ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์

นายสถาพร สอนเสนา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
วิชาเอกกฎหมายธุรกิจ สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2554

Legal Problems on the Enforcement of Computer Crime Act BE 2550 (2007) : A Case Study of Computer Crime caused by Malicious Software

Mr. Sataporn Sonsena

A Thesis Submitted in Partial Fulfillment of the Requirements for

the Degree of Master of Laws in Business Law

School of Law

Sukhothai Thammathirat Open University

2011

หัวข้อวิทยานิพนธ์ ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์

ชื่อและนามสกุล นายสถาพร สอนเสนา

วิชาเอก กฎหมายธุรกิจ

สาขาวิชา นิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา 1. รองศาสตราจารย์ ดร. สราวุธ ปิติยาศักดิ์
2. อาจารย์ธนิต ประภาตนันท์

วิทยานิพนธ์นี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 9 ธันวาคม 2554

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร. พินัย ณ นคร)

..... กรรมการ
(รองศาสตราจารย์ ดร. สราวุธ ปิติยาศักดิ์)

..... กรรมการ
(อาจารย์ธนิต ประภาตนันท์)

..... กรรมการ
(อาจารย์เธียรชัย ณ นคร)

..... ประธานกรรมการบัณฑิตศึกษา
(รองศาสตราจารย์ ดร. สุจินต์ วิศวธีรานนท์)

ชื่อวิทยานิพนธ์ ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 : ศึกษากรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์
ผู้วิจัย นายสถาพร สอนเสนา **รหัสนักศึกษา** 2524000607 **ปริญญา** นิติศาสตรมหาบัณฑิต
อาจารย์ที่ปรึกษา (1) รองศาสตราจารย์ ดร. สราวุธ ปิติยาศักดิ์ (2) อาจารย์ธนิต ประภาตนันท์ **ปีการศึกษา** 2554

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อทราบถึงความหมายและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ โดยการศึกษาและวิเคราะห์ถึงคุณสมบัติและความหมาย ตลอดจนความเสียหายที่ได้รับจากชุดคำสั่งไม่พึงประสงค์ตามนัยแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อค้นหามาตรการทางกฎหมายในการป้องกันภัยคุกคามที่เกิดจากชุดคำสั่งดังกล่าว ภายใต้กรอบของกฎหมายที่เกี่ยวข้องอย่างเหมาะสม

งานวิจัยเรื่องนี้เป็นการวิจัยทางกฎหมาย (Legal Research) โดยการวิจัยเชิงคุณภาพ (Quality Research) ด้วยการวิจัยทางเอกสาร (Documentary Research) โดยการศึกษาข้อมูลจากหนังสือ บทความ เอกสารทางวิชาการ วิทยานิพนธ์ กฎหมาย ร่างกฎหมาย และข้อมูลจากเครือข่ายอินเทอร์เน็ต (Internet) ทั้งภาษาไทยและภาษาอังกฤษ

ผลการวิจัยพบว่า รูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์จะต้องผ่านกระบวนการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลก่อนเสมอจึงจะสามารถนำไปสู่การกระทำที่ก่อให้เกิดความเสียหายและส่งผลกระทบอื่นๆ ตามมา กรณีการเข้าถึงโดยม้าโทรจันและสปายแวร์นั้น แม้ว่าม้าโทรจันและสปายแวร์จะเป็นชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายแต่ก็ไม่อยู่ในความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพราะความเสียหายที่เกิดจากม้าโทรจันและสปายแวร์มิได้ปรากฏให้เห็นโดยชัดแจ้ง เจ้าพนักงานในการยุติธรรมโดยเฉพาะพนักงานเจ้าหน้าที่จึงมิอาจตีความโดยการขยายความเพื่อการดำเนินการหรือเพื่อลงโทษผู้ใช้ม้าโทรจันและสปายแวร์ได้ เพราะการใช้กฎหมายอาญาจะต้องมีบทบัญญัติโดยชัดแจ้งและต้องตีความโดยเคร่งครัด และไม่มีบทบัญญัติในส่วนใดของกฎหมายนี้ที่จะให้ตีความเช่นนั้นได้ ทำให้ผู้กระทำผิดไม่ต้องรับโทษ จึงต้องมีการแก้ไขเพิ่มเติมความหมายของชุดคำสั่งไม่พึงประสงค์ให้ครอบคลุมถึงม้าโทรจันและสปายแวร์ นอกจากนี้ ยังจะต้องมีการสร้างระบบบริหารจัดการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ผ่านทางพนักงานเจ้าหน้าที่ในฐานะผู้เชี่ยวชาญด้านคอมพิวเตอร์และผู้บังคับใช้กฎหมายที่ถือเป็นต้นธารแห่งกระบวนการยุติธรรม โดยจะต้องปรับปรุงกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ให้สอดรับกับวิธีปฏิบัติและข้อเท็จจริงที่เกิดขึ้น จึงจะสามารถจัดการกับชุดคำสั่งไม่พึงประสงค์ได้อย่างแท้จริง

คำสำคัญ ชุดคำสั่งไม่พึงประสงค์ มัลแวร์ อาชญากรรมคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์

Thesis title: Legal Problems on the Enforcement of Computer Crime Act BE 2550 (2007) : A Case Study of Computer Crime caused by Malicious Software
Researcher: Mr. Sataporn Sonsena; **ID:** 2524000607**; Degree:** Master of Laws;
Thesis advisors: (1) Dr.Sarawuth Pitiyasak, Associate Professor; (2) Mr. Thanit Prapatanun; **Academic year:** 2011

Abstract

This thesis aims to understand the meaning and types of computer crime caused by malicious software, and to study and analyse the attributes, meaning and damage derived from malicious software under the Computer Crime Act BE 2550 (2007) in order to find an appropriate legal measure to combat against malicious software.

This study is Legal Research using Qualitative Research carried out by using the documentary research, study of textbooks, articles, academic papers, theses, laws, draft laws and other sources from the Internet in both the Thai and English language.

This study concludes that computer crime caused by malicious software must always commence from Electronic or Digital access before it causes damage or other adverse effects. In case of Trojan Horses and Spyware, although Trojan Horses and Spyware may be considered as malicious software causing harm, they are not within the meaning of "undesirable sets of instructions" under the Computer Crime Act BE 2550 (2007), because the damage caused by Trojan Horses and Spyware is not apparent. As a result, a judicial officer, especially a competent officer, is unable to interpret the law to include the implementation of or punishment for the use of Trojan Horses and Spyware. This is due to the fact that criminal law must have clear provisions which must be strictly interpreted. The law cannot, however, be interpreted in such a way that the use of Trojan Horses and Spyware is an offence. As a result, a person who commits computer crime will not be subject to a penalty. It is therefore necessary to amend the law by amending the definition of the term "malicious software" to include Trojan Horses and Spyware. Besides, it is necessary to create a management system concerning malicious software through competent officers who are computer experts, and law enforcers who are considered as an important part of judicial administration, where enforcement is crucial. This process is intended to improve the Computer Crime Act BE 2550 (2007) so that it is consistent with actual practice and facts so that malicious software can be properly dealt with.

Keywords: Malicious software, Malware, Computer Crime, Computer data, Computer system

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้เป็นการศึกษาและวิจัยโดยใช้พื้นฐานของความรู้ร่วมกันในสองศาสตร์ระหว่างนิติศาสตร์กับวิทยาศาสตร์ (ด้านคอมพิวเตอร์) ซึ่งผู้เขียนมีความรู้ด้านคอมพิวเตอร์เป็นทุนเดิม โดยจบการศึกษาด้านคอมพิวเตอร์จากมหาวิทยาลัยสยามในปี พ.ศ. 2537 และมีประสบการณ์การทำงานในอาชีพที่เกี่ยวกับคอมพิวเตอร์และอยู่ในวงการไอทีทั้งในภาครัฐและภาคเอกชนมาเป็นเวลากว่าสิบปีก่อนที่จะจบการศึกษานิติศาสตร์บัณฑิตจาก มสธ. ในปี พ.ศ. 2548 และโอนมารับราชการในตำแหน่งนิติกร ณ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารจนถึงปัจจุบัน รวมทั้งการปฏิบัติหน้าที่พิเศษในฐานะพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อีกหน้าที่หนึ่งด้วย ตลอดเส้นทางการทำงานและการเรียนที่ผ่านมาผู้เขียนได้รับความอนุเคราะห์จากบุคคลในหลายฝ่าย ทั้งผู้บังคับบัญชา คณาจารย์ผู้สอน เพื่อนร่วมงานและเพื่อนร่วมวงการกฎหมายและวงการคอมพิวเตอร์ จนทำให้ผู้เขียนมีประสบการณ์ในการทำงานทั้งทางด้านคอมพิวเตอร์และนิติศาสตร์ และมีกำลังใจในการเขียนวิทยานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงไปได้ด้วยดี และนับได้ว่าเป็นโอกาสอันดียิ่งที่ผู้เขียนได้ใช้ความรู้ความสามารถที่มีอยู่ในทั้งสองด้านดังกล่าวประยุกต์และรวมเข้าด้วยกัน โดยมีบุคคลสำคัญที่ผู้เขียนจะขอกล่าวถึงและขอกราบขอบพระคุณไว้ ดังนี้

รองศาสตราจารย์ ดร. สราวุธ ปิติยาศักดิ์ ที่กรุณารับเป็นอาจารย์ที่ปรึกษาหลักและได้ให้คำชี้แนะตลอดจนแนวความคิดที่ถูกต้องทั้งในศาสตร์ด้านการวิจัยโดยเฉพาะการวิจัยทางนิติศาสตร์ อันเป็นประโยชน์สูงยิ่งต่อการทำงานและการศึกษา และทำให้ผู้เขียนมีความรู้ความเข้าใจในปรัชญาและวิชาการทางนิติศาสตร์เพิ่มขึ้นเป็นอย่างมาก

นายธนิต ประภาตนันท์ ผู้เชี่ยวชาญเฉพาะด้านกฎหมาย ปฏิบัติหน้าที่ผู้อำนวยการสำนักกฎหมาย สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งในฐานะผู้บังคับบัญชาที่ได้ให้โอกาสผู้เขียนในการประกอบอาชีพเป็นนิติกรภาครัฐ รวมถึงในฐานะอาจารย์ที่ปรึกษาร่วมวิทยานิพนธ์ฉบับนี้อีกด้วย

นายสถาพร สอนเสนา

ตุลาคม 2554

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ประเด็นปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (Computer Crimes) มีประเด็นและขอบเขตที่กว้างขวางมากและไม่ได้ถูกจำกัดด้วยพรมแดนของประเทศ จึงอาจเรียกได้ว่าเป็นอาชญากรรมระหว่างชาติ (Trans-national Crimes) หากศึกษาและวิเคราะห์จากพัฒนาการของอาชญากรรมคอมพิวเตอร์นับตั้งแต่อดีตเรื่อยมาจนถึงปัจจุบันหรือในอนาคตที่จะเกิดขึ้นแล้วก็จะพบรูปแบบของอาชญากรรมคอมพิวเตอร์เกิดขึ้นใหม่อยู่เสมอจนแทบไม่มีที่สิ้นสุด ตราบใดที่มนุษย์ยังมีการค้นคว้าและพัฒนานวัตกรรมด้านคอมพิวเตอร์นี้ต่อไปเรื่อยๆ ปัจจุบันคำว่า “อาชญากรรมคอมพิวเตอร์ หรือ อาชญากรรมไซเบอร์ (Cyber Crimes)” เป็นที่รู้จักและแพร่หลายในหมู่ประชาชนคนไทยไม่ใช่แต่เฉพาะบุคคลที่อยู่ในวงการไอทีเท่านั้นที่มีความตื่นตัวแต่บุคคลที่อยู่ในฐานะผู้ใช้งานทั่วไปก็เริ่มรู้จักและมีความตื่นตัวและให้ความสำคัญกับอาชญากรรมคอมพิวเตอร์มากขึ้น หากจะกล่าวถึงความหมายของคำดังกล่าวก็ยังไม่มีการให้ความหมายหรือคำจำกัดความไว้อย่างชัดเจน เช่น ดร.ครรชิต มาลัยวงศ์ ได้ให้ความหมายไว้ว่า[1] “หมายถึงการใช้คอมพิวเตอร์ทำผิดกฎหมาย เช่น เขียนโปรแกรมไปหักเงินจากลูกค้าธนาคารที่ใช้เครื่องเอทีเอ็มแล้วโอนเงินนั้นมาเข้าบัญชีของตน การแอบแก้ไขเปลี่ยนแปลงข้อมูลของผู้อื่นไม่ว่าจะเพื่อประโยชน์ของตนเอง หรือเพื่อความสนุก อย่างไรก็ตามไม่นับรวมอาชญากรรมที่กระทำต่อคอมพิวเตอร์ เช่น การโจรกรรมเครื่องคอมพิวเตอร์ไปขาย หรือการก๊อปปี้โปรแกรมของผู้อื่นโดยไม่ได้รับอนุญาต” ส่วน พ.ต.อ.ญาณพล ยั่งยืน ก็เป็นอีกท่านหนึ่งที่ได้ให้ความหมายของอาชญากรรมคอมพิวเตอร์ไว้ว่า[2] หมายถึง “(1) การ

---

[1] ดร.ครรชิต มาลัยวงศ์ (2538) “พจนานุกรมคอมพิวเตอร์สำหรับเยาวชน” กองบริการสื่อสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อม กรุงเทพมหานคร หน้า 41

[2] เอกสารประกอบการสัมมนา ณ มหาวิทยาลัยรังสิต กรุงเทพฯ (วันอังคารที่ 22 กันยายน พ.ศ. 2552), เรื่อง “จับฉันให้ได้ ถ้านายแน่จริง : แนวทางสืบค้น แกะรอยอาชญากรรมทางคอมพิวเตอร์” คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต หน้า 2 และ 3

กระทำใดๆ ก็ตามที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และทำให้ผู้กระทำความผิดได้รับผลตอบแทน และ (2) การกระทำผิดกฎหมายใดๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์มาประกอบการกระทำความผิด และต้องมีผู้มีความรู้ทางคอมพิวเตอร์ในการสืบสวน ติดตาม รวบรวมหลักฐานเพื่อที่จะดำเนินคดี" หรือในฝั่งของต่างประเทศก็มี Mr.Kenneth S. Rosendlatt อัยการผู้เชี่ยวชาญคดีอาชญากรรมทางคอมพิวเตอร์ ซึ่งเป็นผู้เขียนหนังสือเรื่อง High Technology Crime ได้อธิบายความหมายของ อาชญากรรมทางคอมพิวเตอร์ไว้ว่า[3] "เป็นอาชญากรรมที่เกิดขึ้นใหม่อันเป็นผลสืบเนื่องมาจากการใช้คอมพิวเตอร์อย่างแพร่หลาย เช่น การล่วงล้ำ[4]เข้าไปในระบบเครือข่ายคอมพิวเตอร์ของบริษัทธุรกิจที่เชื่อมโยงผ่านเครือข่ายโทรคมนาคม นอกจากนี้ยังหมายถึงอาชญากรรมแบบเดิมที่แปรสภาพไป เนื่องจากความก้าวหน้าทางเทคโนโลยีคอมพิวเตอร์ ซึ่งในการสืบสวนคดีประเภทนี้ต้องมีความรู้เกี่ยวกับคอมพิวเตอร์ และคุ้นเคยกับอุตสาหกรรมเทคโนโลยีชั้นสูง" เป็นต้น

อย่างไรก็ตาม เกี่ยวกับความหมายของอาชญากรรมคอมพิวเตอร์นี้ย่อมเป็นที่เข้าใจไปในทำนองเดียวกันว่า "อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำผิดกฎหมายที่ใช้ความรู้ด้านคอมพิวเตอร์ (Knowledge of Computers) เป็นปัจจัยหลักสำคัญในการก่ออาชญากรรม"[5] ตัวอย่าง เช่น หากนาย ก. โดยทุจริตได้ส่งข้อความทางไปรษณีย์หลอกลวงนาง ข. ให้ส่งเงินเข้ามาลงทุนในกิจการที่ไม่มีตัวตน หากนาง ข. หลงเชื่อแล้วส่งเงินมาให้ นาย ก. การกระทำของ นาย ก. เป็นความผิดฐานฉ้อโกงในลักษณะอาชญากรรมพื้นฐาน (Conventional Crimes) แต่หากปรากฏ

---

3 พ.ต.อ. ดร.ธรรมศักดิ์ วิชชารยะ. "อาชญากรรมร่วมสมัย แนวคิดในการป้องกันและควบคุมปัญหาอาชญากรรมทางคอมพิวเตอร์". เอกสารประกอบการสัมมนา เรื่อง "แฮคเกอร์: มหันตภัยยุคไอที"

4 นักวิชาการบางท่านใช้คำว่า "บุกรุก (intrusion)"

5 นิยามของอาชญากรรมคอมพิวเตอร์ดังกล่าวนี้ เป็นนิยามของ Donn Parker ที่ได้ให้ไว้ในหนังสือ Fightion Computer Crime (1983) ความว่า "Computer crime is a criminal offense of which the knowledge of computers is necessary for the successful commission of the offense." ซึ่งอ้างจากบทความทางวิชาการ เรื่อง "อาชญากรรมคอมพิวเตอร์ : กระบวนการยุติธรรมไทยพร้อมหรือยัง ?" ของพันตำรวจเอก ดร. มาโนช ตันตระเธียร ซึ่งได้ถูกนำออกเผยแพร่ครั้งแรกเป็นเอกสารประกอบการสัมมนาทางวิชาการเรื่อง "กฎหมายพาณิชย์อิเล็กทรอนิกส์ (E-Commerce Laws): นวัตกรรมทางกฎหมายที่จำเป็นและเร่งด่วนแห่งสังคมไทย" จัดโดยกองทุนศาสตราจารย์สัญญา ธรรมศักดิ์, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สภาทนายความ, ชมรมนักข่าวสายเทคโนโลยีสารสนเทศ เมื่อวันที่ 6-7 พฤษภาคม 2542 ณ หอประชุมมหิศร อาคารไทยพาณิชย์ ปาร์ค พลาซ่า กรุงเทพมหานคร. และ ถูกนำออกตีพิมพ์ในวารสารทางวิชาการอีกหลายเล่ม

ข้อเท็จจริงฟังได้ความว่า นาย ก. ได้ส่งข้อความหลอกลวงนั้นไปให้ นาง ข. ทางไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) โดยผ่านเครือข่ายอินเทอร์เน็ต และนาง ข. ได้โอนเงินทางอิเล็กทรอนิกส์เข้าบัญชีของ นาย ก. ดังนี้ การกระทำของ นาย ก. แม้ยังคงเข้าองค์ประกอบเป็นความผิดฐานฉ้อโกง แต่รายละเอียดวิธีการกระทำผิดเข้าลักษณะเป็นอาชญากรรมคอมพิวเตอร์ (Computer Crime) ตามนิยามความหมายนี้[6]

ตามนิยามความหมายของอาชญากรรมคอมพิวเตอร์ข้างต้นจะเห็นได้ว่า อาชญากรรมอื่นที่แม้จะมีการใช้หรือเกี่ยวข้องกับคอมพิวเตอร์ แต่การกระทำผิดสำเร็จมิใช่เป็นผลโดยตรงมาจากการใช้ความรู้ด้านคอมพิวเตอร์ เช่น การหมิ่นประมาทผู้อื่นโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด การลักทรัพย์อุปกรณ์เครื่องคอมพิวเตอร์ หรือ การค้ายาเสพติดโดยเก็บบันทึกข้อมูลบัญชีลูกค้าไว้ในเครื่องคอมพิวเตอร์ส่วนตัว เป็นต้น แม้ว่าการกระทำประเภทต่างๆ ที่กล่าวมานี้จะเข้าข่ายเป็นการกระทำผิดตามกฎหมายแต่ก็ไม่ถือว่าเป็นอาชญากรรมคอมพิวเตอร์ตามนิยามความหมายนี้

ด้วยรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นได้ในทุกๆ นาที[7] และความเสียหายที่เกิดขึ้นจากอาชญากรรมทางคอมพิวเตอร์นั้น นอกจากจะเป็นการละเมิดต่อกฎหมายแล้วในบางกรณีก็ยังทำลายศีลธรรมอันดีของบ้านเมือง เช่น การเผยแพร่ภาพลามก การค้าประเวณีทางอินเทอร์เน็ต หรือที่ตรวจพบล่าสุดเป็นการเปิดเว็บไซต์เพื่อเป็นศูนย์กลางและเป็นแหล่งนัดพบสำหรับการสวิงกิ้ง เป็นต้น นอกจากนี้ ยังอาจจะสร้างความสูญเสียให้แก่ประเทศชาติได้อย่างใหญ่หลวง และมีผลให้เกิดความเสียหายรุนแรงทั้งในด้านเศรษฐกิจ ตลอดจนกระทบกระเทือนต่อความสงบสุขของสังคม

---

6 ตามความเห็นของผู้เขียนเห็นว่า เป็นการกระทำความผิดตามมาตรา 14 (1) แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน เนื่องจากมีการกระทำครบองค์ประกอบของความผิดฐานนี้แล้ว กล่าวคือ อีเมล์ของนาย ก. เป็นไปในเชิงฉ้อฉล หลอกลวง นาง ข. จึงเป็นการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ นาง ข.

