinationals, are well positioned to assist nations in seeking out common strategies and standards. Much as the World Health Organization sets safety standards for the handling of epidemics and other health crises, a multi-stakeholder international organization could recommend best practices and minimum standards that would help nations in setting domestic rules while providing businesses with some level of consistency across markets. Otherwise, the cyber security industry will likely develop unimpeded and possibly in ways that make later attempts to regulate it less effective. At the end of the day, each nation or multi-national body must establish rules that represent its values and its priorities, but working together to find common solutions and mechanisms for collaboration will serve the interests of all.

II. Executive Summary
C) Cybercrime

The need for international frameworks to address cybercrime

The Budapest Convention, which was the first international treaty to address Internet and computer crime by trying to harmonize national laws and improve investigative techniques, is a solid international framework for cooperation on cybercrime. However, the Mutual Legal Assistance Treaty (MLAT) process is not sufficiently agile or responsive. While much can and should be done to improve the existing processes, there is also a need for current approaches to evolve. Increased awareness is required to drive development of new approaches; however, those that emerge will likely be different and culturally conditioned. Socially accepted approaches will only emerge through early adoption of multi-stakeholder dialogue. As national security and law enforcement become more intertwined, we will see an inevitable increase in complexity.

Challenges in aligning policy & legal frameworks with the pace of technological innovation

Public-private partnerships and flexible-outcomes goals (specifying desired goals without specifying how to achieve those goals) are favored because governments struggle with the pace of innovation. With increased nation state activity in cyberspace, new challenges emerge; it becomes difficult to ensure appropriate consequences for bad actors—either through prosecution or normative frameworks—due to complexities of attribution (both technical and political). Cyber risk must be integrated into enterprise risk management, making it a C-suite responsibility (not merely an IT responsibility), and both sides need to promote enterprise and government coordination on risk management.

Building coordinated public-private partnerships and information sharing to manage cyber risk

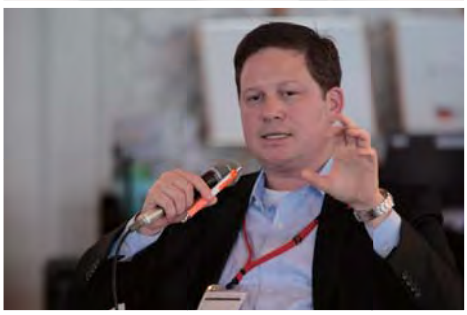
Information sharing is an important tool, not an outcome, and certainly not a panacea. It should not be solely focused on industry-to-government, but also industry-to-industry, government-to-industry, and government-to-government collaboration. There has been substantive progress made in information sharing and developing workable models for

sharing. We need to learn from this (e.g., Interpol, Europol, Microsoft Cybercrime Center) and build on it. Many participants in this Conference feel that the “5 Eyes” model is outdated, and collaboration should be looked at more through the lens of international multi-stakeholder cooperation. There will never be a global one-size-fits-all model, so we must accept diversity. Governments should be participants, not gate-keepers in these efforts. The ultimate objective of information sharing is to protect citizens and systems. To encourage private sector participation, we need to clarify specific goals and identify what kind and what level of information can and should be shared. Sharing threat information and anticipating future trends helps society to become resilient to future potential threats.

Emerging security and privacy challenges

Future innovations will create both security and privacy challenges and new ways to address them. Ensuring that organizations (both companies and governments) can effectively respond to threats requires preparation and practice. This process should include C-suite executives, who must ensure that all cyber incidents are identified.

It is critical to learn and scale practices (e.g., security by design, authentication) that have been learned through the Information Technology (IT) and operational technology (OT) waves, and transfer this knowledge to the IoT. We must continue to develop a skilled anti-cybercrime workforce for government (e.g., specialists in investigation and prosecution) and industry (e.g., security architects). We must recognize that there is no “leader” in information sharing (or in cyber security, for that matter). Everyone has made mistakes. We need to develop a best-practice model based on successes from around the globe.



III. A Look Backward, A Look Forward

Although the Conference featured three apparently separate themes, the three are closely interconnected and interdependent. The inexorable growth of Cyber Connection holds the potential to become an unequivocal good for society; on the other hand, it can easily open the door to a host of new, very serious problems. That outcome hinges on a new, globally coordinated approach to Cyber Security. Without a new security paradigm involving genuine global co-operation, we will certainly open the door to a new wave of Cybercrime.

More than 400 attendees from roughly 30 countries—including policymakers, corporate executives and academic leaders—took part in the Conference and discussed the above issues. The discussion was highly complicated, not only due to the topics involved, but also because these participants represent divergent backgrounds and viewpoints, with varied level of knowledge and experience.

