PROSECUTING COMPUTER-RELATED CRIMES IN THAILAND

*Thongchai Itthinitikul**

I. THE STATE OF CYBERCRIME IN THAILAND

Currently, the Ministry of Information and Communication Technology (MICT) is implementing the digital economy policy declared by the Thai government as a policy statement to the parliament last year (2014). The MICT has played a key role to follow up the Thailand Information and Communication Technology (ICT) Policy Framework (2011-2020).[1] The framework comprises five strategic areas, namely e-Government, e-Industry, e-Commerce, e-Education and e-Society, that aim to enhance the economy and life quality of Thai people and guide Thailand towards a knowledge-based economy and society. This mission has mostly been assigned to the Electronic Transactions Development Agency (ETDA)[2] which is an agency (public organization) under MICT. ETDA serves as the core agency to develop, promote and support electronic transactions to ensure that they are reliable and provide equal opportunities to all. Although this development has brought great benefits and convenience to all Thai people and the country as a whole, it has also produced computer-related crimes which cause severe damage.

To mitigate and handle the aggressive growth of cybercrime, the Thailand Computer Emergency Response Team/Coordination Center, or ThaiCERT,[3] was transferred to ETDA from the National Electronics and Computer Technology Center (NECTEC) under the National Science and Technology Development Agency in 2011. The mission of ThaiCERT emphasizes collaboration with network agencies and concerned entities to cope with known ICT security threats. Furthermore, ThaiCERT has been assigned another proactive role in human resources development to enhance the agency's risk management capacity on cybercrime threats. Supported by ThaiCERT, ETDA's mission to build trust in electronic transactions has therefore been considerably strengthened. However, cybercrime issues in Thailand are still increasing and are becoming more aggressive as seen from the statistics of incidents reported to ThaiCERT from July 2011 till 2015 as follows.

---

*Divisional Public Prosecutor, Executive Director's Office of Criminal Litigation 10, Office of the Attorney General, Thailand.

[1] Available at <http://www.mict.go.th/assets/portals/10/files/e-Publication/Executive%20Summary%20ICT 2020.pdf>.

[2] Available at <http://www.etda.or.th/etda_website/content/background-and-mission.html>.

[3] Available at <http://www.etda.or.th/etda_website/eng/content/background-of-thaicert.html>.

Statistics of Incidents Reported to ThaiCERT[4]
Table 1: Statistics second half of 2011

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content							12	8	6	7	39	5	**77**
Availability							1	2	2	0	1	0	**6**
Fraud							44	38	56	69	66	36	**309**
Information gathering							28	13	18	14	12	8	**93**
Information security							0	0	0	0	0	0	**0**
Intrusion Attempts							9	20	19	19	16	11	**94**
Intrusion							0	0	0	0	0	0	**0**
Malicious code							6	10	14	7	18	8	**63**
Other							0	0	0	1	0	3	**4**
Sum							**100**	**91**	**115**	**117**	**152**	**71**	**646**

Since operating under ETDA for the first six months (1 July to 31 December 2011), ThaiCERT received a total of 646 incident reports which can be categorized into nine incident classes. About 47.8% of the reports are related to fraud concerning phishing at domestic and international financial institutions. This kind of cybercrime directly impacts persons using electronic payment channels. The second most frequently received reports relate to attempts to attack and penetrate systems. In this incident class, 14.6% were intrusion attempts and 14.4% were information gathering incidents. Next were abusive content incidents identified as spam mail reaching 11.9%. The last were malicious code incidents, accounting for 9.8% of the reported attacks.