7 บทความทั่วไปของกองบรรณาธิการในวารสาร สาร NECTEC ฉบับเดือนมกราคม – กุมภาพันธ์ 2548 หน้า 34 ได้แสดงตัวอย่างของการตรวจพบมัลแวร์โดยเทรนด์ไมโครซึ่งเป็นหนึ่งในผู้นำอุตสาหกรรมด้านการผลิตซอฟท์แวร์แอนตี้และกำจัดไวรัสที่ตรวจสอบพบว่า ช่วงวันที่ 21 มกราคม ถึง 20 กุมภาพันธ์ 2548 เทรนด์ไมโครบันทึกมัลแวร์สายพันธุ์ใหม่ได้ทั้งสิ้น 3,185 ตัวหรือมากกว่าเดือนที่แล้วซึ่งมีทั้งสิ้น 2,236 ตัวเกือบ 50% โดยมัลแวร์สายพันธุ์ใหม่ที่พบในเดือนนี้ทั้งหมดกว่า 50% (1,711 ตัว) ซึ่งได้มาจากการรายงานของลูกค้าและการเข้าไปจัดการแก้ปัญหาในแต่ละกรณีแบบ ณ เวลาจริง ตัวเลขมัลแวร์ที่ตรวจจับได้ดังกล่าวเพิ่มขึ้นอย่างสม่ำเสมอนับตั้งแต่เดือนธันวาคม 2547 เป็นต้นมา

และความมั่นคงของประเทศด้วย เช่น บนอินเทอร์เน็ตมีข้อมูลเกี่ยวกับการก่อการร้าย หรือ วิธีการทำระเบิดแสวงเครื่อง การหมิ่นสถาบันเบื้องสูง เป็นต้น ดังนั้น ความเสียหายจากอาชญากรรมคอมพิวเตอร์ในปัจจุบันจึงไม่ได้มีผลกระทบเพียงแต่ความมั่นคงของบุคคลใดบุคคลหนึ่งเท่านั้นแต่ยังมีผลกระทบไปถึงความมั่นคงของประเทศชาติเป็นส่วนรวม รวมทั้งความมั่นคงภายในและภายนอกประเทศด้วย โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวกับข่าวกรองหรือข้อมูลต่างๆ อันเกี่ยวกับด้านความมั่งคง[8]

สำหรับประเทศไทยมีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นมา[9] ทั้งนี้ เมื่อพิจารณาถึงหลักการและเหตุผล[10]ในการประกาศใช้และฐานความผิดของกฎหมายดังกล่าวซึ่งเป็นกฎหมายที่ตราขึ้นเป็นการเฉพาะเพื่อช่วยกำหนดกรอบและกฎเกณฑ์ในการใช้ชีวิตในสังคมยุคเทคโนโลยีสารสนเทศและช่วยจัดการกับปัญหาที่เป็นผลสืบเนื่องมาจากการพัฒนาของเทคโนโลยีและการนำไปใช้อย่างผิดวิธี และที่สำคัญที่สุดคือ เพื่อเป็นการรับมือกับอาชญากรรมคอมพิวเตอร์โดยตรงก็จะพบสาระสำคัญและถือว่าเป็นเจตนารมณ์หลักของพระราชบัญญัตินี้คือ เพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่รวมทั้งหน้าที่ของผู้ให้บริการไว้ด้วย นอกจากนี้ยังเป็นการบัญญัติกฎหมายเพื่อการรองรับปัญหาที่จะเกิดจากการพัฒนาของเทคโนโลยีสารสนเทศในอนาคตอีกด้วย

หากพิจารณาลึกลงไปในฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วจะพบว่า ได้บัญญัติฐานความผิดให้ครอบคลุมถึงการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ในลักษณะต่างๆ ที่จะส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของ

---

8 ทวีศักดิ์ กออนันตกูล, “อาชญากรรมในยุคโลกาภิวัฒน์,” บทบัณฑิตย์ เล่มที่ 55 (มีนาคม 2542)

9 ราชกิจจานุเบกษาหน้า 4 เล่ม 124 ตอนที่ 27 ก ลงวันที่ 18 มิถุนายน 2550

10 เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชน เช่น การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ การดักรับข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่กระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ การเผยแพร่ชุดคำสั่งไม่พึงประสงค์ที่ใช้ในการกระทำความผิด การเผยแพร่เนื้อหาอันไม่เหมาะสมหรือเป็นเท็จ รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลายและความผิดเกี่ยวกับสแปมเมล์ (spam mail) เป็นต้น

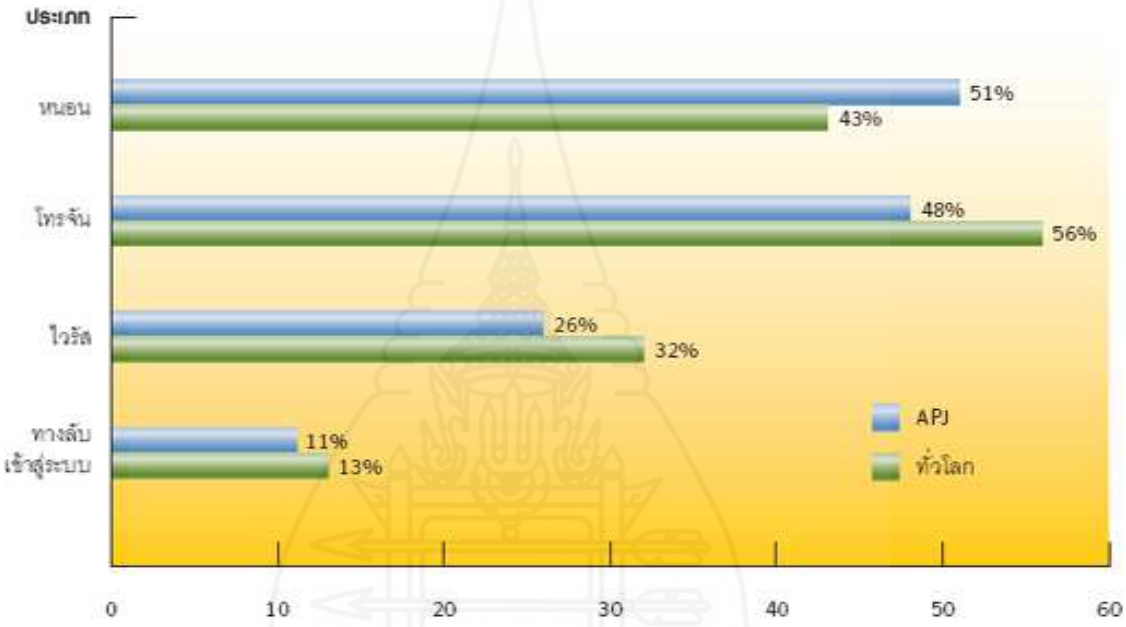
อย่างไรก็ตาม เพื่อให้ประเด็นการศึกษามีความชัดเจนเพียงพอ วิทยานิพนธ์ฉบับนี้จึงมุ่งเน้นศึกษาแต่เฉพาะกรณีของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ (Computer crimes caused by malicious software) เท่านั้น เนื่องจากปัจจุบันพบว่ามีการจัดทำและเผยแพร่โปรแกรมคอมพิวเตอร์ (Computer Program) หรือชุดคำสั่งไม่พึงประสงค์ (Malicious Software) ผ่านทางเครือข่ายคอมพิวเตอร์ (Computer Network) โดยเฉพาะอย่างยิ่งเครือข่ายอินเทอร์เน็ต[11] กันอย่างแพร่หลาย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus)

---

11 วิกิพีเดีย สารานุกรมเสรี.http://th.wikipedia.org/wiki/อินเทอร์เน็ต (อังกฤษ: Internet) หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่มีการเชื่อมต่อระหว่างเครือข่ายหลายๆ เครือข่ายทั่วโลก โดยใช้ภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โปรโตคอล (Protocol) ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ในหลายๆ ทาง อาทิ เช่น อีเมล์ เว็บบอร์ด และสามารถสืบค้นข้อมูลและข่าวสารต่างๆ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้ แก้ไขล่าสุดเมื่อวันที่ 22 กันยายน 2553 เวลา 03:02 น. Retrieved December, 11, 2010

นอกจากนี้ยังมีความหมายตาม http://thaicert.nectec.or.th/paper/basic/paniwat2.0_r1.pdf หมายถึง เครือข่ายคอมพิวเตอร์ที่ใหญ่ที่สุดในโลก ซึ่งเป็นการเชื่อมต่อคอมพิวเตอร์จากทั่วโลกเข้ามาไว้ในเครือข่ายเดียวกัน (global network) เพื่อใช้ในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกันในทุกมุมโลก โดยมีบริการต่างๆ เช่น การสืบค้นข้อมูลบนเครือข่าย การส่งจดหมายอิเล็กทรอนิกส์ การติดต่อสื่อสารกันในรูปแบบของทั้งภาพ ทั้งเสียง เป็นต้น อินเทอร์เน็ต เป็นเครือข่ายที่โยงใยไปทั่วโลกเชื่อมต่อเครื่องคอมพิวเตอร์นับล้านเครื่องจากประเทศต่างๆ กว่า 100 ประเทศเข้าด้วยกันเพื่อแลกเปลี่ยนข้อมูล ข่าวสาร และความเห็น อินเทอร์เน็ตนั้นแตกต่างจากบริการเครือข่ายอื่นๆ ที่มีการควบคุมจากศูนย์กลาง อินเทอร์เน็ตนั้นได้รับการออกแบบให้มีลักษณะกระจาย เครื่องคอมพิวเตอร์ในอินเทอร์เน็ตแต่ละเครื่องนั้นเรียกว่าโฮส (host) จะเป็นอิสระต่อกัน ผู้รับผิดชอบโฮสนั้นจะตัดสินใจว่าจะเปิดบริการใดให้กับเครื่องอื่นในอินเทอร์เน็ตและจะออกไปใช้บริการใดที่มีอยู่ในอินเทอร์เน็ต โดยที่การเข้าถึงหรือเชื่อมต่อกับอินเทอร์เน็ตนั้นสามารถทำได้หลายวิธี เช่น ผ่านผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider – ISP)

หนอนคอมพิวเตอร์ (Worm) ม้าโทรจัน (Trojan Horses) เป็นต้น อันเป็นเหตุให้มีการใช้โปรแกรมหรือชุดคำสั่งดังกล่าวเพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ ความครบถ้วน และเสถียรภาพในการใช้งานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชนเป็นอย่างมาก ดังรายละเอียดปรากฏตามแผนภาพ (graph) แสดงการโจมตีจากชุดคำสั่งไม่พึงประสงค์ทั้งหมดในภูมิภาคเอเชียแปซิฟิกและญี่ปุ่นเทียบกับทั่วโลกที่สำรวจโดย Symantec Corporation ในปี 2009 ตามภาพที่ 1



ภาพที่ 1.1 แผนภาพแสดงการโจมตีจากชุดคำสั่งไม่พึงประสงค์ทั้งหมดในภูมิภาคเชียแปซิฟิกและญี่ปุ่นในปี 2009

ที่มา : ไซแมนเทค (Symantec) (2553 : 11) รายงานสถานการณ์ภัยคุมคามบนอินเทอร์เน็ตของไซแมนเทค เดือนเมษายน 2010 (เอกสารข้อมูลสำหรับภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น)

ดังนั้น จึงมีความจำเป็นที่จะต้องศึกษาค้นคว้าเกี่ยวกับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เพื่อให้ทราบถึงคุณสมบัติและภัยที่ตามมากับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์และเพื่อค้นหาวิธีการรับมือกับปัญหาดังกล่าว ทั้งนี้ โดยการศึกษาและวิเคราะห์ถึงรูปแบบของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากการใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดและทำให้เกิดปัญหาทางกฎหมายขึ้น เพื่อค้นหามาตรการและแนวทางในการป้องกันและปราบปรามการกระทำความผิดดังกล่าวให้มีประสิทธิภาพและได้ผลในทางปฏิบัติมากยิ่งขึ้น ทั้งนี้ ประเด็นปัญหาเกี่ยวกับโปรแกรมหรือชุดคำสั่ง

ไม่พึงประสงค์นับเป็นเรื่องใหญ่และมีความสำคัญมากจนถึงขั้นได้ถูกบัญญัติไว้ในมาตรา 21[12] แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

อนึ่ง หากจะกล่าวถึงคำว่า “ชุดคำสั่งไม่พึงประสงค์” กับบุคคลทั่วไปที่มิใช่นักคอมพิวเตอร์หรือมิใช่บุคคลที่อยู่ในวงการไอทีแล้วก็อาจทำให้บางคนไม่เข้าใจว่า “ชุดคำสั่งไม่พึงประสงค์” หมายถึงอะไร แต่หากจะเพิ่มเติมคำว่า “คอมพิวเตอร์” แทรกระหว่างคำว่า “ชุดคำสั่ง” และคำว่า “ไม่พึงประสงค์” ก็จะได้คำที่สมบูรณ์ว่า “ชุดคำสั่งคอมพิวเตอร์ไม่พึงประสงค์” อันจะทำให้บุคคลทั่วไปที่มิใช่นักคอมพิวเตอร์หรือมิใช่บุคคลที่อยู่ในวงการไอทีจะพึงเข้าใจความหมายของคำดังกล่าวได้ดียิ่งขึ้น อย่างไรก็ตาม เมื่อคำว่า “ชุดคำสั่งไม่พึงประสงค์” ได้ถูกบัญญัติไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว ปัญหาการสื่อความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ก็คงไม่เป็นปัญหาหรืออุปสรรคแต่อย่างใดหากได้มีการกล่าวถึงคำดังกล่าวภายใต้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้บัญญัติให้มีมาตรการในการดำเนินการเกี่ยวกับโปรแกรมหรือชุดคำสั่งคอมพิวเตอร์ไม่พึงประสงค์ไว้ในมาตรา 21 แล้วก็ตาม แต่บทบัญญัติในมาตราดังกล่าวยังมีข้อบกพร่องและความไม่ชัดเจนในทางปฏิบัติที่จะสามารถเอื้ออำนวยและใช้เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ให้มีประสิทธิภาพและประสิทธิผลได้อย่างเต็มที่อยู่หลายประการ ดังนี้

ประการที่หนึ่ง มาตรา 21 วรรคหนึ่ง ที่บัญญัติว่า “ในกรณีที่พนักงานเจ้าหน้าที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไข

---

[12] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 21 ความว่า

“มาตรา 21 ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา”

ข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้" นั้น ในทางปฏิบัติพบว่าโอกาสที่พนักงานเจ้าหน้าที่จะตรวจพบชุดคำสั่งไม่พึงประสงค์ที่แอบแฝงหรือปะปนอยู่กับข้อมูลคอมพิวเตอร์อื่น (ดวงกมล ทรัพย์พิทยากร ได้เรียกโปรแกรมเหล่านั้นว่า "โปรแกรมปรสิต")[13] ได้โดยตัวเองนั้น เป็นไปได้ยากมาก เพราะหากพนักงานเจ้าหน้าที่เข้าไปตรวจโดยไม่ได้รับอนุญาตหรือยังมิได้เกิดอำนาจในการสืบสวนสอบสวนคดีก่อนแล้ว ก็จะกลายเป็นว่าพนักงานเจ้าหน้าที่จะเป็นผู้กระทำผิดกฎหมายเสียเองโดยการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ ซึ่งหากพนักงานเจ้าหน้าที่แจ้งเจ้าของข้อมูลคอมพิวเตอร์ก่อนเข้าไปตรวจ เจ้าของข้อมูลคอมพิวเตอร์ก็คงจะโยกย้าย ทำลาย หรือสับเปลี่ยนที่อยู่ของข้อมูลคอมพิวเตอร์ หรือหาหนทางหลีกเลี่ยงการตรวจก่อนที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจ และในความเป็นจริงพบว่าชุดคำสั่งไม่พึงประสงค์ยังถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลอื่นอีกมาก เช่น แฟลชไดรว์ (Flash Drive)[14], แผ่นซีดี (Compact Disc : CD), แผ่นดิจิทัล

---

13 ดวงกมล ทรัพย์พิทยากร, สปายแวร์ ปรสิตแวร์ แอดแวร์ เครือข่ายแฝง และวิธีการป้องกัน, เอกสารออนไลน์ เผยแพร่เมื่อ 4 ตุลาคม 2544 กรุงเทพฯ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย, 2544 Retrieved March, 11, 2010

