FINISHED FILE

APRIGF 2026

OCTOBER 7, 2026
FROM TECHNICAL DEBT TO STRATEGIC LIABILITY: ARTIFICIAL INTELLIGENCE, CYBER RESILIENCE, AND INTERNET GOVERNANCE IN THE ASIA-PACIFIC
KANCHENGJUNGA HALL
9:00 A.M. NPT

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
719-941-9557
www.captionfirst.com

This text, document or file is based on live transcription. Communication Access Realtime Translation (CART), captioning, and/or live transcription are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. This text, document, or file is not to be distributed or used in any way that may violate copyright law.

>> HOST: Crystal, I will help you here in the room.

>> CRYSTAL HSU: Thank you staff and friends, I'm sorry I couldn't join you in Kathmandu. I hope to visit Nepal and see the great mountains myself. I will introduce myself. I was a founding member of MSG and Board of Directors of Taiwan IGF. I attended and spoke when it was in Taipei twice. We will talk about resilience and emerging threats. Five months later, the picture is sharper. We are watching three tectonic plates moving at once, in the AI race between United States and China and the clock and the infrastructure is beneath our feet.

I put up this panel for one reason because I'm worried. But today I'm not here to spread fear, I'm here to show that we still have a window to act and what we can do together starting from this year.

So I think most of the audience are aware that back in this June, the five cyber Agency issued a rare joint statement indicating that AI is shrinking the discovery to exploit window from years to months and the support systems are not just technology, but strategic liabilities. That is where today's topic comes from.

I think two weeks ago, the White House just signed an EO

renaming AI to SI. Super intelligence across all of the executive branch. The AI signed a voluntary morally binding safety pact on the same day.

Today, I would like to discuss with you from the big picture. And because Cisco the company I'm working for we build and operate the world's infrastructure.

Our observation is frontier AI is shrinking Windows and turning today's stolen traffic into tomorrow's open secrets.

This is really make me up at night. So today, we're going to discuss this topic from a legal, Governance, policy, technical points of view. I'm very honoured to introduce with you about my panelists today. The first one, Joey Chen is a close collaborator at work. A researcher and speaker at major international Conferences. The second speaker is Jofan Yu has been my friend for years. She's a former prosector and now the CEO of TWNIC. And lastly, most important is Professor Aaron Lin. A highly respected reform advocate that took part in the UN human rights covenant. I'm very happy to turn the floor to Joey. Please allow me to share my screen with Joey's slides.

The permission is limited. So let me turn the floor to Joey.

>> HOST: Please share your slides.

>> CRYSTAL HSU: Oh, wait a second. Let us -- trying to ... We have a technical issue.

>> JOEY CHEN: Sorry about that. We need to rejoin the Zoom for screen sharing.

Can you see my screen right now?

>> HOST: All good.

>> JOEY CHEN: All good? Thank you. Wait a minute.

Okay. Yeah, my name is Joey Chen, I will talk about the cyber threat in Asia in 2025 and 2026. I will be focused on two issues. First state-linked Groups that are using devices no longer supported or systems that have not been patched to Internet network and stay there.

Second I will talk about AI can help you work faster and get the vendor less time to understand the threat and take action. For the threat intelligence team the question is connect what we know with those we need to protect. That started with the cases relevant to Asia.

So those four cases showing why devices and servers that age with the network need close attention. First, static tundra, a Russian state sponsored Group. They use an iOS code that had a patch. However using this patch exploit to attack worldwide.

And also in Singapore UNC3886 targeting all four telecom operators. The researcher link the Groups to China state sponsors. Also another China state sponsor is UAT-7290 also

targeting telecom network in South Asia, you see the SSH password attack.

In Taiwan there is an interesting Group of actors UAT-5918 using an unpatched public servers and it without Conference. It is the four selected cases of attacks in Asia.

Next separate to risks. Missing patch and end of life devices. Why they are so important.

So unpatched system has a fix available, but the fix has not been installed. End of life devices have reached the end of vendor support. Those can have problems static tundra shows how long a missing patch can remain useful to attackers. Cisco released the fix in 2018. The Group still using the attack workflow activity and the report is in 2025. Which means they're using this kind of exploit about seven years. And in separate cases, UNC3886 places a back door end of life Juniper routers and the research in 2025. Attackers have gotten insider access before passing the security checks.

Those routers were located not disclosures, but very critical issues in that period of time.

