pexels-tima-miroshnichenko-5380642 /www.pexels.comzh-twphoto5380642

Science and Technology Investigation

Huang, Li-Wei *

Tsao, Tseng-Hao

* The chapter was written by Head Prosecutorial Affairs Officer, Tsao, Tseng-Hao; some of the chapter was added by Prosecutor, Huang, Li-Wei of this office in 2022.

I. Preface

To lay the cornerstones for our science and technology investigation, the Taiwan High Prosecutors Office (THPO) has prepared a "three-year development plan". It is hoped thus to ensure a sound legal system, with technological investigation practice, technology investigation research and development facets, technology investigation personnel training, public-private partnership and external cooperation, for comprehensive development.

II. Three-Year Development Plan

The "Three-Year Development Plan" is described as follows:

(I) Sound legal and administrative system

1. Advocacy and lobbying for legal and regulatory policies: Although the Ministry of Justice has introduced the draft Science and Technology Investigation Act, the legislative processes have not yet been completed. Although the THPO is not the authority responsible for proposing this bill, in accordance with the policy direction of the Ministry of Justice, prosecutors are invited to participate in relevant academic activities or seminars, and then provide assistance to the needs of science and technology aspects of our work.

2. The procedures and regulations are completely ready: The implementation of the policy requires the completion of relevant standard operating procedures and forms for front-line personnel to follow and audit at any time. At present these include the completion of the following:

(1) Digital Forensic operational team plan. (2) Digital Forensic Manual. (3) Database application manual. (4) Manual for cryptographic decryption. (5) Polygraph implementation guidelines.

Then continue to adjust as indicated by the evolving technology and legal system.

(II) Technology Investigation Practice Dimensions

In addition to the continuous integration of big data warehouse intelligent system, the

development of auxiliary investigation and search analysis tools, investigation action APP and data warehouse continuous horizontal interfaces, we also establish the knowledge base required for investigation requirements in national land, drugs, and environmental protection cases. We also systematize information needed to detect various cases, including directive interpretations, meeting minutes, forms, processes, and other information to build a searchable knowledge database system for use in conducting investigations, and enhance the technology for evidence collection on digital electronic devices.

1. Expanding Digital Forensic Technology:

（1）In addition to smartphones, we encounter addition of computer digital forensic evidence responsibilities. Due to the demand for computerized forensic evidence services from the District Prosecutor's Offices in 2020, and taking into consideration the manpower situation in each region, we only allocated computerized forensic equipment to Taipei, Taichung and Kaohsiung, and evaluate whether to allocate to other District Prosecutor's Offices depending on the effectiveness of implementation in each region.

（2）Digital device digital evidence collection: This part is mainly for drones, Carputers and IoT (Inernet of Things) digital acquisition for evaluation, to determine whether to include them in the future scope of this Office’s responsibilities.

（3）The long-term goal is to establish a digital evidence data depository in conjunction with the Justice Alliance Chain: This will collaborate with the Ministry of Justice legislative proposal of the Science and Technology Investigation Act, to adjust the contents of our reference manual for digital evidence collection, coordinate the procurement of all necessary equipment, establish a strict digital evidence collection environment, and establish a supervisory audit mechanism. This will enable each prosecutor's office and investigative agency to preserve digital evidence in accordance with the procedures and ensure the consistency of the digital evidence chain.

（4）Establish a Digital Forensic Laboratory: In response to the development of digital

forensics, the current Digital Forensic Center in the Prosecutor's Offices is insufficient. In the first phase, we plan to establish a Digital Forensic Laboratory in this Office, and to introduce ISO 17025 certification to improve the quality of digital forensics and establish an authoritative Digital Forensic Center.

2. Establish Chemical Analysis Laboratory (long-term goal)

（1）Conduct qualitative analysis: If the laboratory is established, it would be limited to the qualitative analysis portion, and not include quantitative analysis.

（2）Chemical History Tracing Analysis System: The data from the qualitative analysis can be further summarized in a biographical analysis system, such as using a drug knowledge database to query chemical formulas, which can facilitate identification of seized drugs. The trace composition drug history system will allow for trace impurities to be compared and permit traceability analysis.

（3）Installing mechanical examination equipment, so that front-line investigations can obtain the required information at any time.

3. Precision technology lie detectors

At present, polygraph offices have been built in Taipei, Taichung, and Kaohsiung, and four Prosecutor's Investigators went to the United States to obtain professional polygraph licenses in 2019 and 2021. In September 2021, two more Prosecutor's Investigators will be sent to the National Security Bureau for polygraph training to increase polygraph capacity.

4. Electronic monitoring equipment

In order to prevent defendants who are not in custody or who have ceased to be in custody from evading criminal liability by fleeing during the investigation or trial, on July 17, 2019, a new Sub-Paragraph 4 of Paragraph 1, Article 116-2, of the Code of Criminal Procedure was added, ordering defendants to accept appropriate monitoring by technical equipment in conjunction with a suspension of detention. In response to the new system, the Judicial Yuan and the Ministry of Justice reached a consensus to appoint

the THPO to plan and build the Electronic Monitoring Center to effectively achieve the purpose of balancing the protection of defendants' human rights and the public interest of the citizenry.

(III) Technological investigation research and development

1. Developing new forms of technological crime countermeasures

(1) New technological crime countermeasures research and development center

New forms of crime will continue to change and emerge because of the advancement of technology, so the creation and early deployment of a New Technological Crime Countermeasures Research and Development Center, is a necessity. At the present stage, the primary deployment is for cyber-derived crime and digital forensics, with the establishment of the Digital Forensic Laboratory, under which we plan to establish the cybercrime countermeasures and digital forensic technology room.

(2) Research on blockchain in investigations and judicial applications

Blockchain is a "technology for digitally memorializing data", and a "decentralized database". By encrypting the data through complex cryptography and maintaining it collectively through clever decentralized mathematical algorithms, the data in a blockchain is more robustly reliable. It can be interpreted as an electronic record mechanism in which everyone can participate, and the data of each and every record can be saved. This allows users to reach a consensus without the intervention of an outside third party, solving the problem of trust and data value on the Internet at a very low cost. At present, blockchain applications are broadly classified as: Proof of existence, smart contracts, Internet of things (IoT), identity verification, market forecasting, asset trading, e-commerce, social media information, file storage, and data API (application programming development interface). Among them, it is valuable to study whether there is room for the application of digital evidence in an increasing number of judicial fields. For example, in the preservation of digital evidence, a judicial private chain may be established. This means that only the relevant judicial authorities or personnel can access this judicial blockchain, such

as trade secret information, a critically important photo or audio file. This would be encrypted and stored in the judicial blockchain at the beginning of acquisition, and every time it is used in the investigation and trial stage, a record of access or use would be created and added, so that digital data with a highly changing nature can be completely preserved. This will greatly reduce the time required for sending digital evidence and data to third parties for authenticating, so that judicial resources can be truly centrally used.