14 Flash Drive มีชื่อเต็มว่า USB Mass Storage Device ส่วนใหญ่เรียกกันว่า USB Flash Memory Drive , USB Flash Drive Memory หรือ USB Flash Drive เพื่อใช้งานเชื่อมต่อกับ Computer ผ่านทาง Port USB (ย่อมาจาก Universal Serial BUS ซึ่งถูกพัฒนาโดย COMPAQ, Digital Equipment (รวมกิจการกับ COMPAQ), IBM, Intel, Microsoft, NEC และ Northern Telecom เพื่อขยายขีดความสามารถในการทำงานของพอร์ตอนุกรมเป็นอินเตอร์เฟสที่เชื่อมต่อระหว่างอุปกรณ์ I/O กับคอมพิวเตอร์) ใช้ Flash Memory เก็บข้อมูล ทำงานเป็น Drive เหมือน Hard Disk อ่านและบันทึกข้อมูลได้อย่างเดียวไม่สามารถทำอย่างอื่นได้ ซึ่งเป็นยุคต่อมาจาก Thumb drive (เป็นชื่อทางการค้า คุณสมบัติเหมือน CD-R, Floppy Disk, Hard Disk เป็นหน่วยความจำ ที่เสริมเข้าไปในคอมพิวเตอร์ทาง Port USB และถือเป็นการเก็บข้อมูลรูปแบบใหม่ คือไม่ต้องมีตัว Drive ตัว Disk พกพาได้สะดวก มีขนาดเล็กเท่ากับหัวแม่มือ เป็นยุคแรกๆ ของอุปกรณ์จำพวก Flash Drive ความเร็วในการอ่าน เขียน ประมาณ 500KB/Sec มีความจุอยู่ระหว่าง 8 MB - 1024MB ในปัจจุบันอาจมีมากขึ้น สำหรับราคาในยุคแรกๆ ราคาสูง ขนาดความจุน้อย) ราคาถูกลง ความจุมีมากขึ้น ขนาดของตัว Flash Drive เล็กลงด้วย บางยี่ห้อมีขนาดประมาณ 1 นิ้ว ซึ่งต่างจาก Handy drive ที่เป็นชื่อทางการค้ามีคุณสมบัติและการทำงานเหมือน Flash drive แต่ที่เพิ่มขึ้นมาคือสามารถเล่นไฟล์ Mp3 ไฟล์วีดีโอ ไฟล์รูปภาพ ฟังวิทยุผ่านช่องเสียบหูฟัง และฟังก์ชั่นอื่นๆ ที่ผู้ผลิตจะใส่ลงไป ใช้แบตเตอรี่มีทั้งแบบใช้ถ่าน AA , AAA หรือถ่านชาร์ตซึ่งจะชาร์ตถ่านผ่านทาง Port USB รูปลักษณ์สวยงาม แต่มีขนาดใหญ่กว่า Flash drive เนื่องจากต้องใช้แบตเตอรี่ สำหรับราคาแพงกว่า Flash drive เหมาะกับผู้ที่ต้องการใช้งานที่หลากหลาย. แหล่งที่มา http://www.webthaidd.com/flashdrive/webthaidd_article_451_1.html Retrieved February, 18, 2011

อเนกประสงค์ (Digital Versatile Disc : DVD), External Hard Disk[15] เป็นต้น แต่กฎหมายมิได้มีฐานอำนาจรองรับเพื่อให้พนักงานเจ้าหน้าที่เข้าไปตรวจเพื่อหาชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลเหล่านั้นได้ หรือหากมีกรณีการร้องเรียนหรือแจ้งเบาะแสเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์เข้ามายังพนักงานเจ้าหน้าที่ เพื่อร้องขอให้พนักงานเจ้าหน้าที่ดำเนินการกำจัดหรือปราบปรามโดยการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ หรือกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์นั้น พนักงานเจ้าหน้าที่ก็ยังไม่มีอำนาจดำเนินการตามที่มีการร้องเรียนหรือแจ้งเบาะแสดังกล่าวได้ เพราะชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์ มิได้อยู่ในความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ตามนัยแห่งมาตรา 21 วรรคสอง ของกฎหมายนี้[16]

ประการที่สอง ความหมายของ “ชุดคำสั่งไม่พึงประสงค์” ตามมาตรา 21 วรรคสอง ที่ว่า “ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา” นั้น ยังไม่ครอบคลุมถึงลักษณะของการกระทำความผิดที่เกิดขึ้นจริงซึ่งกำลังเป็นที่นิยมกระทำกันอย่างแพร่หลายในบรรดาหมู่อาชญากรจนก่อให้เกิดปัญหาและส่งผลเสียหายต่อประชาชนและประเทศชาติอย่างมากในปัจจุบันนี้ กล่าวคือ มีการก่ออาชญากรรมคอมพิวเตอร์โดยใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดโดยการจัดทำและเผยแพร่โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ผ่านทางเครือข่ายคอมพิวเตอร์กันอย่างแพร่หลายเพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ

---

15 ราชบัณฑิตยสถาน ศัพท์เทคโนโลยีสารสนเทศฉบับราชบัณฑิตยสถาน 2542 กรุงเทพฯ อรุณการพิมพ์ หน้า 141 หมายถึง จานบันทึกแบบแข็งที่มิได้ติดตั้งไว้กับคอมพิวเตอร์แบบถาวร

16 เมื่อพิเคราะห์ถึงเจตนารมณ์ในการกำหนดมาตรการเกี่ยวกับการป้องกันและปราบปรามชุดคำสั่งไม่พึงประสงค์ตามที่บัญญัติไว้ในมาตรา 21 วรรคสอง จะเห็นได้ว่า เป็นการบัญญัติกฎหมายเพื่อรองรับพัฒนาการของเทคโนโลยีในอนาคต กล่าวคือ หากเกิดกรณีมีโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่มีคุณสมบัติหรือคุณลักษณะแตกต่างไปจากคุณสมบัติตามมาตรา 21 วรรคสองดังกล่าวแล้ว ก็สามารถเพิ่มเติมความหมาย คุณสมบัติหรือคุณลักษณะของชุดคำสั่งไม่พึงประสงค์นั้นได้โดยการตราเป็นกฎกระทรวงตามที่มาตรา 21 วรรคสอง ได้ให้อำนาจไว้

ความครบถ้วน และเสถียรภาพในการใช้งานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชนเป็นอย่างมาก โดยเฉพาะอย่างยิ่งการนำข้อมูลเอกลักษณ์บุคคล (Identity) ที่ได้นั้นไปก่ออาชญากรรมด้านการเงินหรือด้านอื่นต่อไป โดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นที่อยู่ในระบบคอมพิวเตอร์ของเจ้าของข้อมูลนั้นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้เมื่อมีการใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจัน (Trojan Horses) หรือ สปายแวร์(Spyware) เป็นเครื่องมือในการกระทำความผิดแต่อย่างใด การกระทำความผิดดังกล่าวจึงไม่เข้าข่ายเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และไม่เป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา เพราะขาดซึ่งองค์ประกอบของความผิดสำคัญที่ว่าข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ตามนิยามและความหมายในประมวลกฎหมายแพ่งและพาณิชย์[17] และไม่เป็นความผิดตามพระราชบัญญัติอื่นที่มีโทษทางอาญาเลย[18]

ประการที่สาม นับตั้งแต่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้เรื่อยมาจนถึงปัจจุบันนั้น ยังมิได้มีการแยกแยะหรือประกาศรับรองชุดคำสั่งไม่พึงประสงค์ที่ถือเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่นตามความหมายในมาตรา 21 วรรคสอง แต่อย่างใด จึงส่งผลทำให้ชุดคำสั่งใดก็ตามที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ถูกสันนิษฐานโดยผลของกฎหมายดังกล่าวว่าเป็นชุดคำสั่งไม่พึงประสงค์ จึงเท่ากับว่าปัจจุบันยังไม่มีชุดคำสั่งไม่พึงประสงค์ใดที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันและแก้ไขชุดคำสั่งอื่นเลย ทั้งที่ในความ

---

17 คำพิพากษาศาลฎีกาที่ 5161/2547 ตัดสินว่าข้อมูลตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริง หรือ สิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อ ป.พ.พ. มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์

18 เป็นความเห็นของผู้เขียนเอง เนื่องจากยังไม่ปรากฏว่าในประเทศไทยมีกฎหมายเกี่ยวกับเทคโนโลยีอื่นใดอีกนอกจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

เป็นจริงแล้วยังมีชุดคำสั่งอีกหลายประเภทที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์อื่น เช่น โปรแกรมแอนตี้และตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ หรือม้าโทรจัน โปรแกรมแอนตี้การส่งสแปมเมล์ เป็นต้น จึงทำให้พนักงานเจ้าหน้าที่ยังไม่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นในกรณีที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยได้ กล่าวคือ ตราบใดที่ยังมิได้มีประกาศดังกล่าวของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร พนักงานเจ้าหน้าที่ก็ไม่อาจทราบได้ว่าชุดคำสั่งไม่พึงประสงค์ใดเป็นชุดคำสั่งที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่น จึงทำให้การบังคับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในมาตรา 21 ที่มีเจตนารมณ์ในการป้องกันและปราบปรามปัญหาเกี่ยวกับการใช้ชุดคำสั่งไม่พึงประสงค์ยังมีข้อบกพร่อง ไม่สมบูรณ์ และไม่สามารถบรรลุวัตถุประสงค์ตามเจตนารมณ์ของกฎหมายได้อย่างแท้จริง

2. วัตถุประสงค์การวิจัย

2.1 เพื่อให้ทราบถึงความหมายและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์

2.2 เพื่อให้ทราบถึงความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ และสามารถจัดประเภทของชุดคำสั่งไม่พึงประสงค์ได้

2.3 เพื่อให้ทราบถึงมาตรการทางกฎหมายที่ใช้อยู่ในปัจจุบันในการจัดการกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์

2.4 เพื่อให้ทราบถึงความหมายและสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ในความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา

2.5 เพื่อให้ทราบถึงความหมาย คุณสมบัติและลักษณะของชุดคำสั่งไม่พึงประสงค์ตลอดจนความหมายของการเข้าถึงและการบริหารจัดการในเชิงกฎหมายกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ในกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ

2.6 เพื่อให้มีระบบการบริหารจัดการชุดคำสั่งไม่พึงประสงค์โดยการแยกแยะและจัดระเบียบชุดคำสั่งไม่พึงประสงค์อย่างชัดเจนและสามารถนำชุดคำสั่งไม่พึงประสงค์แต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่นไปใช้ให้เกิดประโยชน์โดยให้มีบทบัญญัติของกฎหมายรองรับ

3. กรอบแนวคิดการวิจัย

3.1 อาชญากรรมคอมพิวเตอร์และอาชญากรรมพื้นฐาน มีองค์ประกอบของความผิดเดียวกันแต่แตกต่างกันเพียงในรายละเอียดของการกระทำผิด ลักษณะ รูปแบบ และวิธีการก่ออาชญากรรมเป็นสำคัญ

3.2 สภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ เป็นองค์ประกอบเบื้องต้นที่สำคัญที่สุดองค์ประกอบหนึ่ง โดยเฉพาะอย่างยิ่งในฐานความผิดเกี่ยวกับทรัพย์ โดยหากปราศจาก “ทรัพย์” แล้ว ความผิดประเภทนี้ก็จะกระทำสำเร็จมิได้

3.3 ชุดคำสั่งไม่พึงประสงค์ (Malicious Software) หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ (Computer Data) หรือระบบคอมพิวเตอร์ (Computer System) หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ นอกจากนี้ยังสามารถกำหนดความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์เพิ่มเติมได้โดยการตราเป็นกฎกระทรวง

3.4 ความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ยังไม่ครอบคลุมถึงลักษณะของการกระทำความผิดที่เกิดขึ้น ในปัจจุบันได้ทั้งหมด และยังไม่เอื้ออำนวยต่อการบังคับใช้กฎหมายในทางปฏิบัติ ทำให้การบังคับใช้กฎหมายมีข้อบกพร่องและมิอาจป้องกันและปราบปรามชุดคำสั่งไม่พึงประสงค์ได้อย่างแท้จริง

4. สมมติฐานการวิจัย

การก่ออาชญากรรมคอมพิวเตอร์โดยใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดโดยการจัดทำและเผยแพร่โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ผ่านทางเครือข่ายคอมพิวเตอร์พบได้อย่างแพร่หลายในปัจจุบัน ทั้งนี้ก็เพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ ความครบถ้วน และเสถียรภาพในการใช้งานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชนเป็นอย่างมาก โดยเฉพาะอย่างยิ่งการนำข้อมูลเอกลักษณ์บุคคลที่ได้ไปก่ออาชญากรรมด้านการเงินหรือด้านอื่นต่อไป ทั้งนี้ จากการพิเคราะห์ถึงพฤติการณ์ดังกล่าวพบว่า หากมีการก่ออาชญากรรมโดยใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์เป็นเครื่องมือในการกระทำความผิดแล้ว ยังมิอาจปรับเข้ากับฐานความผิดตามพระราชบัญญัติที่มีโทษทางอาญาใด

ได้เลย ไม่ว่าจะเป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญาเพราะขาดซึ่งองค์ประกอบของความผิดสำคัญที่ว่าข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ตามนิยามและความหมายในประมวลกฎหมายแพ่งและพาณิชย์ หรือแม้แต่ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งถือเป็นกฎหมายเฉพาะสำหรับเรื่องนี้ก็ยังมองไม่เห็นทางเลยว่าพฤติการณ์แห่งการกระทำผิดดังกล่าวจะสามารถปรับเข้ากับความผิดฐานใดได้บ้าง

สาเหตุก็เนื่องมาจากการบัญญัติความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคสอง ยังไม่ครอบคลุมถึงพฤติการณ์ดังกล่าว จึงทำให้ผู้กระทำความผิดอาศัยช่องว่างของกฎหมายนี้ทำให้ไม่ต้องรับโทษ จึงจำเป็นต้องค้นหามาตรการและแนวทางการแก้ไขโดยการตรากฎหมายในลำดับรองตามที่กฎหมายแม่ได้ให้อำนาจไว้เพื่อให้ความหมายของชุดคำสั่งไม่พึงประสงค์มีความหมายครอบคลุมถึงพฤติการณ์แห่งความผิดดังกล่าว และเพื่อเป็นการแยกแยะและรับรองชุดคำสั่งไม่พึงประสงค์ที่ถือเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันและแก้ไขชุดคำสั่งอื่น เช่น โปรแกรมแอนตี้และตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ หรือม้าโทรจัน โปรแกรมแอนตี้การส่งสแปมเมล์ เป็นต้น และจะทำให้พนักงานเจ้าหน้าที่มีอำนาจในการยื่นคำร้องต่อศาลเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์ที่มีม้าโทรจันหรือสปายแวร์ระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

5. ขอบเขตของการวิจัย

มาตรา 21 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดอำนาจให้กับพนักงานเจ้าหน้าที่ในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ก็ได้ รวมทั้งได้กำหนดความหมายของชุดคำสั่งไม่พึงประสงค์ไว้ในมาตราดังกล่าวด้วย แต่ความหมายของชุดคำสั่งไม่พึงประสงค์ที่กำหนดไว้นั้น ยังไม่อาจปรับใช้กับชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ได้ นอกจากนี้กฎหมายดังกล่าวยังกำหนดฐานความผิดและบทกำหนดโทษไว้อีกหลายมาตรา ได้แก่ การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ การดักรับ

ข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่กระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ การเผยแพร่ชุดคำสั่งไม่พึงประสงค์ที่ใช้ในการกระทำความผิด การเผยแพร่เนื้อหาอันไม่เหมาะสมหรือเป็นเท็จ รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลายและความผิดเกี่ยวกับสแปมเมล์ (spam mail)

อย่างไรก็ตาม วิทยานิพนธ์ฉบับนี้ จะมุ่งเน้นศึกษาเฉพาะฐานความผิดที่อาจใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดเท่านั้น ทั้งนี้เพื่อที่จะได้ทราบถึงองค์ประกอบ รูปแบบ ลักษณะและวิธีการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ ผลของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ และปัญหาในทางกฎหมายของการกระทำความผิดดังกล่าว นอกจากนี้ ยังจะได้ศึกษาถึงสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ในความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา รวมทั้งการศึกษาถึงมาตรการทางกฎหมายที่ใช้อยู่ในปัจจุบันในการจัดการกับการกระทำความผิดที่อาจเกิดชุดคำสั่งไม่พึงประสงค์ โดยการวิเคราะห์และเปรียบเทียบกับกฎหมายระหว่างประเทศและกฎหมายของต่างประเทศในประเด็นที่เกี่ยวกับ ความหมาย คุณสมบัติและลักษณะของชุดคำสั่งไม่พึงประสงค์ ตลอดจนความหมายของการเข้าถึงและการบริหารจัดการในเชิงกฎหมายกับการกระทำความผิดดังกล่าวในกฎหมายระหว่างประเทศและกฎหมายต่างประเทศว่า มีรูปแบบการบริหารจัดการอย่างไร เพื่อให้ทราบแนวทางการปฏิบัติ ปัญหาและอุปสรรค และนำมาพัฒนากฎหมายของไทยโดยหามาตรการทางกฎหมายหรือกลไกที่เหมาะสมกับการแก้ไขปัญหาต่อไป

ทั้งนี้ โดยการศึกษาค้นคว้าข้อมูลจากตำราและงานวิจัยภายในประเทศ และตำราจากต่างประเทศ บทความ ข้อมูลจากอินเทอร์เน็ต และรายงานการสัมมนาทางวิชาการในเรื่องที่เกี่ยวข้องแล้วนำข้อมูลที่ได้มาวิเคราะห์กับกรณีการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์

6. นิยามศัพท์เฉพาะ

เนื่องจากวิทยานิพนธ์นี้มีการกล่าวถึงและเกี่ยวโยงกับกฎหมายหลายฉบับ เพื่อความกระจ่างและความเข้าใจตรงกันระหว่างผู้เขียนกับผู้อ่าน ผู้เขียนจึงขอให้คำจำกัดความสำคัญๆ โดยนำมาจากกฎหมายที่เกี่ยวข้อง ดังต่อไปนี้

6.1 ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย[19]

6.2 ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ[20]

6.3 ข้อมูลจราจรทางคอมพิวเตอร์ หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น[21]

6.4 ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้นตามที่รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารประกาศในราชกิจจานุเบกษา[22]

6.5 ข้อมูลอิเล็กทรอนิกส์ หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษาหรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร[23]

6.6 พนักงานเจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[24]

6.7 ผู้ให้บริการ หมายความว่า หน่วยงานของรัฐหรือเอกชนซึ่งจัดให้มีบริการที่ให้ผู้ใช้บริการสามารถติดต่อสื่อสารโดยอาศัยระบบคอมพิวเตอร์ หรือหน่วยงานอื่นใดที่ทำหน้าที่

