# Transcript

## Section A

00:00:00 Interviewer

Alright, next we are going to conduct an interview with TPU4. First, I will start from section A, and the first question doesn't need to be answered, you are obviously from the public sector. The second question is about your unit at work.

00:00:13 TPU4

Our unit is the [a government criminal investigation unit].

00:00:18 Interviewer

Okay, and how long have you been working in this unit?

00:00:22 TPU4

12 years, yes.

00:00:24 Interviewer

Wow, very experienced. And the fourth question is what kind of position do you hold?

00:00:29 TPU4

Currently, I am the Assistant Supervisor.

00:00:33 Interviewer

And what are your main responsibilities?

00:00:35 TPU4

Mainly to handle cases related to internet crimes in Taipei city. The major cases will be issued to us.

00:00:43 TPU4

And our whole….

00:00:47 TPU4

We are mainly responsible for handling internet crime cases in Taipei city, and we also handle the procurement of equipment related to technology crimes in Taipei city. So, all the equipment related to technology crimes in Taipei city is managed by our team.

00:00:58 Interviewer

OK, so you also mainly investigate criminal cases?

00:01:05 TPU4

Yes, we also investigate criminal cases.

## Section B

00:01:07 Interviewer

Okay, got it. Let's move on to part B. The first question in part B is about your understanding. What do you think is the main network attack that Taiwan is currently facing, and what are the methods used? Can you give an example?

00:01:17 TPU4

What we often see are things like DDOS attacks. For example, there are also attacks where data is stolen, such as sequel injection, where the entire database of personal information on a network is stolen, packaged and sold to scam groups for fraud. Another example is a few years ago when Taiwan was invaded by ATM hackers. After they broke in, they had control of the entire ATM system, which was then jumped over to the First Bank financial center from London, and then to the ATMs. They had direct control.

00:02:10 Interviewer

Wow, London?

00:02:13 TPU4

Yes, because London and the headquarters here are part of the same internal network.

00:02:19 TPU4

The internal network is better because it doesn't go through the firewall. It's an internal network. Because it comes directly through a VPN, it's the fastest and easiest way, and there's no way to block it.

00:02:34 Interviewer

I see.

00:02:37 TPU4

There are also attacks where web pages are replaced.

00:02:40 Interviewer

I see.

00:02:40 TPU4

Hackers from the other side of the strait (China), for example, are often able to access some important facilities like the Presidential Office and other important websites because their management is not strict enough. Later on, like at National Taiwan University, they replaced their webpage with the flag of five stars.

00:03:01 Interviewer

Oh, I see. This has been reported in the news. Okay, then the second question is, what are the targets of cyber attacks in Taiwan currently?

00:03:14 TPU4

In general, we mainly see DDoS attacks on banks, which were very popular recently. The entire bank is blocked, and then after the attack, they send an email to extort money...

00:03:21 Interviewer

I see.

00:03:29 TPU4

Okay, this extortion. We often see this kind of thing, as well as stealing data.

00:03:34 Interviewer

I see.

00:03:41 TPU4

This is mainly done by looking for vulnerabilities in websites and systems, and if there are any, they will exploit them to retrieve data.

00:03:52 Interviewer

Okay, why do you think this is happening? Is it because their network security measures are not strict enough?

00:04:00 TPU4

I feel that the cybersecurity concept of the cybersecurity professionals is not yet fully mature. Additionally, there are simply too many vulnerabilities at present, and these are not something that security personnel can entirely control. Many of these vulnerabilities are discovered in various high-tech domains, such as penetration testing and foreign vendors, where they are extended and developed into commercial products based on those vulnerabilities. Over time, as knowledge about these vulnerabilities becomes widespread, they start to leak out gradually. Naturally, these vulnerabilities become targets for attacks and testing purposes.

00:04:59 Interviewer

Okay, let's move on to the third question. What do you think are the factors that affect the overall cybersecurity in Taiwan?

00:05:09 TPU4

For Taiwan's internet...

00:05:12 Interviewer

Why are there so many cyber attacks happening in Taiwan?

00:05:19 TPU4

Well, it's because there are too many vulnerabilities, as I mentioned earlier.

00:05:27 Interviewer

I see. Too many vulnerabilities.

00:05:28 TPU4

And the knowledge of cybersecurity professionals cannot catch up immediately. Also, some of the systems, such as websites, need maintenance and funding.

00:05:45 Interviewer

I see.

