Finished Transcript

2013 APrIGF SEOUL

5 September 2013

Concerns for Securing Cyberspace of Asia-Pacific Region

SEOUL TIME: 4:30 p.m. CST: 02:00

\*\*\*\*\*\*\*

This text is being provided in a rough draft format.  Communication access realtime translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.

>> Would like to make a presentation and decide ‑‑ we'll talk about the response system in Korea. And according to some reports, the cyber crime cost $110 billion in the last year in the 24 countries so with everything going mobile, becomes the target for the cyber crime too. And this ‑‑

[no audio]

How cyber security is affecting the infrastructure ‑‑ happened and the nuclear infrastructure has become the target and just used. And many types of cyber warfare that are taking place in the world.

This is the Korea in terms of ICT, everyone can use internet and the Wi‑Fi connectivity; however, even though the users are increasing the usage of the internet, because of the increasing use of the internet, they have become more vulnerable to cyber attacks. That's kind of challenge. In the 2011, I classify that the cyber security threats, the first one is a mobile security threat becoming a reality, because many people ‑‑ secondly, massive personal information leakers happens and the instance posing a lot of threats and financial gains because micro ‑‑ taking place, and as I mentioned taking place continuously on the steadily. Cyber attacks are turning into cyber warfare. You can see kind of changes. They have published a Tallinn manual. It is about mobilizing the defense capability in the case of cyber warfare. Because of the cyber ‑‑ the attackers of the cyber warfare can become the attacker of missiles and other conditions of weapon, but it is not legally binding. The international discussions on the cyber warfare and ‑‑ strategy of a cyber attack.

For example, attacker targets special groups or individuals when they attempt to do that they predicted the sites the targets of interest, in that case they have the potential sites and then the people with the ‑‑ they are also affected and then in the wake of the infection it is possible to get the data out of that target, that individual or organization. I would like to take one example in 2011, the ‑‑ the Department of The state agency so of the U.S. had become the victim of a watering hole. I would like to talk about the cyber attack that happened in Korea. The financial institutions became the target of the attack. As a result 48,700 PCs and ATMs are affected. The vulnerability of software across was maximized. I would like to talk about more details of this attack, a hacker sent e‑mail and distributed the malicious account. When the internet are affected and the days ‑‑ and the effects in cyber at a certain time at the ‑‑ updates the antivirus vaccine, while doing so the pieces of the ‑‑ are affected and this is how this attack happened in reality.

Launched an emergency team in order to respond to the incident and they analyzed 76 malicious codes that damaged the systems and supported recovery. In order to prepare for the potential the following, they took some steps and monitoring too. And June 25 cyber attack and it's similar to the previously mentioned and the targets were the companies and the house ‑‑ so I have been explaining about the trend of the cyber attacks.

How responding to cyber attack trend. I would like to explain about this response system. In Korea there are three response systems. One is the public sector and the private and the other is the ‑‑ for the private sector to prepare the data, but at this instance, we have a cyber threat information system and there is the classify, so we issue warnings depending on visibility of the incidents. I would like to now explain about cyber attack response process. Security firms and they receive information, but it is information other types of information and the base on that information we analyze and report the incidents and based on that we analyze and issue warnings and we seek operation with related agencies. Because of the time constraint I would like to skip some details.

It is malicious behaviors and activities on the internet and this is KISA control and monitoring office, so from this office we do monitoring to find out the malicious activities and if something happens, we respond to that activity. Users increasingly using internet if malicious code are distributed through the internet to practice from happening. Every day checks and monitors malicious account. There is the precious of malicious activity in 2.3 home pages in Korea, found out something, we notify the affected organization. Then it's now I would like to talk about DDoS about the SME system, and we provide a report to SME to respond to DDoS and the shelter. That is the ‑‑ go to KISA and we block the DDoS attack, and we can go to our chapter so that can be used as intended. DDoS attack is being exercised and in order to repair and the cure PC, so we have a partnership, and we notify the whether your PCs are affected. We also provide the system so that people can make PC infection disappear. We also do international cooperation too. We need to have a more international cooperation to have a better response.

