Chapter 10
Cyber Crime Investigation Center

I. Purpose of establishment and mission

To establish the national information and privacy crimes reporting and liaison point of contact, the Taiwan High Prosecutors' Office created the "Taiwan High Prosecutors Office Cyber Crime Investigation Center", to handle the scope of cases running the gamut from internet hacking attacks (ransomware), to major financial and trans-border telecommunications fraud, integrating our Office's Science and Technological Investigation Center and Internet Crime Investigation Assistance Unit. Aiming to expeditiously ensure comprehensive domestic and international criminal intelligence across the entire span of major criminal activity, to accord timely guidance to all District Prosecutors' Offices, to take appropriate responsive measures and reduce potential damages, while efficaciously integrating our Office's internal resources and creating robust channels of clear communication and command in combating information and privacy crimes.

II. Functions

(I) Multilevel longitudinal (vertical) supervision

1. Enhancing investigative entities reporting of information and privacy crimes, to ensure robust criminal intelligence of the nation's overall information and privacy crime cases.
2. Deploying longitudinal analysis, judgement determinations, and supervision of District Prosecutors' Offices in real time investigation of information and privacy crime cases.

(II) Multidimensional horizontal integration domestically and abroad

1. Inter-agency liaison and coordination, to integrate all manner of criminal investigation resources (including information, communications, and computer technology crimes, in conjunction with our Office's telecommunications fraud, gambling, racketeering organization, and money laundering supervision units).

2. Cooperating with relevant agencies and professional organizations, for unified investigation teams, combined with professionals to strengthen case investigation and evidence gathering practices and activities.

3. Our Office's Science and Technological Investigation Center has established an internationally accredited Digital, Information and Privacy Laboratory (ISO 17025, 27001), working in conjunction with its' professional capabilities to assist human competencies, offer professional consulting, and evidence identification and authentication.

III. Organizational planning

(I) Creating the Consulting and Coordination Committee

The committee convenes for meetings every three to six months, and on an ad hoc basis as necessary, with responsibility to consider computer crime prevention policies and guidance, and coordinate in practical implementation.

(II) Operational assistance and coordination

study Unit

1. Executive Yuan Information Security reporting, policy promotion and implementation.

2. Coordinate and integrate the Information and Privacy Crimes Center professional units and District Prosecutors' Office investigative jurisdictional scopes of authority.

3. Provide a uniform point of contact for reporting of specialized hacker attack and ransom crime victim organizations (individuals), and create standard operating guidelines in such matters for District Prosecutors' Offices.

4. Integrate all units case intelligence analysis, relevant resources, controls and tracing and tracking information crime cases, as well as providing management reports, and comprehensive criminal trend analysis and future directions guidance.

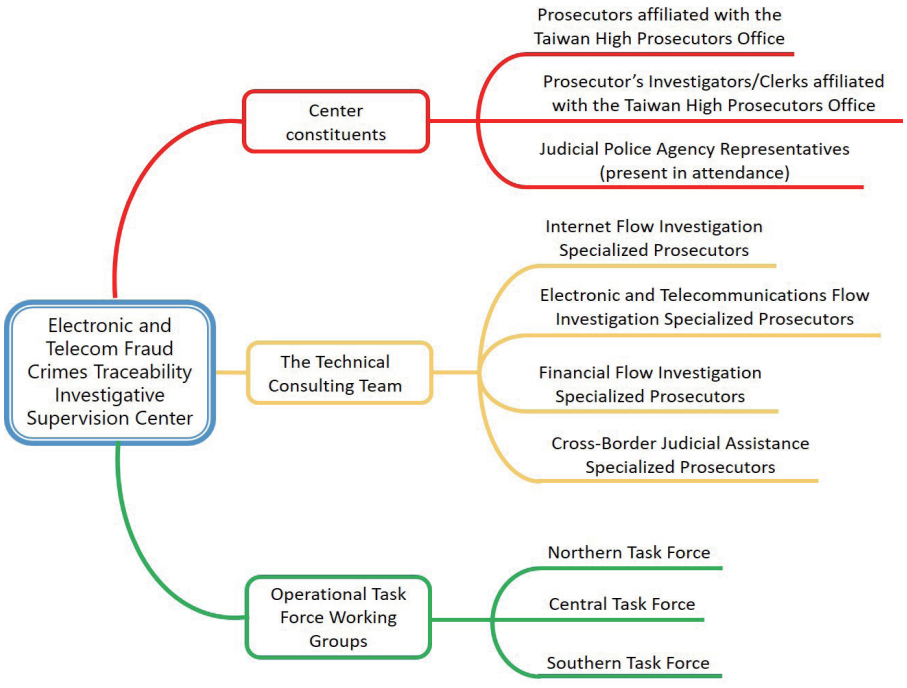
5. Coalesce all of the said Prosecutors' Office resources to create corporate information security and information crime promotion teams, for a single point of contact operational platform.