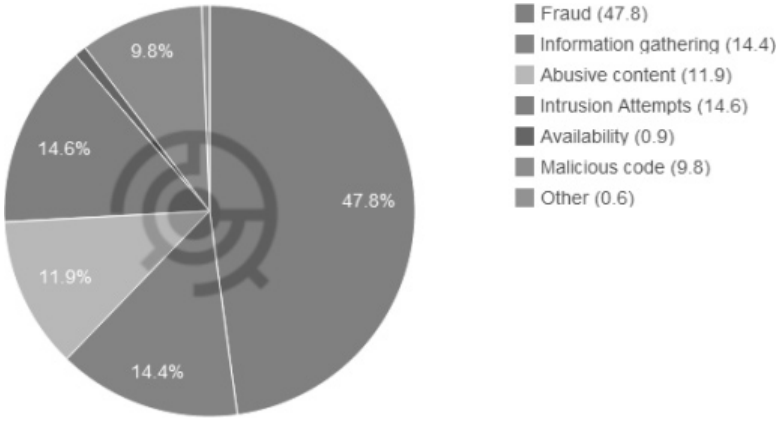

Figure 1: ICT Incidents between 1 July and 31 December 2011 by Incident Class
Statistics of Incidents Reported to ThaiCERT for the last two years 2013 and 2014

[4] Available at <https://www.thaicert.or.th/statistics/statistics-en2011.html>.

Table 2: Statistics 2013

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content	1	2	3	1	1	2	0	0	0	1	2	0	**13**
Availability	1	0	0	0	0	0	0	8	0	1	0	0	**10**
Fraud	36	48	49	56	78	56	110	53	53	54	59	42	**694**
Information gathering	3	0	0	0	0	2	0	0	0	3	0	0	**8**
Information security	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Intrusion Attempts	56	23	17	23	16	11	24	16	24	46	24	36	**316**
Intrusion	6	3	50	61	115	94	67	63	89	46	27	10	**632**
Malicious code	1	4	6	4	3	11	9	7	5	6	5	12	**73**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Sum	**104**	**80**	**125**	**145**	**213**	**176**	**210**	**147**	**171**	**157**	**117**	**100**	**1745**

Table 3: Statistics 2014

Incident Type / Month	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Sum
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	**8**
Availability	0	0	2	2	0	0	1	3	0	0	0	0	**8**
Fraud	59	68	69	72	145	85	94	66	98	88	101	65	**1010**
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	**29**
Information security	0	1	0	0	0	2	0	0	1	0	0	0	**4**
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	74	**503**
Intrusion	9	150	77	33	55	50	69	47	86	32	35	68	**711**
Malicious code	3	7	129	125	102	226	304	161	263	98	132	185	**1735**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Sum	**112**	**257**	**315**	**291**	**352**	**393**	**514**	**319**	**482**	**265**	**316**	**392**	**4008**

Compared to the figures in Table 1, the cybercrime incident reports in 2013 are similar in that the majority is still fraud followed by intrusion and intrusion attempts, respectively. Significantly, in 2014 the number of incident reports related to malicious code outnumbered the figures of the top three incidents reported in 2011 and 2013, and the total number of all attacks reported in 2014 is more than twofold compared to that of 2011 and 2013.

It could be concluded that cybercrime threats in Thailand are still increasing significantly even though both government and the private sector are aware of them and try to mitigate and handle this state of cybercrime. This trend is possibly attributed to the fact that a large number of computers and operating systems together with software downloaded are out of date and lack security. These computers may have been infected with malware a long time ago and were never fixed by the old users.[5] Another possible cause is that, currently, whereas smartphone and tablets have become the most popular applications, their operating systems, both Android's and Apple's applications, do not have security measures equal to the

[5] <http://www.etda.or.th/etda_website/files/system/ThaiCERT_Annual_Report_th_2013.pdf>, page 47.

operating systems on desktop computers. Therefore, these portable devices are being attacked first by cybercriminals.[6] Consequently, according to reported statistics from multiple sources, Thailand was identified as a high-risk country. In the report of the "World Competitiveness Ranking 2013" issued by the International Institute for Management Development (IMD), which assessed cybersecurity of organizations in each member country, the cybersecurity of Thailand is ranked 48th of 60 member states and ranked 4th among the ASEAN countries behind Malaysia, Singapore and Indonesia. Additionally, the Anti-Phishing Working Group (APWG), whose mission is to counteract Phishing, reported that a high proportion of websites under Thai domain names have been hacked as a base for fraud by Phishing among websites registered under other country domain names.[7] With these aforesaid reports, the state of cybercrime in Thailand is critical, and urgent countermeasures and international cooperation are needed in order to cope with the issues. The following sections examine the prosecution of cybercrime and countermeasure against cybercrime in Thailand, respectively.