---

19 ความหมายตามมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

20 อ้างแล้วในเชิงอรรถที่ 19

21 อ้างแล้วในเชิงอรรถที่ 19

22 อ้างแล้วในเชิงอรรถที่ 19

23 ความหมายตามมาตรา 4 แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

24 อ้างแล้วในเชิงอรรถที่ 19

ประมวลผลหรือจัดเก็บข้อมูลคอมพิวเตอร์อันเนื่องจากการให้บริการด้านการติดต่อสื่อสารหรือข้อมูลการใช้บริการ[25]

6.8 โปรแกรม หมายถึง ชุดคำสั่งที่ทำหน้าที่สั่งการให้คอมพิวเตอร์ทำงาน[26]

6.9 ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล เช่น การศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติอาชญากรรม ประวัติการทำงาน หรือประวัติกิจกรรม บรรดาที่มีชื่อของบุคคลนั้นหรือมีเลขหมาย รหัส หรือสิ่งบอกลักษณะที่ทำให้รู้ตัวบุคคลนั้นได้ เช่น ลายพิมพ์นิ้วมือ แผ่นบันทึกลักษณะเสียงของคน หรือรูปถ่าย และให้หมายความรวมถึงข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของผู้ที่ถึงแก่กรรมแล้วด้วย[27]

7. ประโยชน์ที่คาดว่าจะได้รับ

7.1 ทำให้ทราบถึงความหมายและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์

7.2 ทำให้ทราบถึงความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ และสามารถจัดประเภทของชุดคำสั่งไม่พึงประสงค์ได้

7.3 ทำให้ทราบถึงมาตรการทางกฎหมายที่ใช้อยู่ในปัจจุบันในการจัดการกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์

7.4 ทำให้ทราบถึงความหมายและสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ในความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา

---

25 Convention on Cybercrime ได้ให้ความหมายของคำนี้ไว้ว่า service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service

26 ความหมายตามหนังสือแนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) พ.ศ. 2546 หน้า 15

27 ความหมายตามมาตรา 3 แห่งร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... (ณ วันที่ 14 กรกฎาคม 2551)

7.5 ทำให้ทราบถึงความหมาย คุณสมบัติและลักษณะของชุดคำสั่งไม่พึงประสงค์ ตลอดจนความหมายของการเข้าถึงและการบริหารจัดการในเชิงกฎหมายกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ในกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ

7.6 ทำให้มีระบบการบริหารจัดการชุดคำสั่งไม่พึงประสงค์โดยการแยกแยะและจัดระเบียบชุดคำสั่งไม่พึงประสงค์อย่างชัดเจนและสามารถนำชุดคำสั่งไม่พึงประสงค์แต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่นไปใช้ให้เกิดประโยชน์โดยให้มีบทบัญญัติของกฎหมายรองรับ

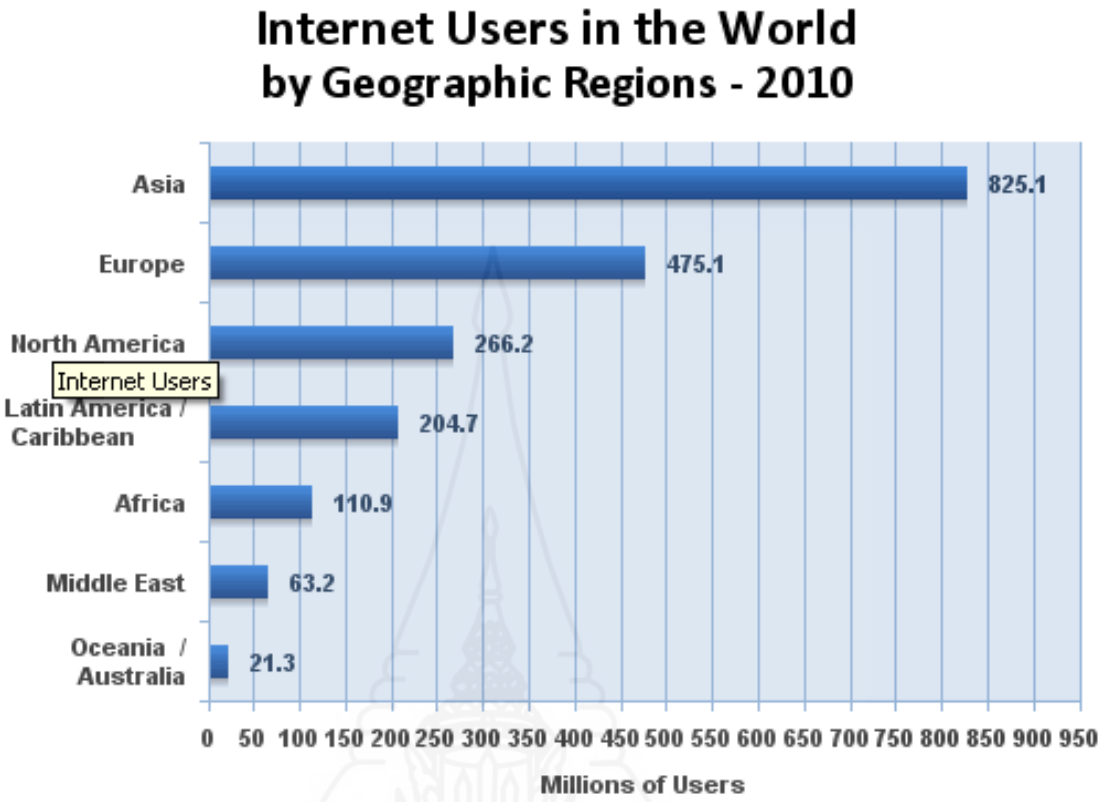
บทที่ 2
ความเบื้องต้นเกี่ยวกับชุดคำสั่งไม่พึงประสงค์

จากสภาพโดยธรรมชาติของอาชญากรรมคอมพิวเตอร์ที่ผู้กระทำความผิดจะอยู่ที่ใดในโลกก็ได้ ดังนั้น ระบบคอมพิวเตอร์และเครือข่ายจึงอาจถูกคุกคามหรือถูกโจมตีจากนักเจาะระบบ (Hacker) หรือผู้ใช้งานทั่วไปที่มีความคึกคะนองหรืออยากรู้อยากทดลองซึ่งอาจจะเป็นคนภายในองค์กรเองหรือนักเรียนนักศึกษา ทั้งนี้ โดยการใช้โปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ที่จัดทำขึ้นเป็นการเฉพาะเพื่อเป็นเครื่องมือในการเข้าถึงหรือการโจมตีทรัพยากรด้านคอมพิวเตอร์โดยผ่านทางระบบเครือข่ายสื่อสารในหลายๆ ด้านและหลายๆ ทางด้วยกัน ไม่ว่าจะเป็นการโจมตีผ่านทางระบบเครือข่ายคอมพิวเตอร์โดยทั่วๆ ไป หรือผ่านทางระบบเครือข่ายคอมพิวเตอร์ระดับโลกอย่างเครือข่ายอินเทอร์เน็ตซึ่งถือเป็นเครือข่ายสาธารณะที่เชื่อมต่อคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์กว่าพันล้านคนเข้าด้วยกัน สาเหตุก็เนื่องมาจากความนิยมในการใช้อินเทอร์เน็ตที่เพิ่มขึ้นทั่วโลก และจากสถิติอาชญากรรมคอมพิวเตอร์ที่มาจากการใช้งานอินเตอร์เน็ตเป็นสื่อกลางในการติดต่อก็พบว่ามีสถิติเพิ่มขึ้นเป็นเงาตามตัวเช่นกัน โดยบรรดาอาชญากรหรือผู้ไม่หวังดีได้อาศัยเครือข่ายอินเทอร์เน็ตเป็นช่องทางในการโจมตีเหยื่อหรือเป้าหมายดังรายละเอียดปรากฏตามแผนภาพ (graph) แสดงปริมาณการใช้อินเทอร์เน็ตตามภาพที่ 2.1-2.4

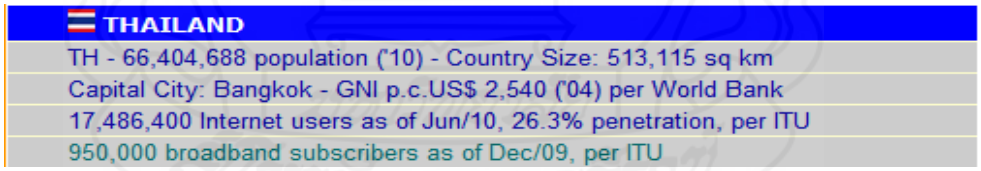
WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

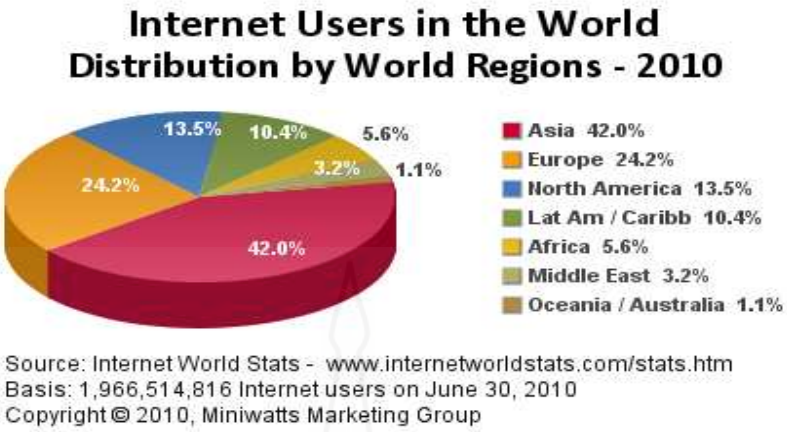
ภาพที่ 2.1 ตารางแสดงปริมาณการใช้อินเทอร์เน็ตทั่วโลก



ภาพที่ 2.2 แผนภาพแบบแท่งแสดงปริมาณการใช้อินเทอร์เน็ตทั่วโลก



ภาพที่ 2.3 แผนภาพแสดงปริมาณการใช้อินเทอร์เน็ตของประเทศไทย



ภาพที่ 2.4 แผนภาพแบบวงกลมแสดงปริมาณการใช้อินเทอร์เน็ตทั่วโลก

ที่มา : http://www.internetworldstats.com/

1. ความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองนักคอมพิวเตอร์

โดยธรรมชาติของโปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ย่อมต้องมีพัฒนาการของตัวเองไปเรื่อยๆ ตามยุคสมัยและตามความต้องการของเหล่าอาชญากรหรือผู้ใช้งานที่ไม่มีขีดจำกัด ซึ่งแนวโน้มของอาชญากรรมคอมพิวเตอร์ทั้งในปัจจุบันและอนาคตจะมีความซับซ้อนและเพิ่มความรุนแรงและผลกระทบมากขึ้น เกี่ยวกับเรื่องนี้ ดร.ปริญญา หอมอเนก ได้กล่าวไว้ว่า[28] “เนื่องจากอาชญากรรมคอมพิวเตอร์ในปัจจุบันมีการทำงานในลักษณะ"Organized Crime" กล่าวคือ มีการกระทำความผิดเป็นกลุ่มหรือเป็นองค์กรและมีการโจมตีเพื่อหวังผลและมีจุดประสงค์ชัดเจนที่เรียกว่า "Targeted Attack" ซึ่งส่วนใหญ่จะมุ่งหาประโยชน์ทางด้านการเงิน เช่น การโจมตีระบบอินเทอร์เน็ตแบงก์กิ้ง หรือ การโจมตีระบบบัตรเครดิต เช่น การแฮก (Hack) ระบบเครือข่ายของบริษัทสื่อสารใหญ่ๆ เพื่อแอบขโมยโทรศัพท์ฟรีโดยการเปลี่ยนแปลงข้อมูลในระบบ Pre-paid ดังที่เป็นข่าวหน้าหนึ่งของหนังสือพิมพ์หลายฉบับมาแล้ว เป็นต้น” ทั้งนี้ จากการรวบรวมข้อมูลของโปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ตั้งแต่อดีตจนถึงปัจจุบันพบว่า

---

[28] ปริญญา หอมเอนก, “ยุทธศาสตร์การเตรียมพร้อมป้องกันภัยจากมัลแวร์อย่างได้ผลในทางปฏิบัติ Understanding MalWare Point-of-Entry and How to protect by implementing practical Anti-Malware strategy”, บทความออนไลน์ซึ่งนำมาจาก eWeek Thailand ปักษ์แรก ประจำเดือนธันวาคม 2549 ที่มา http://www.acisonline.net/article_prinya_eweek_011249.htm เผยแพร่เมื่อ 30 พฤศจิกายน 2549 Retrieved June, 30, 2010

มีชุดคำสั่งไม่พึงประสงค์อยู่หลายๆ ประเภทและมีคุณลักษณะหรือวัตถุประสงค์ในการใช้งานและมีชื่อเรียกแตกต่างกันออกไป เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) ซึ่งเป็นชุดคำสั่งไม่พึงประสงค์ประเภทแรกที่ตรวจพบและถือกำเนิดขึ้นมาในโลกนี้มากว่ายี่สิบปีแล้ว[29] รวมทั้งหนอนคอมพิวเตอร์ (Worm) ม้าโทรจัน (Trojan Horses) สปายแวร์ (Spyware) เป็นต้น ซึ่งต่อไปนี้ผู้เขียนจะขอเรียกชื่อโดยรวมว่า "ชุดคำสั่งไม่พึงประสงค์ (Malicious Software)" หรือเรียกโดยย่อว่า "มัลแวร์ (Malware)"

อย่างไรก็ตาม การใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เหล่านั้นล้วนแต่มีวัตถุประสงค์ไปในทำนองเดียวกันคือ เพื่อมุ่งก่อให้เกิดความเสียหายและส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และระบบเครือข่ายคอมพิวเตอร์ (Computer Network Security) ทั้งต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์[30] (ในสากลเรียกหลักนี้ว่า "หลัก CIA")[31] ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชน ดังปรากฏตามรายงานร้อยละของประเภทความ

---

29 ปริญญา หอมเอนก, อ้างแล้วในเชิงอรรถที่ 28

30 วิธีการที่จะทำให้ข้อมูลคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์มีความปลอดภัยนั้นจะต้องมีกระบวนการในการดำเนินการด้านความปลอดภัย ซึ่งกระบวนการต่างๆ ได้ถูกกำหนดไว้เป็นมาตรฐานซึ่งมีอยู่หลายมาตรฐานด้วยกัน บางมาตรฐานถูกดัดแปลงมาจากมาตรฐานความปลอดภัยทั่วๆ ไป บางมาตรฐานถูกดัดแปลงมาจากมาตรฐานการดำเนินธุรกิจ ซึ่งมาตรฐานที่มักจะถูกนำมาใช้เพื่อยกระดับความปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่ายมากที่สุดคือ ISO/IEC 27001 ส่วนมาตรฐานในการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ที่ถูกนำมาปรับใช้เพื่อการตราเป็นกฎหมายนั้นมีองค์ประกอบพื้นฐานความปลอดภัยที่สำคัญอยู่สามประการด้วยกัน คือ การรักษาความลับ (Confidentiality) ความครบถ้วน (Integrity) และเสถียรภาพในการใช้งาน (Availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์

31 หลัก CIA ประกอบด้วย

1. การรักษาความลับ (Confidentiality) หมายถึง การปกป้องข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยมีเงื่อนไขว่าข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์นั้นใครมีสิทธิ์จะล่วงรู้ เข้าถึง ใช้งานได้ และการทำให้ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์สามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

2. ความครบถ้วน (Integrity) หมายถึง การป้องกันเพื่อให้ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ไม่ถูกแก้ไข เปลี่ยนแปลง หรือถูกทำลายได้

3. เสถียรภาพในการใช้งาน (Availability) หมายถึง ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์จะต้องมีสภาพพร้อมใช้งานอยู่ตลอดเวลา

เสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2004-2008 ของสถาบันรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security Institute : CSI)[32] ซึ่งเป็นหน่วยงานที่ทำหน้าที่ประสานความร่วมมือระหว่างหน่วยงานที่เป็นสมาชิก โดยจัดตั้งขึ้นในประเทศสหรัฐอเมริกาในมลรัฐซานฟรานซิสโก (San Francisco) ตั้งแต่ปี ค.ศ. 1974 โดยมีวัตถุประสงค์หลักเพื่อต้องการสนับสนุนและฝึกอบรมบุคคลให้มีความรู้ความเชี่ยวชาญเกี่ยวกับความมั่นคงของเทคโนโลยีสารสนเทศ คอมพิวเตอร์และระบบเครือข่าย และวัตถุประสงค์ที่สำคัญของการจัดตั้งสถาบันรักษาความปลอดภัยคอมพิวเตอร์อีกประการหนึ่งก็เพื่อที่จะสร้างความตระหนัก (awareness) ในปัญหาที่เกิดขึ้นจากความไม่ปลอดภัยในระบบคอมพิวเตอร์และเครือข่ายด้วยการดำเนินการที่สำคัญประการหนึ่งคือ การสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์โดยร่วมมือกับสำนักสอบสวนกลางแห่งมลรัฐซานฟรานซิสโก (the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad) ประเทศสหรัฐอเมริกา โดยได้มีการดำเนินการอย่างต่อเนื่องตั้งแต่ปี ค.ศ. 1996 เรื่อยมาจนกระทั่งถึงปัจจุบัน (ปีที่มีการรายงานและสามารถเข้าถึงข้อมูลได้ล่าสุดคือ ปี ค.ศ. 2008) จากรายงานผลการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2004-2008 ทำให้ทราบว่า การกระทำที่ก่อให้เกิดความเสียหายมากที่สุดในบรรดาประเภทความเสียหายที่เกิดขึ้นจากภัยดังกล่าวตั้งแต่ปี ค.ศ. 2004-2008 คือ ความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์ รองลงมาคือการกระทำละเมิดจากภายใน (ซึ่งระบบอาจมีช่องโหว่และถูกกระทำละเมิดผ่านช่องโหว่นั้นทั้งทางกายภาพ (Physical) และทางดิจิทัล (Digital หมายถึงเชิงเลข)[33] โดยการส่งมัลแวร์ไปฝังไว้แล้วกระทำการละเมิด) และการโจรกรรมหรือการฉ้อโกงผ่านทางคอมพิวเตอร์ Laptop รวมทั้งการเข้าถึง โดยมิชอบและการยึดเครื่องของเหยื่อให้กลายเป็นบ๊อท (BOT ย่อมาจาก Robot ซึ่งเป็นการเปรียบเทียบว่าเหมือนหุ่นยนต์ซึ่งถูกควบคุม) ตามลำดับ ซึ่งความเสียหายเหล่านั้นมักจะใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิด ดังภาพที่ 2.5 ต่อไปนี้

---

[32] เป็นเพียงการสำรวจความเสียหายที่เกิดขึ้นทั่วโลกเท่านั้น โดยไม่มีการแสดงสถิติความเสียหายของแต่ละประเทศไว้ด้วย อย่างไรก็ตาม เนื่องจากประเทศไทยยังไม่มีหน่วยงานใดรับผิดชอบ ดำเนินการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ทำให้การอ้างอิงสถิติความเสียหายต่างๆ จึงต้องอาศัยข้อมูลจากหน่วยงานต่างประเทศเป็นหลัก และสามารถดูข้อมูลเพิ่มเติมที่ http://www.gocsi.com