(III) Trans-border and telecommunications fraud investigation supervision unit

Contemporary fraud crimes have emerged as racketeering organizations with professional divisions of labor for their respective internet, telecommunications and financial flows, and their operations have often expanded abroad. Our Office has established the Nationwide Telecommunications Fraud Database within our Science and Technological Investigation Center, to aid and supervise all District Prosecutors' Offices in their deployment and use status of the database, while collecting their recommendations for improvements to the system, and in May 2019, through confidential encrypted emails, we provided the Criminal Investigation Bureau Fraud Crime Combatting Center and the MOJ Investigation Bureau Economic Crimes Prevention Section with database analysis of persons on the list for entry ban or departure control orders.

Our office relies on our experience gained over the years in combating fraud, which has taught us that without concentrating prosecutorial and law enforcement task force resources together for investigations across the downstream and upstream parties, our efforts will merely treat the symptoms but not get at the cause. To focus on traceability to destroy the crime at its roots, we established the "Electronic and Telecom Fraud Crimes Traceability Investigative Supervision Center", serving as the responsible core entity dedicated to combating electronic fraud. Working in conjunction with active operational intelligence from our office's pre-existing Science and Technological Investigation Center's "Nationwide Anti-Electronic and Telecom Fraud Database", we concentrate resources to combat fraud at the roots with an emphasis on major cases, delegating tasking to working groups composed of prosecutors specializing in supervising these investigations, in collaboration with the Electronic and Telecom Fraud Crimes Traceability Investigative Supervision Center and technical consulting teams working with prosecutors to provide ongoing guidance and assistance. Our priority offers case handling expertise and resources along with support for coordination with other agencies to emphasize major cross-border electronic and telecommunications fraud cases with the opportunity for traceability and disrupting racketeering organizations at the roots, while deploying our primary objective in detecting the key mid-level and senior-level parties in domestic and foreign electronic and telecommunications, internet, and financial flow criminal organizations.

Administrative Organization



(IV) International mutual judicial assistance

1. Serve as the liaison point of contact for overseas investigative agencies for information and privacy crimes.
2. Assist District Prosecutors' Offices in mutual legal assistance to obtain evidence, and provide joint efforts in combatting transnational information and privacy crimes.
3. Accord District Prosecutors' Offices with mutual legal assistance education and training and hold international workshops for personnel combatting information crimes.
4. Analyze case intelligence and integrate resources, apply controls, and trace information crime cases along with providing forward-looking reportage.

(V) Information Crime Studies and Analysis Supervision Unit

1. The Information Crime Prevention technology research and development and planning special unit is situate in our Office's Second Office Building, due to needs for confidentiality and security, with members enjoying (sensitive compartmented information facilities) independent offices and private conference rooms.

2. Analyzes the latest information crime modalities and cases, for in-depth research and development of financial tools deployed in digital currency and emerging criminal modes, while proposing streamlining and suggestion reports, which can enhance the prosecutorial system case handling capabilities, and also providing our Office's Science and Technological Investigation Center and Finance Crimes Supervision Center team members with information useful to establish new crime fighting tools, strategic development, and legal and regulatory recommendations.

3. Plan for all District Prosecutors' Offices information crime personnel lectures and occupational advancement workshops on information crimes, cryptography, hacker attacks, and white hat hacker operations.

4. Closely collaborate and maintain exchange with domestic and overseas forensic information authentication and information security laboratories, for constant awareness of evolving and emerging technologies, and provide reportage.

5. Broadly unify efforts among government, the civil sector professionals and resources, to plan for major critical infrastructural facilities and enterprises red team drills and exercises. (Written by Prosecutor Huang,Li-Wei and Lin,Yen-Liang)

Opening Ceremony for Cyber Crime Investigation Center

Taiwan High Prosecutors Office Cyber Crime Investigation Center organizational structure chart