And this response depends on the problem.

We can patch supported assistance, we may need to replace or isolated unsupported devices. But attacker may leave access behind.

Let's look at how they stay inside the network.

This slide brings together the analytics of several reports. These steps can be one to another. They know what floor or stolen account. They can copy device settings and stolen credentials. Next they may use the access to reach other systems and can also use and compromise devices and attract traffic through another network. To stay inside they may be back door and hide activities. We look for change settings, expected connections or missing logs. A patch alone does not prove that attacker is gone.

So AI had another challenge for speeding up this part of the attack.

What AI can do? It can reduce time of attack spend on the research and worktime workflow. In May 2026 Google intelligence team report a suspected Chinese link agent in Japan and East Asia targeting. Those two help to explore the targeting and check the witness. In a separate report show how the workflow can be. After that it could be Cloud environment or network environment. Suspect cybercriminal actors to plan, build wrong credentials in the campaign. In under six hours. These victims are like worldwide. And pretty much most in Asia specifically.

The last part is about the threat intelligence to help us to decide what we should do next. First, connecting reports about the attackers to our own systems and check if the devices

are exposed and whether they are still receiving support. And give priority to those attackers are using. Second, fix the exposure patch on supported systems and replace unsupported devices. Check for back doors and stolen access are already outside of the network. Third using AI to match the right report to our systems and reveal all of those. People still need to check those results and make response decisions. Yeah.

So the goal is simple. To fix the exposed system early and act before attack move further. That is what we think in our assessments. So thank you.

>> CRYSTAL HSU: Thanks, Joey. A quick key takeaway from what Joey just spoke about. The median time to explore for new disclosure went from 30 days to five days. So this is a very urgent situation that all the Government and industry and public need to face.

So next I would like to turn the microphone to COO Jofan Yu. I'm wondering from the operators Chair, what should the Government and the relevant parties should do?

>> JOFAN YU: Thank you, Crystal. I also have slides. I'm not sure if APrIGF Secretariat can help me to share the slides?

Thank you again Crystal. I'm Jofan Yu, it is a pity I can't join on-site to meet everyone in person. I apologize for this. Due to local commitment. I hope I will meet you in the future, maybe next year.

So today, I would like to approach this discussion from perspective of Internet infrastructure perspective.

So when we talk about the technical debt, we think about old server, outdated software or device that should be replaced maybe five years ago. From the perspective of Internet perspective like a link. We think of it also as a Governance problem. Sometimes I think the question is not simply whether something is old. Next slide, please.

I think the difficult question are usually who is responsible for keeping debt, the device of everything in the environment is secure. And who is responsible for replacing that? And who pays for the transition? And what happened when responsibilities divided among the many different actors?

So I would like to share Taiwan's experience especially the experience related to IPv6 and IP abuse. And recently in the supply chain regulations as well. Next slide, please.

Okay. First IPv6. So we have been working IPv6 transition for many, many years.

So by 2025, finally, IPv6 capability and usage in Taiwan have reached roughly 58%, depending on the measurement and methodology. Of course, we are happy with this progress. But we also notice that so when you have a margin network that supports IPv6 very well. But somewhere in the ecosystem, you

still have the old device and old application and old operational system and old automated system where it is not ready to make the transition.

We think that is actually where the real difficulties begin. IPv6 is not only the technical deployment exercise, it actually requires like the coordination amount of the network operators of course. Also include the equipment manufacturers, like routers, servers, application providers and enterprises and also the uses and also sometimes Government agencies.

Actually it is not only the deployment of technology by ISP, but it also requires a life cycle planning as well.

So if we don't have any life cycle planning, meaning also do that, we will create another layer of techno debt. Because then in the whole system, we will have old device and software. But the new protocol. Or sometimes the new and old protocol together. Then we make the environment very complicated. And less resilient as well.

Okay. Next slide, please.

Okay, let me also turn to compromised devices and IP abuse experienced in Taiwan. Maybe you know that TWNIC is a Taiwan CCDOD. As a registry we set at an interesting point of the Internet. We don't manufacture the device. We don't operate the network, we don't control the application and we are not a Cybersecurity regulators or expert. But if we do manage the IP address. And when the device is compromised, the abuse eventually appears on the Internet and often through the IP address. So IP address may be where the problem becomes visible, but it is very rare that it is where the problem started.