[33] ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 31

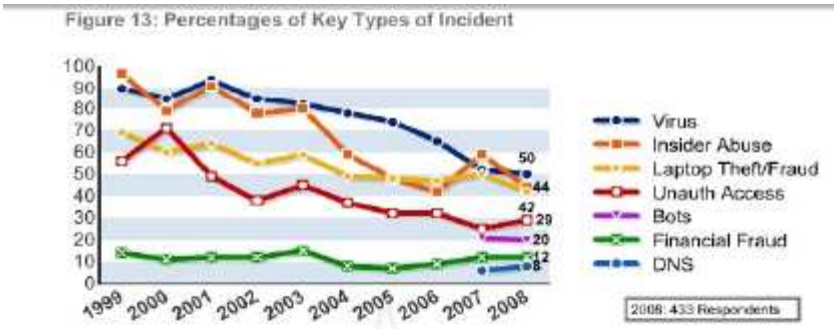


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

ภาพที่ 2.5 แผนภาพแสดงร้อยละของประเภทความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2004-2008 ของสถาบันรักษาความปลอดภัยคอมพิวเตอร์

ที่มา : http://www.gocsi.com

จากรายงานผลการสำรวจความเสียหายที่เกิดขึ้นอันเนื่องมาจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2004-2008 ของสถาบันรักษาความปลอดภัยคอมพิวเตอร์ดังกล่าว จึงเป็นเหตุผลสำคัญอย่างยิ่งที่จะต้องมีการศึกษาแบบเจาะลึกเกี่ยวกับความหมายและคุณสมบัติของ

ชุดคำสั่งไม่พึงประสงค์และภัยที่ตามมา เพื่อค้นหาวิธีการรับมือกับปัญหาดังกล่าว โดยจะขอแยกกล่าวถึงชุดคำสั่งไม่พึงประสงค์ตามความหมายและคุณสมบัติ ดังนี้

1.1 ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย เป็นชุดคำสั่งที่เป็นสาเหตุและทำให้เกิดอาชญากรรมคอมพิวเตอร์มากที่สุด (จากรายงานผลการสำรวจความเสียหายที่เกิดขึ้นจากการก่ออาชญากรรมทางคอมพิวเตอร์ในปี ค.ศ. 2004-2008 ของสถาบันรักษาความปลอดภัยคอมพิวเตอร์ที่ได้กล่าวไปแล้วในข้อ 1 ข้างต้น) โดยแฮกเกอร์หรือผู้ไม่หวังดีหรือผู้ใช้งานทั่วไปที่มีความคึกคะนองหรืออยากรู้อยากทดลองมักจะนิยมนำโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ไปเป็นเครื่องมือในการโจมตี เนื่องจากปัจจุบันโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ทั้งหลายได้ถูกพัฒนาและออกแบบมาเพื่อให้มีรูปแบบการใช้งานที่สะดวกและง่าย (User friendly) มากขึ้น และส่วนใหญ่จะมาในรูปแบบของการทำงานแบบกราฟฟิค (Graphic User Interface) โดยผู้ใช้งานเพียงแต่คลิกหรือเลือกและทำตามฟังก์ชั่นการทำงานที่โปรแกรมกำหนดไว้ก็จะสามารถใช้เป็นเครื่องมือในการโจมตีเหยื่อหรือคุกคามระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ได้อย่างง่ายดาย ซึ่งแตกต่างจากโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในยุคอดีตที่จะมีรูปแบบของการใช้งานแบบคำสั่งงานเป็นรายบรรทัด (Command Line) จึงทำให้ใช้งานได้ยากและผู้ใช้งานจะต้องมีความรู้เกี่ยวกับคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในระดับที่เข้าใจและสามารถเขียนโปรแกรมด้วยภาษาคอมพิวเตอร์ได้จึงจะสามารถใช้งานชุดคำสั่งไม่พึงประสงค์ได้

อย่างไรก็ตาม การโจมตีโดยพวกที่มีความคึกคะนองหรืออยากรู้อยากทดลองส่วนใหญ่จะทำไปเพื่อทดลองใช้เครื่องมือโจมตีต่างๆ เช่น Remote Exploit[34] เป็นต้น การโจมตี

---

[34] Exploit เป็นคำที่มาจากภาษาฝรั่งเศสเกิดจากการนำคำสองคำมาผสมกันมีความหมายว่าการบรรลุผลสำเร็จหรือผลสัมฤทธิ์โดยเป็นโปรแกรมที่ได้รับการออกแบบมาเพื่อให้ทำการเจาะระบบโดยอาศัยช่องโหว่ของซอฟท์แวร์ (software) ฮาร์ดแวร์ (hardware) หรือช่องโหว่ต่างๆ ในคอมพิวเตอร์แม่ข่าย (server) เพื่อที่จะเข้าทำการครอบครองหรือควบคุมคอมพิวเตอร์ให้กระทำการบางอย่าง เช่น การขโมยข้อมูลหรือใช้ในการทำให้คอมพิวเตอร์ปฏิเสธการทำงาน (denial of service attack) เป็นต้น และเมื่อ Exploit สามารถเข้ามาในระบบได้แล้วก็จะเริ่มทำการเปลี่ยนแปลงข้อมูลต่างๆ ในระบบ หรือโปรแกรมต่างๆ ของคอมพิวเตอร์แม่ข่ายเพื่อส่งข้อมูลไปหาตัวเองหรือเพื่อให้ Exploit สามารถเข้าสู่ระบบได้อีกครั้งในภายหลัง แม้ว่าช่องโหว่ (backdoor) เดิมจะได้ถูกปิดไปแล้ว โดยปกติเมื่อ Exploit สามารถเข้ามาสู่ระบบได้แล้วก็จะทำการเพิ่มบัญชีผู้ใช้งาน (user) ที่มีสิทธิเหนือกว่าบัญชีผู้ใช้งานทั่วไปซึ่งอาจเทียบเท่าหรือเหนือกว่าสิทธิของผู้ดูแลระบบ (administrator) เข้าไปในระบบ ทั้งนี้รูปแบบการโจมตีของ Exploit สามารถแยกได้เป็น 2 รูปแบบคือ remote exploit ซึ่งทำงานโดยจะทำการเจาะระบบ

ดังกล่าวอาจทำให้ระบบหยุดให้บริการหรือทำให้ประสิทธิภาพของการให้บริการลดลงหรือข้อมูลภายในระบบอาจได้รับความเสียหายโดยที่ผู้ทดลองอาจจะไม่รู้ตัวว่าได้ทำสำเร็จแล้วหรือไม่ ซึ่งอาจจะยังไม่เข้าข่ายถึงขั้นที่จะเรียกว่าเป็นอาชญากรรมทางคอมพิวเตอร์ หรือถึงขั้นที่จะเรียกผู้โจมตีโดยการทดลองว่าเป็นอาชญากรทางคอมพิวเตอร์ ทั้งนี้ เนื่องจากความแตกต่างของการโจมตีและวัตถุประสงค์ของการโจมตีที่แตกต่างจากพวกแฮกเกอร์ซึ่งมีวัตถุประสงค์และเป้าหมายในการโจมตีที่ชัดเจนมากกว่า

สำหรับความหมายของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายนี้ได้มีผู้รู้ ตลอดจนนักวิชาการและแหล่งความรู้จากหลายแหล่งพยายามให้ความหมายและเรียกชื่อไว้แตกต่างกันออกไป ซึ่งก็สุดแท้แต่ว่าผู้รู้หรือนักวิชาการแต่ละท่านหรือแหล่งความรู้แต่ละแหล่งเหล่านั้นจะเรียกชุดคำสั่งไม่พึงประสงค์ว่าอย่างไร แต่หากได้มีการพิจารณาถึงความหมายโดยรวมของชื่อที่ถูกเรียกเหล่านั้นแล้วก็คงหมายถึงชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายนั่นเอง ซึ่งในที่นี้จะขอนำตัวอย่างของการเรียกชื่อชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายตามที่ปรากฏและพบเห็นได้โดยทั่วไปมาให้ทราบ ได้แก่ มัลแวร์ (Malware)[35], แทรคแวร์

ที่ได้รับการป้องกันที่ไม่ดีโดยอาศัยสิทธิที่มีมาก่อนหรือเซอร์วิสที่กำลังรันอยู่ในเครื่องคอมพิวเตอร์แม่ข่ายที่ตกเป็นเหยื่อ และ local exploit ซึ่งเป็นการโจมตีที่หากเข้ามาในระบบได้แล้วจะทำการเพิ่มสิทธิต่างๆ เข้าไปในบัญชีผู้ใช้งานที่เคยสร้างเอาไว้แล้วโดยอาศัยความช่วยเหลือของผู้ดูแลระบบ

35 มัลแวร์ ย่อมาจากซอฟต์แวร์ที่เป็นอันตราย (บางครั้งเรียกว่า pestware) เป็นซอฟต์แวร์ที่ออกแบบมาเพื่อแอบเข้าสู่ระบบคอมพิวเตอร์โดยไม่มีการแสดงความยินยอมของเจ้าของ ซึ่งความเห็นของผู้เชี่ยวชาญด้านคอมพิวเตอร์หมายถึงความหลากหลายของรูปแบบของซอฟต์แวร์ที่ไม่เป็นมิตร, โปรแกรมรบกวนหรือน่ารำคาญ ที่มา http://en.wikipedia.org/wiki/Malware Retrieved July, 12, 2010

นอกจากนี้ยังมีเว็บไซต์ภาษาอังกฤษที่ให้คำจำกัดความ Malware ไว้ ดังนี้

- The superset of malicious software, that often used as shorthand method for referencing multiple categories of software such as viruses, trojans, worms, spyware, etc. ที่มา www.antispywarecoalition.org/documents/2007glossary.htm Retrieved July, 12, 2010

- Malicious software (mal-ware) is a form of computer program designed with malicious intent. This intent may be to cause annoying pop-up ads with the hope you click on one and generate revenue, or forms of spyware and viruses that can be used to steal your identity or track your activities. ที่มา www.albany.edu/its/glossary.htm Retrieved July, 12, 2010

(Trackware)[36], ไฮแจ๊คแวร์ (Hijackware)[37], ธีฟแวร์ (Thiefware)[38], สนู๊ปแวร์ (Snoopware)[39] หรือสคัมแวร์ (Scum ware) นอกจากนี้ยังมีนักวิชาการของประเทศไทยคือ ดร.ปริญญา หอมอเนก ก็ได้ให้ความหมายชุดคำสั่งไม่พึงประสงค์ไว้ว่า[40] หมายถึง รูปแบบหนึ่งของไวรัสทั้งในปัจจุบันและอนาคตที่มักจะมาในรูปของ Malicious Mobile Code (MMC) คำว่า "Malicious" หมายถึง มุ่งร้าย หรือปองร้ายเมื่อรวมกับ "Mobile Code" ก็คือ การประสงค์ร้ายที่มาในรูปแบบของโค๊ดที่เคลื่อนที่ได้ หรือโปรแกรมคอมพิวเตอร์ประเภทหนึ่งซึ่งถูกออกแบบมาเพื่อเคลื่อนที่จากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งโดยมุ่งหวังที่จะปรับเปลี่ยนข้อมูลในระบบคอมพิวเตอร์โดยที่เจ้าของหรือผู้ใช้ไม่สามารถล่วงรู้ เป็นต้น

1.2 ชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหาย

ชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายในชีวิตจริงที่มักประสบและรู้จักกันดีก็ได้แก่ บรรดาโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆ เป็นต้น โดยมีผู้ผลิตโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันหรือแก้ไขความเสียหายเหล่านั้นให้เลือกมายมายมีทั้งที่ต้องเสียเงินซื้อมาและแบบที่ให้ใช้กันฟรีๆ แต่ส่วนใหญ่แล้วจะต้องเสียเงินหรือซื้อมาโดยมี License สำหรับการใช้งานด้วย ทั้งนี้เพื่อเป็นการปกป้องระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ โดยผู้ใช้สามารถใช้หรือติดตั้งชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายภายใต้เทคโนโลยีต่างๆ ที่มีอยู่ในปัจจุบัน ยกตัวอย่าง เช่น การติดตั้งระบบการตรวจจับการบุกรุก (Intrusion Detection) หรือการติดตั้ง

---

36 โปรแกรมซอฟต์แวร์ใดๆ ที่ไม่พึงประสงค์ที่สามารถติดตามกิจกรรมในระบบของผู้ใช้หรือการเก็บรวบรวมข้อมูลของระบบและให้ข้อมูลกับบุคคลที่สาม Trackware ไม่ได้รวบรวมข้อมูลที่สามารถระบุตัวบุคคล ที่มา http://www.webopedia.com/TERM/T/trackware.html Retrieved June, 12, 2010

37 เป็นชนิดของโปรแกรมที่จะเปลี่ยนแปลงการตั้งค่าเบราว์เซอร์ของคอมพิวเตอร์เพื่อที่จะเปลี่ยนเส้นทางไปยังเว็บไซต์ที่ไม่ได้ตั้งใจจะเข้าไปเยี่ยมชม ที่มา www.networkdictionary.com/security/h.php Retrieved June, 12, 2010

38 ซอฟต์แวร์ที่ลักลอบสำเนาข้อมูลจากคอมพิวเตอร์ของผู้ใช้ไปยังเว็บเซิร์ฟเวอร์บนอินเทอร์เน็ต ที่มา www.networkdictionary.com/security/h.php Retrieved June, 12, 2010

39 ซอฟต์แวร์การตรวจสอบของพนักงานและช่วยเหลือผู้บริหารขององค์กรในการตรวจสอบและดูแลเครื่องคอมพิวเตอร์ของพนักงานจากส่วนกลาง ที่มา en.wikipedia.org/wiki/Snoopware Retrieved June, 12, 2010

40 ปริญญา หอมเอนก, เจาะลึก Malicious Mobile Code (MMC) ตอนที่ 1 , เอกสารออนไลน์ เผยแพร่เมื่อ 31 พฤษภาคม 2545 (กรุงเทพฯ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์, 2545). Retrieved June, 15, 2010

กำแพงไฟ (Firewall)[41] เพื่อป้องกันหรือรักษาระบบคอมพิวเตอร์ให้มีความปลอดภัย ซึ่งในปัจจุบันและอนาคตเทคโนโลยีความปลอดภัยข้อมูลสารสนเทศใหม่ๆได้ทยอยออกสู่ตลาดด้านความปลอดภัยข้อมูลสารสนเทศอย่างต่อเนื่องเพื่อตอบรับกับเทคนิคการโจมตีของแฮกเกอร์ในรูปแบบใหม่ๆ เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายนี้ ดร.ปริญญา หอมอเนก ได้ให้ความเห็นว่า บรรดาโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆ ไม่ใช่คำตอบสุดท้ายในการปราบมัลแวร์[42] เนื่องจาก โปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆในปัจจุบันนั้นไม่สามารถจัดการกับมัลแวร์หรือโปรแกรมไม่พึงประสงค์ต่างๆ ที่มีอยู่ได้ทั้งหมด แม้จะมีการติดตั้งโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆ ที่ได้ปรับปรุงแก้ไขโปรแกรมเหล่านั้นเพื่อให้รู้จักมัลแวร์ชนิดใหม่ ๆ (Update Malware Signature) ล่าสุดแล้วก็ยังไม่สามารถป้องกันได้ ซึ่งเหตุผลก็เนื่องมาจากมัลแวร์นั้นมีลักษณะเป็นการผสมผสาน (Blend Threat) ทั้งคุณสมบัติของไวรัส หนอน ม้าโทรจัน และอีกหลายๆ รูปแบบของการโจมตีไว้ในมัลแวร์เพียงโปรแกรมเดียวดังที่พบเห็นเป็นประจักษ์ก็คือ Sasser Worm, Bagle Worm, Netsky Worm และ Mydoom Virus เป็นต้น จึงมีผู้รู้เรียกมัลแวร์ดังกล่าวว่า “ไฮบริดมัลแวร์”[43]

---

41 Firewall เป็นกำแพงที่มีไว้เพื่อป้องกันไฟโดยที่ตัวมันเองนั้นไม่ใช่ไฟตามดังคำแปล Firewall ในสิ่งปลูกสร้างต่างๆ นั้นจะทำด้วยอิฐเพื่อแยกส่วนต่างๆ ของสิ่งปลูกสร้างออกจากกันเพื่อที่หากเกิดไฟไหม้ไฟจะได้ไม่ลุกลามไปทั่วสิ่งปลูกสร้างนั้นๆ หรือ Firewall ในรถยนต์ก็จะเป็นแผ่นโลหะที่ใช้แยกส่วนของเครื่องยนต์และส่วนของที่นั่งของผู้โดยสารออกจากกัน สำหรับในเครือข่ายอินเทอร์เน็ตนั้น Firewall อาจถูกใช้สำหรับป้องกันไม่ให้ “ไฟ” หรือ “ภัยคุกคาม” จากเครือข่ายอินเทอร์เน็ตภายนอกลามเข้ามาภายในเครือข่ายคอมพิวเตอร์ภายใน หรืออาจถูกใช้เพื่อป้องกันไม่ให้ผู้ใช้ในเครือข่ายคอมพิวเตอร์ภายในถูก “ไฟ” หรือ “ภัยคุกคาม” จากเครือข่ายอินเทอร์เน็ตภายนอกได้ อย่างไรก็ตาม ตามคำจำกัดความแล้ว Firewall หมายความถึง ระบบหนึ่งหรือกลุ่มของระบบที่บังคับใช้นโยบายในการควบคุมการเข้าถึงระหว่างเครือข่ายคอมพิวเตอร์สองเครือข่าย โดยที่วิธีการกระทำนั้นก็จะแตกต่างกันไปแล้วแต่ระบบ แต่โดยหลักการแล้ว Firewall ประกอบด้วยกลไกสองส่วนโดยส่วนแรกมีหน้าที่ในการกั้น traffic และส่วนที่สองมีหน้าที่ในการปล่อย traffic ให้ผ่านไปได้ ปัจจุบัน Firewall มีทั้งที่เป็นฮาร์ดแวร์ (hardware) และซอฟท์แวร์ (software) หรือเป็นโซลูชั่นสำเร็จรูปอย่างมิดเดิ้ลแวร์ (middleware)

42 ปริญญา หอมเอนก, “เมื่อโปรแกรมป้องกันไวรัสไม่ใช่คำตอบสุดท้ายในการปราบไวรัส”, บทความออนไลน์ซึ่งนำมาจาก eWeek Thailand ปักษ์แรก เดือนกรกฎาคม 2547 ที่มา http://www.acisonline.net/article_prinya_virus.htm เผยแพร่เมื่อ 1 กรกฎาคม 2547 Retrieved August, 20, 2010

43 ธวัชชัย ชมศิริ Computer & Network Security ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ กรุงเทพฯ บริษัท โปรวิชั่น จำกัด หน้า 293