II. PROSECUTING COMPUTER-RELATED CRIMES IN THAILAND

A. The Public Prosecutor in Relation to the Power of Criminal Investigation and Inquiry

In general, agencies and organizations responsible for criminal investigation and inquiry are administrative or police officials as stipulated in section 17 and 18 of the Criminal Procedure Code B.E.2477 (1934).[8] Administrative or police official means an official vested by law with the power and duty to maintain public order; this shall include a warden, an official of the Excise Department, Customs Department, Harbor Department, an immigration officer and other officials when acting in accordance with arresting or suppressing crime. The inquiry official means an official vested by law with the power and duty to conduct an inquiry.[9] The development of the criminal investigation and inquiry progressed in 2004 when the Department of Special Investigation (DSI) under the Ministry of Justice was created by the Special Case Investigation Act B.E. 2547 (2004) amended by the Special Case Investigation Act (No.2) B.E. 2551 (2008). This new government agency is vested with the power and duty to prevent and control crime that has a devastating impact on the economy, social security and international relations. A special inquiry official is empowered to investigate a special case subject to section 21 of the Special Case Investigation Act B.E. 2547 (2004). Finally, the latest improvement of the criminal investigation and inquiry occurred in 2008 when section 20 of the Criminal Procedure Code was amended as follows:

> "Section 20.- If an offence punishable under Thai law has been committed outside the Kingdom of Thailand, the Attorney-General or the person acting for him shall be a responsible inquiry official or such duty may be assigned to any public prosecutor or inquiry official to exercise the power of inquiry on his behalf.
>
> In the case where the Attorney-General or a person acting for him assigns responsibility of holding an inquiry to any inquiry official, the Attorney-General or a person acting for him may let any public prosecutor participate the holding an inquiry together with the inquiry official.
>
> The public prosecutor assigned to be a responsible inquiry official or to hold an inquiry together with an inquiry official shall have the same power and duty as the inquiry officials do. All other power and duty provided by law shall be the public prosecutor's power and duty.
>
> In case a public prosecutor joins an inquiry official in holding an inquiry, the inquiry official shall conform with the public prosecutor's order and advice on collecting evidence.
>
> In case of necessity, the following inquiry officials shall be empowered to inquire in the period of waiting for the order of the Attorney-General or a person acting for him.
> (1) An inquiry official of the jurisdiction where an alleged offender is arrested.
> (2) An inquiry official requested by the government of other country or an injured person to punish an alleged offender.

---

6 <http://www.etda.or.th/etda_website/files/system/ThaiCERT_Annual_Report_th_2013.pdf>, page 48.
7 Ibid. page 105.
8 Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions>.
9 Criminal Procedure Code B.E.2477 (1934) section 2 (5) (6).

If the public prosecutor or the responsible inquiry official in holding an inquiry, as the case may be, deems that the inquiry is completed, the opinion pursuant to Section 140, Section 141, or Section 142 shall be made and sent, together with a file, to the Attorney-General or a person acting for him."[10]