So we have seen very concrete examples of this in Taiwan. So for example, the Taiwan security Authorities constantly reported cases involving the compromise of routers, aged devices and network equipment including EOL products for which updates are no longer available. When we see this, we have a simple answer. Okay, just patch any device, block the IP address. Sometimes of course the actions are necessary. Actually in our view, they don't really address the Governance problem.

Because when we trace back the problem, we may find a whole chain of responsibilities. So the manufacturer may no longer support the product anymore. Or update.

The owner may not know that the device is vulnerable. And I think it is usually is the case. The ISP may only see the suspicious or malicious traffic but nothing more.

The registry, and we receive abuse information. Law enforcement they need information from several different party stakeholders.

Now single actors actually have the whole picture, complete

picture.

So that is why I think the Internet resilience requires it to move beyond the idea that the Cybersecurity is simply the responsibility of the person operating the device. We also need to ask whether the product was designed to be secure. Whether it asking receive security update and how long you will be supported. And whether the owner knows when the product reach the end of the life. So this bring me to the third point. The next slide, please.

So some of you may be aware that there is an interesting development in Europe. The European Cyber Resilience Act, the CRA. It is an interesting development and very important development as well. In terms of Cybersecurity.

So why I think it is important or is a significant about the CRA? Because I think it is moved part of the responsibilities upstream.

Now we always just talk about who operate the device and who is victim but this act starts to move the responsibility upstream. Moving to the manufacturers. So instead of asking whether an operator patch of the device, the framework actually asks what responsibility belong to the manufacturer and the supply chain. And also the importers and the disputers as well. The CIA introduce requirement around the Cybersecurity risk assessment for the management security update define support period. They make it an application. And also bring greater visibility into the software exponent and dependencies including the use of software materials.

So in other words, it starts to ask more fundamental questions. If we are going to connect millions of product to the Internet, who is responsible for the security throughout their life cycle? I think it is a really important discussion and direction. Maybe also useful for Asia-Pacific as a reference as well.

If AI is dramatically shorter time between discovery and exploration we cannot continue to operate the infrastructure according to the life cycle design for a much slower threat environment.

A device that previously remain in operation for maybe 10 or 15 years is quite common, I mean, now, may no longer be acceptable if you stop receiving security update after three or five years

Create a very critical Governance challenge. What shall we do? Next slide, please.

I think I am over time. I just quickly, I mean just explain what I think. Then I maybe leave the details until later Q&A time.

So for me, I think the most important things, actually, is

the visibility. So we have lot of information, but I think the visibility is still not so high. So how we improve it is important. Second, the cooperation. Not the local cooperation, the Regional cooperation. We know Internet is connected globally. When you are safe in your country, that does not mean you safe globally on the Internet.

So how we do the cooperation Regional, globally is important.

The third one is very practical. It is that how we use the procurement system to have more incentive for like manufacturers and ISP to move. To more secure environment. I think it is also an important thing.

So my next slide, please.

I think in the end, I would like to share just one thought. We often describe tech debt as something we can deal with later. I think especially now, with AI and the Internet environment, I think later will become very expensive. So technical debt is more like a strategic liability, when the time is to fix the infrastructure becomes longer than the time the tech needs to explore it. If AI is continuing to compress the window, like Crystal mentioned, the life cycle management is no longer IT issue. It is a digital infrastructure Governance issue as well.

So I think resiliency is not only how quickly we respond and fix and when something goes wrong, in my view, it is whether we replace to upgrade and secure it before it becomes the next crisis. Thank you.

>> CRYSTAL HSU: Thank you for the excellent sharing. The key takeaways from the Jofan Yu presentation is for the system, geopolitics does not wait for Treaties, it travels through your unpatched routers.

I think everybody knows this now, later the stealing happens today at this point in time, then the equipping later. The migration window is the same window we have for (audio skipping) and this needs Regional and global cooperation.

So I think Taiwan sits where we meet.

We understand the threat with Cybersecurity legislation in motion, including the retire, PQC, so on. That can model Governance for the whole Region.

Right now, our last but not least speaker, Professor Aaron Lin. I think we really hear his voice at this Forum but always need. Professor Aaron Lin when the infrastructures fell what happens to evidence, and (?) and due process. Because justice is the last to fall. Here you go Professor Aaron Lin.

>> AARON LIN: Hello, everyone. It is good to be here with you today. I apologize we can't meet on-site in Nepal.