I think that the next, more detail the information and more detailed presentation on the international cooperation. KISA is doing a lot of things and the project in order to respond to more sophisticated cyber attacks including ATP. Thank you ‑‑ thank you for the presentation and the presenter talked about the cyber attacks that have happened in Korea and the types were also covered. And 90% of the financial transactions are being made through the internet, and financial ‑‑ some of the financial institutions are the victim of the cyber attack. I think can teach other countries about how to respond to cyber attacks and the next presenter is Hong Soon Jung from KISA. He will talk about the cooperation ‑‑ the international corporation is the internet itself is there are no boundaries. We can have a better, a stronger defensive system and I would like to invite Hongsoon Jung from KISA.

>> HONGSOON JUNG: Good afternoon. My topic is the CERT and the international cooperations made by CERT. So as you see, collaboration is very important, as Mr. Lee pointed out. So cyber attacks involve many countries, not only apply to individual country, so to reduce cyber attacks so the international cooperation, international cooperation is required. So cooperation between the CERT is made to reduce the number of cyber attacks. As you see on the slide, so we have a simulated cyber attack scenario, so we have executed some scenario, so in this scenario, hacker in Europe is attacking the PCs in other countries, and so they actually so go through the Africa and then the server in Asia, and infecting the PCs in many countries throughout the world, so the targets are very ‑‑ is located in north America, and this is just a scenario, but this scenario can really happen. So to prevent this type of the cyber attack, so we definitely need the international cooperation.

CERT was created at Carnegie Mellon University specifically by ‑‑ CERT II was designed to handle the cyber crimes, so it was created in the United States, but these days many countries are running CERT, and even many organizations are running this programme, so CERT has many alternative names because it has its own trademark. So CSCIRT, CIRC. SIRT or SERT. As I told you, the many companies are operating their own CIRT. As you see on the side, so many dots. So many dots, the national representative of CERT, so national C‑CERT, so I just call it the national CERT. So let me explain the CERT functions. So there are views from the technical point of view and the administrative point of view. So we usually monitor and analyze and then respond to the incidence and then we recover the system. So organizations such as private companies and the schools can run their own CRT. So it involves all running and you see them handling, vulnerability handling and artifact handling as you see on the slide. And national CERT has a similar functions, but as you see, they serve as a trust Point of Contact, the Point of Contact is usually called the POC.

So national CERT users serve as a Point of Contact, trusted Point of Contact, so the United States has the CERT, Japan is JE. So each country has a trusted focal point for contact. So national CERTs have the technical functions, and at the same time they have all the ministry to function, so they develop the national security policies and so they raised those just probably security‑related policies, they actually publicize the national efforts for the security, national security, so they are engaged in very wide variety of activities.

And domestic collaboration among the international CERTs. In Korea, in 2005 KISA has internal function of a CERT, concert was separated from KISA, now it is an independent organization. So it now it has just the private companies as they are members, so they set up kind of this cyber attack response system. And other types of cooperation, bilateral cooperation and multilateral cooperation. So bilateral cooperation presents the state to state cooperations between the different countries, between Korea and Japan and between Korea and the U.S., so bilateral means that just the cooperation between the two countries, they usually sign up on MOU. And multilateral cooperation is made different regions, CERT, MI CERT from middle east. Or Africa CERT and other regional CERT and on the global level we have a first, the 280 organizations are involved in this global CERT organization.

And the every year national CSIRT annual meeting is held. So national CERTS get together and have a meeting in this annual gathering. So this international cooperation is very important because cyber crimes, cyber attacks, these days not only affect individual country, usually involve many countries so this type of multinational cooperation is essential. So I'd like to take an example of AP, Asia‑Pacific CERT. So in countries, the organizations from 20 countries, national represented CERT and the non‑for profit CERTs are members of this APCERT. So they have an annual meeting and the conference and then they ‑‑ actually the exercise and drill for any incident they share the information through e‑mail and throughout the communication channels. As Mr. Lee explained, I would like to take an example of this international cooperation case. Let's take the example of Korea and Japan, March 20 ‑‑ March 11 and ‑‑ so ‑‑ so on specific daylights as between the couriers, we have any just to recall background, so only the Kr CERT and the JPCERT, they usually launch monitoring because to prevent any attack from each country, so they catch any sign of the cyber attack, they just make joint effort to prevent this one to spread to other sites. This is one of the examples of bilateral cooperation.