In addition, many cryptocurrencies derived from blockchain technology, such as Bitcoin, Ether and other virtual currencies, are used to conceal the flow of criminal money and hide the proceeds of crime. Studying blockchain technology is expected to allow breakthroughs in tracing the money flow trajectory of these virtual currencies, and interdicting the flow of funds and seizing the criminal proceeds.

（3）Countermeasures to the Dark web and new forms of cybercrime

The dark web is accessed through the Tor (Onion Routing) browser and I2P (Invisible Internet Project) networks, mainly because Tor provides anonymous access to the Internet, while I2P focuses on anonymous web hosting. Dark web layered encryption technology protects user identity and anonymity by transmitting user data through a large number of intermediary servers, making it virtually untraceable. The transmitted information can only be decrypted by subsequent nodes in the path, which then lead to the exit node. Because the system is so complex, it is almost impossible to regenerate node paths and decrypt information layer by layer. Thus, the Dark web is often used for illegal activities such as drug dealing, gun trading, illegal forums and communications among pedophiles or terrorists.

2. Forward-looking inter-disciplinary research

（1）Sewage detection and analysis for drug precursors and components

The Institute of Environmental Engineering at National Taiwan University has been commissioned for a research project in 2020 to conduct microscopic testing of the

effluent from the Dihua wastewater treatment plant in Taipei to analyze whether it contains drug components and assessing the feasibility of backdating the drug use rate.

According to the 2020 commissioned research project, it is indeed possible to conduct microscopic testing and analysis of wastewater to reveal the abuse rate of specific drugs, to set long-term targets on metropolitan areas with a high rate of groundwater pipe connection, and to limit the scope of wastewater testing, to understand inordinate use of drugs. In 2022, based on the aforesaid research results, a new phase of the testing program will be launched, expanding to include water testing at the Neihu, Dihua, and Bali wastewater treatment plants in the greater Taipei area, and microscopic sampling and analysis of sewer nodes in specified administrative areas.

（2）Air gas detection and analysis for drug use prevalence

In comparison with the feasibility of sewage testing and analysis, the feasibility of planning gas testing and analysis of drugs can be targeted at large and small areas of air gas composition, permitting testing and analysis, to determine the type of drugs used. In the long term, handheld detectors can be developed to detect gases in specific areas, such as apartment building or condo communities which are often troubled by drugs used indoors, where handheld detectors could determine the drug levels, as a basis for which to take action.

3. New forms of crime and warning dissemination (medium and long-term work)

（1）Statistical analysis of the trends in new forms of crime

Given THPO's high visibility, it already analyzes the current drug situation, but in the future should also regularly publish statistics and alerts on new types of crimes. For example, press conferences should be held to let the citizenry know and participate in interdicting the new types of drugs, new types of fraud, and new types of crime. With the high mortality rate of MMA (PMMA) cases this year, THPO issued an alert at the beginning of 2020 to strengthen countermeasures and outreach, so the number of

cases was reduced to only 2 in September of the same year.

（2）Domestic and foreign literature research on new forms of crime

A new crime analysis group has been established to analyze and compile literature on new forms of crime both domestically and internationally for policy promotion and reference by higher officials, and review by their subordinates.

（3）Thesis and Book Publication

On specific issues of literature research and practical operations, we should write papers for publication in domestic and international journals, and after compilation into a book, print and publish these works.

4. Establishing a professional library for technological investigation

（1）Order papers from domestic and foreign professional journals

（2）Order papers from domestic and foreign professional journals

5. Organize seminars

Plan to hold seminars in the form of biennial meetings, and invite domestic and foreign experts, scholars and practitioners to participate.

（IV） Cultivation of scientific and technological investigation human capital

1. Establish structured professional education and training

（1）Offer initial, intermediate and advanced training

According to the current education and training plan, the effort is divided by the content of initial, intermediate and advanced training for digital forensics personnel and also plans for regular technical exchanges. The difficulties encountered in a case and the means to solve them will be exchanged and discussed as needed to improve digital forensics or forensic technology.

（2）Original manufacturer's (developers) and international license training

For technological equipment and tools required for technological investigation, most offer original manufacturer's training, but there are also foreign educational

institutions planning professional training, such as CEH, CHFI, or the United States EC Council certification program.

2. Participate in domestic and foreign technological investigation related seminars, forums or workshops

（1）Technology related

Technology is changing rapidly, so that specialized staff need to often participate in new technology seminars, forums or workshops, which can help them obtain the latest technology development and applications for our prosecution entities.

（2）Legal related

For seminars, forums, or workshops related to technological investigation, staff can also participate as speakers or panelists to promote THPO policy and respond to possible misunderstandings in a timely manner.

（V）Public-private cooperation and external cooperation

1. Vertical communication among public agencies

（1）Higher-level guidance: Executive Yuan, Ministry of Justice

① To prepare action plans for implementation of national criminal policy.

② Offer proposed amendments to the law for the front line investigation needs, and after study provide them to the Ministry of Justice for reference.

2. Horizontal connection and integration of investigative auxiliary agencies

Considering drug enforcement as an example, THPO leads the six systems concerned with drug enforcement, and is establishing a unified approach to the process related to technological investigation to reduce wasteful duplication of resources.

3. Administrative cooperation among administrative agencies and county and municipal governments

The Ministry of Education, the Ministry of Health and Welfare, and the Drug Abuse Prevention Center of each county and city government should be involved in mutual

cooperation through the Public Security Committee meeting system, the Inter-Ministerial meeting system, or collaboration among the Central Government Ministries and Municipalities' subordinate bureaus and departments.

4. Academic and Technical Cooperation

（1）Cooperation with research universities: National Taiwan University and National Tsing Hua University: For example, commissioned research projects on wastewater drug residue testing and drug item database creation.

（2）Cooperation with research or professional organizations or research institutes: the ITRI: This includes cooperation on communication's monitoring technology.

（3）Cooperation with specialized technical institutes such as the Bar Association, the Academy of Forensic Sciences, or the Computer Association.

5. Collaboration with social media and non-governmental organizations

（1）Collaboration with professional or public service NGOs to create soft power, such as with public interest groups like the CTBC Anti-Drug Educational Foundation and the Telecom Technology Development Association.

（2）Cooperation with telecommunication providers, such as Cell Broadcast to send anti-drug and anti-fraud messages.

（3）Engage with spontaneous anti-drug groups on the Internet, such as the Facebook Coalition for Victims of Ketamine, and if people provide information on their own initiative, we can work together to carry out investigations or other cooperation, so that people can feel empowered and involved.

III. Conclusions

We hope to integrate the past, improve and streamline the present, and plan for the future, so that we can carry on the best from the past and inspire the future, lay the foundations for technological investigation, ensuring core values and the main character of the prosecutor's office are ever more stable, and fulfill our duty of ferreting out the evil and protecting the good.