In attack wars almost everybody is familiar with the idea of technical debt. The classic card where you shift code today

to pay compounding interest in budgets, patches and system failures down the road.

Today, I want to explore how the dynamic plays on our critical systems taking Taiwan as the concrete idea.

In July 2024 Taiwan updates the code of procedure to ratify the investigation. The law enforcement was given formal statutory authority to use tools to operate in legal grey zones. Things like GPS trackers, catchers and civilian devices and emergence.

On paper it sounds like an important step forward? Right? Yeah.

If we look at this through the lens of scientific science and other studies we see patterns. The social, technical imagery. The trap of the technology illusion. The writing of new technology into the legal status would ask as a civil budget for tackle complex cybercrime and transnational events and so on.

The reality is different. Considering bureaucratic infrastructure and public and private partnership likes transparency. When no one budgets for the long-term maintenance of technology, the system falls under the technical debt.

Because of that the real world information is the digital forensics in the handling has been limited.

To really see what is happening here, we can break it down into through key dimensions. The first, the new law completely misses the important compounding of majors.

It strikes to a rigid checklist style approach that simply enumerate the steps of the specific device but that list just can't keep up with the ready technology change.

Nor does it capture the combination when multiple tours work together.

When police by the tools from the private vendors, Officers can only click around in the user interface. They have zero control over the online code or the system logs. This leaves the entire process, the digital forensics and the cause, to what is thought to be the scientific validity and integrity.

And third for chasing and maintaining this specific specialized gear is incredibly expensive. Even now, the majors are written into the status. But police still can't actually afford to use them.

On top of that, mobile forensic tools frequently expire without updates. Creating a real practical bottleneck in gathering evidence.

In other words simply chasing this is not enough. The Government also has to set up and invest in basic infrastructure and build across Agency collaboration with proper founding in place. And they need to weigh across the different device and

keep the lines of communication open between the Public and Private Sector. Tech investigation is the product of legal and social network working together. Simply tackling new powers on to the books and the law is never an effective solution on its own. Look at this through the relationship between the technology and the social networks.

The nature as it is imposed is deploying it relies heavily on the hands-on experience of individual operators. These Officers, the Officers past the prolonged exposure to high electronic radiation while the organisation lacked the proper update of the rotation and regimes. The hard earned experience is lost and talent is out the door.

What this tells us is the technical personnel is not just about the technical. It is about taking seriously the relationship between the technology and the human being and the substance.

Or through the lens of regulatory Governance. Truly effective tech isn't about chasing gear for its own. It is about the cross-Agency collaboration. If the Government can use the integrity platform to manage the operators, coordinator the request and the delivery, the routes of the path ourselves, we can curve the commercial politics through low intensity monitoring.

To rev up the Court issued tech invitation needs to be reframed around the infrastructure and the technical debt management. Rather than believing that technology is racing to catch up with the crime and the solution. Only by bringing together technologies, budgets, personnel, agencies, social network can we fix our infrastructure as part of the legal resilience and truly meet the demand of the Digital Governance, human rights and properly trust in the system. Thank you very much.

>> CRYSTAL HSU: Thank you Professor Aaron Lin for your extraordinary sharing of the judicial systems.

Right now, is my time for four minutes to conclude the session. I want to state that the previous exploitive from Asia-Pacific including the port of Nagoya paralyzed by an aware. And in 2024 there were 10. And a fire destroyed 96 systems in Korea National data centre just last year. All those bills for deferred maintenance need to be paid.

So (audio skipping) (distorted) for angles from tech to Governance to legal and policy. So these are the five life risks.

Today, I would like to reiterate again, the first one is AI shrinks the exploitation window. And the second is EOL, the tech debt liability about how local, Regional and Global Government, what we should do next. And third one is age device

are durable first thought. Then like Professor Lee just said, the rule of law is institution targeted. The final one is the data with the decryption. These are the five urgent life risks we are seeing.

Right now, I need one from each panelists from my learnings.

So my first question to Joey Chen, the researcher. If a Government CEO in this room my fund one thing this year, patching or replacement, what does Talos data suggest?