This was done because the key to finding workable solutions often rests on creating precisely such conditions of diversity and contrary options. Participants who come from various backgrounds to discuss shared topics naturally bring their different perspectives to the discussion. When they exchange their opinions in an open-minded way, and listen sincerely to each other's views, they often come to see that what once seemed a black-and-white issue has, in fact, a wide spectrum of valid opinion and perspectives. This process of using multi-stakeholder dialogues to reach comprehensive solutions is more essential than ever before, especially when dealing with complex issue that transcend national, cultural and ethnic boundaries.

This approach is not new, but it is extremely important today. Active multi-stakeholder participation assures a wide variety of opinion, which is the worthwhile starting point for such a discussion.

Needless to say, this kind of approach and this kind of event should be repeated in the future. The content of Cyber[3] Conference, as well as summaries presented in this document, are not static words on paper; they are an organic entity that must continue to evolve through ongoing discussion and debate. Efforts such as this are important beginning; the discussion must not be allowed to stop here, but should be cultivated and promoted and expanded in other forums with other participants.

As the Cyber security Track noted, Japan will be hosting some important events over the next few years, including the Ise-Shima Summit in 2016 and the Tokyo Olympic and Paralympic Games in

2020. In particular, further improvements in cyber security will be essential for the success of Tokyo Olympic and Paralympics. Based on the discussion in this Conference, it is clear that increased cooperation between the public and private sectors as well as a higher level of international cooperation are necessary to ensure the success of the Games.

IV. Appendix:
What was Discussed in the Plenary Sessions

Recognition of the importance of cyber security
We are living in a world where we are increasingly connected, whether we know it or not. The IoT generates tremendous new opportunities for local and worldwide economies and improved quality of life, but where there is opportunity, crime will sooner or later follow. Cyber security experts say there are two types of enterprises: those that know they have been hacked and those that don't yet realize they have been hacked. These experts and others in the field must predict future challenges and adapt as technology progresses and cybercrime increases in both frequency and sophistication. Currently, cyber security is not evolving at the same pace as cyber connectedness, and this situation must change.

Internet as the economy
The Internet is not merely essential to economic growth; in a very real sense, it is the economy. That is, there is no concept of the global economy, now or in the future, that does not include the Internet as an integral part of its core infrastructure. Companies have traditionally focused on risk as defined in financial terms, but they do not fully understand cybercrime risks and thus do not place sufficient emphasis on cyber security. They also do not understand how a leak of information could undermine company trust and brand value. The cyber liability insurance market will be a new area in the economics of cyber security with increasingly accurate valuation of cyber risks.

Information sharing
Information sharing raises the general level of security for the parties sharing that information. The overuse of "classified" information can invite threats. Companies should recognize the importance of information sharing to prevent security risks, and not be solely focused on keeping information away from their competitors. Information sharing between governments and companies is also vital. Governments should be participants, not gatekeepers, in information sharing. Companies should not be obligated to provide information and get nothing in return. There will also be a revolution in information sharing through artificial intelligence.

Encrypted data
Governments must listen to the advice of cyber security experts. The US Senate's anti-encryption bill would create security risks, and governments should not be allowed to have backdoor access to encrypted data. Governments must do their utmost to protect citizens and national security, but they must have a comprehensive and well thought-out strategy and listen to both the cyber security community and their own cyber security experts.

Role of government in promoting a healthy cyber environment

A new form of public-private partnership is vital for the future of cyber security. Cyber security is not a problem of technical tools, but a human problem. Thus, it must be thought about strategically in human terms. Experts must create roadmaps to protect the public, and also to help the public to protect themselves, since most people are unaware of just how connected their lives are. The public also needs to recognize the potential for systematic and collateral attacks. At the same time, Government must listen to personal privacy advocates: While user identification is important, there should also be opportunities to be anonymous on the Internet.

Manifestations of cybercrime

Cybercrime can be carried out by individuals and groups, including the many cyber criminals who operate in underdeveloped countries. Nothing is safe from cybercrime and the Internet does not recognize geographic boundaries. Nation states can also carry out attacks, including both physical and non-physical ones.

Thus, there must be a clear understanding of all the different types of attacks. Examples with economic implications would be causing delays in stock market trading or tampering with bank clearance and settlements. Real world examples include the cyberattack in Saudi Arabia. In Operation Global Blackout in 2012, a message was posted threatening to take down the entire Internet, which led to unprecedented international collaboration and information sharing.