Applications of Electronic Monitoring Equipment

Huang, Li-Wei*

* The author, who wrote this Chapter in 2021, then serving as a Head Prosecutor of this offices.

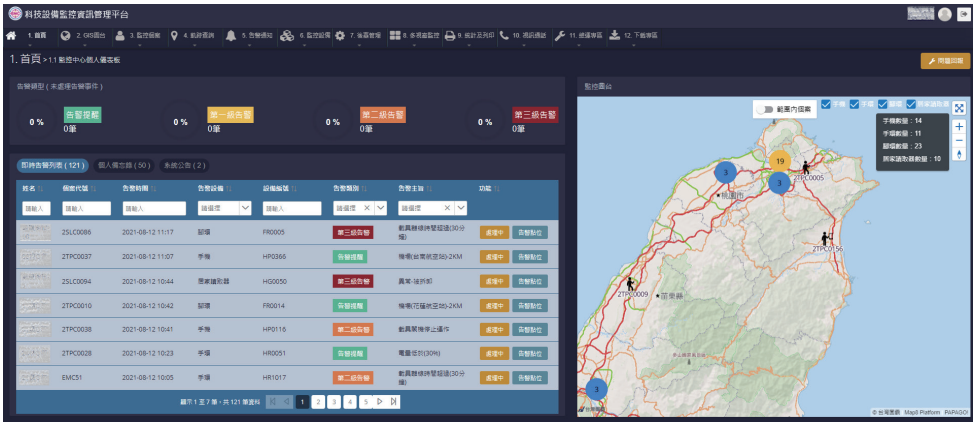
I. Preface

In the present time when there are such a plethora of prevalent technological crimes, appropriately deploying technology to detect crimes and monitor criminals, to achieve the objectives of crime prevention and improving the social safety net with the least amount of time and labor costs, poses a really important issue in the era of superior judicial technology.

II. Applications of Technology Surveillance Equipment

In order to achieve the goal of "technological detection and crime prevention", the Taiwan High Prosecutor's Office has developed and applied technological surveillance equipment as follows:

(I) At this stage, Electronic Monitoring is only based on the real-time location information output from the carrier, and cannot grasp the behavior of the person under surveillance, so regrettable incidents may still occur under the existing monitoring system; [1] In order to avoid such situations, the combination of a CCTV system with the location information from the monitored person's carrier and AI intelligent face recognition system from the Ministry of the Interior's National Police Agency can provide a more effective and real-time view of the monitored person. This can effectively check the real-time location of the case and judge the behavioral patterns, to facilitate determining the monitored person's current behavior risk and considering subsequent disposition.



1.https://udn.com/news/story/7317/5653926。

(II) We also have developed a smartphone APP software for early warning of monitored cases, for specific cases, such as of domestic violence, sexual assault, and sexual harassment cases, which specific victims may download and use according to law. Without affecting the personal information and privacy of the monitored persons, we can use the positioning information to analyze the locations and appropriately allow the public to quickly grasp whether there are people under surveillance in their immediate vicinity, so as to raise their vigilance and prevent the occurrence of inappropriate acts, to achieve crime prevention and early warning for public safety.

(III) We also connect with the M-Police system of National Police Agency, Ministry of the Interior, for some cases of urgent danger to the person, including: domestic violence, sexual assault, and sexual harassment cases, with the planning of electronic warrants for arrest. When a monitored person loses contact or escapes, the Electronic Monitoring System can immediately transmit the last known location of the monitored person and the electronic arrest warrant issued by the prosecutor to the M-Police system, so that the

judicial officers can efficiently arrest the non-compliant monitored person.

(IV) In view of Weng, Mao-Chung's case of Community Service in Lieu of Execution, when the sentenced person is allowed to engage in community service work, the sentence implementation procedure may be combined with the use of technological monitoring equipment, Geofencing settings and electronic photo reporting to ascertain and verify whether there is actual compliance, thereby preventing any such non-compliance.

(V) For sexual assaut offenders who are on parole, and judged to be high risk recidivists, will be subject to technology monitoring. The system has been in place for years, but it is based on the same technological principle as the technological equipment monitoring used in the investigation phase, and relies on the location information transmitted by the carrier. On this basis, it is proposed to evaluate the feasibility of integrating the two systems, within a consistent budget period, scientific control platform, and management integration. It is expected that the national budget will thus be used more efficiently and save on administrative manpower.

pexels-nataliya-vaitkevich-7236026 /www.pexels.comzh-twphoto7236026

Combating Trans-Border Telecommunication Fraud racketeering organizations

Lin, Yen-Liang *

* The author, who wrote this Chapter in 2022, then serving as a Head Prosecutor of this offices.

I. Preface

The President proposed five major social stability programs in 2016 and tasked the Executive Yuan to implement them. Among them, the "Security Protection Plan" prioritizes drug prevention and control, anti-fraud, and women's personal safety, ensuring the citizenry can live in peace of mind. The long-term efforts of prosecutors and judicial police agencies at all levels have been very effective to date in combating such fraud. According to the results of a survey conducted by National Chung Cheng University on the satisfaction of the Taiwanese citizenry with our administration of justice and crime prevention, the public agree that "the government's efforts to prevent fraud" have proven effective. Except for the first half of 2014, when the survey results rose to 60%, the overall satisfaction rate has been decreasing since 2011, and in 2018, it returned to over half (51.0%). In 2019, the satisfaction rate exceeded 70% (72.4%) for the first time, marking the best performance in recent years. According to the most recent "2020 Annual Survey on Taiwan Citizenry Satisfaction with Justice and Crime Prevention "[1], the media continues to report the occurrence of such frauds. Nevertheless, the satisfaction rate for government efforts at fraud prevention still reached over 65% (66.7%), showing a steady trend of support. This indicates that the government's overall fraud prevention efforts are showing initial effectiveness.