>> JOEY CHEN: Yeah, from our perspective view, we suggest to replace the EOL devices. Because as we know, we saw a lot of cases, the customers or probably victims they're trying to use a new firewall or probably using SS control, trying to fix those already known exploit or vulnerability, trying to fix that and protect their aged devices. However, if the Director found another way to get inside and access to the aged devices they can directly use those known exploitations and do that. For example, we saw cases where the threat actor found the bots in their internal network. And targeted victim did not replace the devices. However they put out a new firewall outside of those aged devices. When the threat filed their SS they can get an SS into the internal network. It is not probably through those firewall. Probably through another way. When they get access, they can use the known exploit vulnerabilities to use the vulnerability of the devices and to do the movement.

So our suggestion is to replace and or isolate those EOL devices will be a better choice than just fixing those bugs or vulnerability devices. It is more faster than, you know, blocking those vulnerability devices. Yeah, that is our solution. Our suggestions.

>> CRYSTAL HSU: Thank you, Joey. The second question is according to what you shared this morning, what is the one mandates or legislative thing you wish the local, Regional, global to do?

>> JOFAN YU: Okay. The mandates?

>> CRYSTAL HSU: Or resources.

>> JOFAN YU: Thank you, it is an interesting question. Usually the registry, I think we think it is a security or resilience, it should not count on the Governance and resources. Or the mandate. I think it is actually I think it is a whole ecosystem cooperation.

So I think for me, it is my first reactions. And second, I think what actually the Government can do actually is the regulation and policy.

So we have been, you know just promoting like IPv6 and RPKI and now of course, continue promoting like DNS sec. If you only rely on the market, the progress will be so slow because you

involve the cost and the benefit. And also, I think it is very interesting point. I mean, for security and resilience, actually either you do it, you know, if you are very good to comply and deploy everything. But in the whole system, most of the people they don't do it. It is still not so, you know, useful.

So we need to have more collaboration in the ecosystem to have more deployment in the ecosystem. Based on our experience, usually you really rely and need the support from the Government.

And I think of course, what I mentioned in the Cyber Resilience Act, the EU is a good example. I think through this kind of effort even in Taiwan because we have a lot of the manufacturers, you know, like the routers, the device, phone, and everything, servers. So I can see, you know, only when a draft was released, all the manufacturers in Taiwan they start to start it. And they start to think about how to deploy it.

Then they target to get the mark. Before the effective date. I think it is the power of the policy, the Government policy and regulation. How we can just use that to accelerate and also persuade. Most of the major players in the ecosystem to deploy new protocols or standards or new obligations, it is actually what the Government can do.

>> CRYSTAL HSU: Thank you, Jofan Yu. Before we go to a lightning round with the audience, to Professor Aaron Lin if there is a broach today, what is the one thing you tell prosecutors, lawyers or judges must have done today?

>> AARON LIN: Thank you, Crystal. I think the core evidence systems were hacked today, tomorrow morning. Best discussions on the tech and tech enabled indications, the very first thing the lawyer, prosector and judge must do today is strictly secure and verify the chain of custody. That is the most important thing for the criminal justice system and to get the links of integrity. It is for the forensics.

To highlight, when we led the underlying code and logs, it is not a serial bot. We must address infrastructure vulnerabilities and techno debt rather than building the black box systems.

I want to discuss the role of Government. Not the lawyer side. The Government must go beyond chasing the statute and the vast infrastructure across Agency collaboration to support this kind of thing.

Second, the adequate budget is essential to weigh the events and resolve the bottlenecks I said before, like expired forensic tools and mentality issues.

The Government needs to strengthen the private and public communication. That is important for the earth to be talking.

To ensure the transparency of the underlying code and log. That is something like that is needed, it is very important.

Finally we must tag the technology between the human and security. And the proper upkeep to safeguard for the police to do these kind of things and to the judge and prosector.

Sure, the Government must reframe the attack around the theft management. Building truly legal resilience through the integration of technology. Budgets, personal, and some social net worth. That is the most important thing. Thank you.

>> CRYSTAL HSU: Before I open the floor to the audience, I would like to conclude that from what we have heard today, I think I can conclude five asks for the local, Regional, global Government as the legislative seats. The first one is the EOL retirement framework which we spoke a lot today. The second one is procurement security requirements.

To be aligned with EUCRA direction like Jofan Yu mentioned. The third is integration timelines and the fourth is the drills.

Through the APrIGF document we need Regional cooperation and build procurement language and EOL related information shared across the Region.

Okay.

So before the lightning round, I have one single question for the audience. What is the single most urgent piece of legislation for Asia-Pacific Government in 2027, which is next year? Okay?