As I told you national CERTs have various functions, but the coordination with other countries, this is the most important ‑‑ the function of national CERTs. So for example, one vendor from a local market, so attack the vendor, but the company is not the best, so national CERT catch that information so then usually that just the national CERT has to inform the specific company of that incident, so sometimes other country national CERT can inform that information to my country, so ‑‑ so the national CERTs, the function is that kind of coordination. And like an example of a presentation from one conference. Symptoms of a cyber attack, so relationship between people, between organizations, between states. How to build up cooperative relationship is very important, so I would like ‑‑ in that sense I would like to encourage everyone to participate in this national conference and I'd like to invite more and more countries to this type of international conference. And then more and more companies or the government organizations have to sign off more MOUs for their whole operation.

So I hope there's more and more stakeholders are to be involved in this effort. Thank you.

[ APPLAUSE ]

As he mentioned in the Asia‑Pacific region, so we have APCERT.

So he already gave us the examples of the bilateral or multilateral cooperation. In 2013 JPCERT, and the CERT, they are the representatives visited Korea, and then they kind of shared this symposium, so from the private sector and also from the academic sector, so they have some malware detection, so technologies, so the next speaker we'll introduce those new technologies, detection technologies, and then the how we just coordinate the efforts from ‑‑ with the private sector. I would like to invite Mr. Choi.

>> SANG‑YONG CHOI: Good afternoon, everyone. Today I'm going to talk about as the moderator explained the cyber security. I believe there are ways to enhance our corporation, so I would like to make two key points. The first one is about the introductions about my organization, the center. I would like to make a concrete proposal about hour detection technology center divisions. First, let me introduce my organization, the KAIST, center, research and the developing core technologies are the main missions of our center, and we have a ‑‑ and the main areas of research are real time malware analysis system and the malware collection and the analysis technology, and also we are expanding our research areas to moble platform.

So these are the main areas of research that we do. The vision of CSRC are two. One is the first one it's a foundation of the cyber security, so strengthening cyber security we aim to make Korea a strong nation in cyber security, and second vision is to produce that the key points to do the job. And this is the history of our organization. The CSRC, so you can just have a look at it when you have time. And it was established in 2011, and we have developed SIMon, a system, in two years of development, we have developed the SIMon software registration, and we do the reporting as well. We provide about 120 organizations. There are three roles that we do. Research and development. Education and service. So you can read the details about that.

Now I'd like to talk about SIMon. Suspicious information monitoring system for websites. These are the architecture and the three tier architecture. At the bottom we have agent. There is virtualized agent and they are clustered so they can monitor the website, and we have a manager, database server between, and on the top we have a web user interface. It is aware ‑‑ you can see the configuration on the top layer. With this assignment system, we have been monitoring about 420,000 websites and I think the target are likely to increase and if you need our service, we can expand this service to other countries as well. And what we have achieved in terms of SIMon is monitor the suspicious activity on the website and we have achievement, we have applied a patent and also we registration about the software that we developed. This malware trends, whether it is cyber attacks, usually it starts with a malicious code, PCs are infected, malicious code, and how to distribute the malicious code are changing.

A recent attack ‑‑ user justify access into the infected site, they are malware affected site, and during this infection stage, the existing security systems are not able to attack the attack.