Computer-related crime investigation and inquiry under the Computer-Related Crime Act, B.E.2550 (2007), differs from the traditional criminal investigation and inquiry due to the nature of complexity of the computer-related offence mostly committed by offenders who are knowledgeable experts in the use of computers or electronic devices. In this regard, an investigator and an inquiry official who conduct the investigation and inquiry pursuant to making an arrest of the offender, as well as collecting evidence, needs to have the knowledge and expertise in computers and electronic devices in order to conduct such duty efficiently. Therefore, the Computer-Related Crime Act, B.E.2550 (2007) Chapter 2[11] has determined competent officials who shall be empowered to conduct computer-related crime investigations and searches for evidence as stipulated by the law. In addition, cybercrime is borderless and keeps on rising due to the fact that the global use of smartphones and development of cloud computing has engaged in cross-border computer networking. Therefore, the investigation and inquiry require international cooperation in criminal matters. Apart from examining the lawfulness of the investigation and inquiry, the public prosecutor also plays a key role in international mutual legal assistance in criminal matters and extradition. The Office of the Attorney-General is the central authority to facilitate requests from other nations and Thai government agencies.

Realizing how prosecuting computer-related crime differs from that of traditional crime, in 2012 the Office of the Attorney-General issued a guideline for public prosecutors in handling computer-related crime inquiry and prosecution. According to the guideline, where the computer-related offence is committed outside the Kingdom of Thailand, the Attorney–General or a person acting for him has to decide and make an order in relation to who will be responsible for holding an inquiry between the public prosecutor or the inquiry official. The decision could be one of these two choices pursuant to Section 20 of the Criminal Procedure Code.[12]

1. The Inquiry Official is Responsible for Holding the Inquiry and a Public Prosecutor is Assigned to Participate in the Inquiry

In this regard, the assigned public prosecutor has the same power and duty as the inquiry officials do and all other powers and duties provided by law shall be the public prosecutor's. Additionally, the inquiry official shall, with respect to the collection of evidence, abide by the orders and instructions of the public prosecutor.

The reason for this amendment of the law is that the investigation and inquiry under Section 20 of the Criminal Procedure Code is required to be investigated and inquired into thoroughly, lawfully and correctly within this stage of inquiry before submitting the case file to a public prosecutor in charge who will follow up with the criminal proceedings according to the Criminal Procedure Code. This is because the public prosecutor is entrusted, by the people, in his/her competence, expertise, impartiality and integrity in the criminal justice system.

2. The Public Prosecutor is Assigned to Be a Responsible Inquiry Official to Hold the Inquiry

In this regard, the public prosecutor has the same power and duty in conjunction with all other powers and duties vested in him/her by law as the inquiry officials do.

On 1 October 2013, the Office of the Attorney-General set up the Department of Investigation under the Office the Attorney-General. One of its missions is, by itself or together with an inquiry official, to conduct the criminal investigation and inquiry pursuant to Section 20 of the Criminal Procedure Code. This is a big change in the Thai Criminal Justice System from the previous one where only the inquiry official was the investigator or inquirer and the public prosecutor did not have any power to interfere during the investigation and inquiry process, just like the Crown Prosecution Service of England used to be.

---

[10] Criminal Procedure Code, *Translated Thai-English update (No.29) 2008 by Dr. Preecha KANEITNOOK*.
[11] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.
[12] Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions> (n.8)

The guideline for the public prosecutor in handling computer-related crime inquiry and prosecution has thoroughly imposed how to conduct the cybercrime investigation and inquiry in both aforesaid options. However, in both cases, the assigned public prosecutor must have a basic knowledge in regard to digital forensics applicable to tracing and identifying criminals together with how to preserve and collect digital evidence in accordance to the threshold set by the International Organization on Computer Evidence (IOCE) which, in this paper, will be shortly demonstrated.

The assigned public prosecutor needs to know methods of detecting and tracking down the person responsible for cybercrimes committed. He/she needs to know how to collect the evidence that will be used to build the case file and to be presented at trial. Furthermore, he/she must know that computer forensics engages in identifying, extracting, documenting and preserving information stored and transmitted in electronic or magnetic form known as digital evidence. Digital evidence can be visible, such as files accessible by using standard file management tools as Windows Explorer, or it can be latent such that it requires special software or techniques to locate and identify it.[13] In addition, he/she must know that only competent officials should undertake investigation, otherwise collection of evidence will contribute to the failure of the prosecution.