00:05:46 TPU4

However, their budgets may be insufficient, so they tend to just leave the websites as they are, saying they haven't done anything important with their websites yet. In fact, some websites are still there, but their networks have already been compromised and turned into relay stations. For example, we have intercepted data theft from our government agencies by China through such relay stations, sending the data to cloud services in Australia. Not every cybersecurity professional can understand these things such as they are publicized or something like that. So, we have seen a lot like this. You want a factor? Actually, because there are too many vulnerabilities in the network, we cannot trust that it is 100% safe. We have to be careful with any actions taken on the network.

00:06:50 Interviewer

Okay.

## Section C

00:06:59 Interviewer

Okay, then let's move on to the next section, which is next page, part C. So, the first question is quite general. What do you think about the overall plan of the Taiwanese government for internet security based on your knowledge?

00:07:13 TPU4

Our Executive Yuan has actually established a National Communications and Information Security Development Plan. This plan provides a general direction and important guidance, but when it comes to ensuring that every unit's information security personnel reach a certain level, there is still room for discussion. Some people's level of information security is uneven, which can lead to more vulnerabilities in some areas which is serious.

00:07:50 Interviewer

I see. So, you think that there needs to be more emphasis on training information security personnel, even with the general direction set by the plan.

00:08:02 TPU4

Yes, there needs to be more emphasis on that.

00:08:03 Interviewer

Got it. Now, for the second question, do you know of any strategies currently being used to prevent internet threats? And what do you think about these strategies? For questions 2 and 23, which can be answered together, where do you think these strategies can be improved?

00:08:22 TPU4

Actually, we have many cybersecurity measures in place currently. For example, there are network activities and behaviors. For example, we often see the use of social engineering to infiltrate networks, where individuals such as employees unwittingly clicked on a data engineering link and then the system was infected with a Trojan horse.

00:08:41 TPU4

After being infected with a Trojan horse, it exhibits certain behaviors. For example, the Trojan horse may periodically transmit data externally, and these behaviors are detected by our computer systems during network monitoring. For instance, if a machine is observed to transmit data during late hours irregularly, it triggers an alarm or alert, indicating a potential infection. Security personnel would then investigate that particular machine. It's important to note that, currently, no system can claim to be 100% secure. Nobody can confidently assert that.

00:09:37 Interviewer

So in that case, where do you think we can improve?

00:09:42 TPU4

Maybe in some aspects, like the social engineering technique that I mentioned earlier, the Trojan model may need to add some modules, such as behavioral patterns. You can create several sets of similar alarms or mechanisms to detect these patterns.

00:10:05 Interviewer

So it will become easier to detect?

00:10:06 TPU4

Yes, that's right.

00:10:07 Interviewer

I understand.

00:10:09 TPU4

However, if you add too many layers of protection, it may cause your network to slow down, and sometimes you may not be able to connect to the internet or it may become slower. This is the negative impact.

00:10:34 Interviewer

So it may become more troublesome?

00:10:37 Interviewer

That's okay, please continue.

00:10:38 TPU4

Another issue is that when we implement these security mechanisms, some users may feel uncomfortable and find them inconvenient. They may feel that they have already gotten used to the old system, the security measures now make them very uncomfortable and are not user-friendly. This creates a dilemma.

00:11:03 Interviewer

Yes, it's a dilemma.

00:11:03 Interviewer

Okay, let's move on to questions four and five,which can be answered together. Since we were discussing preventive measures earlier, do you have any specific strategies or methods in place for responding to network attacks when they occur? What do you think about these strategies and their effectiveness?

00:11:25 TPU4

Actually, over the past two years, we've encountered a hacker who spreads false information on the internet, claiming to be someone who will attack the government or plant bombs. He goes by the name Takahiro Karasawa, and he imitates the behavior patterns of previous individuals who have made similar threats. He uses them as targets, and the police are constantly looking for him.

00:12:04 TPU4

As a result of these incidents over the past two years, there have been over 30 cases of security threats in Taipei this year alone.

00:12:13 Interviewer

I see.

00:12:16 TPU4

If someone is constantly threatening like this, we will try to collect evidence of their behavior patterns. For example, their language and the methods they use, such as using Tor to send emails through an onion browser or using 10-minute mailboxes for two-factor authentication. We will also collect evidence of their behavior, such as visiting government websites that do not require two-factor authentication. For example, the Intervieweref's Public Opinion Mailbox or the Presidential Office Public Opinion Mailbox.

00:13:14 TPU4

As long as they log in to the website, they can send their intimidating messages directly. However, we can analyze the behavioral patterns from this to identify certain patterns. For example, we can collect information from the web log of the website he logged into. We can collect data such as the IP address of the person logging in.

00:13:37 Interviewer

I see.