II. Problems

(I) The public satisfaction rating is an overall assessment of the government's performance in education, telecommunications and capital management, and detection and combating fraud. If we further analyze the results of crime investigation and detection in terms of the "efforts at detection and combating", there still remains room for concern. For example, in July 2019, the "Nationwide Simultaneous Anti-Fraud Campaign" was implemented. The initiative's main focus was on the core leaders of the crime syndicates, the money

1. The survey of a sample of 1,835 citizens nationwide was conducted and completed on January 11 and 12, 2021, with a maximum sampling error of plus or minus 2.29% at 95% confidence level. After sampling, each sample was weighted by raking method, such that the weighted sample did not differ significantly from the parent group. After the survey was conducted and analyzed, the "2020 Annual Survey on Citizen Satisfaction with Justice and Crime Prevention in Taiwan" results were announced at a press conference held in Taipei on February 26, 2021.

mules and the proceeds of crime. However, of the 2,280 members of the fraudulent syndicate, only 6 (0.26% of the total number of persons seized) were found to be the heads behind funding telecom fraud rooms. Another 188 (8.2% of the total number of persons seized) were low-level capital flow operators. This is a good indication that the middle and high ranking members of the frauds are still at large and continue to recruit money mules who can be replaced at any time. In practice, the "fraud case assembly line" involving (victims report the case > to the 165 database to identify the area of jurisdiction where the ATM handlers operated > the police officers of the police station in the area of jurisdiction identify the money mules > the investigation team of the police precinct act on the prosecutor's command or their own authority to detain or arrest the money mules) has evolved as the means of actual performance in current anti-fraud operations. While a large number of mules are seized, but because they constitute the lowest levels of the organization, their information is limited, making it difficult to trace the ultimate bosses with the money. Although the money mules and drivers are the lowest-ranking members of the racketeering organization, they are involved in multiple driver groups and inter-jurisdictional payments, making the determination of the actual number of crimes very complicated[2] and the cases of repeated referrals and prosecutions are also more frequent than ordinary criminal cases. And each case exhausts the resources of the prosecutors, police and the judiciary for investigations and trials, resulting in a lack of time and ability to trace the ultimate sources of the frauds. The impact of the fraud syndicates and their leaders has not yet been eliminated, and the cases of low-level members of the organization have flooded or even paralyzed our criminal justice system. According to the National Police Agency, the total amount of fraudulent property losses in 2020 still reached NT$4.14 billion. This demonstrates that the perpetrators of telecom boiler room fraud are not even adversely affected by the new COVID-19 epidemic. The fraudulent activities of Trans-Border Telecommunication Fraud (TBTF) continue to grow and flourish in terms of cross-border, technological, and organizational criminalization, with the help of their network and capital flow accomplices.

2. Refer to the Supreme Court's decision reported at Taiwan Appeals Tzu No. 1066 of 2018.

(II) Fraud syndicate leaders have not been eliminated, endangering Taiwan's international reputation: The current efforts of the police to eliminate the low-level members of fraudulent syndicates, and to eliminate the tools of crime (such as phishing SMS, DMT, VoWiFi, and malware) are unable to stop the middle and high level members of fraud syndicates from continuing to accumulate illegal gains and criminal power, as described above. What is even more worrying is that when the epidemic subsides, the fraud ringleaders and the upstream elements will be strong enough to recruit members to set up fraudulent boiler room operations all over the world to defraud Chinese language speakers domestically and abroad. If, unfortunately, China gains a head start in detection or diplomacy efforts, the Kenyan case and the Spanish case will be repeated, which will harm Taiwan's international reputation.

III. Prospects

(I) Prioritization of traceability and pulling out the roots: We must clearly understand the nature of telecommunication fraud as a transnational organized crime, and focus on the key cases that have the opportunity to be traced and taken out at the roots. The Taiwan High Prosecutors Office (THPO) "Preventing international trans-border crime supervision unit" is at the core in our investigation of telecommunication fraud. The team was established with special detailed prosecutors of the Taiwan High Prosecutor's Office and the District Prosecutor's Offices, who are experienced in fighting trans-border telecommunication fraud and interdicting the leaders of such operations. Efforts combine the effective intelligence information from the National Anti- Telecommunication Fraud Database of the Science and Technology Investigative Center at the Taiwan High Prosecutor's Office. We focus on trans-border major telecom fraud cases with the opportunity of tracing the origin and taking it out from the roots, while concentrating on the capacity to fight fraud, optimize case tools, assist the prosecutor in charge in directing the investigation, and provide the experience and resources for the case with coordinated support of the authorities. The main goal is to detect the upper level leaders of domestic and foreign telecommunication, network, and capital flow criminal racketeering organizations and to confiscate and recover the proceeds or return them to the victims.

(II) For the cases of the initial members of the organization that cannot be traced back to the roots, we will consider feasible ways to improve the efficiency of the investigation and trial, focusing on the inevitability of the fight and the swiftness of conviction, to avoid misplacement of resources in fraud investigations.

(III) The victim's damages must be compensated as a first priority. Based on the successful experience of prosecutorial entities in returning the crime proceeds in Taiwan and abroad, we will study the mechanisms for compensating the crime losses to the local victims and make use of the existing mediation, restorative justice and trial plea bargain negotiation mechanisms to promote apologies and repayment of crime proceeds by the perpetrators to the victims in Taiwan, which will enhance the citizenry's perception of government fraud fighting and vigorous law enforcement.

(IV) The detection of illicit financial flows is closely related to the seizure of illegal proceeds, and responsive to demands of front-line prosecutors to quickly grasp crime proceeds' information. With the assistance of the Ministry of Justice, the Taiwan High Court of Justice has sent a directive instruction to 38 banks in Taiwan through the Banking Association on April 16, 2021, requesting assistance in completing the uniform revision of the CSV format for financial information within one year. This will avoid the long retrieval process and the failure of data format conversion for the current "financial information electronic document retrieval". To further establish an "online inquiry" mechanism for investigative agencies and optimize their tools for handling financial cases.

(V) In light of contemporary Trans-Border Telecommunication Fraud relying on information technology for cybercrime. The Taiwan High Prosecutor's Office "Preventing international trans-border crime supervision unit" collaborates with the "Supervisory Center for the Investigation of Cybercrime" to apply the methods and experience in investigation of cybercrimes to the fight against frauds. For example, we study the seizure of domain names and the suspension of resolution to block websites involved in fraud outside Taiwan, and strengthen techniques for detecting virtual goods and third-party payment flows in order to trace their origins. We will also communicate with the executive branch agencies to promote a sound administrative legal system and strengthen communications

through the online platform for data retrieval. And from the administrative side to the judicial side, we will fully protect the rights of the citizenry.

(VI) Establishing a platform partnering mechanism for feedback on case experience. In the process of front-line investigations and detection of crimes, the prosecution and police investigation teams often find emerging techniques and loopholes in the prevention of fraudulent crimes, so it is advisable to establish an interdepartmental anti-fraud strategy platform at the Ministry level. Without violating the regulations governing confidentiality in investigations, the teams can provide information and suggestions to the competent authorities of jurisdiction governing financial management, telecommunications management, internet network management, and crime prevention outreach efforts, thereby implementing interdepartmental, inter-agency, and inter-disciplinary cooperation.

Interdicting and Investigating cybercrime

pexels-josh-sorenson-1714208 /www.pexels.comzh-twphoto1714208

Wu, Hui-Lan *

* The author, who wrote this Chapter in 2021, then serving as a Head Prosecutor of this offices.