The result of the monitoring of the data with their assignment and it is a basis, it is a number of hot sites and the up to 900 sites became the victims of hackers, and during the weekend the hacker activities are ‑‑ there are a lot of organizations that set up and run their response system, but normally during the weekends people don't have a strong response system, that's why we have more and increase in number of hacking incidents during the weekend. This about watering hole, presenter, and we detect the watering hole with our resolution. The characteristics of the watering hole is they haven't specified the target. So from that perspective it was ‑‑ the target was not the site that everyone access, rather the target website was something only interest to people. Second thing is about something that happened all the time. It's about the phishing attack that usually happens against financial institutions and the sites where phishing code are affected and implemented. The sister organization of financial institution became the target of phishing so we detected it and we notified that the affected organizations about our monitoring result. Some social issues so we analyze the behaviors malicious activities and it is something that we do as well. Every week we report security, this is the cover of our security report that we issue every week. It includes the analysis and the monitoring result.

So I have been explaining about the monitoring service of the SIMon, and we provide a weekly security report and the other thing that I would like to cover during my presentation is Web‑based and malicious code are becoming the most serious attacks. The case in point is ‑‑ Korea has ITC, but strong ITC capability doesn't only matter when it comes to be coming the target and the victim of the cyber attack. The SIMon solution that we ‑‑ our institution developed can do wide and comprehensive monitoring and we also provide the related services, if you need our service, we will respond to your requests. We can monitor any website over seas website, and we are ready to provide technical services. Thank you. Thank you for listening.

>> Thank you for the presentation and the presenter explains that SIMon can also provide the services to depart the malicious code on the website of other countries, other Asia‑Pacific countries, Korea, China, U.S., Israel are other countries we see becomes the victim of hackers often, so I think SIMon can be very useful addition to our countries as well.

So the next speaker comes from the NEOWIZ gaming company. So the next speaker is an employee of the most popular company in Korea. He will share with us the cyber security applicability and the appliances.

>> YONG KIL KWON: Good afternoon. My name is Yong Kil Kwon from Neowiz games. I introduce my company, Neowiz games. Neowiz was created in 1997. Neowiz games was a spinoff from the Neowiz in 2007. So we are specialized in online game development and the total number of employees is more than 1500, so as of the end of 2012, so our the annual revenue is more than the 650 billion, so we were listed in the crane town market. So this is the history of the Neowiz games. Our parent company Neowiz was created in 1997. Neowiz games was a spinoff from the parent company in 2007. So Neowiz was established to allow internet connection from home users. So Neowiz developed a very simple cyber software for this internet connection. So at the time usually in 1997 so the users have to use very complicated software to access the internet, but the Neowiz developed a very simple software for end users.

So then ‑‑ and then so Neowiz ‑‑ the second thought, what kind of service we could provide for end users, so we thought about the internet chatting, so we developed the internet chatting system, so we made a huge success with that system, and with this chatting platform so with all about the applicability of that chatting platform and then so we just invited many experts in the field, so with this infrastructure and the resource, we came up with a game software development, so we launched the game software business in 2003. And we developed a line which made a huge success in the Korean market as well as the international market. Close fire were another major international game created by Neowiz, so we were a spinoff in 2007. So we acquired Japanese company, so now Neowiz games is extending our internet game from the sports and other type to another news ‑‑ so we are expanding our business call.

And you see on the slide, so we are engaged in this type of online games. Shooting games and sports games, so we developed a line last year, we just closed our service of this line, and now we are facing games and the games are being provided. So recently the core masters in the Asia office, so we developed MMORPG games these days. So these game services are provided to the local market. So after the spinoff, Neowiz games has launched our business so we are very active, other countries, more than 20 countries. Are being sold to more than 20 countries. So in 2004, we launched the global business, so that the revenue from the overseas market is $10 million, but now the revenue from markets more than $100 million. So China is the biggest overseas market. Cross fire is the Chinese market, so they earn us more than $300 million. So I have to stop my ‑‑ the introduction of my company.

So we face the new challenges. So we have developed strategies. The extension of a game and the extension of our existing market, we are the game developer, we also think about those what types of contribution we can make. So this is our social country vision is one of the parts of our strategies, so we set up an incubation center called the NERPLY center, it was set up in July of this year. So $30 million was invested into this incubation center. So we set up an investment fund for this incubation center. So I introduced the activities and the types of games we have developed. Now I've explained the security threats that are involved in online games.