00:13:42 TPU4

When you log in with your IP address and the UC engine of the machine you used, we will make some records. Then we will collect all these things and cross-referecne with the victimized units of each case. Once we confirm that it was the same person who did it, we will find the person. In this case, we found out that the person was actually on the other side of the strait because he was a student from China.

00:14:12 Interviewer

I see.

00:14:13 TPU4

He studied in Taiwan before, and later because he was pursuing a girl, yes, but the girl didn't like him, so he became crazy and wrote reports everywhere, using the instructor's report to threaten others. His behavioral pattern is similar to the current one. In the process of investigating this case in recent years, we have pulled out the entire behavioral pattern and confirmed the identity of the suspect.

00:14:47 Interviewer

Okay.

00:14:50 Interviewer

I saw in the news that he was trying to do something to the Japanese railway...

00:14:52 TPU4

Yes, he caused nearly 200 schools to be affected.

00:14:57 TPU4

Yes, it was him.

00:14:59 Interviewer

But now he has returned to the other side of the strait, so there is no way to continue tracing?

00:15:02 TPU4

Actually, we have used Cross-strait Division to constrain this person in China, but they are also very aware that….

00:15:12 Interviewer

Hmm.

00:15:14 TPU4

After they constrained him today, because he is considered mentally ill and has some major mental problems. They were afraid that after we constrained him, he would go after Xi Jinping, so they said they won't deal with it.

00:15:33 Interviewer

And it's very difficult, and it also requires cooperation.

00:15:36 TPU4

Yes, that's right.

00:15:37 TPU4

So, we will focus on some of his behaviors and patterns and do some defense, for example.

00:15:48 Interviewer

Okay.

00:15:50 TPU4

Now, for those who don't use security mechanisms and people can directly submit some messages, we will suggest…. For example, last month, we told the Taipei Metro that their security mechanism and public opinion mailbox cannot be set up like this. If you set it up like this, attackers will keep sending messages and threatening your website, so you need to have two-step verification in your public opinion mailbox.

00:16:16 Interviewer

Okay.

00:16:17 TPU4

For example, you need to use your real name or a verified email address or phone number to leave a message, and you will only allow the message to be posted after verification. After setting it up, there seemed to be fewer problems. This is a protective measure, similar to using certain methods to protect against threats.

00:16:41 Interviewer

I see. In what areas do you think this kind of protection mechanism can be further improved?

00:16:51 TPU4

It really depends on the individual case. Each case is different, so how to pursue it depends on the specifics of each case.

00:16:53 Interviewer

Um, it's okay that every case is different. Okay, let's move on to the sixth question. Questions six and seven can be answered together. Since we talked about the attack just now, the sixth question is about the measures you will take for reflection after the attack. What do you think about these measures? Which aspects can be improved further?

00:17:15 TPU4

For example, about five or six years ago, many domestic banks in our country were hit by DDOS attacks, and it was different banks each time. This caused their entire order system to hang, and they couldn't place orders at all. So everyone started thinking about how to solve this situation caused by large-scale bandwidth DDOS attacks. Later, it was realized that, fortunately, before entering the website, they had a traffic cleaning mechanism, which redirected large amounts of traffic to another location.

00:17:55 Interviewer

Mm-hmm.

00:17:55 TPU4

Because of the large volume of fixed IP addresses or similar behavior… because our system requires a response after sending out a request.

00:18:05 TPU4

So for strange traffic that only sends requests without requiring a response, we will redirect it to another location outside of our country. This ensured that the website could operate normally. At that time, traffic cleaning was very expensive and was calculated based on the amount of traffic. Currently, only China Telecom and a few other larger second-tier telecom providers can afford it. So we teach them to set up traffic cleaning mechanisms, so that their websites will not be attacked in the future, or even if they are attacked, the traffic will be directed to another server.

00:18:54 Interviewer

Okay, got it.

00:18:59 Interviewer

So do you think the measures you mentioned earlier are enough?

00:19:05 TPU4

Of course not, of course not. As I said earlier, many cases need to be assessed individually because nobody knows about them until they happen. If it never happened, no one will know. After a case happens, everybody then realizes they need to take preventive measures for similar cases in the future.

00:19:22 Interviewer

So we need to target them specifically, since their cyber attack methods are constantly evolving?

00:19:27 TPU4

Yes, that's right.

00:19:29 TPU4

Actually, we see many fraud syndicates nowadays.

00:19:34 Interviewer

Fraud syndicates?

00:19:35 TPU4

Yes, they're not centralized but rather dispersed. For example, the first step for a fraud syndicate is to steal personal data. They have some cybersecurity personnel in our country. For example, cybersecurity personnel in China scan the databases of Taiwan's businesses, such as Kingstone Bookstore, for vulnerabilities. If they find any vulnerabilities, they start attacking and stealing data. After stealing the data, they sell it to the fraud syndicates.

00:20:12 TPU4

Furthermore, they may put some of the stolen data on the dark web for sale. The fraud syndicates will buy it, and then start their own operations, such as the "water rooms" and money…. Each group operates independently, and they use different fake accounts and identities.

00:20:31 Interviewer

I see.

00:20:35 TPU4

You can see a lot of fake accounts now, which are very expensive compared to before when they were very cheap. One fake account is very expensive now, so they sell these accounts. That's why they were suppressing others recently and doing something like "Tai -bodia"...

00:20:55 Interviewer

What are they doing?

00:20:55 TPU4

Like Tai -bodia, Cambodia, they lock 30 people in a room, right?

00:21:05 Interviewer

Oh, you mean in Cambodia, right.

00:21:06 TPU4

Yes, that's how it is in Cambodia. And in Taiwan, it's similar to that. So we call it "Tai -bodia"

00:21:11 Interviewer

Taiwan also has this? Wow.

00:21:14 TPU4

Because fake accounts are very valuable now. The water room is no longer just supplying to one fraud group, but they are collecting accounts and using them to the fullest. They are now supplying to more than a dozen or 20 fraud groups. When you come to withdraw money, they will use this account to do it all.

00:21:44 Interviewer

OK, so they will use one account... they will not just use it once, right?

00:21:48 TPU4

Yes, in the past, after the account has been used and it became useless, or it would be frozen by the police and 165 frozen line. Now, they want to control people first.

00:21:59 TPU4

Once they start using these accounts, all the different scam groups start using them. I only provide the mechanism for using the water rooms, but you guys can scam people on your own. So they are categorized into different groups - stealing information is one thing, scamming is another, and running the "water room" is yet another. They are completely separate.

00:22:20 Interviewer

I see.

00:22:24 Interviewer

Alright, moving on to the eighth question: what do you think about the general public's awareness of internet security these days?

00:22:34 TPU4

Most people still don't have a clear understanding of internet security mechanisms. To be honest, nowadays... if you ask anyone outside whether their mobile phone is secure or not, I cannot say it is safe because there is always a possibility of a Trojan horse being present.

00:22:58 Interviewer

Right.

00:23:01 Interviewer

So basically, the general public doesn't have much awareness about the cyber attacks that can happen?

00:23:06 TPU4

Yes, their awareness is really too little... too little.

00:23:09 Interviewer

I see.

00:23:10 Interviewer

That may respond to the ninth question, because what you just said is that people generally have a low awareness of online security. Does the government have any plans for education on internet security?

00:23:25 TPU4

So for example, many people are victims of scams. After a scam, the police will create some cheat sheets based on these scam patterns.

00:23:39 TPU4

For example, there have been scams on Telegram. We tell people not to screenshot and send it to others because recently everyone uses Telegram and screenshots. Once the victim screenshots and sends it to others, hackers can log in directly using the verification code from the screenshot, and then take away all of the victim's account permissions.

00:23:59 Interviewer

I see.

00:24:03 TPU4

Even if you want to delete the account on your phone, you can't. The situation is like this, so... we will make cheat sheets for the public and tell them to be careful when someone asks them or their friends to screenshot. We need to call on the public to pay attention to their information security. We also often tell people that free things are the most expensive.

00:24:35 Interviewer

That's right.

00:24:37 TPU4

Yes, that's true. People sometimes download free software or use cracked software. For example, recently there was a situation like this where they provided free license keys for download. These license keys were capable of genuinely cracking the software. However, at the same moment of cracking, all the information on your computer, including account passwords for things like virtual currencies, would be stolen. Hackers exploit this method to transfer all the funds from your financial accounts. This is a common scenario we often come across.

00:25:15 Interviewer

So about the cheat sheet you mentioned earlier, do you think it's useful?

00:25:19 TPU4

Hmm, I wouldn't say it's not useful. At least we have done something, and we can use it to promote awareness among the public if they're willing to read it.

00:25:31 Interviewer

But it depends on whether the public are willing to read it?

00:25:32 TPU4

Yes, that's right, that's right, that's right.

00:25:37 Interviewer

I see. So for the tenth question, what are the government's plans for recruiting or training cybersecurity personnel for both in and out of schools?

00:25:48 TPU4

Actually, we often train people with cybersecurity skills, such as sending them to classes. But these cybersecurity courses are not cheap. One class could cost about 50-60,000 NTD. We also have ISO certification and certain requirements for cybersecurity. For example, not everyone can enter our laboratory, and we have strict control mechanisms in place.

00:26:19 Interviewer

I see.

00:26:25 TPU4

So, the government should put more effort into training cybersecurity talents because there are not enough people in this field.

00:26:34 Interviewer

There are not enough people, I see.

00:26:35 TPU4

Yes, there are not enough people, so training in this area is really necessary.

00:26:40 Interviewer

I see.

00:26:42 Interviewer

Okay, understood. Besides having fewer people, it's possible that the knowledge of the cybersecurity talent may be uneven?

00:26:50 TPU4

Of course, of course, it's definitely uneven, so we, for example…

00:26:56 TPU4

We have established our own digital forensics laboratory. We also have mobile forensics capabilities in each branch of the Taipei City Police Department. We require all units to join our group so that we can share new techniques or methods. For example, if there are new methods or approaches, we will share them in the group and discuss how to retrieve data or gain insights. This way, we gather internal expertise and continuously educate and train our team in the field of cybersecurity. We often invite external experts and teachers to provide training and lectures as well.

00:27:40 Interviewer

Hmm, that's good, yes. It's a way to steadily improve knowledge.

00:27:45 TPU4

Yes, to improve our police officers' understanding of cybersecurity concepts.

00:27:49 Interviewer

Okay, got it.

## Section D

00:27:51 Interviewer

So let's move on to section D. The first question in section D is about cybersecurity. What are your thoughts on the concept of collaboration between the public and private sectors in terms of cybersecurity? Can it really be effective in promoting the development of cybersecurity?

00:28:08 TPU4

Um, hold on a second. Oh, time is almost up.

00:28:10 Interviewer

Oh, sorry, how much time do you still have ?

00:28:14 TPU4

I may have to go downstairs in three minutes.

00:28:17 Interviewer

OK, no problem.

00:28:18 TPU4

Regarding cybersecurity, we, like banks, for example, in the event of a DDoS attack, we would require them to provide us with some logs for analysis. After analysis, we would confirm the tactics used in the case, the sources of the IP, and then we would cooperate with other agencies such as the Investigation Bureau and the Criminal Investigation Bureau.

00:28:50 Interviewer

I see.

00:28:51 Interviewer

So do you think that the current level of collaboration is enough?

00:28:55 TPU4

It's not enough. We should work with some private entities that are more authoritative and selfless, and they should be willing to provide some information to government agencies. This will be better, yes.

00:29:10 Interviewer

Okay, I understand. So, the second question is what we just talked about. Do you have any experience with public-private partnerships in Taiwan?

00:29:24 TPU4

We are currently working with some public and private sectors.

00:29:27 TPU4

Public-private sectors...

00:29:27 Interviewer

It means collaborating with some private enterprises, like the businesses you just mentioned. Do you have any such experience?

00:29:33 TPU4

Actually, we work with some companies, like digital forensics, who provide some products for us to test. As for private sectors... private sectors... Well, I'm not sure at the moment.

00:29:51 Interviewer

So, it's relatively few, right?

00:29:53 TPU4

Yes, relatively few.

00:29:56 Interviewer

Okay. How do you think you can work with private sectors if you want to collaborate with them? And what can you do to improve?

00:30:06 TPU4

I think we should work with cybersecurity, for example, some cybersecurity companies that are more familiar with some new criminal methods. They must be more aware of these things because they are already doing some virus defense and researching these things every day. Therefore, they should provide some new methods to government agencies.

00:30:30 Interviewer

Do you think there are any difficulties in this kind of cooperation?

00:30:38 TPU4

Actually, some departments, such as the Investigation Bureau, our Criminal Investigation Bureau, and Taipei City, when they want to cooperate, they are still faced with difficulties. So, there may be some difficulties with cybersecurity companies.

00:31:01 Interviewer

So, you think that cooperation with cybersecurity companies may be more difficult?

00:31:05 TPU4

Yes, because cybersecurity companies are just after the money.

00:31:05 Interviewer

Haha.

00:31:06 Interviewer

Okay, so overall, do you think that cooperation with cybersecurity companies is the right direction?

00:31:14 TPU4

I believe that is correct. As for cybersecurity companies like Trend Micro, we don't directly interact with them. It is the Investigation Bureau and the Criminal Investigation Bureau that have contact with them. They don't have direct contact with us in a similar manner. Yes, companies like Trend Micro, which are major players in the cybersecurity industry. I might not be able to provide further details on this topic. Is that alright with you?

00:31:36 Interviewer

Okay, I think that's about it. Yes, OKOK, yes, thank you.