I. Preface

Since 1990, Taiwan has been using computers and the Internet to commit cybercrimes, including Internet pornography and Internet fraud. In September 1997, the case of the "Godfather of Arms" occurred, where the defendant was suspected of using the Internet to sell firearms, resulting in cybercrime becoming front page news, and garnering the community's and government attention. The judicial authorities also created the Investigation Supervision Unit for Computer Crime to actively investigate cybercrime. Since then, the Internet has flourished and the number of users has multiplied because it is largely free and has sharing functions, and it has swept the society with its very fast and extensive reach. The prevalent type of crime has also thus changed from traditional crime to a large number of cybercrimes. In addition to cyber hacking, pornography, fraud, and firearms sales, cyber threats, sabotage, cyber intrusion, privacy, drug sales, harm to reputation, copyright infringement, and other crimes are also occurring, and the number of victims is increasing daily. The anonymity of the Internet highlights its free nature, coupled with the development of virtual financial instruments that are not yet well regulated by law, including virtual cryptocurrency and third party payments, which enable criminals to hide their crimes by using virtual financial instruments, making cybercrime difficult to detect and interdict. In addition, the sharing nature of the Internet aggravates the spread of cybercrime, which expands the extent of damage to victim's rights much more rapidly and extensively than with more traditional crimes. The Internet knows no boundaries, which makes it more difficult to detect cybercrime because of the cross-border nature of its' syndicated crime networks. As a result, cross-border cybercrime has become the most rampant, obscured and profitable form of crime in Taiwan.

In response to the difficulties in detecting cybercrime and to develop strategies to combat current and potential future cybercrime, the Taiwan High Prosecutor's Office established the Supervision Unit for Cybercrime Investigation in August 2021. The Center will study the criminal structure of major types of cybercrime, create investigation strategies, and construct an investigation platform for law enforcement units to unify the investigative power, and actively combat cybercrime to protect the rights of the citizenry.

II. Promoting investigation and detection of major types of cybercrime

（I） Internet gambling

1. Development of online gambling

With the development and popularity of the Internet, Internet gambling has become a new industry in the digital age, especially because the Internet has the unique characteristics of no geographical or time restrictions. Anyone who has a computer and an Internet-connected device can access Internet gambling. The Internet gambling industry is growing in size year by year and has become one of the most profitable economic sources for criminal racketeering groups. And it has given rise to derivative crimes such as fraud, money laundering, and violent debt collection. Nowadays, Internet gambling has become an industry with professional division of labor, resulting in cross-border criminal problems, and the use of third party payment and virtual currency layers of transfer, forming many breakpoints in investigations. In addition to being a tool for money laundering, it is also difficult to seize the proceeds of crime. How to effectively investigate and detect online gambling, cut off the illegal flow of money to criminal racketeering enterprises, and reorganize the social and economic order, is indeed a major issue now.

2. The characteristics of online gambling

（1）The majority of gambling websites' server rooms are located outside Taiwan, while domestic management departments are created to be responsible for product development, customer service and information security settings, using the information industry as a cover, and developing into the "Neihu Technology Park one stop gaming street" phenomenon.

（2）The previous centralized management of online gamblers has been changed to one in which manpower is scattered to conduct online gambling in their own homes or small office premises, affecting the effectiveness of investigation and detection.

（3）Virtual Currency and Third party payment are used as the payment tools for wagering

and funds transfers. The anonymity and immediacy of virtual currency and third party payment make it difficult to uncover the criminal syndicates behind the scenes by means of tracing their financial flows.

3. Investigating focal points

（1）It is imperative not to be misled by the external names of the information industry enterprise, and to collect evidence that the relevant information industry participant is indeed a stronghold of online gambling by means of open and surreptitious visits, and to investigate based on it.

（2）We must also strengthen online investigation skills, find out the back-end management pages of gambling websites, collect evidence to identify management staff to be investigated, and follow the money flow and trace the sources upwards.

（3）We also need to strengthen the detection techniques of virtual currency and third party payment, and communicate with the executive branch authorities to promote the establishment of a sound administrative legal system for legitimate virtual currency and third party payments..

（4）To assist in the blocking of offshore gambling websites by means of domain name seizure and stop resolution (DNS RPZ).

（II） Chinese funded gaming industry cross-border illegality

1. Unfair Competition of Chinese-funded Game Operators

The Act Governing Relations between the People of the Taiwan Area and the Mainland Area provides in Article 40-1, Paragraph 1, that "Unless permitted by the competent authorities and having established in the Taiwan Area a branch or liaison office, no profit-seeking enterprise of the Mainland Area shall be allowed to engage in business activities in Taiwan." The Chinese game industry may use APP downloads or create a strawman subsidiary in Taiwan to handle small sums of player fees, game backend maintenance and customer service business, in order to circumvent the supervision of the Taiwan government and encourage people to participate in online games. They also use virtual currency and third party payment as tools to transfer huge business profits

out of Taiwan for the benefit of the Chinese game industry. In addition to violating the above law, these acts also affect the assessment of Taiwan's business taxes and causes unfair competition to the legal game industry in Taiwan.

2. Unique features of cross-border illegality

（1）Currently, gamblers mostly play online games through direct downloading of APPs, and Chinese game operators seldom create branches, offices or agents in Taiwan, with most of their customer services located abroad to circumvent the above-mentioned laws and regulations.

（2）According to the current form of teleworking from home, one person and one household can engage in the online game backend, maintenance and customer service business, without setting up a company, and the business can thus also be divided into pieces, which not only impedes investigation and detection, but also leads to ineffective investigations.

（3）As a result, even though the online game companies, offices and agents in Taiwan do have financial flows with Chinese companies, it is difficult to infer from this that the financial flows were related to the establishment and operation of the companies, offices or agents in Taiwan, and that the companies, offices or agents in Taiwan were operated by Chinese companies, in violation of the abovementioned legal regulations. This determination is still dependent on the defendant's confessions, witness testimony, or other physical evidence such as the financial flow accounts' ledgers.

3. Promoting investigative focal points

（1）We must encourage, either legislatively or administratively, that strawman persons nominally in charge of the companies, offices and agents created by Chinese capital companies in Taiwan take the initiative in reporting and informing, so that those who cooperate in generating interdictions can be exempted or have their sentences reduced.

pexels-pixabay-163064 /www.pexels.comzh-twphoto163064

（2）We need also to collect evidence on Chinese capitalized games that have a large audience and downloads of game software, check whether the online games have created headquarter companies, offices and agents in Taiwan, and investigate them in order to curb the unhealthy trend of Chinese game operators illegally creating operations in Taiwan.