So on a high level we have three types of security threats. So the first target is the gamer. Consumer. The next ‑‑ the second target is a service provider, or publisher. And a third target is studio ‑‑ game‑developing studio or content supplier.

So many malicious codes in Korea usually are Targeting the gamers, so ‑‑ or consumers, they usually steal the identification of consumers. This is the first type of a threat. So with this IDs or pass words they get from end users, they steal digital assets within games. So digital asset usually present game items, so what ‑‑ so some times the individual game item is more than 20 million one, so the owners will be really surprised. So but this type of just fast is done by other gamers. So when we talk about the auto play, other gamers run auto play, one of the threats, and for the second target, publisher, as they usually steal the membership data. The games have 23 million users, members, so if one hacker steals this membership information, they set up this membership information into another server, and just that they can just provide this online game for free, and the third type of attack is for a studio. So studio here represents game developer, so they are usually very vulnerable to these attackers, because many of the studios are very small in the business size, so they usually do not have the mechanism to protect their assets, so usually easy for hackers to steal the source ‑‑ game source codes from these studios.

So these threats are realized so we will have this type of just realities, so we'll play is run, if that is run, the fairness of online games will be breached. So if anybody ‑‑ any gamer who has auto player, he can just abnormally create menu online game items, so if he just has online game, plays online game with other suppliers, then so he will enjoy his games by stealing those items. So it will hamper the fairness of online games so... so the ‑‑ if that happens, the online ‑‑ the game's life cycle will be shortened.

So if this auto play programmes are actually wrong, many programmes actually are wrong, then just lower the performance of the online game server, then the publisher has to provide some more servers than the ‑‑ we'll also reduce the profit of the publishers.

And also another risk is that the user's identities will be leaked, then not only IDs, but also they are game items so we'll hand it over to hackers. So for those who have lost the game items, so the sometimes they could loss against the publishers, so these are the anticipated impacts of security breach, and then also lower the brand value of this specific online game or online game company. And as the game's life cycle will be reduced and also deteriorate as the profitability of publishers so you might wonder why I'm just talking about the protecting the assets of my company. But I will give you another story.

I talked a lot about auto play, so usually so cyber attack against the online games, they are attackers are also game players. So that should be how to protect end user, actually gamers.

So to prevent those game‑hacking programme, my company has developed security programmes, and so we run this programme, but before running this programme, the security programme, so would he have two types of cases, though. In the first one usually so auto programmes are just distributed very easily so many just players preferred to use these auto programmes, so it is very difficult for some game companies to run the security programmes.

So according to our research of many countries, so many users prefer to use this auto programmes. So this is the security programmes are not designed to only protect our assets. Sometimes ‑‑ so nowadays, they serve as a profit‑making mechanism. So we can actually make a profit from those programmes. So any company that is running this online business, I will always emphasize that information security management mechanism is very important and so we have to monitor all the activities that are made with the system.

In Korea we ‑‑ our government has set up so many regulations to control this online game businesses, and so if there is any incidents we even have the requirement to report to the government agency, so we don't think just the ‑‑ it is just the making of busy, so we believe that these kind of regulations help us protect our assets. In that sense we are heavily investing in information security.

>> So he talked about applicability and the compliance of his business, so for the continuity of our business, we have to invest in the security mechanism development, so these are four presentations are already available into APrIGF 2013 website, so you can download them, so you can refer to them, and the last speaker. The last presenter will deliver presentation on analysis from the regulatory perspective. She was working at the University. So she will provide the updated perspective. Please welcome.

>> Good afternoon. Previous presentation talked about that the institutional and the technical side of the security as the moderator explained, I like to talk about the security issue from the finisher perspective and I will also ‑‑ the homeland security. The previous presenter emphasized that regulation is not about the development business and the regulation is about creating an environment to have a thriving business and the ‑‑ with that, I would like to take a deeper look. For the interest of public, regulation is a setup, and monitor are the administrative activities of the public and the regulation is economic regulation and the social regulation and regulation, the government make correct or intervention in the market to provide economic benefit to the players and it is ‑‑ economic regulation and social regulation, labor and the other environment that affects people's lives, the target of social regulation and the market driven and driven the regulations and so if something that cannot be addressed, the government intervenes and provide solutions. That's about the regulation.

