I. Introduction

To strengthen Taiwan's capability to deal with information and communication security issues, the National Information and Communication Security Taskforce (NICST) was established on January 17, 2001. The NICST is a national level taskforce, responsible for developing national information and communication security policy and notification and response mechanisms, review and consultation on major programs, and coordination and supervision of inter-ministerial affairs concerning information and communication security. Cyberspace Protection System and Cybercrime Investigative System are the two major parts in the NICST. Please refer to the following figures:

The Office of Information and Communication Security (OICS) is the Secretariat of the Cyberspace Protection System. And the major law enforcement agencies (LEAs) in detecting cybercrimes, the Ministry of Justice Investigation Bureau (MJIB) and the Nation Police Agency (NPA), Ministry of the Interior are both included in the
Cybercrime Investigative System.

II. Taiwan’s Recognition and Efforts regarding the Global Information Threats on Cybersecurity

Taiwan is one of the most important hubs through the world. As we all know, the Internet has brought great convenience and speed to our lives. However the prevalence of the Internet and related changes in consumer behavior mean that issues such as cybercrime and protection of personal information and privacy have become a source of great concern affecting national security and social stability. Due to this situation, we recognize the world is now facing some serious information security threats, such as: rampant organized cyber crime, theft of personal information and financial fraud incidents abound, increasing information security risks on critical information infrastructures, intensification of advanced persistent threat, and zero-day attack resulting in difficulties in information security defense.

Since the NICST was established in January 2001, major information security plans or programs, each lasting four years, implemented over three phases have been introduced (see the following figure for details). These initiatives have effectively achieved a high degree of information security readiness in Taiwan. The highlights of each program or plan are outlined below.

III. Cybercrime Overview in Taiwan

Ministry of Justice (MOJ) has established a Cybercrime Prevention and Fighting Center in the District Prosecutors’ Office to conduct the cybercrime
investigations. The 9th Investigation Corp of the Criminal Investigation Bureau (CIB), NPA is one of the strongest LEAs in detecting cybercrimes. Besides, the Information and Communication Security Division of the MJIB also has the mandate to detect cybercrimes. The said authorities are the key pillars of anti-cyber crimes networks.

As per the statistics of the NPA, there are more than seven thousand cybercrime cases being referred to the District Prosecutor’s Office each year (see the following figure for details).

According to the analysis of the NPA, the main trends of the cybercrimes (78.34%) in 2014 are the offences impairment to use of computers (40.35%), fraud (30.52%) and offences against reputation and credit (7.48). The case numbers of the offences impairment to use of computers are 4,536 while frauds are 5,714, increasing 2,597 cases compared with 2013. That is the major cause of the rising of cybercrimes (see the following figure for details).

IV. Conclusions and Suggestions

I) Raising information security issues to the level of national security.

II) Emphasizing the importance of protecting citizens’ rights, in particular protection of personal information and privacy.

III) Increasing emphasis on security issues related to cloud computing and
mobile Apps (eg. Line).

IV) Emphasizing government/private sector or industry-academic cooperation issues.

V) Enhancing international cooperation on combating cross-border cybercrimes and information exchange.

Reference materials:


3. Chou, Ching Ming (November 4, 2015), “An Overview of Anti-Cybercrime Efforts Made by MJIB” (as the appendix report)
Appendix Report:

An Overview of Anti-Cybercrime Efforts Made by MJIB

By Chou, Ching Ming, Investigator of MJIB on Nov 4, 2015

Abstract

According to the survey conducted by Taiwan Network Information Center in 2013, 83 percent of Taiwanese households are hooked up to the Internet. Along with the expansion of Internet access, expansions of internet crimes are paralleled simultaneously. Recognizing cyberspace as an important new frontier in law enforcement, Taiwanese authorities are taking positive action toward fight cybercrime. In 2003, Taiwan took a major step forward by passing a number of amendments and the addition of an entirely new chapter to Taiwan's Criminal Code. The code's new Chapter 36: "Offenses against Computer Security" considerably enhances the protection of computers and computer systems. In 2006, Investigation Bureau, Ministry of Justice (MJIB) established a computer forensic laboratory (CFL) at MJIB Headquarters along with the Cybercrime Investigation Unit (CIU), a branch responsible for implementing the national strategies in combating computer crimes.

I. Introduction

The development of new technology such as computers and the internet are bound to have both positive and negative effects. Cybercrime, with the nature of low risk, high rewards, develops a variety of forms including network attack, mail fraud, intimidation, and copyright infringement. This commonly involves economic crimes such as identity theft, credit-card fraud, and bank fraud which in turn, costs businesses and individuals billions of dollars. Special task forces, such as the CIU Investigation Bureau, have been set up to fight cybercrime in Taiwan since 2003. The CIU investigates computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts, for instance the G-8 24/7 Computer Crime Network.