Digital evidence is fragile and vulnerable to damage and alteration by improper handling or examination. Collecting, preserving, documenting and examining this sort of evidence should be done with special precautions that ensure the integrity of the electronic evidence at a later stage. The room and computer where a cybercrime is committed is regarded as a crime scene and needs to be sealed off to ensure evidence is not tampered with. This practice is extended to the victim's computer as well. In early stages, the immediate surroundings of the subject devices are very critical. If the computer is on, it should be left on; if it is off, it should be left off. If the collection of evidence is mishandled and does not comply with the law, such as the legal warrant of search and seizure, the data collected can be challenged and may not be admissible evidence in court. Additionally, taking photographs of the crime scene and seizing and securing any papers, disks, flash drives, printouts and other electronic devices in the vicinity of the crime scene are very necessary as well.[14]

As for tracing and identifying criminals, the assigned public prosecutor must be able to analyse criminal acts in order to impose proper cybercrime charges. This is because each computer-related charge has different elements which means that the investigator sometimes needs to use a different approach. However, he/she needs to have basic knowledge of what information or evidence could be found from computer forensics such as Website and webpage, domain name, IP address, server, hosting server, Internet Service Provider, search engine, e-mail and e-mail header, username and password, URL, Whois, Internet browser, log file, chat logs, and social networking. This basic knowledge is necessary for tracing and identifying cybercriminals.

B. Criminal Litigation Process

When an inquiry official deems an inquiry completed, he/she will give an opinion pursuant to Section 140, Section 141 or Section 142[15] and submit it together with the case file to a public prosecutor in charge who will make the judgement as stipulated in Section 140, Section 141 or Section 143. There are many details in this process that the public prosecutor in charge has to take into account prior to making the decision on whether the indictment should be made. In this paper, just some core parts will be examined in regard to cybercrime prosecutions.

1. The Public Prosecutor Will Consider the Lawfulness of the Jurisdiction and the Power of the Investigation and Inquiry

When considering the computer-related crime offence as defined in the Computer-Related Crime Act, the public prosecutor in charge needs to take into account Section 17 of the law, which states:

"Any person committing an offence against this Act outside the Kingdom and;

---

[13] Scene of the Cybercrime: Computer Forensics Handbook By Ed Tittel (ed) 2002 chapter 9 (introduction).
[14] Collecting Digital Evidence of Cyber Crime: Misbah Soboohi, available at <www.academia.edu/1375440/COLLECTING_DIGITAL_EVIDENCE_OF_CYBER_CRIME>.
[15] Available at <http://en.wikisource.org/wiki/Criminal_Procedure_Code_of_Thailand/Provisions> (n.8).

(1) the offender is Thai and the government of the country where the offence has occurred or the injured party is required to be punished or;
(2) the offender is a non-citizen and the Thai government or Thai person who is an injured party or the injured party is required to be punished;
shall be penalized within the Kingdom."

In this case, the Attorney-General or a person acting for him shall be the responsible inquiry official pursuant to Section 20 of the Criminal Procedure Code and a relevant competent officer as defined in Section 18 and 19 of the Computer-Related Crime Act will have the authority to conduct an investigation and search for evidence.[16] If the public prosecutor in charge has found that the investigation of the aforesaid offence violated said provisions, he/she has to return the case file for re-opening the investigation by the competent inquiry official.

2. The Public Prosecutor in Charge Must Know What and Where the Evidence Necessary to Prove the Guilt of the Accused Is Located and How to Acquire It Lawfully and Correctly

The public prosecutor in charge needs to have the knowledge of how the computer system operates and how to use computers and programmes concerned in order to be able to correctly make a judgement whether the accused should be indicted; if so, it raises the question of how to exhibit the evidence at the court hearing. It is very essential that the public prosecutor in charge must understand the facts and elements of each related offence as to how the various steps were taken to commit the crime. Such actions, where the evidence used to prove each element of the crime is stored. The facts and the evidence acquired from the inquiry must be lawful and enough to indict the accused before the lawsuit is filed against him/her.