ทั้งนี้ มัลแวร์รุ่นใหม่ๆ เหล่านั้นต่างมีพิษสงรอบด้านและมีความฉลาดเปรียบได้กับเป็นแฮกเกอร์ไปในตัวซึ่งจะมีความสามารถในการเจาะระบบโดยอาศัยช่องโหว่ต่างๆ ในระบบที่ยังไม่ได้รับการติดตั้งชุดแก้ไขข้อบกพร่อง (Patch) เช่น ไวรัส Sasser อาศัยช่องโหว่ของ Windows LSASS หรือ MS04-001 ของไมโครซอฟต์ ในการโจมตีระบบที่เป็น Windows ตั้งแต่ Windows NT ขึ้นไปจนถึง Windows 2003 เป็นต้น ถึงแม้ว่าจะมีโปรแกรมป้องกันมัลแวร์แต่ก็ไม่สามารถจะช่วยปิดช่องโหว่ได้ การปิดช่องโหว่ต้องติดตั้งชุดแก้ไขข้อบกพร่องที่มีให้ดาวน์โหลดจากเว็บไซต์ของเจ้าของผลิตภัณฑ์จึงจะสามารถแก้ไขปัญหาได้อย่างถูกจุด ดังนั้น จึงจำเป็นต้องมีโปรแกรมหรือชุดคำสั่งที่สามารถจัดการกับมัลแวร์โดยเฉพาะเช่น โปรแกรม Ad-aware, SpyBot Search & Destroy หรือ PestPatrol เป็นต้น ซึ่งผู้ผลิตโปรแกรมป้องกันไวรัสหลายค่ายในอุตสาหกรรมชนิดนี้กำลังปรับตัวโดยการปรับปรุงแก้ไขคุณสมบัติของโปรแกรมให้มีความสามารถมากขึ้น เช่น เพิ่มการตรวจจับมัลแวร์โดยการตรวจในระบบตรวจจับการบุกรุก (Intrusion Detection System : IDS) หรือการตรวจจับใน Zip File, การเพิ่มคุณสมบัติ Personal Firewall และ IPS (Intrusion Prevention Systems)[44] และการบริหารจัดการจากส่วนกลาง เป็นต้น

กล่าวโดยสรุป แนวความคิดใหม่ในการทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์มีความปลอดภัยจากมัลแวร์ต่างๆ นั้น โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันความเสียหายนอกจากจะเป็นโปรแกรมป้องกันมัลแวร์ซึ่งถือเป็นโปรแกรมขั้นพื้นฐานที่จำต้องมีไว้ในเครื่องคอมพิวเตอร์แล้ว ควรมีช่องทางให้ปรับปรุงรูปแบบมัลแวร์ของโปรแกรมนั้น (Malware Signature) ให้ทันสมัยกับมัลแวร์รุ่นใหม่ๆ อยู่เสมอ ทั้งนี้ หากสามารถควบคุมหรือบริหารจากส่วนกลางได้ก็จะได้ผลในการป้องกันมัลแวร์ได้ดีมากขึ้น กล่าวคือ เมื่อมีการออนไลน์

---

44 IPS (Intrusion Prevention System) คือซอฟท์แวร์ (software) หรือฮาร์ดแวร์ (hardware) ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆ กับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือฮาร์ดแวร์ตัวอื่นๆ IPS นั้นจะจู่โจมผู้โจมตีโดยการส่งสัญญาน TCP Reset โต้ตอบกลับไปหรือจะสั่งการ Firewall เพื่อปรับเปลี่ยนกฎบางข้อเพื่อป้องกัน Packet อันตรายไม่ให้เข้ามาในเครือข่าย การทำงานของ IPS นั้นจะใช้หลักการ Inline คือจะนำ IPS เข้าไปวางไว้ขั้นกลางการส่งข้อมูล (โดยทั่วไปจะวางไว้หลัง Firewall)โดยจะไม่มีการกำหนด IP Address เอาไว้เพื่อป้องกันการโจมตี (front end) ซึ่งในกรณีนี้อาจเกิดข้อเสียตรงที่ว่าถ้า IPS เกิดมีปัญหาหรือ Block Packet ผิดพลาดอาจส่งผลต่อการทำงานได้ IPS สามารถแบ่งได้เป็นสองประเภทคือ Network Based Intrusion Prevention System (NIDS) คือ IPS ที่ได้รับการติดตั้งไว้ที่ส่วนหนึ่งของระบบเครือข่ายเพื่อป้องกันการบุกรุก และ Host Based Intrusion Prevention System (HIDS) คือซอฟท์แวร์ที่ติดตั้งเข้าไปที่เครื่อง Server เพื่อป้องกันการบุกรุกหรือการโจมตีต่างๆ ตัวอย่างของโปรแกรมประเภทนี้ก็คือ Antivirus, AntiSpyware เป็นต้น

ที่มา http://www.viruscom2.com/defence/intrusion-prevention-system.html Retrieved August, 25, 2010

เครื่องคอมพิวเตอร์ไคลเอนท์ก็จะติดต่อไปยังเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลางของเจ้าของผลิตภัณฑ์หรือโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันความเสียหายนั้น แล้วปล่อยให้เป็นหน้าที่ของส่วนกลางที่จะควบคุมและบริหารจัดการเรื่องมัลแวร์ให้ นอกจากนี้ยังจะต้องเป็นโปรแกรมที่มีคุณสมบัติในการตรวจจับมัลแวร์ได้ดีอีกด้วย

2. ความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองนักกฎหมาย

จากพัฒนาการทางเทคโนโลยีสารสนเทศโดยการนำมาประยุกต์ใช้และก่อให้เกิดประโยชน์มากมายแก่มนุษย์ แต่ขณะเดียวกันก็มีการนำเทคโนโลยีสารสนเทศไปใช้ในทางมิชอบซึ่งก่อให้เกิดความเสียหายหรือส่งผลกระทบอย่างร้ายแรงแก่สังคมเช่นกัน ทำให้เกิดภัยคุกคามในรูปแบบของอาชญากรรมที่เกิดจากการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด จึงทำให้มีการพัฒนา “กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law)” หรือที่บางประเทศเรียกว่า “กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางมิชอบ (Computer Misuse Law)” ขึ้น หรือในบางประเทศอาจต้องปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่ให้ทันต่อการกระทำความผิดดังกล่าวด้วย การกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์หรือการใช้คอมพิวเตอร์ในทางมิชอบขึ้นภายใต้ความเหมาะสมของแต่ละประเทศ ทั้งนี้ การบัญญัติกฎหมายเหล่านั้นก็อยู่ภายใต้หลักการและข้อเท็จจริงตามลักษณะของการกระทำความผิดหรือการก่อให้เกิดภยันตรายหรือความเสียหายอันเนื่องมาจากการก่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งอาจแบ่งออกได้เป็น 2 ลักษณะตามวัตถุหรือระบบที่ถูกกระทำคือ การกระทำต่อระบบคอมพิวเตอร์ (Computer System) และการกระทำต่อข้อมูลคอมพิวเตอร์ (Computer Data)

สำหรับความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองของนักกฎหมายนั้นก็อยู่ภายใต้หลักการและข้อเท็จจริงตามลักษณะของภัยคุมคามต่างๆ ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ตามที่นักคอมพิวเตอร์ได้รวบรวมและวิเคราะห์ไว้ ซึ่งลักษณะของการกระทำความผิดทางคอมพิวเตอร์มักเป็นการคุกคามหรือลักลอบเข้าไปในระบบหรือเจาะระบบโดยไม่ได้รับอนุญาตหรือโดยไม่มีอำนาจให้กระทำการดังกล่าวอันเทียบเคียงได้กับลักษณะการบุกรุกในทางกายภาพ หรือในบางกรณีอาจเป็นการเข้าไปโดยความยินยอมของเจ้าของคอมพิวเตอร์นั้น หรือบางกรณีอาจใช้เทคนิคหลอกล่อเพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป ซึ่งวิธีการเข้าไปเหล่านั้นมักมีการพัฒนาโปรแกรมคอมพิวเตอร์ในรูปแบบต่างๆ โดยกำหนดคำสั่งให้กระทำการใดๆ อันก่อให้เกิดความเสียหายหรือภยันตรายขึ้นได้ด้วย เช่น ไวรัสคอมพิวเตอร์ซึ่งสร้างขึ้นเพื่อทำลายระบบและมักมีการแพร่กระจายตัวได้ง่ายและรวดเร็ว หรือมัลแวร์ในรูปแบบอื่นๆ เป็นต้น

ทั้งนี้ นักกฎหมายได้นำข้อเท็จจริงที่รวบรวมจากภัยคุกคามหรือการลักลอบเข้าไปในระบบหรือการเจาะระบบโดยไม่ได้รับอนุญาตมาวิเคราะห์หาสาเหตุจนได้ข้อยุติแล้วจึงนำมาบัญญัติเป็นภาษากฎหมายเพื่อรองรับกับภัยคุมคามต่างๆ เหล่านั้นนั่นเอง

อย่างไรก็ตาม ในปัจจุบันมีหลายประเทศได้บัญญัติกฎหมายเพื่อใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องคอมพิวเตอร์ซึ่งรวมทั้งประเทศไทยด้วย เนื่องจากกฎหมายอาญาที่มีอยู่เดิมไม่สามารถใช้บังคับได้ โดยบางประเทศได้บัญญัติเป็นกฎหมายพิเศษ เช่น ประเทศอังกฤษ[45] มาเลเซีย[46] สิงคโปร์[47] เป็นต้น ส่วนบางประเทศได้ทำการแก้ไขกฎหมายเดิมที่มีอยู่ เช่น ประเทศเยอรมัน[48] ออสเตรเลีย[49] เป็นต้น และในบางประเทศอาจใช้ทั้งสองวิธีคือทั้งการปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่และบัญญัติเป็นกฎหมายพิเศษเพื่อการกำหนดฐานความผิดและบทกำหนดโทษขึ้นมาเป็นการเฉพาะเป็นเรื่องๆ ไป เช่น ประเทศญี่ปุ่น[50] เป็นต้น นอกจากนี้องค์การระหว่างประเทศหลายองค์การได้ตระหนักถึงความร้ายแรงของปัญหาอาชญากรรมทางคอมพิวเตอร์ จึงพยายามกำหนดแนวทางให้กับประเทศภาคีสมาชิกนำมาตรการที่กำหนดไปปฏิบัติ เช่น คณะมนตรีแห่งยุโรป (Council of Europe)[51] องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization

---

45 ประเทศอังกฤษมีกฎหมายการใช้คอมพิวเตอร์ในทางมิชอบคือ **Computer Misuse Act 1990**

46 มาเลเซียมีกฎหมายอาชญากรรมคอมพิวเตอร์คือ **Computer Crime Act 1997**

47 สิงคโปร์มีกฎหมายการใช้คอมพิวเตอร์ในทางมิชอบคือ **Computer Misuse Act**

48 ประเทศเยอรมันมีการแก้ไขประมวลกฎหมายอาญาเดิมคือ Penal Code เพื่อให้รองรับในส่วนของความผิดฐานฉ้อโกงทางคอมพิวเตอร์ (Sec. 263a - Computer fraud) การก่อวินาศกรรม (Sec. 303b - Computer sabotage) และการสอดแนมข้อมูล (Sec. 202a - Data spying)

49 ประเทศออสเตรเลียมีกฎหมายกลางของประเทศคือ **Computer Related Commonwealth Law**

50 ประเทศญี่ปุ่นมีทั้งกฎหมายเฉพาะสำหรับความผิดในการเข้าถึงโดยไม่มีอำนาจคือ **Unauthorized Computer Access Law 2000** และมีการแก้ไขประมวลกฎหมายอาญาเดิมคือ **Penal Code** เพื่อให้รองรับในส่วนของความผิดฐานการปลอมแปลงทางคอมพิวเตอร์(Section 161-2 Unlawful production of electronic-magnetic records) การทำให้เสียหายซึ่งข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ (Section 258 Destruction of official electronic-magnetic records) และการลักลอบดักข้อมูล (Section 234-2 Interference with business transaction by computer system)

51 1. RECOMMENDATION No. R (89) 9 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON COMPUTER-RELATED CRIME adopted by the Committee of Ministers on 13 September 1989

2. RECOMMENDATION No. R (95) 13 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES CONCERNING PROBLEMS OF CRIMINAL PROCEDURE LAW CONNECTED WITH INFORMATION TECHNOLOGY adopted by the Committee of Ministers on 11 September 1995

for Economic Corporation and Development : OECD)[52] สหประชาชาติ[53] (United Nations) เป็นต้น ทั้งนี้ คณะมนตรีแห่งยุโรปนั้นถือได้ว่าเป็นองค์การระหว่างประเทศที่โดดเด่นที่สุดในเรื่องเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ กล่าวคือ คณะมนตรีแห่งยุโรปได้เล็งเห็นถึงความสำคัญของอาชญากรรมทางคอมพิวเตอร์และได้เห็นชอบอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime)[54] ซึ่งเป็นอนุสัญญาเพื่อให้ประเทศภาคีสมาชิกบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์เป็นไปในแนวทางเดียวกันและใช้บังคับกับรูปแบบการกระทำความผิดทางอาญาที่เปลี่ยนไปมากที่สุด โดยมีเนื้อหาครอบคลุมการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ เช่น การฉ้อโกง (Computer-related Fraud) การปลอมแปลงเอกสาร (Computer-related Forgery) สื่อลามก (Offences related to child pornography) ทรัพย์สินทางปัญญา (Offence related to infringements of copyright and related rights) เป็นต้น

อนึ่ง แม้รูปแบบของการพัฒนากฎหมายในแต่ละประเทศจะหลากหลายแตกต่างกันไปบ้างแต่การกำหนดฐานความผิดหลักมักจะคล้ายคลึงกัน โดยคำนึงถึงลักษณะหรือพฤติการณ์ที่กระทำต่อคอมพิวเตอร์และการใช้คอมพิวเตอร์ในการกระทำความผิดเป็นสำคัญ กล่าวคือ ฐานความผิดในกฎหมายของแต่ละประเทศจะมุ่งไปในการคุ้มครองการกระทำต่อระบบคอมพิวเตอร์ (Computer System) ข้อมูลคอมพิวเตอร์ (Computer Data) และระบบเครือข่ายซึ่งใช้ในการติดต่อสื่อสาร (Computer Network) และมักจะมีมาตรการที่มุ่งไปในการป้องกันและปราบปรามการใช้ชุดคำสั่งไม่พึงประสงค์ในทางมิชอบรวมอยู่ด้วย ซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยก็มีการบัญญัติในลักษณะและทำนองเช่นนั้นด้วย

---

52 GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS 26 November 1992

53 International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime

54 สามารถอ่านรายละเอียดเกี่ยวกับอนุสัญญาเพิ่มเติมที่ http://conventions.coe.int/

3. ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายจากอดีตจนถึงปัจจุบันตามที่ได้รวบรวมและสืบค้นจากแหล่งข้อมูลต่างๆ ไม่ว่าจะเป็นการค้นคว้าจากหนังสือ บทความ เอกสารจากการสัมมนา เอกสารทางวิชาการ และเอกสารออนไลน์นั้น สามารถแยกตามคุณลักษณะหรือวัตถุประสงค์ในการใช้งานเป็นประเภทได้ ดังนี้

3.1 ไวรัสคอมพิวเตอร์ (Computer virus)

ไวรัสคอมพิวเตอร์ ซึ่งต่อไปผู้เขียนจะขอเรียกเพียงว่า “ไวรัส” เป็นโปรแกรมคอมพิวเตอร์ขนาดเล็กชนิดหนึ่งที่สามารถสำเนา (copy) ตัวเองแล้วเกาะติดและแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้อย่างรวดเร็วโดยมีวัตถุประสงค์ไปในทางที่ไม่ดี ความสามารถของไวรัสนั้นจะมีตั้งแต่การสร้างความรำคาญเล็กๆ น้อยๆ ไปจนถึงกระทั่งทำลายหรือล้างข้อมูลในฮาร์ดดิสก์ (Hard Disk) คำว่า “ไวรัส” นั้นอาจจะหมายถึงโปรแกรมอันตรายชนิดอื่นๆ ด้วย เช่น หนอนคอมพิวเตอร์ (Worm) ม้าโทรจัน (Trojan Horses) และสปายแวร์ (Spyware) เป็นต้น ทั้งนี้เพื่อให้เกิดความง่ายต่อการสื่อถึงโปรแกรมอันตรายต่างๆ เหล่านั้น ซึ่งความจริงแล้วควรจะใช้คำว่า “มัลแวร์ (Malware)”[55] อย่างไรก็ตาม ความหมายของไวรัสนั้นก็ขึ้นอยู่กับความตั้งใจของผู้พูดหรือกล่าวถึงว่าต้องการให้หมายถึงโปรแกรมอันตรายทุกชนิด (มัลแวร์) หรือหมายถึงเฉพาะโปรแกรมไวรัสจริงๆ เท่านั้น ถึงแม้ว่าไวรัสไม่ได้มีความหมายรวมถึงโปรแกรมมุ่งร้ายทั้งหมดแต่ความหมายจะครอบคลุมเพียงโปรแกรมที่สามารถแพร่กระจายตัวเองได้เท่านั้น ในบางครั้งก็มักจะทำให้เกิดความสับสนระหว่างไวรัสกับหนอนคอมพิวเตอร์และม้าโทรจัน ซึ่งความแตกต่างระหว่างไวรัสและหนอนคอมพิวเตอร์คือ หนอนคอมพิวเตอร์จะสามารถแพร่กระจายตัวเองไปได้โดยที่ไม่ต้องอาศัยพาหะ (Host) ในการแพร่กระจายแต่อย่างใด ส่วนไวรัสนั้นไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเองแต่ไวรัสมีความจำเป็นที่จะต้องอาศัยพาหะเพื่อที่จะอาศัยไปสู่เครื่องที่ยังไม่ติดไวรัสโดยมักจะแพร่กระจายผ่านทางระบบสื่อสารต่างๆ เช่น Floppy disk, แผ่นซีดี, USB drive หรือแม้แต่การทำไฟล์แชร์ (File share) ที่เปิดโอกาสให้เครื่องอื่นๆ เข้ามาดูหรือใช้ทรัพยากรประเภทไฟล์ในเครื่องของผู้เป็นเจ้าของได้ ปัจจุบันคนจำนวนมากสามารถที่จะเข้าถึงอินเทอร์เน็ตได้อย่างรวดเร็วและง่ายดาย ดังนั้นไวรัสจำนวนมากจึงได้ประโยชน์จากการใช้เครือข่ายอินเทอร์เน็ตในการแพร่กระจาย ตัวอย่างเช่น การแพร่กระจายผ่านการให้บริการในรูปแบบ

---

55 ธวัชชัย ชมศิริ, อ้างแล้วในเชิงอรรถที่ 43 หน้า 290

เวิลด์ไวด์เว็บ (World Wide Web : WWW), อีเมล์ (e-Mail), โปรแกรมสนทนา (Instant Messaging) หรือไฟล์แชร์ เป็นต้น