Now, let me talk about the types of regulations and there are price regulations and from the economic perspective, fair trade regulation and the regulations that can be also mentioned. Different types of regulations also include the self voluntary regulation and if there is a collusion that has also become the target of the regulation from the perspective of the society, so as I told you, there are different types of regulation, and we have discussions on the regulation and the types for a long time, and involved in the regulation impact, and what I mean regulation impact analysis, what kind of social impact can we have from the regulation? Before apply and the implementing regulation, the analysis is used as a means to justify certain types of regulations, so it is about to predict the impact of regulation before introduction, so that it can provide this support and guidance and objective evidence that policy makers are regulating. So it is about the analysis and the decision making analysis, the process. And the regulation is set up that are good, better regulations and with the better regulations, it can be used as a means to justify the regulation or less regulation can exist too. This is about the areas of research, about the regulation, and there are three types of, one is a cost benefit analysis. The second is risk‑benefit analysis, and third, contingent valuation method. First of all, let me start with the cost benefit analysis from the economic perspective. It is most frequently used. The benefit from the public sector project is a review to analyze the economic values of a certain project.

What we talk about the securities and the ‑‑ we set up the regulations. We look at the cost side and the benefit and we come up with the over the benefit. The benefit the aim of the cost benefit analysis and the issue that comes up with the qualified data and result after the disability, we provided support to the policy makers, and the second one, the risk benefit, it is mostly user in the security area. It compares that the benefits and the risks of the measure that is ‑‑ established method that it is kind of a unique method to analyze the risk and benefit. This can be easy, the threat can lead to indirect threat in the case the risk benefit analysis can have limitations that effort is contingent valuation method. If I explain this method, it is about the evaluating the value based on the fact that how much a player are willing to play. Willingness to payment is evaluated and based on that, the economic convenience and cost are calculated. It can be applied to homeland security. It is about analyzing the impact of the regulation.

So cost benefit analysis ‑‑ but it cannot happen a lot because it is an idea, so we cannot have a risk, the threat are difficult too, and it is difficult to but the result of the analysis are needed in the development ‑‑ we are facing a lot of challenges in evaluating the economic values and the first challenges that limit in the excess seeing values and the second one is about the uncertainty and the third challenge is how ‑‑ how reliable is the results analysis. Not only security but also after have limitations and how to overcome their limitation is something we have interest in and I think further research will be needed in in area. The incidental beneficial also covered, we talk about the risk and we have to think about that future too and it is uncertain and it is substantive, and the characteristics which are intrinsic in this discussion captured to have more accurate analysis result because it is difficult to do the effective analysis, it is difficult to have a high reliability, but a lot of expertise focus on coming up with more evidence. And the cost and the benefit analysis involves uncertainty.

When we have a discussion about this, safety ‑‑ the analysis are not because we don't need for research. These are the responses sometimes I get. Previous speakers said a lot of different types of threats and the market earlier and the government should be considered too. The patterns of the market players should become the target of this as well.

The economic perspective of a cost benefit analysis are immersing and gaining attention from researchers in the world. Let me take a look at the homeland security economic evaluation and the assessment that at first ‑‑ it is about change about to happen in that future. It is globalized environment and it's an individual environment. It is a selective environment, and this is environment. Homeland security involves a number of factors and the components and is increasing. When we talk about homeland security it is biologics and the land and the sea. The compliance cost of ‑‑ the long‑term cost should be considered. In case of logistics it is individual and it is also selective. And energy facilities are in transition from individual to global regulation and the obligations are getting stronger in case of airplane and the ‑‑ and they are becoming a subset to deglobalize the limitations.