（3）We must also collect evidence in specific cases, find out the backend management websites of online games, analyze the relevant connections to find out the specific computers and IP addresses involved, identify the computer and IP users as the management of the Chinese game industry, and conduct investigations.

pexels-alesia-kozik-6765373 /www.pexels.comzh-twphoto6765373

（III） Virtual Currency

1. Virtual Currency uses blockchain technology, which is decentralized, highly anonymous, easy to circulate across borders, and fast to transact across. It is currently used as a payment instrument and an investment commodity in the international arena, and is used in various forms of crime. For example, by claiming a higher rate of return on investments, the public is attracted to buy and sell virtual currency, and after absorbing a considerable amount of money, the criminals may abscond with the invested funds. There is also the problem of theft of virtual currency by hacking, obtaining private keys or hacking into the online wallets of individuals or large corporations with virtual currency addresses, and then stealing and transferring bitcoins to virtual currency. Due to the real-time and anonymous nature of Virtual Currency, in order to avoid the risk of withdrawal and tracing, perpetrators often use payment tools to require the victim to pay a ransom, such as kidnapping software that requires payment in virtual currency. The use of virtual currency as a payment instrument makes it difficult to trace the real identity of the payer, so virtual currency

has been widely used in illegal transactions, including the purchase and sale of guns, drugs, and child pornography, as well as illegal money laundering, fraud, and terrorism crimes. In recent years, it has become a new money laundering channel for various fraud, drug trafficking, and gambling crime groups. Virtual currency has become the most advantageous tool to conceal traces of cybercrime and the proceeds of crime.

2. In order to strengthen the management of virtual currency, Article 5, paragraph 2 of the Money Laundering Control Act, specifically regulates "virtual currency platforms or transactions". The regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction" took effect as of July 1, 2021, with the Financial Supervisory Commission as the competent authority. The regulations' main points focus on the following: 1. The requirement for industry to verify customer identities, and the promotion of a real-name system for virtual currency platforms. 2. The platform acting as the transferring party should transfer the information of the transferring party and the recipient involved in the virtual currency transfer to the platform that acts as the receiving party. 3. Cash transactions of NT$500,000 or more should be reported to the MOJ Investigation Bureau, and any suspicious transactions should also be reported to the MOJ Investigation Bureau. The inclusion of virtual currency in the Money Laundering Control Act will not only affect the willingness of criminal groups to use virtual currency as a payment instrument, but will also facilitate the tracing of cybercrime and seizure of criminal proceeds.

3. Tracing crimes committed with Virtual Currency

（1）Law enforcement agencies can develop and use virtual currency user transaction tracking technology, to grasp the flow of suspicious user transactions and methods, and consider long-term investment in human and material resources to establish big data, analysis of virtual currency illegal users' transaction characteristics, then according to the illegal transaction money flow and addresses, engage in proactive investigation.

（2）We also require strengthening network detection technology, after determining the possible illegal users, combined with traditional detection techniques, such as retrieving network IP addresses, contact records and financial transaction data for analysis, in order to elicit the real identity and criminal behavior of the perpetrators, and to detect crime with the search, detention, interviewing and other traditional investigative techniques.

（3）Virtual Currency is a cross-border type of crime, so in addition to extraterritorial cooperation in government supervision, it is also necessary to combine international mutual legal assistance channels to jointly trace the actual identity of the perpetrators and the flow of funds, then to seize the proceeds of crime, to combat this emerging type of crime.

（4）Virtual currency trading "account opening information", "transaction details" and "wallet location" are important forms of evidence in crime investigation, so how to establish an effective and rapid retrieval mechanism with virtual currency trading platforms is also a key focus of the THPO's future work.

（IV） Virtual Currency

1. Lawfulness and feasibility of domain name seizures

The Internet has no borders, and it is very easy to register a new domain name or create an extraterritorial server or co-location. Therefore, domain name abuse has become a new type of Internet crime, with fraudulent one-page advertisements, gambling, malicious programs with information security threats, phishing sites, and sites that violate copyright, or child and juvenile sexual exploitation prevention laws. The IP addresses of these illegal websites are often located outside Taiwan, and the domain names are registered in foreign countries, which affects the investigation of crimes and leads to continuous violation of the rights of the public. The future of justice mandates us to effectively detect crimes of domain name abuse and to prevent the continued expansion of harms against the public.

The United States has recognized that a domain name can be seized by finding the registry of the domain name and having the state take control of the domain name, and the Swedish Supreme Court has also recognized that a domain name can be confiscated. Through the process of seizure and confiscation of domain names, perpetrators are prevented from using the domain names to continue their criminal activities, and the public is saved from the risk of continued victimization. It is worth exploring whether judicial practice in Taiwan recognizes domain names as a proper subject of seizure, so that the seizure of domain names can become a powerful tool for our crime investigation and prevent the public from being victimized. In addition, since most of the illegal domain names are located outside Taiwan, even after the court rules on a seizure, the seizure still needs to be executed through mutual legal assistance, which may be too slow to meet urgent needs. The Taiwan Network Information Center (TWNIC) has integrated domestic Internet critical infrastructure providers (ISPs) to build a DNS RPZ (Response Policy Zone), which can restrict access to malicious domain names or IP addresses both domestically and abroad, to strengthen the effect of domain name seizure. One of the means of enforcing a court's decision on domain name seizure is by DNS RPZ (Stop Resolution), and it is necessary to further explore this avenue of enforcement.

2. Proactive Measures

（1）To explore the legality and feasibility of seeking court seizure orders for domain names and enforcing DNS RPZ, the Chief Prosecutor of THPO assigned a prosecutor with expertise in computer crimes to create a task force to discuss the issue and held a special meeting on April 6, 2021 to discuss the legality of domain name seizure efforts. On June 17, 2021, the Taiwan High Prosecutor's Office held the "2021 Global Cooperation and Training Framework (GCTF) Online International Seminar - Virtual Conference on New Developments in IP Protection and Combating Digital Infringement" where we discussed with scholars, prosecutors and judges on the topic of "Combating Internet Infringement and the Responsibility of Internet Service

Providers (ISPs)". The THPO Cybercrime Investigative Assistance and Coordination Unit invited the Department of Prosecutorial Affairs, MOJ, and the Department of International and Cross-Strait Law, MOJ, to discuss the topic of "How to Conduct Seizure of Domain Names and Enforcement of DNS PRZ", to reach a consensus on such efforts. On August 27, 2021, the Department of International and Cross-Strait Legal Affairs discussed the feasibility of cooperating with the relevant authorities in order to achieve breakthroughs after broadly gathering ideas.

（2）The THPO assigns special prosecutors with expertise in computer crimes to provide professional assistance in specific domain name abuse cases to the prosecutors in charge, for each District Prosecutor's Offices, including the consolidation of legal opinions and communication and coordination with relevant authorities, and will continue to pay attention to the interpretation of court rulings and the effectiveness of enforcement, so as to thereby observe the feasibility of judicial implementation of domain name seizure and DNS RPZ (stop resolution).