ไวรัสคอมพิวเตอร์ในปัจจุบันสามารถแพร่กระจายออกไปอย่างกว้างขวาง รวดเร็วและมีความรุนแรงในการทำลายล้างสูงกว่าในอดีต ส่วนม้าโทรจันนั้นเป็นโปรแกรมที่มีความสามารถในการเปิดแบ็คดอร์ (Backdoor)[56] และทำตัวเองให้เป็นโปรแกรมที่ดูไม่เป็นอันตรายในสายตาของระบบรักษาความปลอดภัยของคอมพิวเตอร์ สำหรับความแตกต่างระหว่างหนอนกับม้าโทรจันก็คือ หนอนจะมุ่งเน้นไปที่การทำให้เกิดอันตรายต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ส่วนม้าโทรจันนั้นถือเป็นโปรแกรมที่สอดคล้องกับการทำงานของคอมพิวเตอร์โดยไม่มีคำสั่งหรือการปฏิบัติการที่เป็นอันตรายต่อตัวคอมพิวเตอร์

อย่างไรก็ตาม ไวรัสบางชนิดได้รับการออกแบบมาเพื่อที่จะทำลายล้างคอมพิวเตอร์ด้วยการโจมตีโปรแกรม การลบไฟล์หรือแม้กระทั่งการเข้าไปแก้ไขข้อมูลต่างๆ ในฮาร์ดดิสก์ แต่ไวรัสบางชนิดไม่ได้ออกแบบมาเพื่อที่จะทำลายล้างแต่ได้รับการออกแบบมาอย่างง่ายๆ เพื่อทำสำเนาตัวเองแล้วแพร่กระจายไปเรื่อยๆ หรือบางทีอาจจะแสดงข้อความหรือวีดีโอ (video) เล็กๆ เพื่อก่อกวนหรืออาจสร้างปัญหาให้ถึงขึ้นที่ระบบปฏิบัติการคอมพิวเตอร์ล่มหรือปฏิเสธการทำงานได้ ทั้งนี้ ประเภทของไวรัสที่สามารถตรวจพบจากอดีตจนถึงปัจจุบัน ได้แก่

3.1.1 ไวรัสตั้งต้น (Germs)

ไวรัสตั้งต้น เป็นโปรแกรมไวรัสรุ่นแรกสุด ก่อนที่จะมีการแพร่กระจาย กล่าวคือ เป็นไวรัสที่ถูกคอมไพล์ (Compile หมายถึง การแปลภาษาคอมพิวเตอร์ที่มนุษย์เขียนขึ้นเป็นภาษาที่คอมพิวเตอร์เข้าใจโดยผ่านทางโปแกรมแปลโปรแกรมที่เรียกว่าคอมไพเลอร์ (Compiler))[57] ออกมาจากซอร์สโค้ด (Source Code หมายถึง รหัสต้นฉบับ, รหัสต้นทาง)[58] ในครั้งแรกซึ่งจะมีอยู่ในลักษณะพิเศษและไม่จำเป็นต้องมีไฟล์พาหะให้ฝังตัว

---

56 หมายถึง ทางลับสำหรับเข้าสู่โปรแกรมที่นักเขียนโปรแกรมมักจะกำหนดเป็นรหัสกันไว้ คนที่ไม่รู้รหัส (หรือทางเข้าประตูหลัง) จะเรียกใช้โปรแกรมนั้นไม่ได้ คล้ายๆ กับรหัสผ่าน (password) ที่มา http://guru.sanook.com/search/backdoor Retrieved August, 25, 2010

57 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 23

58 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 91

3.1.2 ไวรัสบูต (Boot viruses)[59]

ไวรัสประเภทนี้จะฝังตัวที่ส่วนเริ่มต้นของแผ่นดิสเก็ตหรือมาสเตอร์บูตเรคคอร์ด (boot record หมายถึง ส่วนที่มีการบันทึกข้อมูลเพื่อการปลุกเครื่องไว้)[60]ของฮาร์ดดิสก์ ส่งผลทำให้เครื่องคอมพิวเตอร์โหลดโปรแกรมไวรัสเข้าไปสู่หน่วยความจำก่อนในขณะเปิดเครื่องแทนที่จะโหลดระบบปฏิบัติการ ตัวอย่างของไวรัสประเภทนี้เช่น ไวรัสที่ชื่อว่า Form, Disk Killer, Michelangelo และ Stone เป็นต้น

3.1.3 ไวรัสโปรแกรม (Program viruses)

ไวรัสโปรแกรม เป็นไวรัสที่ฝังตัวเองไว้ในไฟล์โปรแกรมที่สามารถถูกเอ็กซิคิวต์ (Execute)[61] ได้ ซึ่งส่วนใหญ่จะเป็นไฟล์ที่มีนามสกุล .BIN, .COM, .EXE, .OVL, .DRV (driver) และ .SYS (device driver) เป็นต้น โดยโปรแกรมเหล่านี้จะถูกโหลดเข้าสู่หน่วยความจำในขณะเอ็กซิคิวต์ จึงส่งผลให้โหลดส่วนการทำงานของไวรัสเข้าไปด้วย ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า Sunday และ Cascade เป็นต้น

3.1.4 Multipartite viruses

เป็นไวรัสที่มีการทำงานหลากหลายรูปแบบ กล่าวคือ สามารถแพร่กระจายทางไฟล์ปกติและสามารถแพร่กระจายในส่วนของบูตเรคคอร์ดได้ เมื่อมีการเอ็กซิคิวต์ไฟล์ไวรัส ก็จะมีการคัดลอกตัวเองไปยังบูตเรคคอร์ด แต่เมื่อมีการบูตเครื่อง ครั้งต่อไปก็จะถูก

---

59 http://computer.yourdictionary.com/boot-virus “A virus written into the boot sectors of a floppy disk. A popular way to spread a virus when floppy disks were widely used, the boot virus relied on people forgetting to remove the last floppy they inserted when they turned the machine off. When turned back on, the machine read the boot sector program, which normally loads the operating system, but ran the infected program instead. Once infected, the boot virus replicated itself onto all subsequent floppies used in the machine. The Michelangelo virus was a famous boot virus that infected DOS computers on March 6th, Michelangelo's birthday. However, there has always been doubt whether the date was really on account of the celebrated artist and sculptor. See virus. An MS-DOS virus that infects the boot record program on hard disks and floppy disks or the master boot record on hard disks. The virus gets loaded into memory before MS-DOS and takes control of the computer, infecting any floppy disks subsequently accessed” Retrieved August, 25, 2010

60 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 15

61 ภาษาในวงการคอมพิวเตอร์นิยมเรียกว่า “รัน (run)” ส่วนราชบัณฑิตยสถาน ได้ให้ความหมายไว้ในศัพท์เทคโนโลยีสารสนเทศฉบับราชบัณฑิตยสถาน 2542 (กรุงเทพฯ อรุณการพิมพ์) หน้า 41 ว่า “กระทำการ”

โหลดเข้าไปยังหน่วยความจำและฝังตัวในไฟล์อื่นๆ ต่อไป ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า Invader, Flip และ Tequila เป็นต้น

3.1.5 Stealth viruses

ไวรัสเหล่านี้จะใช้เทคนิคเพื่อหลีกเลี่ยงการตรวจจับ โดยทั่วไปจะใช้วิธีการขัดขวาง (Interrupt) การทำงานของกระบวนการอ่านของระบบดิสก์โดยเมื่อไฟล์ที่ไม่มีไวรัสถูกอ่านขึ้นมาก็จะถูกแทรกส่วนโปรแกรมไวรัสเข้าไป (Read Stealth Virus) นอกจากนี้ยังมีไวรัสที่สามารถเปลี่ยนขนาดของไฟล์หรือไดเรกทรอรี่ของข้อมูล (Size Stealth Virus) เมื่อไวรัสทำงานจะทำการแทรกส่วนโปรแกรมไวรัสระหว่างการอ่านข้อมูล เช่นไวรัสมีขนาดข้อมูล 1,024 ไบต์ และไฟล์ข้อมูลเดิมมีขนาด 4,096 ไบต์ ขนาดของไฟล์ที่ถูกไวรัสฝังตัวก็จะมีขนาด (1,024 + 4,096) 5,120 ไบต์ ซึ่งขนาดไฟล์มีการเปลี่ยนแปลงและจะถูกตรวจจับได้ ดังนั้นไวรัสนี้จะเข้าขัดขวางการทำงานระบบของไดเรกทรอรี่ โดยการอ่านค่า 5,120 ไบต์ขึ้นมา และลบออกด้วยขนาดของตัวไวรัสเอง จากนั้นจึงส่งผลที่ได้ไปยังระบบเพื่อแสดงผลอีกครั้ง ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่ชื่อว่า Frodo, Joshi และ Whale เป็นต้น

3.1.6 Polymorphic viruses

เป็นไวรัสที่สามารถเข้ารหัสที่โค้ดของไวรัสด้วยค่าคีย์เฉพาะ ส่งผลทำให้การตรวจจับนั้นทำได้ยากมากยิ่งขึ้น ตัวอย่างของไวรัสประเภทนี้ เช่น Involuntary, Stimulate, Cascade, Phoenix, Evil, Proud และ Virus 101 เป็นต้น

3.1.7 Macro viruses

ไวรัสมาโครเป็นไวรัสที่สามารถติดไปกับไฟล์ต่างๆ ที่มีความสามารถในการใช้งานมาโครได้ เช่น ไฟล์เอกสารไมโครซอฟท์ออฟฟิศ (เช่น Word และ Excel เป็นต้น) เมื่อเปิดไฟล์เอกสารที่มีไวรัสมาโครฝังอยู่แล้ว ไวรัสมาโครจะแฝงตัวเข้าไปอยู่ในไฟล์เทมเพลตที่ชื่อ Normal.dot ซึ่งเป็นไฟล์ที่เอกสารทุกชิ้นต้องอ้างอิงถึง ตัวอย่างของไวรัสประเภทนี้ เช่น ไวรัสที่มีชื่อว่า DMV, Nuclear และ Word Concept เป็นต้น

3.1.8 Active X

ไวรัสประเภทนี้มุ่งโจมตีโดยอาศัยฟังก์ชั่นการทำงานของเว็บเบราเซอร์ที่อนุญาตให้รันโปรแกรมจากเว็บไซต์ได้อย่างอิสระ ตัวอย่างของไวรัสประเภทนี้เช่น ไวรัสที่ชื่อ JS.ActiveXComponent เป็นต้น

อนึ่ง ยังมีประวัติและความเป็นมาของไวรัสที่น่าสนใจอีกว่า ในปี ค.ศ. 1970 โปรแกรมเมอร์ชื่อ Bob Thomas ได้ทดลองเขียนโปรแกรมที่สามารถคัดลอกตัวเองไปสู่โปรแกรมอื่นบนคอมพิวเตอร์เครื่องอื่นในเน็ตเวิร์กของ ARPANET (Advenced Research Projects Agency

Network หมายถึง เครือข่ายสำนักงานโครงการวิจัยชั้นสูง)[62] ได้ โปรแกรมนี้จะแสดงข้อความออกมาว่า “I’m the Creeper, Catch me if you can!” การที่โปรแกรมนี้สามารถแพร่กระจายตัวเองได้ จึงถูกเรียกว่าเป็น “ไวรัสคอมพิวเตอร์” และจากข้อความที่มันแสดงออกมาทางหน้าจอไวรัสตัวนี้จึงมีชื่อเรียกว่า “ไวรัส Creeper” และถือเป็นไวรัสตัวแรก อย่างไรก็ตาม บางแหล่งข้อมูลก็เชื่อว่าไวรัสตัวแรกเกิดขึ้นก่อนปี ค.ศ. 1969 โดยทีมวิศวกรของ Bell Telephone Laboratories ที่ได้สร้างเกมชื่อว่า “Darwin” ที่ฝังตัวในหน่วยความจำ ทำสำเนาตัวเองได้ ซึ่งจุดประสงค์หลักของเกมนี้ก็คือ ทำลายโปรแกรมของคู่แข่งและครอบครองหน่วยความจำ

โปรแกรมไวรัสตัวแรกที่แพร่ตัวเองออกนอกห้องทดลองไปสู่โลกภายนอกได้คือ “Rother J” ซึ่งเขียนขึ้นโดย Richard Skrenta ในปี 1981 ไวรัสตัวนี้แพร่ตัวเองโดยการเกาะติดไปกับแผ่นฟล็อปปี้ดิสก์ ระบบปฏิบัติการ Apple DOS 3.3 ซึ่งในสมัยนั้นเน็ตเวิร์กหรืออินเทอร์เน็ตยังไม่แพร่หลาย ดังนั้นการถ่ายโอนโปรแกรมจึงต้องใช้วิธีการสำเนาหรือก๊อปปี้ (copy) จากแผ่นหนึ่งไปยังอีกแผ่นหนึ่ง ซึ่งหากแผ่นต้นฉบับมีไฟล์ใดไฟล์หนึ่งที่ติดไวรัสอยู่ก็จะทำให้ไวรัสมีโอกาสแพร่กระจายไปสู่แผ่นอื่นหรือคอมพิวเตอร์เครื่องอื่นได้

อย่างไรก็ตาม ยังมีไวรัส Brain ที่ถูกสร้างขึ้นเมื่อปี 1986 โดยโปรแกรมเมอร์อายุ 19 ปี ชาวปากีสถานชื่อ Basit Farooq และพี่ชายของเขาชื่อ Amjad ไวรัส Brain เป็นไวรัสคอมพิวเตอร์ตัวแรกที่เกาะบู๊ตเซคเตอร์ (ไวรัสตัวอื่นก่อนหน้านี้จะเกาะที่ไฟล์) กล่าวได้ว่าในยุค 1980-1990 ถือเป็นยุครุ่งเรืองของไวรัสที่เกาะติดไฟล์โปรแกรม (executable file) และบู๊ตเซคเตอร์ (boot sector) ในยุคนี้มีไวรัสใหม่ๆ ถูกเขียนออกมาจำนวนมาก การแพร่กระจายของไวรัสนอกจากจะติดมากับแผ่นฟล็อปปี้ดิสก์ที่สำเนาต่อๆ กันมาแล้ว ไวรัสยังสามารถติดมาจากไฟล์ที่ดาวน์โหลด (Download[63] หมายถึง บรรจุลง) จาก BBS (Bulletin Board System) ได้อีกด้วย

นอกจากนี้ ยังมีไวรัสที่เขียนโดยคนไทยในราวปี 1990 โดยเป็นไวรัสขนาด 512 ไบต์ ที่เขียนขึ้นด้วยภาษาแอสแซมบลีและติดต่อโดยเกาะที่บู๊ตเซคเตอร์ การทำงานของไวรัสตัวนี้คือ บังคับให้มีเสียงเพลงออกมาที่ลำโพงโดยเพลงที่ไวรัสตัวนี้เล่นออกมาเป็นเพลงไทยเดิมที่ชื่อ “ลาวดวงเดือน” จึงทำให้ไวรัสตัวนี้มีชื่อว่า “ไวรัสลาวดวงเดือน” และในราวๆ ปี 1995 ได้มีการค้นพบไวรัสที่เกาะติดไฟล์เอกสาร แทนที่จะติด executable file หรือ boot sector ไวรัสดังกล่าวถูกเรียกว่า “มาโครไวรัส (Macro virus)” มาโครไวรัสเป็นไวรัสประเภทหนึ่งที่ถูกเขียนขึ้นด้วยภาษาสคริปต์ที่รันภายใต้โปรแกรม Microsoft Word หรือ Microsoft Excel หลังจากนั้นก็พบว่ามีไวรัส

---

62 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 7

63 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 33

ประเภทสคริปต์ถูกเขียนออกมาเป็นจำนวนมากรวมทั้งไวรัสที่โด่งดังอย่างไวรัส “I Love You” ซึ่งถูกเขียนขึ้นมาด้วยภาษาคอมพิวเตอร์ที่ชื่อ VB Script ในปี 2000

3.2 ม้าโทรจัน (Trojan Horses)

ม้าโทรจันเป็นโปรแกรมที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบคอมพิวเตอร์และจะทำงานโดยการดักจับเอารหัสผ่านต่างๆ หรือข้อมูลจากปุ่มของคีย์บอร์ดที่ถูกกดในเครื่องคอมพิวเตอร์ที่ถูกม้าโทรจันฝังตัวไว้ แล้วส่งกลับไปยังผู้โจมตีเพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ม้าโทรจันบางตัวยังสามารถจะดาวน์โหลดและติดตั้งภัยคุกคามอื่นๆเพิ่มเติมได้อีก จึงทำให้ผู้โจมตีได้ข้อมูลส่วนบุคคลต่างๆของเจ้าของเครื่อง เช่น ชื่อ รหัสผ่าน หมายเลขบัญชีธนาคาร รวมทั้งหมายเลขบัตรเครดิต ไป แต่ตัวม้าโทรจันเองจะไม่ได้ทำอันตรายใดๆ ต่อระบบ ม้าโทรจันสามารถแฝงตัวเข้ามาได้ในหลายรูปแบบ เช่น เกม การ์ดอวยพร หรือจดหมายต่างๆ เป็นต้น

อย่างไรก็ตาม ด้วยความที่ม้าโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ ม้าโทรจันจึงแตกต่างจากไวรัสและหนอน กล่าวคือ ม้าโทรจันจะไม่สามารถทำสำเนาตัวเองและแพร่กระจายตัวเองได้ แต่สามารถที่จะอาศัยตัวกลางซึ่งอาจเป็นโปรแกรมต่างๆ จดหมาย หรือการไปดาวน์โหลดไฟล์จากแหล่งต่างๆ เมื่อเรียกใช้งานไฟล์เหล่านี้ ม้าโทรจันก็จะทำงานและจะเปิดช่องทางต่างๆ ให้ผู้บุกรุกเข้าโจมตีระบบได้ ประเภทของม้าโทรจัน ได้แก่ Backdoor และ Password-Stealing ตัวอย่างม้าโทรจันที่เป็นที่รู้จัก เช่น Backorifice, Downloader-EV, Pest Trap, Sub7 (SubSeven), Zbot, Fostrem, Swifi, Kuaiput, Bredolab, Ergrun, Keyloggers/Keystrokers และ Password Retrievers เป็นต้น

3.3 สปายแวร์ (Spyware)

สปายแวร์ เป็นโปรแกรมที่มีจุดมุ่งหมายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ ภายในเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งอยู่ และเทคนิคที่ใช้นั้นได้แก่ การดักข้อมูลที่ถูกกดปุ่มคีย์บอร์ด การบันทึกเว็บไซต์ที่เคยเข้าเยี่ยมชมมา หรือไฟล์เอกสารต่างๆ ที่อยู่ภายในเครื่อง เป็นต้น ตัวอย่างโปรแกรมประเภทนี้ เช่น CoolWebSearch เป็นต้น