Cybersecurity and Japan

Japan recognizes the potential for cybercrime in technological areas where Japanese companies are world leaders, such as autonomous driving and medical technology. In January 2015, Japan passed the Basic Act on Cyber Security and in September 2015 the Cyber Security Strategy was approved. With the advent of the Olympics, Japan has an opportunity to be a model for the world in developing effective cyber security strategies, but all these policies and practices will mean nothing if they are not implemented.

Cyber norms

Public and private relationships are essential to success in securing cyberspace. The self-correcting nature of a democratic government and efforts to promote public awareness will help facilitate improvements in the area of cyber security. Those in positions of responsibility have difficulty simply understanding the risks of cyberattacks. Promoting clear discussion with government and having a principled approach can help improve

bilateral relationships. Any single group's resources and information are by definition limited, which will place greater importance on collaboration.

My number (Social Security and Tax number)

In January 2016, every resident in Japan can be identified online through the use of electronic certificate on ID card commonly referred to as Individual Number Card. In the future, Individual Number Card can also be used with credit cards and health insurance cards, and with the aggregation of nationwide health-related information, medical R&D will continue to grow. Due to the large amount of personal data involved, privacy protection will become increasingly important.

Cyber information gathering and sharing

The Internet has become an established form of social infrastructure, and confidential information is in a constant state of vulnerability. By enhancing information gathering and sharing, police are able to handle more issues, such as taking down websites on the Dark Web. Japan is lacking in both human and budgetary resources in the area of cyber security, but mobilizing private sector resources can help to compensate for this. Close cooperation between the public and private sector is Japan's greatest strength in this area.

Education

Education is a key point in developing cyber security. Large numbers of new IT security engineers are needed to make the online world more secure, so investment in cyber security education is critical.

Law enforcement and international cooperation

The pace of legislation today cannot match the speed of cybercrime. There is a need for strong international collaboration to increase efficiency. Regulation of consumer devices might harm competition, but state regulation of critical infrastructure is vital.

Technology pipeline

Basic research should be connected to applications in an efficient way. Creating an environment that supports intellectual curiosity at universities can help improve innovation and research.


Day 2: Plenary Sessions
KASPERSKY
Telecoms
Finance
Transportation
KASPERSKY

V. Speakers and Discussants

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

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

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.

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

Technology Lead
Jarno LIMNÉLL
Professor, Cybersecurity, Aalto University; Vice President of Cybersecurity, Insta Group Ltd.

Academic Lead
Christopher TREMEWAN
Secretary General, Association of Pacific Rim Universities

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

Cyber Security Track

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

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

Technology Lead
Phillip MORRIS
CTO, BT Japan

Academic Lead
Jim FOSTER
Professor of Political Economy, Graduate School of Media and Governance, Keio University

Secretariat
William "Bud" ROTH
Senior Manager, Cyber & National Security of Public Sector, Deloitte Tohmatsu Consulting LLP

Cybercrime Track

Track Chair
Noboru NAKATANI
Executive Director, INTERPOL Global Complex for Innovation

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

Technology Lead
David BURG
Principal, PwC Global and U.S. Cybersecurity Leader, PricewaterhouseCoopers LLP

Secretariat
Lena RYUJI
External & Community Affairs Manager, Microsoft Japan

Other Speakers and Discussants
(by alphabetical order)

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

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

Raman Jit Singh CHIMA
Policy Director, Access Now

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

Mike FLYNN
Former Director, Defense Intelligence Agency (USA)

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

Ross FOWLER
Vice President, Digital Transformation & IoE Acceleration, Asia Pacific & Japan Cisco Systems, Inc.

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)

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

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

Rick HOWARD
Chief Security Officer (CSO), Palo Alto Networks

Rex B. HUGHES
Co-Director, Cyber Innovation Network, The Computer Laboratory, Cambridge University

John C. (Chris) INGLIS
Distinguished Visiting Professor in Cyber Studies, US Naval Academy; Former Deputy Director, NSA

Steve INGRAM
Partner and National Cyber Leader, PwC Australia

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

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

Eugene KASPERSKY
Chairman and CEO, Kaspersky Lab

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

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

Taro KONO
Chairperson of the National Public Safety Commission, Government of Japan

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

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

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

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

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

Miroslaw MAJ
Founder and President, Cybersecurity Foundation; CEO, ComCERT

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

Francisco García MORÁN
Chief IT Advisor, European Commission

Carlos MOREIRA
Chairman, Chief Executive Officer, and Founder, WISeKey SA

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

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

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

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

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

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

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

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

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

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

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)

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

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

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

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

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

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

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

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

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

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

Giuseppe TARGIA
Vice-President, Security Business Unit, Nokia

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

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

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

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

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


C3
CONFERENCE
OKINAWA 2015