3. The Future Outlook

The cyber world is so vast that the damage caused by crimes committed in the virtual world of the Internet is many times greater than that caused by crimes in the physical world. Interdiction depends on the creation of new legal concepts and investigation methods, such as the domain name seizure system, in order to strengthen our powers of crime detection. In addition, due to Taiwan's special international status, it takes a long time to complete mutual legal assistance. If we can use domestic technical skills, such as DNS RPZ, to stop crimes from being committed outside Taiwan before mutual legal assistance is realized, we can also improve the detection of crimes for the purpose of protecting the lives and property of the citizenry. We hope that the Taiwan High Prosecutor's Office can find new ways to detect the criminal abuse of domain names by discussing related issues and observing the operations of DNS RPZ in judicial practice.

pexels-brett-jordan-5426402 /www.pexels.comzh-twphotoios-5426402

(V) Data Collection from Online Social Media: Communication and Coordination with Online Social Media Platforms

1. In view of the fact that cybercrime is becoming increasingly prevalent, and that most of the cybercrime communities are located outside Taiwan, if all cybercrime cases involving cybercrime communities can only be retrieved through mutual legal assistance, the amount of data retrieved will be too large and time-consuming to comport with standard investigative timeframes. Therefore, the Ministry of Justice signed an agreement with Facebook, GOOGLE and LINE in 2019, which allows the Ministry to request information from Facebook and other online communities. However, the content and duration of the online communities and the information available for retrieval therefrom are limited, and often do not meet the requirements of the investigation, or after retrieval and search, it may often take 3 or 4 months to obtain a reply as to whether or not they agree to the retrieval, which causes further delays and problems for progress in the prosecutor's case.

2. Proactive Measures

（1）Strengthen communications with the online community

① The Taiwan High Prosecutor's Office has consolidated the requests and searches made by the prosecutorial offices and police investigation agencies to certain online communities, and convened a video conference on July 9, 2020 to discuss the matter. The meeting proposed that Taiwan and Japan have different national conditions in investigating criminal cases, but that both sides have common interests in fighting crime, and that it is the trend of international conventions to work together to fight crime. And Taiwan and Japanese law enforcement agencies

have different standards, so the meeting discussed the relaxation of the investigation period, the nature of the investigation cases, the search process, the establishment of a point of contact window, and accelerating the speed of obtaining the investigation data.

② On December 1, 2020, the Ministry of Justice was asked to consult with the social media on consolidated issues relating to retrieval of information from social media by each District Prosecutor's Office.

③ The Facebook window has a dedicated staff to liaise with the unified point of contact window of the Taiwan High Prosecutor's Office to communicate and resolve problems arising from the retrieval of information as needed at any time.

④ After consultation with the online community, the speed of data retrieval and simplification of the search process have been significantly improved.

（2）Enhancing the functions of the unified point of contact point

Facebook has created a separate window to connect with the Taiwan High Prosecutor's Office's unified point of contact point, while LINE has appointed a domestic lawyer as their contact point with the Taiwan High Prosecutor's Office. For special cases, the Taiwan High Prosecutor's Office can communicate directly with Facebook and LINE through the centralized contact window. In most cases of intimidation involving freedom of expression, the online social media platforms refuse to provide access to the information. However, in specially sensitive cases, after coordination with the Taiwan High Prosecutor's Office's unified window, the online social media platforms are receptive and agree to provide access the information. For special crimes involving national conditions, after the Taiwan High Prosecutor's Office's unified contact window explains the infringement of national and social interests, the online social media also gladly accept the explanations and deliver the relevant information.

（3）The Future Outlook

The Taiwan High Prosecutor's Office will continue to respond to the opinions of District Prosecutor’s Offices to the online community platform and deepen

communications with the online community in order to facilitate the retrieval of information and the investigation of cases. We also intend to request the Ministry of Justice to sign data access agreements with other online communities such as WECHAT and TWITTER to avoid criminals using online community communications to conceal their criminal acts and to facilitate crime investigation.

III. Milestones in cybercrime investigation

(I) We are establishing a cybercrime platform with other law enforcement agencies to promote the investigation of information and communication crimes and to unify investigation activities

In the investigation of cybercrime, the various law enforcement agencies do not have shared communication channels, resulting in fragmentation of the investigation. The Taiwan High Prosecutor's Office will establish a platform for law enforcement agencies to promote their investigations of cybercrime, so that resources can be shared, group efforts can be united, and we can strengthen the momentum of the investigation.

(II) To provide professional and integrated services for District Prosecutor's Office prosecutors and to establish a platform for cooperation

The Taiwan High Prosecutor's Office Supervisory Center for the Investigation of Cybercrime has a special professional nature. The Supervisory Center will establish a cooperative platform with District Prosecutor's Offices on major cybercrime cases, integrate various case resources, and provide professional consultation channels to fully assist in the investigation of cases from the beginning to the end.

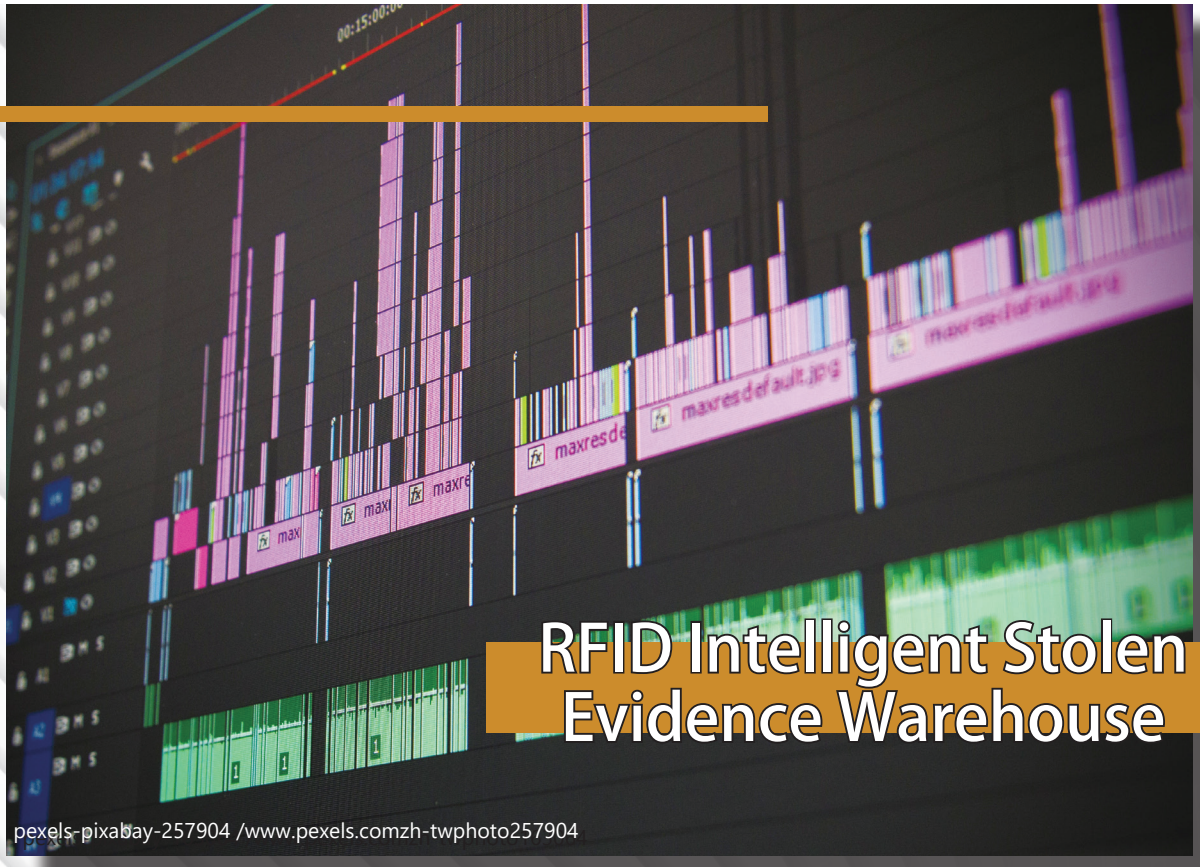
(III) We endeavor to investigate and detect cybercrime cases, and we have developed new investigative techniques for investigating cases that require