II. Fighting Cybercrime in Taiwan

Cyber-crime may involve making unauthorized use of individuals' personal information, stealing companies' confidential business information or selling state secrets; these new types of crimes thus affect every level of society. Although certain forms of unauthorized computer access were criminalized in earlier laws, those laws suffered from a number of problems, including being too limited in scope. From the standpoint of law enforcement, it is better to have laws that are widely applicable rather than laws that focus on narrowly defined types of
criminal behavior. To Recognize and respond to the need for plugging the gaps in the existing legal and regulatory framework in the face of cyber-crime and to eliminate any loopholes in Taiwanese law, on June 25, 2003 the Taiwanese government added a new chapter, Chapter 36 (Offenses against computer security) to Taiwan’s Criminal Code. Chapter 36 is designed to cover a wider range of conditions and provide the flexibility necessary to deal with future cybercrime variations.

Besides MJIB, the Ministry of Justice has established a Cybercrime Prevention and Fighting Center in the Prosecutors’ Office. Based on the Ministry of Justice statistics, in 2013, prosecution of computer related crime totaled 3,357 persons, with 2,635 convections. As to Chapter 36, there were 74 persons charged with 29 convections. In 2014, prosecution of computer related crime totaled 3,159 persons, with 2,525 convections. As to Chapter 36, there were 67 persons charged with 42 convections. Between the years 2012-2013, there was a 5.9% decrease in the overall prosecution of computer related crime persons, and a 9.5% decrease in persons subject to Chapter 36, also was a 4.2% decrease in the overall convection of computer related crime, and 44.8% growth in persons subject to Chapter 36 in 2013 compare to the pervious year.


III. An introduction of Chapter 36 of Criminal Law and Frequently Used Statutes

Taiwan’s Criminal Code Chapter 36 Offenses against computer security) contains six articles covering four types of crime: unauthorized access (Article 358), the unauthorized acquisition, deletion or alteration of electromagnetic records (Article 359), unauthorized use of or interference with a computer system (Article 360) and creating computer programs specifically for the perpetration of a crime (Article 362). Article 361 specifies that more severe punishment should be imposed in the case of violations carried out against the computers or other equipment of a public service organization, and Article 363 states that the provisions of Articles 358–360 shall apply only after prosecution is instituted upon complaint. These new articles provide a clear legal basis for the punishment of common types of cybercrime such as unauthorized access by hackers, the spreading of computer viruses and the use of Trojan horse programs.

The following statutes are used most frequently by the MJIB to investigate computer-related crimes:1. Chapter 36 of Criminal Law as

IV. How the MJIB investigate computer crime

The Ministry of Justice, Investigations Bureau (MJIB) is responsible for national security and investigating major crimes. The MJIB also investigates public corruption, economic, drug, money laundering, and cybercrime. The Cybercrime Investigation Unit (CIU), a division of MJIB, is responsible for implementing national strategy in combating computer crimes in Taiwan.

MJIB use sophisticated methods to investigate and coordinate cyber incidents. The CIU processes complaints of cybercrime and coordinates computer crime investigations. The MJIB’s Cyber Division Headquartered in Taipei, coordinates investigations in which networks or computers are exploited as instruments in criminal activity or as targets. High priority is given to investigations that involve terrorist organizations or intelligence operations sponsored by foreign governments. The MJIB trains computer investigators to work in MJIB field offices on current cybercrime issues, techniques and cases. The MJIB also maintains a Computer Forensic Laboratory (CFL) used for advanced data recovery, research & development, and prosecution.

The MJIB maintains a Computer Forensic Laboratory (CFL) at MJIB Headquarters in Taipei for advanced data recovery and for research and development. Technology has made it easier for criminals to hide information about their crimes. Because of the sophistication of the digital environment, evidence is collected and handled differently than it was in the past and often requires careful computer forensic investigation. CFL is a one-stop, full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations. Four MJIB field offices also have specialized cyber squads called Cyber Action Teams which their major duties are to investigate and aid in cybercrime investigations.

The MJIB is sensitive to the victim's concerns about public exposure, so any decision to investigate is jointly made between the MJIB and the Prosecutor in order to safeguard the victim's fundamental human rights.
V. Conclusion

Some of the challenges faced by law enforcement on the international front include: harmonization of countries' criminal laws; locating and identifying perpetrators across borders; and securing electronic evidence of their crimes so that they may be brought to justice. Complex jurisdictional issues arise at each step. The Ministry of Justice is attending many anti-cybercrime international organizations and working with foreign governments through many channels to address global threats related to computer crime.

Cybercrime greatly affects individuals, businesses, and national security due to the pervasiveness of the Internet. We believe that different countries should work together and use legal, organizational, and technological approaches to combat cybercrime, to reduce the damage to critical infrastructures, and to protect the Internet from being abused.