So now talk about the analysis on homeland security from a regulatory perspective and why we need the economic perspective. Cost should be identified. It is important to know such a cost that are not many development data that we can acquire and benefit and cost and how they can be qualified ‑‑ quantified, sometimes psychologists challenging. Let's say if the case of reduced by half, the cost will reduce as well and then the kind of benefit can be quantified. Statistics analysis or data can be readily available, the reduce in case of the cyber certification, by 5%, by that 5%, so we can have economic benefit and if it involves a very important economic matters there is a strong correlation so it is difficult to have independent analysis and some time can take the place and It's difficult to have quantified judgment when it comes to this because sometimes the costs can be exaggerated.

For example, because of the limitations, we can have this kind of situation. Sometimes the cost and the risk about extent that can happen, the ones can be also considered by the policy makers of regulations. One call from terrorist and one from a suspicious person, one has direct, it is not something that really the simple judgment. There are a lot of different perspectives about the defensive protection, so sometimes it increases at the interest of cost. So more on the quantification. The homeland security include the fiscal and other types of securities depending on the regulation, we can have different cost and benefit and more research will be needed in this area and I will be one of those working in ‑‑

>> So from the point of the homeland security she has introduced the cost benefit analysis, and then I'd like to invite Mr. Fred woo.

>> I'm Alfred woo from, Singapore management University, it's really a pleasure to be here as a member of the panel. So I just go into why I'm here. What I do is really as a researcher into smart CT, from the ICT lab. So we ‑‑ we come from the perspective, we focus more on how the CT can serve the people better, the angle, right? So today, like order ‑‑ the cyber security that you presented in terms of the ‑‑ from the national security angle, from the Korean perspective which is important for digital security, an also I think from just now really the speaker ‑‑ let me do this.

Some also mention about some of the regulation and policy consideration, so in the next few minutes I would like to probably bring you some perspective that what we are thinking about, the importance of cyber security, and then some of the perspective that not really from an expert who knows how to deal with the attacks, how to monitor the network, how to fight the battle, but really more from an angle that how to all of these things made sense, from someone who want a better future all for us that we need to use all the underlying infrastructure such as internet. Okay. Here the first point I want to make here is why's cyber space security critical?

Number one, without a secure environment we will not have the confidence to use whatever we use. And then that will have an impact on the economy, the digital economy, which is the transactions will not happen, like the financial transactions in particular. And also it's not just about economy, but also the social activities that we actually use some form of ‑‑ I would say everybody these days in the more developed economies, we use internet, we use Facebook, all kinds of activities happen through the browsers, or the mobile phone, and that matters to us, that's a lot of value to us, social values.

The last point I would like to bring up and very important point, it's about our future, so actually a couple of years ago, as someone who really pay attention to the development of smart CTs, there is an idea that when I see the reality and the virtualization actually coming together, so someone used this word, which is the gentleman that ‑‑ from U.S., his name is Ray ‑‑ Raymond Courage, so he's currently ‑‑ he's from MIT but currently work at Googles with the director of engineer. He is a futurist. Okay? He has this idea of singularity. You can check it out. I'm not in complete agree with his vision, but that is so called extreme thinking about what will be the future, that means the virtual world and the real world will become one. Become a single world. Human being is no longer the human being we are today. That could be an extreme view. I'm not going to debate on that. That shows in the future cyber space is actually our space, that kind of situation, so when we talk about Cyberspace security, that's critical.

I would mention that my research would focus on the interaction of the people, more about services, so we consider different perspective of the future of the CT which we have to look on the demographic point of view which are the population, and the economy point of view, and also the governance point of view from the government, management, in terms of resources, we have to view a better future. Not go into the details now. There are other things I just want to emphasize the point, we pay a lot of attention to services, our contest will be digital services, because what we become, what we enjoy, what matters to us, like how we feel the experiences all come from the services we kind of receive every day. More and more of these services would actually happen in what we call the Cyberspace that matters. So this is the vision that we are kind of thinking about how the future ICT award like which I'm not going to ‑‑ okay. There are some interests why I come here, one of the interests is about open data, I had an orientation just now, and the interests are about the Cyberspace security.