Although data, computer data and computer traffic data acquired from the inquiry are admissible as evidence, the public prosecutor in charge must examine whether the acquiring of the said evidence complies with Section 25 of the Computer-Related Crime Act, which stipulates:

"Data, computer data or computer traffic data that the competent official acquired under this Act shall be admissible as evidence under the provision of the Criminal Procedure Code or other relevant law related to the investigation, however, it must not be in the way of influencing, promising, deceiving or other wrongful ways."[17]

3. Exhibiting Evidence at a Court Hearing

Presenting evidence in court is the most important of all stages of criminal prosecution. As aforesaid, the cybercrime investigation differs from a traditional crime investigation, as does the exhibiting of evidence used to prove the guilt of the accused at the court hearing.

As a matter of fact, much of the cybercrime evidence is likely to be electronic, such as computer code and network logs; a question is whether the court will be able to understand the technical evidence. In this regard, the public prosecutor in charge needs to take more time to clearly explain the facts and the evidence used to prove the elements of the crime and how to present a timeline demonstrating the defendant's involvement.

Expert testimony will possibly be essential to helping the judge understand the evidence together with how the crime was discovered, how it operated and how it caused damage to the system or the injured person. The potential experts could be network specialists, programming language experts to illustrate how malicious code was created to operate, forensic examiners and others. In addition, visual diagrams of the network and a timeline to focus the hidden events of planning and preparation together with demonstrating the involvement of the defendant is highly recommended.

C. Current Challenges for the Office of the Attorney General

Although the Office of the Attorney General has been playing a vital role in bringing cybercrime criminals to justice, it has not yet set up a particular unit or division to deal directly with this particular

[16] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.
[17] Available at <http://www.it.chula.ac.th/sites/default/files/doc/Computer_Crimes_Act_B_E__2550_Eng.pdf>.

issue. According to the laws regarding jurisdiction, cybercrime cases may be assigned to various departments/divisions subject to whether there are other traditional offences. However, most of the cases are submitted to the Department of Economic Crime Litigation, the Department of Intellectual Property and International Trade Litigation, or the Department of Criminal Litigation. Even though the Office of the Attorney General issued a guideline for the public prosecutor in handling the investigation and prosecution of computer-related crimes in 2012, it is relatively new and little training in this field for the public prosecutors has been organized. These issues could probably affect the performance of the public prosecutor in cybercrime prosecutions.

III. COUNTERMEASURES AGAINST CYBERCRIME

A. In General

In Thailand, ThaiCERT has played a pivotal role in developing systematic measures for securing digital infrastructures and best practices for human intervention by people who are ready to serve as soon as the threat report is received. It has also been developing human resources with expertise by providing training and granting certificates. Furthermore, it is a focal point to coordinate with other nationCERTs in building cooperation with international organizations and agencies.

B. In Cybercrime Prosecution

Because electronic evidence is susceptible to disappearing rapidly and changing easily, immediately obtaining or preserving that evidence is the first step in any cybercrime investigation. These problems are not as significant if the evidence is located within the territory of the injured state, but increasingly, it is located outside its borders. Therefore, quickly preserving and obtaining evidence abroad is more important than ever, and prosecuting cybercrimes increasingly needs cooperation from other countries. It is fortunate that substantial resources such as the G8 Subgroup on High-Tech Crime are available to give help to the member states for handling the investigation taking place overseas.

As for Thailand, currently both government and the private sector are aware of the damage that cybercrime has caused and how to handle this trend of threats. The challenges are that the investment necessary for securing the digital infrastructure is costly, and there are not enough experts in this field. This means that training should be held for developing the human resources to be ready to respond to the threats. Therefore, assistance, support, and cooperation from developing countries are desperately needed.