Cybercrime is a new type of crime, which traditional investigative techniques have been unable to effectively detect and deter, and the formulation of the law is often behind the curve and too slow to meet emergent needs. How to revitalize the existing laws to find new means of crime investigation is the focus of the Taiwan High Prosecutor's Office

Supervisory Center for the Investigation of Cybercrime.

（IV）Promoting enactment of administrative and judicial regulations, to completely deter cybercrime

Cybercrime uses a large number of advanced online tools and technologies to conceal crimes and expand damages to victims, including through illegal online advertisements, virtual currency and third party payments. Interdicting these online tools and technologies is inadequate in terms of legal regulation and administrative management, and they have become the tools of crime. It is difficult to be effective with solely traditional investigation methods, and it is necessary to create new investigation methods and to make the best use of them. The Taiwan High Prosecutor's Office will promote and facilitate the enactment of relevant laws and regulations to curb cybercrime, and urge the executive branch agencies and authorities to actively manage the relevant network tools in order to fully curb the advent of cybercrime.



pexels-pixabay-257904 /www.pexels.comzh-twphoto257904

RFID Intelligent Stolen Evidence Warehouse

Hsieh, Chih-Ming*

* The author, who wrote this Chapter in 2022, then serving as a Head Prosecutor of this offices.

I. Preface

Given the importance of managing stolen evidence during the investigation and trial of cases, as well as to enhance the prosecution of crimes and prevent the loss of stolen evidence, it is imperative to use technological equipment to enhance the efficiency of administering stolen evidence. In 2011, the Taichung District Prosecutors Office (TCPO) of the Taiwan High Prosecutors Office (THPO) took the initiative to apply for a technology project. The first phase of the Radio Frequency Identification (RFID) system was completed on October 31 of the same year and was initially used only for control of guns and ammunition. On June 7, 2016, the TDPO sought additional funding from the National Development Council for the second phase of the RFID system, which was completed and accepted on October 31, 2016. In addition to optimizing functions from the first phase, the system also incorporates the management of drugs into the technology, which has been well received.

In 2017, the National Conference on Judicial Reform resolved that "the Executive Yuan, in conjunction with the Judicial Yuan, should establish a system for the supervision of evidence and the safekeeping of evidence after a verdict is finally confirmed, regulating the methods of supervision and the period of safekeeping for evidence, and clearly regulate legal effects of any violations. To implement the resolution of the National Conference on Judicial Reform, the Ministry of Justice and THPO continued to plan and refine measures for the evidence custody system. Recent incidents involving losses of drugs have attracted much attention from the public. To avoid recurrence of such regrettable incidents and considering the need for homogeneity and security of the evidence transferred to prosecutorial entities for inspection, the policy direction for introducing technology-based evidence administration was created. The Taiwan High Prosecutor's Office will assist the Ministry of Justice in promoting establishment of a digital management system for drug seizures, drawing on the experience of the RFID warehouse at the TCPO.

Taiwan Taichung District Prosecutors Office RFID Workstation

II. Objectives

The purposes of establishing the digital drug seizure management system are as follows:

Taichung District Prosecutors Office Intelligent Armory

(I) To use IoT RFID to manage drug seizures, to reduce the consumption of manpower in the management and supervision of stolen evidence, to effectively improve administrative efficiency, to reduce the occurrence of fraud in management of stolen evidence, and to achieve the uniformity of drug seizures from the time they are entered into the inventory to the time when the punishment is determined.

(II) Introduce automatic logistics detection technology to enhance accuracy, correctness, and timeliness of drug management.

(III) Build automated storage equipment (intelligent cabinets) to save labor expenses, reduce manual

RFID Adhesive Labels

errors, and improve administrative efficiency and correctness in evidence management.

(IV) Integrate information and communication platforms and automated logistics technology to bring into play the benefits of intelligent Internet of Things to strengthen transparency of inventory administration.

(V) Establish a warehouse environment monitoring mechanism to ensure safety and stability of the drug storage environment and personnel operations.

III. Present Status Quo

After conducting on-site investigation and survey of drug seizure cases and the condition of the warehouses in each prosecutorial office, THPO plans to implement the project in phases. After assisting the Ministry of Justice to request funding from the Drug Prevention Fund (DPF), The Taiwan Taipei District Prosecutors Office will complete the first phase in the second half of FY2021, and will launch and complete the architecture for the second phase from FY2022. The THPO has also already assisted in submitting the application for the Drug Prevention Fund for FY2023 (currently under consideration) and will continue to assist in the nationwide implementation in all District Prosecutor's Offices.

IV. Anticipated Benefits

This project involves new innovations in administering stolen evidence in Taiwan, and will be of great benefit to improving efficiency and security in managing stolen evidence. To fully exploit the value of RFID technology and to spread out the costs of use, we will continue to plan both "horizontal expansion" and "vertical expansion" of the technology management. We will continue to strive for additional budget appropriations to assist in promoting use of technology-based management of stolen evidence in prosecutors' offices nationwide, and fostering the related industries to improve their technologies in these areas. Also, we hope to integrate the upstream direction of stolen evidence, share resources and implementation experience with courts, judicial police agencies and other related agencies, and start using RFID technology to identify stolen evidence from the onset of judicial police seizure cases. In addition, we also hope to integrate the downstream direction, including the identification unit, the court and drug destruction units to use RFID as the core of the technology management system, so we can share the benefits of RFID technology. We fully expect that one day, from the crime scene, forensic units, courts, stolen goods warehouses and even the drug destruction unit, that RFID technology can be used as a pervasive tool, ensuring more effective and secure management of stolen evidence, and provide for uniformity with stolen evidence.

pexels-torsten-dettlaff-971546 /www.pexels.comzh-twphoto971546

pexels-pok-rie-139975 /www.pexels.comzh-twphoto139975