So we have 15 minutes left. So the floor is now open to the Moderator and the audience online and onsite. Thank you.

>> HOST: Thank you, Crystal. I guess this is a cue for people in the room, your comments, thoughts, especially what should be the priority on these type of technical debts and EOL systems problems? Thoughts?

>> ATTENDEE: Okay. First, thank you for the presentation. My name is sim Jan I'm from Korea. I have a question to the person that have Orange background. I know Australia has made baseline device security. Singapore and Japan are using schemes from the virtual recognition. These are compliance tools that mainly apply to new products. EOL devices already deployed are hard to address.

My question is what Governance structure should handle this problem and diversion. Thank you.

>> JOFAN YU: May I confirm, you mean the question in the APAC, the Governance structure? Is my understanding correct?

>> HOST: The question is about the part you suggested is for.

(Overlapping conversations) (distorted)

>> HOST: This is the highlight of end of life, what is the suggestion? Did I get it right?

>> ATTENDEE: Yeah.

>> JOFAN YU: Okay. I'm not sure if I can have specific advice. But I understand that EOL, it is really becoming the problems for many people. I think it is also very common problems for users as well. I remember in Cyber Resilience Act, they request the manufacturers to support or update for the whole life cycle.

I think it is at least like 10 years or something after they release the products.

So I think I'm not sure if it is really, you know, a specific and good proper balance because you need to balance a lot of different things, from the manufacturers, users, everything.

But I think then it is good that we can learn from EU's experience because remember, this application will be effective next year. Maybe November or December. Through the process, a lot of discussion in Europe. I think it will be a good reference for us for Asia-Pacific. But of course, we don't have an EU European Union we have a different hierarchy structure.

How to deploy in the local country or have more collaboration in the Asia-Pacific, I think that is what we can think about.

>> HOST: This is Edmon. I can add a little bit. Maybe one things that can be looked at. If the system is widespread use and the provider decides to end it life, maybe there are coordination that requires the provider to extend for more so people can transition to newer devices. That would be a Governance and policy potential perspective. But since I have the mic, I have one more thing that came to mind as this was being discussed. Especially when Aaron Lin responds to the last question.

Today, we have the things called triple bottom line. A lot of companies need to report on environmental impact and those kind of things. Maybe technical debt is something that needs to be part of the financial accountability as well. That could change a lot of things, right? Today we have in accounting principles we know how to depreciate property. It is very, you know, specific. But we don't have a very specific depreciation for these technical systems. Some companies do it. Not all companies do it. It is not a requirement. Maybe part of this is to require companies to include depreciation on the systems and also to report on the technical debt, essentially that they're racking up. That might be an interesting approach. I don't know if the room or Crystal, I guess back to you, in a way, have any other thoughts?

>> CRYSTAL HSU: Thank you for this question. I would like to bring up the Washington model and Australia model. For the

Washington model, I think this day in local Cybersecurity programme is the answer for the U.S.-Government related issues. It is a grant linked framework. Not a blanket EOL mandate for all the state Governments.

Like you mention, where the money flows the requirement follow.

For the Australia model they issued a new directive two weeks ago, indicating requiring commonwealth agencies to strengthen management of legacy and EOL technology. The non-corporate commonwealth must complete a stock take and larger risk plan. I think looking at the two models, it ties the security to facing our Internet as accessible EOL systems.

Then compara has given the Federal agency debt. The direction of travel is set. The only question is whether we move by grant, directive, or by law. I'm not saying the Washington model or Australia model is the best for Asia-Pacific Governments to follow.

Like my initial thought to present at this session, I would like to call for consensus. And align action to combat these new emerging risks. I hope this address your question.

>> HOST: Well, we have 10 minutes left. Any other questions or thoughts from the room? Or online? It is a bit of a quiet room this morning.

I guess in that case, perhaps, Crystal, you can talk about the current situation since you are in Taiwan. What is Taiwan's kind of progress on this, whether it is, you know the -- by motivation or by legal regulation? How is this issue progressing in Taiwan?

>> CRYSTAL HSU: I think for example, from my observation there are two layers. The first layer is the budgetary problem. The Government cannot prioritize its budget to renew all the machines. The second is the legal framework. In Taiwan we have 10 SLP to retire the machine. You cannot easily throw away.