In iCity lab, we're looking at a security matter, we're not looking at a angle, but from the angle that we think about, you know, how this matters to users, which you can consider that's related to the other session to talk about a privacy issue. But here are the points that I like to highlight to you very briefly, but we can go into more discussion later on. Number one really is between the user, when we try in the security, we make it usable, that event, individual, I'm not talking about government, I'm not talking about the large corporation, at this point in time I'm talking about the individual, you and me, how those things matter to me. And then assets actual goods against virtual goods. What are the risks and how much is that going to cost us, and for all of these things can we make the experience more convenience, it's a battle between the usability consideration. So that ‑‑ that kind of balance we would create the future user experience, so when we come to the consideration of cyber security, the dimension, the second points really what I hear is the ‑‑ actually I should write it, strategy and governance, the end is gone. So we should really, as I heard from the presenters, really has to be driven by some kind of international bodies and governance ‑‑ governance at a country level, but there are four P here that matters.

One is the policy, which is rule of law. Do we have the rule of law for the internet? That's a good question. The rule of law, how do we play? I mean that ‑‑ that matters. We cannot only fight this thing at a lab, we need to have that ‑‑ if we talk about collaborations we have that rule of law, when someone do these bad things, how this particular bad guy is punished, so that's a very simple thinking about rule of law, second thing is the best practices. What is the best practices ‑‑ okay. Sorry. Thank you.

The best practice I'm referring to is actually about, you know, some of the things that in any transition usage, how should we behave, that's the process how we have that in for the security consideration, and then add a level, can we do better with security and usability, so people can use ‑‑ can we have security better designed so that will not be so much intervention, there will not be you have to memorize all of those pass words. Lots of security problems because we cannot imagine ‑‑ use simple pass word or default pass word which actually cause security problems. Not but not least is the player, here roles and responsibilities. The government, the large corporation, which are probably in better place because they have specialty, they have expert at them, but what we're here today is the most worst case with individuals, we probably don't have the kind of practice that the help from the others in terms of what we should do to contribute to a better secure cyber space, so these are the things that we need to consider, so I think I would like to kind of stop here just as some other consideration, but not like go into the details, but that's some considerations around the personal data, which might not be a appropriate for this particular session. That is my so called a little bit of sharing. Thank you.

>> Thank you. (Speaking in Non‑English Language).

And because we have five presenters and they prepared our big slide, we are running out of time, but I would like to open the floor and y'all would like to ask questions or comment, I would like to take one or two questions, or ‑‑ if you want to ask us some questions to the panel, presenters, if you would like to make a comment about the presentation, please raise your hand and make a question or comment.

>> Please use microphone.

>> So how much data are being exchanged with the other countries full cooperation or collaboration with other countries? I would like to ask this question to the presenter from KISA. I am ‑‑ I would like to respond to the question. So your question is in the Asia‑Pacific how much data has been shared and exchanged in terms of a CERT. So how much data regarding threat are being exchanged on AP countries at the CERT level. That is the question.

>> I don't know how to respond to the question, because it's a case by case depending on the relationship with the other party. There is a when it comes to sharing the data, so it depends on what kind of relationship we have with the other party. So it is difficult to answer the question. That is why you are having difficult time answering my question. Yes, it is. If we have a relationship between the two parties, between the two countries, then I believe that in depth data can be shared. I think I would like to provide this response to the question. So it all depends on the between countries, so it decides how all countries can respond to the cyber attacks so do we have any other questions?

If you don't have any other questions, I would like to ask one request. Mr. Alfred, can you post ‑‑ can we post your materials on the Web page? Then ‑‑ you can deliver your presentation, then will be posted as a presenter of this session and your material will be also posted on our website. Many countries in the Asia‑Pacific have been joining us with this session and we have the internet governance, especially we just have the security session, I think there is a lot of work that we have to do to get there. I think all can be summarized to how much we have between individuals or between companies, organizations with the countries, and the legal of trust may impede security in cyber space. That's my closing remarks. Thank you for your cooperation. Thank you.

\*\*\*\*\*\*\*

This text is being provided in a rough draft format.  Communication access realtime translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings.