# Transcript

## Section A

00:00:03 Interviewer

Alright, now I am going to interview TPU1. Let's start the interview. First, I want to ask about Section A. The first question is: what type of organization do you belong to?

00:00:21 TPU1

I belong to the public sector.

00:00:22 Interviewer

In the public sector, OK. The second question is: what unit do you work in?

00:00:28 TPU1

Um, I work at the [a national criminal investigation agency].

00:00:35 Interviewer

I see, the [a national criminal investigation agency].

00:00:37 TPU1

The [a national criminal investigation agency].

00:00:39 Interviewer

The [a national criminal investigation agency].

00:00:41 TPU1

Yes, the [a national criminal investigation agency].

00:00:44 Interviewer

I see. I'll write that down.

00:00:48 TPU1

[a national criminal investigation agency].

00:00:54 TPU1

Then….[a national criminal investigation agency].

00:00:54 Interviewer

Then….

00:01:04 Interviewer

OK, the third question is: how long have you been working in this unit?

00:01:12 TPU1

I have been working in the police force for 3 years and in the [a national criminal investigation agency]. for about half a year.

00:01:17 Interviewer

OK.

00:01:23 Interviewer

What is your current position?

00:01:26 TPU1

I am an investigator.

00:01:30 TPU1

Mainly responsible for investigating criminal cases.

00:01:34 Interviewer

OK, so it’s the fifth question. Your responsibility is to investigate criminal cases?

00:01:35 TPU1

Yes, that's right.

00:01:44 Interviewer

Are there specific areas of criminal cases that you investigate or is it just general?

00:01:48 TPU1

I mainly handle fraud, fraud cases, and drug cases.

00:01:51 Interviewer

OK.

00:01:52 TPU1

Yes, that's right.

## Section B

00:01:58 Interviewer

So let's get to the main topic, Section B. The first question is, based on your experience, what are the main types of cyber attacks Taiwan is facing now? And what are their methods? Can you give some examples?

00:02:18 TPU1

For example, there is ransomware, like the WannaCry attack before. They would encrypt your files and demand ransom payment, which could be made with virtual currency. There was also the DDoS attack that paralyzed some important websites, like the presidential office's website.

00:02:32 Interviewer

I see.

00:02:46 Interviewer

So, it's about... targeting some... maybe government organizations...?

00:02:54 TPU1

Yes, it could be targeting government organizations with large-scale DDoS attacks, or targeting private enterprises with ransomware attacks, for example.

00:03:10 Interviewer

Okay, the second question is, what are the main targets of cyber attacks in Taiwan now? And what do you think the reasons are?

00:03:20 TPU1

Well, for private companies, the targets may be their confidential information, and hackers may want to extort some important data.

00:03:37 Interviewer

I see.

00:03:40 TPU1

Or, like the case of First Bank before, they hacked into the ATM. That's also in the private sector. As for the public sector, it's mainly the websites, like government websites.

00:03:56 Interviewer

I see. So, government websites?

00:03:59 TPU1

Government websites, yes.

00:04:00 TPU1

Or, like the case of household registration data leakage before, it involved personal information.

00:04:11 Interviewer

I see. Can you tell me more about the ATM case you mentioned earlier? Because I'm not familiar with it... I'm in the UK, you know.

00:04:22 TPU1

Oh, okay. The ATM case is about someone discovering that the ATM was dispensing a lot of cash without any interface being used. Yes, then someone reported it and when we reviewed the surveillance footage, we found out that when someone approached the ATM, the money would be dispensed automatically without any interaction.

00:04:44 Interviewer

When a person approaches, the money is dispensed automatically?

00:04:45 TPU1

Yes, they had already set it up remotely. When their people went over, the money just came out on its own. And then, they used this method to make tens of millions. You can go back and look at the news about it. This was a foreign criminal group that has committed many crimes overseas as well. Luckily, Taiwan has many surveillance cameras, which allowed us to eventually track down these people.

00:04:58 Interviewer

Okay, got it.

00:05:15 Interviewer

I want to ask you if this happened in Taiwan before. I've seen news about this happening in other countries, where the card slot is a green circle with the slot in the middle, but in Taiwan, the design is just a hole to insert the card. In other countries, criminals make fake green circle card slots and attach them to the ATM to steal people's information when they enter their PIN codes. So their data gets leaked and the suspects will come and collect the information. That's why in foreign countries, people are advised to check whether the card slot is moving when they withdraw cash because if it does, there may be a second layer to steal their data.

00:06:24 TPU1

So they can steal the PIN code and other information?

00:06:25 Interviewer

Yes, that's right.

00:06:29 TPU1

Hmm, I don't think we've encountered that before.

00:06:31 Interviewer

It's possible the designs are different.

00:06:32 TPU1

Yes, that's right.

00:06:34 Interviewer

Okay, so, based on your previous discussion, you were mentioning about the targets of attacks. When it comes to the government being a target, do you think there might be specific reasons or patterns in terms of timing or focus during different phases? For example, during election periods or other specific events. Could you provide some examples to illustrate this?

00:07:14 TPU1

During elections, there tends to be more false information, and does this false information also include in your internet attacks?

00:07:21 Interviewer

Yes, that's right. It should be quite comprehensive.

00:07:24 TPU1

In terms of false information, this year has seen relatively fewer instances because it's a year with local elections, specifically county and city mayor elections. In contrast, during the previous national presidential election, there were numerous false information campaigns, including a significant number of false messages circulating during the pandemic period.

00:07:47 TPU1

Yes, and false information's content usually starts with false traces. For example, they might claim that a certain person has contracted a disease and list the places they have visited. As time goes on, it evolves into other forms, such as sending SMS messages about whether someone is eligible for certain subsidies or not.

00:08:12 Interviewer

Okay, yeah, that's right. It's really quite... Especially during the pandemic, it had quite an impact, right?

00:08:22 Interviewer

So... moving on to the third question. Actually, these questions are quite similar. Just wondering what factors you think are affecting the entire internet security of Taiwan?

00:08:33 Interviewer

You can... It's kind of like a macro perspective, not a micro one. What do you think you know about this?

00:08:45 TPU1

Hmm, in the case of the public sector, for example, the police department may have an information technology department responsible for data security. However, when it comes to cybersecurity, there are certain exercises they can conduct, such as social engineering drills. In these drills, they might send fake emails to their employees' official email accounts, and these emails would look very convincing. For instance, they might pretend to be from the HR department, warning about abnormal leave records. The intention is to test if employees would click on the provided links in these fake emails.

00:09:44 TPU1

During this period, they would announce in advance that there will be a social engineering drill, warning us about the possibility of such drills. The purpose is to prevent us from clicking on these fake links, as a precaution against similar situations where hackers might attempt to infiltrate our internal network using deceptive links.

00:10:02 Interviewer

I see.

00:10:07 TPU1

Yes, that's something we would do more often. For instance, some websites or our internal network might directly block those suspicious links.

00:10:12 Interviewer

I see, so what you just talked about is part of your training?

00:10:24 TPU1

It's like training or exercise. In case we encounter such a situation, our reflex action is not to click on these things.

00:10:35 Interviewer

I see, so if you click on it, you won't actually fall for the trick, but the backend will know that it was you who has interacted with the link or email.

00:10:43 TPU1

Yes, because the email is sent to everyone, and they will test to see who clicks on it. If someone does, there will be a review, and...

00:10:47 Interviewer

OK, they will test who wants to click on it? But there won't be a real virus attack?

00:10:56 TPU1

No, there won't be, that's right.

00:10:56 Interviewer

OK, I understand now.

00:11:01 TPU1

It seems like this is not a factor, right? This is just our approach, yes, yes, yes.

00:11:13 TPU1

From a macro perspective...

00:11:14 Interviewer

You don't need to take a macro perspective, just your own understanding...

00:11:22 TPU1

Take cross-strait relations for example, if China wants to invade us using their internet army, such as important national websites, then it may involve some network attacks from the other side.

00:11:43 Interviewer

Hmm, yeah. Okay. Yeah, when I was looking for those documents, the cross-strait relations also played a big role in Taiwan’s cyber attacks.

00:11:56 TPU1

It's a more common motivation for attacks, hmm.

## Section C

00:12:00 Interviewer

Okay, now we are moving into Part C, which is about discussing strategies for defending against cyber attacks. So the first question is, what do you know about the Taiwanese government's overall cybersecurity plan? And how would you evaluate these plans?

00:12:24 TPU1

Well, the cybersecurity plan... is this about policy? Because, for example, the recently established MODA (Ministry of Digital Affairs) has been established which specifically focuses on cybersecurity. It's like the disaster response department that my colleague went to. It's for setting up SOPs for handling things like the aftermath of hacker attacks, and for subsequent processing. So currently, Taiwan's government is continuously working on this cybersecurity aspect, of course, we may face more and more diversified attacks in the future.

00:13:04 Interviewer

Okay.

00:13:22 TPU1

Yes, but currently we see that establishing this department is a big thing.

00:13:29 Interviewer

When was this department established?

00:13:32 TPU1

Around... last year or the year before.

00:13:35 Interviewer

Last year, that's quite recent.

00:13:37 TPU1

Yes, it was established during the Tsai government, and many of the people in it came from the police force.

00:13:51 Interviewer

OK, then onto the second question, what do you think about the current network threats... in terms of the prevention strategies for government agencies, what do you know about them? Like some plans or strategies, and how would you evaluate them? I think questions 2 and 3 can be answered together, because you are evaluating these strategies... Besides, do you think these strategies can be improved in any direction?

00:14:24 TPU1

The strategy is a bit like the social engineering drill I just mentioned. Yes, it involves training the staff, particularly the frontline employees. The first step is to provide training to the personnel, making them aware of social engineering techniques, so they can recognize and prevent potential threats like suspicious links and emails.

00:14:51 TPU1

And then...

00:14:58 Interviewer

It's okay, take your time to think, but what do you think about the social engineering drill you just mentioned? Do you think it's helpful or not? Or do you think there's something that can be improved?

00:15:19 TPU1

The voices of frontline employees probably feel frustrated because these things look very real, and if they accidentally click on something wrong, they might face consequences and have to write reports.

00:15:28 Interviewer

I see.

00:15:29 TPU1

Yes, but the intention behind it is good, and I think there is still a need for it, because it is still a means of prevention.

00:15:47 TPU1

It's just that if it becomes too standardized, using the same method all the time, then the effectiveness may not be as good in the long run.

00:16:00 Interviewer

Right, because you will get used to it?

00:16:02 TPU1

Yes, we will get used to it that there will be occasional spam emails.

00:16:06 Interviewer

In that case, do you think that in which aspect you can improve and develop to better prevent cybercrime?

00:16:23 TPU1

I think this is like our general academic training where it should be a fundamental concept. As law enforcement officers, our instincts should tell us if something seems suspicious, and we should avoid interacting with it. Of course, it's still essential to start from the basics and establish a cybersecurity mindset through basic education and training.

00:16:57 Interviewer

So, what you mean is that you believe it's better to focus on these more fundamental aspects...

00:17:05 TPU1

Exactly, even in police academies during education, they should instill these concepts. It's not only for police officers, but cybersecurity awareness should be a part of general education for everyone in society.

00:17:16 Interviewer

OK.

00:17:18 TPU1

And then, just thought of another aspect, some counties and cities have USB ports that are locked after a USB is inserted...

00:17:26 Interviewer

Oh, some counties and cities?

00:17:29 TPU1

Like... from what I know, Tainan... Tainan is like this, they do this to prevent viruses from entering the government's computers. And in Kaohsiung, for example, after we finish taking notes, when we want to copy the file, they have to unlock it first, yes, yes.

00:17:54 Interviewer

OK, I understand.

00:17:55 TPU1

Yes, this should also be considered a preventive measure.

00:17:57 Interviewer

Yes, yes, exactly.

00:18:00 Interviewer

Yes, my school's computers are like this too, not that they are locked, but there is a program that can lock them, and there is an unlock function.

00:18:08 TPU1

Yes, you have to unlock it before you can copy it.

00:18:12 Interviewer

Yes... you mentioned that the locked part is in the public... computers of the government?

00:18:19 TPU1

The government's public computers, the ones for official use.

00:18:21 Interviewer

OK.

00:18:25 Interviewer

Let's move on to the fourth question. I think we can also discuss questions four and five together. We talked about prevention earlier, but now suppose we are facing a cyber attack. For example, there are already some hackers attacking us. What strategies do you know of to respond to this? Do you think these strategies are helpful? Also, which direction can we improve in?

00:18:57 TPU1

If an ongoing issue is reported to the investigation unit, they will try to quickly find the attacker. That is, they will try to find the suspect. For example, they may use IP tracing to locate the target. In our unit, we would not focus on prevention, but rather on responding to the situation.

00:19:39 Interviewer

Right, we're not talking about prevention, but rather what strategies you should use to respond to the underway situation.

00:19:43 TPU1

Yes, the strategy. For example, during the Chinese New Year, there was a threat on the Taipei MRT that there would be a bomb. It wasn't really a fake message, but it was posted on the internet. When we hear about such a case, we first check whether the MRT has reported it to the National Police Agency as a serious crime, and then whether the National Police Agency has assigned the case to the Criminal Investigation Bureau's field team.

00:20:24 Interviewer

I see.

00:20:25 TPU1:

So, is this field team ours? If so, do we need to send someone to the scene to deal with it?

00:20:32 Interviewer:

Hmm.

00:20:33 TPU1:

Right, our thinking is more about how to handle these things in the subsequent investigation.

00:20:39 Interviewer:

Hmm.

00:20:41 Interviewer:

OK.

00:20:42 Interviewer:

Yes, that's true. In my reading of various literature, I've come across the observation that not only law enforcement agencies but also other entities, such as antivirus software developers or solution providers, tend to focus more on prevention rather than having effective countermeasures when facing attacks. It seems that there is a lack of effective response strategies in place. While prevention is important, there are still instances where breaches occur despite preventive measures. This aspect has been noted by some scholars, but I agree that finding comprehensive solutions can be challenging. This is just my personal perspective.

00:21:30 TPU1:

I think... You know the Red Team and the Blue Team? They simulate hacker invasions, with the Red Team attacking and the Blue Team defending!

00:21:42 Interviewer:

Hmm, I see.

00:21:44 TPU1:

Right, the government sounds like the Red Team (should be Blue Team), like the defense side. We need to prevent attacks from hackers, but on the other hand... From the perspective of the reconnaissance unit, we would like to play the role of the Red Team. For example, for a gambling website, we use hacking methods to access their backend and then find the actual operators or gamblers. That's how we are different from the general government's way of thinking.

00:22:17 Interviewer:

OK, so you mean that the reconnaissance unit is more like... A bit like the Red Team, taking the initiative to attack?

00:22:22 TPU1:

Yes, we need to take the initiative to attack.

00:22:25 Interviewer:

What about the general government?

00:22:27 TPU1:

The general government is more about how to prevent... Preventive work. Let's say... not just the general government. For example, police stations or precincts, they all receive reports, right? But for the Criminal Investigation Bureau, it becomes, we need to find where the important cases are, we need to... go there... and find out who... who we need to investigate.

00:22:56 Interviewer

So let's move on to the sixth question, and questions six and seven can be answered together. After a cyber attack, do you conduct reviews or reflection measures? When you are conducting these reviews and reflection measures, what kind of mechanism do you have? Do you think that these reviews and reflections are helpful in improving the prevention of cyber attacks? Or do you think there is room for improvement?

00:23:40 TPU1

Reviews or reflection measures…

00:23:49 TPU1

I think the measures we are currently engaged in are reflective of past experiences, such as the social engineering exercise we mentioned earlier. It was initiated because we had previously experienced attacks, and that's why we started conducting these drills.

00:24:02 Interviewer

I see.

00:24:03 TPU1

Yes, I believe that these measures are common in many companies, such as locking up USB drives or implementing email security measures, which were introduced because of past events.

00:24:28 Interviewer

So do you think that these reviews and reflections are helpful?

00:24:38 TPU1

Um, they are somewhat helpful.

00:24:44 TPU1

Because after previous incidents, we had to do these extra works which were more complicated, but it was all to prevent these issues from happening again.

00:25:01 Interviewer

Okay, let's move on to the eighth question. The eighth question is about your opinion. What do you think is the general public's understanding of internet security? Do they have enough knowledge? Do they understand the importance of internet security? Or are there some tricks they might not know about?

00:25:26 TPU1

In my opinion... currently, I think that society... they don't trust internet security, because for example, when we shop online, we often receive fraudulent phone calls. This is because hackers or engineers from scamming groups go to the backend of the shopping website and pull out some of the ordering information. So...

00:26:07 TPU1

Therefore...in this kind of situation, it creates a lack of trust for our personal information and other things on the internet.

00:26:21 Interviewer

I see.

00:26:21 TPU1

Yes, so...

00:26:22 Interviewer

What do you mean? Please continue.

00:26:31 TPU1

Okay, so that's it.

00:26:31 Interviewer

Oh, so you mean that the public doesn't trust the internet much?

00:26:41 TPU1

Yes, that's what I think. I think it's because it's too easy to leak personal information and data.

00:26:48 Interviewer

So does that mean that they have some basic awareness of internet security, that is, they know that there are risks associated with the internet?

00:26:59 TPU1

I believe that the general public, through our many years of anti-fraud dissemination, should know that, for example, internet passwords should not be logged in on the internet, that is, stored on the internet, and personal information should not be easily leaked.

00:27:16 Interviewer

I see.

00:27:17 TPU1

Yes, so I think people's perception of the internet should be...it's very convenient, but they should also know that personal information on the internet can be easily abused.

00:27:34 Interviewer

Okay.

00:27:37 Interviewer

Okay, so this can explain question 9. What do you think about the government's plans for educating the public about internet security? Do you think their plan is good or not?

00:28:01 TPU1

Education about internet security... well, we're not quite sure if middle and high school students are receiving this type of education nowadays, but... I remember we had computer classes back then.

00:28:16 Interviewer

Oh, I see.

00:28:16 TPU1

Yes, in computer class, we would talk a bit about what we just mentioned, like not leaking personal information on the internet, and not storing passwords carelessly.

00:28:36 Interviewer

Or for the general public, because, as far as I know, they may promote it on their government websites, or through advertisements and media to raise awareness. Do you know if they do that?

00:28:52 TPU1

That would be considered anti-fraud propaganda. If it's done by the police department, they would conduct anti-fraud campaigns, such as educating about new fraudulent tactics.

00:29:03 TPU1

And the front-end of these tactics, as mentioned earlier, involve situations like personal information being leaked during online shopping or when filling out forms, which then provides fraudulent groups with the necessary data to target individuals for scams. Therefore, from the police's perspective, a significant part of their crime prevention efforts includes crime prevention awareness campaigns, such as organizing school fairs or community events.

00:29:37 Interviewer

School fairs? So, they would set up booths?

00:29:38 TPU1

Yes, we would set up a booth, and have some interactive games, and tell everyone that this is... this is fraud, and this is more dangerous.

00:29:49 Interviewer

I see.

00:29:54 Interviewer

So what do you think... do you think these... these, uh, strategies and plans you just talked about, do you think they're good or not? Or do you think... what we can do... to make it better?

00:30:12 TPU1

That's the tenth question, oh, we're still on the ninth question. How can we make it better?

00:30:13 Interviewer

No, actually we're still on the ninth question, yes.

00:30:19 TPU1

Yes, a better approach would be to increase the outreach efforts. For example, when Facebook is popular, use it to post informative content, and when Instagram is popular, use it to post relevant information. Utilize both online platforms and physical events to ensure that people in the community are well-informed about the current scamming techniques.

00:30:45 Interviewer

Hmm.

00:30:46 TPU1

Yes, or... actually the most important thing is to go home and talk to the elders about these issues, yes.

00:30:53 Interviewer

So the elders are less aware of these things?

00:30:57 TPU1

It depends, some age groups are different, for example, online shopping scams are more prevalent among the younger generation, around their thirties or forties, while investment scams or scams involving columbaria are more common among retirees,… or fake prosecutors... yes, those are usually over fifty or sixty years old.

00:31:22 Interviewer

Fake prosecutors?

00:31:24 TPU1

Yes, they may tell you that your account has been frozen, and then... then print a... a document for you, yes, and then tell you that your account has been frozen, so you have to follow my instructions to unfreeze it, and then teach you how to operate your account and transfer the money out.

00:31:45 Interviewer

Will they send the document to your home or will they give it to you face-to-face?

00:31:48 TPU1

Oh, face-to-face is a bit more stupid. If they know how to use the printing machine at the convenience store, which has a fax function, they'll ask you to go there and get the document.

00:32:03 Interviewer

Oh, so he might call you first and tell you that?

00:32:06 TPU1

That's also a type of telecom fraud, the front end is sort of telecom fraud.

00:32:12 Interviewer

Wow, there really are a lot of different methods.

00:32:14 TPU1

Yes, there are many.

00:32:17 Interviewer

Okay, now let's move on to the tenth question. Do you know if the government has any training programs for future internet security personnel in schools and outside of schools? And what do you think of these training programs, are they good or not?

00:32:36 TPU1

What do you mean by "inside and outside of schools"?

00:32:38 Interviewer

Oh, it means that maybe, for example, the police department may send people to campuses to do promotions. This may attract high school students to pursue this field in the future. And then after university, it depends on whether people are interested in this field or not. It's like attracting talent.

00:33:10 Interviewer

Or the government may provide some training programs, which are open to the public. This is what I know.

00:33:23 TPU1

If we talk about before high school, it may not be clear yet. After high school, some students may choose to study information-related majors such as computer science and information management. After they finish the training, some may go into the cybersecurity department. Regarding the police unit, we have the Criminal Investigation Bureau with the 9th Investigation Unit, as well as the Research and Development Division, the Information Division, and the Telecommunications Investigation Division. They mainly handle cybercrime cases.

00:34:00 Interviewer

Okay.

00:34:03 Interviewer

What was the first unit you mentioned just now?

00:34:07 TPU1

Ah, the 9th Investigation Unit. Then there's the Research and Development Division, the Information Division, and the Telecommunications Investigation Division.

00:34:19 Interviewer

Telecommunications Investigation Division is about the telecommunication aspect, right?

00:34:20 TPU1

Yes, it is our team.

00:34:24 TPU1

Yes, and telecommunications investigation, that's right.

00:34:24 Interviewer

Oh, telecommunications investigation, okay. I understand.

00:34:30 TPU1

In terms of training, we will find some people to plan and take some information-related certificates, such as the CH certificate, which is the certificate for the Red Army. It is a certificate for simulating attacking the other parties.

00:34:51 Interviewer

CH is the certificate for the Red Army?

00:34:59 TPU1

Yes, if there are information-related cases, we will also be asked to investigate. So, the training part is also something we mainly handle.

00:35:09 Interviewer

So, will you also participate in the training plan? Does that mean you will teach them?

00:35:15 TPU1

We will receive training first, and then after completing the training... if there is an opportunity, we will go to the counties and cities, because there are also technology investigation teams in the counties and cities, yes, to share... share some information, that's right.

00:35:30 Interviewer

So you will go to the technology investigation teams in various counties and cities?

00:35:32 TPU1

Um, yes.

00:35:33 Interviewer

So the technology investigation team, is it also considered a police unit?

00:35:39 TPU1

Well, to put it this way, for example, in Taipei City, the Criminal Investigation Division has many teams, teams 1, 2, 3, 4, 5, 6, 7, and then there will be a... technology investigation team, yes.

00:35:50 Interviewer

Oh, I see.

00:35:53 TPU1

Actually, they mainly do mobile phone forensics, and then, they may also be asked to deal with internet crimes, yes, and of course, they also deal with general criminal cases, yes.

00:36:05 Interviewer

Oh, general criminal cases?

00:36:06 TPU1

General criminal cases, that is, traditional criminal cases, such as drugs and fraud are the most... traditional.

00:36:14 Interviewer

And then you just mentioned the first one, mobile phone, and mobile phone forensics?

00:36:16 TPU1

Mobile phone forensics, mobile phone forensics is about the area of forensics.

## Section D

00:36:20 Interviewer

Hmm, okay, then let's move on to section D, which is about public-private cooperation in internet security. The first question is: What is your opinion on the concept of collaboration between the public and private sectors in internet security and whether you think it really helps to develop internet security?

00:36:49 TPU1

Okay, I think... I think this is a direction that is urgently needed in the future. Yes, because...

00:36:57 Interviewer

Oh.

00:37:00 TPU1

n fact, in terms of police education, we can talk about the police force. The education for police officers mainly comes from Taiwan Police Colleges and Central Police University. Those who have a direct connection with information technology are mostly from the Department of Information Management at Central Police University. However, at Taiwan Police Colleges, there are relatively fewer specialized departments focusing on information technology.

00:37:18 TPU1

Yes, that's right. In the police force, the number of graduates with a background in information technology is relatively small, perhaps only around 10 to 20 people per year. Compared to the overall number of police personnel, it is indeed quite limited. Each county and city police department, including the Criminal Investigation Bureau at the central level, requires its own information technology department. These departments are usually composed of a small group of people, so the external communication and interaction with others in the field are relatively limited.

00:37:52 Interviewer

Okay.

00:37:53 TPU1

So, the training with Central Police University, it may be different from the training of external computer science departments.

00:38:01 Interviewer

Okay.

00:38:02 TPU1

That is to say, they are trained for future police officers, so they may have less emphasis on research and development or design concepts. Police education mainly focuses on investigating and solving crimes.

00:38:21 Interviewer

Okay.

00:38:22 TPU1

So I think if we can introduce people with computer science backgrounds from outside the police force, it will enrich our resources, like our weapons will be more abundant, and resources will be more abundant.

00:38:40 Interviewer

Okay, got it.

00:38:42 Interviewer

So, moving on to the second question. Since we've discussed your opinion earlier, do you think there's currently a mechanism for public-private cooperation in Taiwan regarding cybersecurity as a whole? Have you heard of any relevant experiences or information?

00:39:07 TPU1

Regarding cybersecurity, our forensics investigation team mainly cooperates with telecommunications operators. For example, we can seek resources from them to deal with some telecommunication fraud-related cases involving certain machines. However, if it's related to cybersecurity, the research and development department may have some cooperation mechanisms.

00:39:38 TPU1

We've encountered cases before where we investigated an IP address used for website intrusion. After finding the IP address, we traced it back to a young person who owned a company that detected intrusion. He had a solid background in information technology and was even absorbed by the Investigation Bureau to help solve cases.

00:40:24 TPU1

For this kind of talent, we may consider inviting him to teach us or assist us in handling some cases. For example, we could utilize his hacking techniques to infiltrate fraud or gambling websites and take them down or catch the people behind them.

00:40:56 Interviewer

OK, so... So there is a mechanism in place? Has he already helped you guys or did he refuse?

00:41:04 TPU1

Well, he owns many companies, but because he was born in the 1990s and is still very young, he's very busy. There may be a chance in the future though. Currently, such mechanisms are rarely seen, as cooperation with technology companies is basically non-existent.

00:41:34 TPU1

Therefore, if we can introduce these elements, it may be better for the internet security.

00:41:49 Interviewer

OK.

00:41:52 Interviewer

Okay, actually I think questions 2, 3, and 4 can be discussed together. And the reason why I separated them earlier was because I did some interviews and felt that it would be better to have them separated. But... I think it depends on each interview being different. So, what do you think? For example, what assistance can you get from technology companies?

00:42:24 TPU1

For example, as far as I know, we have some platforms for intelligence information, which are databases. The establishment of these things is done through outside companies or telecommunications companies. We work with telecommunications companies to obtain data, which can be very complex.

00:42:43 TPU1

The communication platforms are all built by outsourced telecommunications companies, which are technology companies. So, things like the establishment of databases and the analysis of data can be analyzed by us, but the mechanism and tools can be developed by technology companies.

00:43:07 Interviewer

Okay. So, in terms of network security, what kind of assistance do you think you can provide to technology companies since you mentioned that you can get assistance from them earlier?

00:43:31 TPU1

Oh, of course, as a police unit, we are responsible for investigating cases, such as when they are hacked. So, we can help each other and find the suspect behind it.

00:43:45 Interviewer

Okay, great.

00:43:50 Interviewer

The fifth question is asking whether your unit has any experience or mechanisms for collaboration between the public and private sectors, since earlier we talked about the current collaboration between the public and private sectors in Taiwan.

00:44:10 TPU1

Currently... I don't have such a mechanism on hand, but as I just mentioned, with the young hacker, sometimes when we are handling a case, there may be opportunities to encounter such talented individuals, and then we can learn from them or ask for their assistance.

00:44:35 Interviewer

Regarding that young hacker you mentioned, did he help the police investigate and which cases did he help with?

00:44:46 TPU1

Yes, he helped the Investigation Bureau, but I'm not sure about the specific cases.

00:44:54 Interviewer

OK.

00:45:00 TPU1

Ah, I just thought of a question. When we collaborate with the private sector to handle cases, we may encounter an issue with non-disclosure of investigations. Some information can be highly sensitive, and if it leaks or the other party becomes aware of it beforehand, we might even suspect internal leaks. So, if we are to establish a cooperation mechanism in the future, we need to consider how to avoid this problem. After all, they are not public servants or police officers.

00:45:38 TPU1

Moreover, their level of understanding with the outside world might be different from ours. Especially for information technology companies, they might have some suspects who happen to be former employees of the company, and they may have personal connections with them. In this regard, maintaining confidentiality is crucial for our investigative work.

00:46:09 Interviewer

I understand.

00:46:11 Interviewer

Yes, this is quite difficult to achieve. How do you get their assistance from their side when the investigation is not open to them? It seems very limited.

00:46:29 TPU1

Exactly, for example, if I want to find hackers to attack a gambling website, right? Then we would know who the targets are, the IPs. They also know which IPs they should target. So, this division of labor can be further detailed during the cooperation discussion.

00:46:48 Interviewer

So in this case, it should be the overall...you know, the cooperation between public and private sectors in Taiwan should still be...there is currently no really formal mechanism, but sometimes you might hear about some cooperation happening?

00:47:08 TPU1

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

00:47:12 TPU1

The most common situation we might encounter is what I mentioned earlier, where technology companies, oh, get hacked and invaded. It could be the work of a former employee. The technology companies tell us, oh, it might be this person, this person...

00:47:26 TPU1

Yes, but this doesn't really count, this doesn't really seem like cooperation, it's more like...the reporter providing information to the police...

00:47:34 TPU1

Yes, because in reality...the public thinks that the people who handle cases are the police, yes, currently speaking we haven't seen a clear mechanism for cooperation yet.

00:47:47 Interviewer

Okay.