I would like to make a point that the AI risk is very away in the public. We cannot do it alone. We shared learned lesson and transparent investigation. Not each company or single Government can do its own work. I do have a question for the audience onsite and online.

Outside of Taiwan, Nepal, Southeast Asia or the Pacific, what does it look like for your economy? Or do you have any hands-on experiences on tackling this issue?

>> HOST: In the room or online?

I would admit that I'm not sure of the situation in Hong Kong. I don't think it is a very high priority topic at the moment. I would need to find out.

Perhaps other speakers, on how to take this forward?

>> JOFAN YU: I will start my understanding with the Taiwan

situation. I think that maybe like most countries, I mean, yes, I think in Taiwan it is still also not a lot of attention paid to this. From Government side the critical infrastructure. How to look at the critical infrastructure is still a top priority for the Government.

But I think then, if you are talking about -- to move to a more whole ecosystem, how we make sure, you know, everyone is responsible for their own, you know, work? It is still a complicated issue. It is not on the table yet. So I think it is a situation.

On the business side, I also think, I mean, the life cycle, this kind of management to retire the product is also not so common. I mean, in the industry.

People know it is a life cycle and maybe people will buy some update. But I think it is for, the concept, how we control that, I think the industry still focuses more on the cost, not, you know, to have more like security. So I think that is the situation.

I do see a positive side. Because a lot of Taiwan manufacturers, they export their products and devices to Europe. Europe is a big market for Taiwan. So I did see that when, you know, maybe in the market, I mean, maybe most of the device have already comply with the European standard maybe it is a time for Taiwan and Government to have more clear policy and also regulation. Because they would not be so many pressures. I mean ... pull back at the time then.

>> HOST: You agree very much with what Jofan Yu just mentioned. I think what I was saying we know how to depreciate the hardware, in terms of patching and end of life of systems, there isn't a mechanism for corporates to think about it.

I think you want to jump in? The speaker?

>> JOEY CHEN: Okay. I think -- yeah. Because I think your conclusion is right. It is mine. Okay. Yeah, because about the question, I think the whole Cybersecurity for this EOL my recommendation is we should -- because doing Cybersecurity we should take one team together. For example, from Taiwan's point of view, do a lot of forensic response in Taiwan's cases. I saw there is a lot of devices, not just one product. Because the threat knows we have a lot of devices that probably including a lot of brand in one of the critical infrastructure, maybe in telecom. In hospital. Probably in Government. They have a lot of devices there they of not only targeting one of the devices they were targeting all of the aged devices. So retiring one of your devices is probably very important. My suggestion is retire all of your devices will be the best way to protect all of the environment. Because they were not just targeting one. They will focus on what you have. If you are trying to protect

it with only one firewall or using the SS control to protect the network's ability to the outside network, this is just making, you know, the ability for the infrastructure that looks protected and looks safe. However the threat actor will always find a way to get access to it using a known vulnerability in your device to do that. So on. So, yeah. I know the budget issue is a very critical issue. My suggestion is if you do not protect this one, if you don't cost the money or the time, later on the critical infrastructure will be damaged, the damage will increase in the future. Yeah. That is my point of view.

>> HOST: We have two minutes left. I will pass it back to you Crystal, for the ending remarks.

>> CRYSTAL HSU: Thank you panelists, Moderator online and onsite. I'm glad we have a chance to discuss about this serious situation. Of course APJC.

I think my key takeaway is this is too important and too urgent to do this alone.

So this is real teamwork and team sport. With the advancement of AI and quantum we need to use AI to combat by AI. That is the final conclusion line. Thank you Moderator, audience and extraordinary panelists today.

(Thank-yous)

>> HOST: Thank you, panelists and speaker, I will make a quick announcement. Up next at 1015 here in this room, will be next session is the right to be forgotten in AI, who owns the Foundation in the models. This room, the right to be forgotten by AI. The session for the next room next-door in room 1 will be from shut down to solidarity, co-designing a rapid response protocol for Internet shutdowns. Those are the two upcoming sessions. Don't forget to add your thoughts from the synthesis document. Go to comment.APrIGF Asia. Join us for the Town Hall session in the main room, which is on the ground floor this time.

(Music)

The last Town Hall for the synthesis document at the ground floor auditorium.

(Concluded)

This text, document or file is based on live transcription. Communication Access Realtime Translation (CART), captioning, and/or live transcription are provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. This text, document, or file is not to be distributed or used in any way that may violate copyright law.