สปายแวร์มีหลายประเภทนับตั้งแต่ประเภทที่เป็นคุกกี้จากการเข้าดูเว็บไซต์ จนกระทั่งถึงประเภทที่เป็นโปรแกรมซึ่งล่วงล้ำเข้าไปในเครื่องคอมพิวเตอร์ของผู้ใช้เพื่อรายงานข้อมูลกลับไปยังผู้ผลิตว่าผู้ใช้ใช้งานโปรแกรมที่ติดตั้งนั้นอย่างไร โปรแกรมที่ล่วงล้ำนี้โดยทั่วไปจะเป็นซอฟต์แวร์ที่ผู้ใช้ดาวน์โหลดมาจากอินเทอร์เน็ตและติดตั้งเพื่อใช้งานในจุดประสงค์หนึ่ง และผู้ผลิตซอฟต์แวร์นั้นก็ย่อมจะต้องการทราบลักษณะการใช้งานของผู้ใช้เพื่อใช้เป็นข้อมูลในการปรับปรุงซอฟต์แวร์ของตนต่อไป จึงล่วงละเมิดผู้ใช้โดยแอบติดตั้งโปรแกรมในส่วนของการรายงานผลกลับไปยังผู้ผลิตด้วย

3.4 หนอนคอมพิวเตอร์ (Worm)

หนอนคอมพิวเตอร์ ซึ่งต่อไปผู้เขียนจะเรียกเพียงว่า “หนอน” เป็นโปรแกรมประยุกต์ที่ไม่จำเป็นต้องฝังตัวเองในไฟล์ที่เป็นพาหะและมีการแพร่กระจายตัวเองผ่านระบบเครือข่าย โดยทั่วไปแล้วหนอนจะเอ็กซิคิวต์ตัวมันเองบนเครื่องคอมพิวเตอร์ที่อยู่ในระยะไกลอย่างอัตโนมัติหรือถูกผู้ใช้งานเป็นผู้ทำการเอ็กซิคิวต์เองก็ได้ ซึ่งจะทำให้สามารถแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก ซึ่งหนอนสามารถแบ่งแยกย่อยออกไปได้อีก ดังนี้

3.4.1 หนอนอีเมล์ (Email Worms)

หนอนอีเมล์ หรือมีอีกชื่อว่า Mass-Mailers Worm เป็นหนอนที่สามารถแพร่กระจายตัวเองโดยอาศัยอีเมล์ ซึ่งอาจจะใช้การส่งเนื้อหาที่เป็นลิ้งค์ (Link[64] หมายถึง เชื่อมโยง, โยง) ให้ดาวน์โหลดไฟล์หนอนจากบางเว็บไซต์ หรืออาจจะแนบไฟล์ของหนอนในรูปแบบของเอกสารที่แนบมาพร้อมกับอีเมล์ ตัวอย่างของหนอนชนิดนี้ เช่น หนอนในตระกูล Mydoom, Netsky และ Bagle เป็นต้น

3.4.2 Instant Messaging Worms

เป็นหนอนที่แพร่กระจายโดยการส่งลิ้งค์หรือไฟล์ของหนอนไปกับข้อความที่ถูกส่งในโปรแกรมประเภท instant messaging (อันได้แก่ MSN, Yahoo หรือ ICQ เป็นต้น) ไปให้กับผู้อื่นที่มีรายชื่ออยู่ในเครื่องที่ถูกหนอนประเภทนี้คุกคาม ตัวอย่างของหนอนชนิดนี้ เช่น หนอนตระกูล Bropia เป็นต้น

3.4.3 Internet Worms

เป็นหนอนที่จะสแกนไปทั่วทั้งระบบเครือข่ายเพื่อค้นหาเป้าหมายที่เป็นเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่มีช่องโหว่ จากนั้นก็จะพยายามทำการติดต่อเข้าควบคุมเครื่องดังกล่าว เปรียบเสมือนกับการได้ครอบครองเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายนั้น หรืออีกวิธีหนึ่งในการแพร่กระจายของหนอนชนิดนี้คือ หลังจากที่ค้นพบเครื่องคอมพิวเตอร์เป้าหมายที่ยังไม่ได้รับการซ่อมแซมช่องโหว่ ก็จะทำการส่งแพ็กเก็ต (Packet)[65]ที่เป็นไฟล์ของหนอนหรือไฟล์ที่ใช้ในการดาวน์โหลดหนอน ถ้าหากทำได้สำเร็จหนอนก็จะทำการเอ็กซิคิวต์ตัวเอง

---

64 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 60

65 แพ็คเก็ต (Packet) หมายถึง ข้อมูลจำนวนหนึ่งซึ่งถูกส่งไปบนเครือข่าย ซึ่งข้อมูลนี้จะประกอบด้วยสิ่งบ่งชี้ตัวตนของทั้งผู้ส่งและผู้รับ ข้อมูลควบคุมความผิดพลาด และตัวข้อความ ที่มา http://folding.stanford.edu/education/P.html Retrieved August, 30, 2010

และทำการส่งเช่นนี้อีกต่อๆ ไป ตัวอย่างของหนอนชนิดนี้ เช่น หนอนในตระกูล Blaster, Welchia และ Sasser เป็นต้น

3.4.4 IRC Worms

หนอนที่อาศัยช่องทางสำหรับการสนทนาผ่านอินเทอร์เน็ตทางพอร์ท (Port หมายถึง ช่องทางเข้า/ออก มีความหมายเหมือนกับ input/output port)[66] IRC (Internet Relay Chat หมายถึง การคุยผ่านอินเทอร์เน็ต (ไออาร์ซี))[67] ซึ่งกระบวนการแพร่กระจายนั้น หนอนจะทำการส่งไฟล์หนอนหรือลิ้งค์ของเว็บไซต์ที่ถูกหนอนฝังตัวอยู่ซึ่งวิธีการนี้จะไม่ค่อยมีผลกระทบมากนักเพราะว่าผู้รับจะต้องมีการยืนยันที่จะจัดเก็บและเปิดไฟล์นั้นก่อน ตัวอย่างของหนอนชนิดนี้ เช่น Aplore, Maldal, Gokar, Spester, Irok และ Nymph เป็นต้น

3.4.5 File-sharing Networks Worms

หนอนชนิดนี้จะใช้วิธีการคัดลอกตัวเองไปยังโฟลเดอร์ที่เปิดแชร์ไว้เหมือนกับเป็นโฟลเดอร์หนึ่งภายในเครื่องคอมพิวเตอร์ที่ถูกหนอนประเภทนี้คุกคาม โดยชื่อไฟล์ของหนอนนั้นดูเหมือนจะไม่มีอันตราย และในปัจจุบันหนอนประเภทนี้ก็สามารถอาศัยระบบเครือข่ายแบบ P2P[68] ในการแพร่กระจายได้อีกด้วย ตัวอย่างของหนอนชนิดนี้ เช่น หนอน Duload ที่แพร่กระจายผ่านเครือข่ายผู้ที่ใช้งานโปรแกรม KaZaA ซึ่งเป็นโปรแกรมช่วยในการแชร์ไฟล์แบบ P2P เป็นต้น

สำหรับประวัติความเป็นมาของหนอนนั้น ใน ปี ค.ศ. 1988 มีการค้นพบหนอนชื่อมอร์ริส (Morris) ที่ทำให้คอมพิวเตอร์จำนวนมากในสหรัฐอเมริกา รวมทั้งคอมพิวเตอร์ในศูนย์วิจัยขององค์การบริหารการบินและอวกาศแห่งชาติ (The National Aeronautics and Space Administration : NASA) ติดเชื้อไปด้วย และส่งผลกระทบให้การปฏิบัติงานหยุดชะงัก การระบาดครั้งนั้นทำให้เกิดความเสียหายเป็นมูลค่าราว 100 ล้านเหรียญสหรัฐ

---

66 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 79

67 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 55

68 เครือข่ายแบบนี้จะเก็บไฟล์และการเชื่อมต่อกับอุปกรณ์ต่างๆ ไว้ที่เครื่องคอมพิวเตอร์ของผู้ใช้แต่ละคน โดยไม่มีคอมพิวเตอร์ส่วนกลางที่ทำหน้าที่นี้ เรียกได้ว่าต่างคนต่างเก็บ ต่างคนต่างใช้ แต่ผู้ใช้ในเครือข่ายสามารถเรียกใช้ไฟล์จากคอมพิวเตอร์เครื่องอื่นได้ ถ้าคอมพิวเตอร์เครื่องนั้นทำการแชร์ไฟล์เหล่านั้นไว้ เครือข่ายแบบ Peer-to-Peer นี้เหมาะสำหรับองค์กรขนาดเล็กที่มีคอมพิวเตอร์เชื่อมต่อกันไม่เกิน 10 เครื่อง เนื่องจากติดตั้งง่าย ราคาไม่แพง และการดูแลไม่ยุ่งยากนัก ที่มา http://www3.ipst.ac.th/research/assets/web/mahidol/computer(10)/network/ net_nettype10.htm Retrieved August, 30, 2010

3.5 แอดแวร์ (Adware)

แอดแวร์ เป็นโปรแกรมหรือซอฟต์แวร์แบบซ่อนตัวอีกชนิดหนึ่งที่มีรูปแบบการทำงานและการติดเชื้อคล้ายกับสปายแวร์มาก ต่างกันตรงที่สปายแวร์จะเน้นในการขโมยข้อมูลแล้วส่งกลับไปยังเจ้าของสปายแวร์ ส่วนแอดแวร์จะเน้นที่การโฆษณา โดยจะแสดงหรือดาวน์โหลดโฆษณามายังเครื่องคอมพิวเตอร์หลังจากที่ถูกติดตั้งโปรแกรมนี้แล้ว หรือจะสร้างหน้าจอ Pop-up หรือการ์ตูนน่ารักต่างๆ เพื่อหลอกล่อให้เหยื่อเผลอคลิกเข้าไปยังเว็บไซต์ขายสินค้าในขณะที่มีการเรียกใช้งาน เช่น เว็บไซต์ขายภาพหรือวีดีโอโป๊ เว็บไซต์ของธุรกิจขายตรง เป็นต้น ทั้งนี้ แอดแวร์มักจะถูกแนบมากับอีเมล์ขยะ (spam mail) หรือโปรแกรมประเภทพักหน้าจอ (Screen Saver) โดยแอดแวร์สามารถทำงานได้โดยอัตโนมัติเมื่อเหยื่อเริ่มใช้งานหรือเข้าสู่อินเทอร์เน็ต ตัวอย่างแอดแวร์ เช่น TopMoxie, 123 Messenger, 180 Solutions เป็นต้น

3.6 โปรแกรมทดสอบช่องโหว่ (Exploits)

โปรแกรมทดสอบช่องโหว่ เป็นโปรแกรมที่ใช้ในการเจาะระบบคอมพิวเตอร์เพื่อให้ได้มาซึ่งสิทธิ์เพื่อควบคุมระบบดังกล่าวได้ ซึ่งจำเป็นจะต้องอาศัยการโจมตีผ่านทางช่องโหว่ของระบบด้วย แต่แฮกเกอร์ที่เรียกว่า “White hat” จะนำโปรแกรมประเภทนี้ไปใช้ในการ Penetration testing ซึ่งเป็นการทดสอบเจาะระบบคอมพิวเตอร์โดยที่มีการว่าจ้างจากเจ้าของระบบเพื่อค้นหาว่าในระบบนี้มีช่องโหว่หรือจุดอ่อนหรือไม่ ตัวอย่าง เช่น โปรแกรม zgv เป็นต้น

3.7 โปรแกรมเจาะระบบ (Auto-Rooters)

โปรแกรมประเภทนี้เป็นเครื่องมือในการเจาะระบบ เพื่อให้ได้มาซึ่งสิทธิ์เป็นผู้ดูแลระบบและสามารถควบคุมเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่เป็นเป้าหมายจากระยะไกลได้ โปรแกรมประเภทนี้ส่วนใหญ่จะถูกใช้โดยแฮกเกอร์ที่ไม่ดีหรือที่เรียกว่า “Script-Kiddie”

3.8 โปรแกรมดาวน์โหลดไวรัส (Virus Downloaders)

โปรแกรมดาวน์โหลดไวรัส เป็นโปรแกรมที่ถ้าถูกติดตั้งและถูกเอ็กซิคิวต์จะดาวน์โหลดโปรแกรมอื่นๆ ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์และระบบเครือข่ายจากเว็บไซต์หรือแหล่งอื่นๆ แล้วทำการรันโปรแกรมนั้นโดยอัตโนมัติด้วย ตัวอย่าง เช่น Luder.A เป็นต้น

3.9 โปรแกรมปล่อยไวรัส (Virus Droppers)

โปรแกรมปล่อยไวรัส เป็นโปรแกรมที่ใช้ในการปล่อยไวรัสจากโปรแกรมไวรัสเอง เมื่อเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งจะถูกดาวน์โหลดไฟล์ไวรัส หนอน หรือม้าโทรจันอื่นๆ มาไว้ในเครื่องคอมพิวเตอร์นั้นได้ ซึ่งโปรแกรมประเภทนี้อาจจะเป็นโปรแกรมธรรมดาที่แอบลักลอบดาวน์โหลดไวรัสมาหรืออาจจะมาพร้อมกับไวรัสหรือหนอนชนิดอื่นๆ ก็ได้ ตัวอย่าง เช่น หนอนที่ชื่อ Klez นั้นจะมีโปรแกรมนี้เพื่อดาวน์โหลดหนอนที่ชื่อ Elkern เป็นต้น

3.10 โปรแกรมฉีดไวรัส (Virus Injectors)

โปรแกรมฉีดไวรัส เป็นโปรแกรมที่คล้ายกับโปรแกรมปล่อยไวรัส (Droppers) แตกต่างกันที่โปรแกรมประเภทนี้จะทำการติดตั้งและโหลดส่วนของไวรัสไปไว้ในหน่วยความจำได้ เหมือนกับการฉีดไวรัสเข้าไปสู่หน่วยความจำ นอกจากนี้โปรแกรมประเภทนี้อาจจะฉีดไวรัสเข้าไปกับข้อมูลที่เคลื่อนที่อยู่ในระบบเครือข่ายคอมพิวเตอร์ได้ ตัวอย่างของหนอนหรือไวรัสที่มีลักษณะนี้ เช่น CodeRed ที่ใช้โปรแกรมนี้ในการทำสำเนาตัวเองและส่งออกไปในระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

3.11 โปรแกรมชุดสร้างไวรัส (Kits-Virus Generators)

นักเขียนไวรัสคอมพิวเตอร์ (Virus writers) ได้พัฒนาโปรแกรมชุดสร้างไวรัส เช่น Virus Creation Laboratory (VCL) หรือ PSMPC generator เป็นต้น เพื่อสร้างไวรัสตัวใหม่ๆ โดยอัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อให้สามารถสร้างไวรัสตัวใหม่ๆ และไม่จำเป็นต้องมีความรู้ด้านคอมพิวเตอร์มาก ตัวอย่างของไวรัสที่ถูกสร้างด้วยโปรแกรมชุดสร้างไวรัส เช่น VBS/VBSWG.J หรือเป็นที่รู้จักในชื่อของไวรัส Anna Kournikova ที่ถูกสร้างโดยเครื่องมือที่ชื่อ VBSWG ซึ่งผู้ที่สร้างไวรัสนี้ก็ถูกจับและถูกดำเนินการทางกฎหมายไปแล้ว เป็นต้น

3.12 โปรแกรมสำหรับส่งสแปม (Spammer Programs)

โปรแกรมประเภทนี้ส่วนมากมักถูกใช้เพื่อส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่างๆ ผ่านทางอีเมล์ โปรแกรมสนทนา (Instant Messaging) รวมทั้งอีเมล์และ SMS ในโทรศัพท์มือถืออีกด้วย

จุดมุ่งหมายของโปรแกรมประเภทนี้ก็เพื่อให้ผู้ส่งได้รับเงินจากผู้ที่ได้รับข้อความและเข้าเว็บไซต์ที่ปรากฏในข้อความ อีกทั้งโปรแกรมประเภทนี้ยังอาจถูกนำไปใช้ในการบุกรุกแบบฟิชชิ่ง (Phishing)[69] ส่งผลให้เหยื่อนั้นสูญเสียทรัพย์สินหรือข้อมูลส่วนตัว เช่น รหัสผ่าน หมายเลขบัตรเครดิต หมายเลขบัญชี เป็นต้น ตัวอย่างโปรแกรม เช่น Harvesters เป็นต้น

---

69 วิกิพีเดีย สารานุกรมเสรี.http://th.wikipedia.org/wiki/ ในวิทยาการคอมพิวเตอร์ “ฟิชชิ่ง” (อังกฤษ: phishing) คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล์หรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้ผู้ใช้ต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงค์ไปนั้น มักจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง phishing แผลงมาจากคำว่า fishing แปลว่าการตกปลา ซึ่งมีความหมายถึง การปล่อยให้ปลามากินเหยื่อที่ล่อไว้ Retrieved August, 25, 2010

3.13 โปรแกรมระเบิด (Bombs Programs)

โปรแกรมระเบิด เป็นโปรแกรมการทำงานที่ผู้โจมตีตั้งใจพัฒนาขึ้นมาเพื่อให้เกิดการทำงานผิดปกติขึ้น โดยจะแฝงอยู่ในโปรแกรมที่ใช้งานตามปกติ และจะกำหนดให้มีการทำงานภายใต้เงื่อนไขที่กำหนดไว้ เช่น Time Bomb เป็นโปรแกรมที่มีการตั้งเวลาให้ทำงานตามที่กำหนดเวลาไว้ หรือ Logic Bomb เป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใดๆ เกิดขึ้น ลักษณะที่พบ เช่น โปรแกรมจะถูกลบเองเมื่อถูกรันไปแล้ว 2-3 ครั้ง เป็นต้น

3.14 โปรแกรมโทรศัพท์อัตโนมัติ (Dialers Programs)

โปรแกรมโทรศัพท์อัตโนมัติหรือมีชื่อเรียกอีกว่า Porn dialer หากมีการติดตั้งโปรแกรมประเภทนี้ในเครื่องคอมพิวเตอร์ จะมีการต่อโทรศัพท์อัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อที่จะให้เหยื่อนั้นต้องจ่ายค่าโทรศัพท์ในอัตราที่แพงที่สุดหรือทำให้เสียค่าโทรศัพท์ระหว่างประเทศ ตัวอย่าง เช่น โปรแกรมที่ชื่อ Dialer เป็นต้น

3.15 โปรแกรมล้อกันเล่น (Joke Programs)

โปรแกรมประเภทนี้จัดได้ว่าเป็นโปรแกรมที่ไม่ได้ตั้งใจทำอันตรายต่อเครื่องหรือระบบโดยตรง หากเพียงแค่ต้องการก่อกวนหรือสร้างความรำคาญให้แก่ผู้ใช้งาน โดยการเข้าไปเปลี่ยนพฤติกรรมปกติของเครื่องคอมพิวเตอร์ เช่น หากโปรแกรมนี้เป็นสกรีนเซฟเวอร์ก็อาจจะทำการล็อกหน้าจอได้เองทั้งๆ ที่ผู้ใช้งานเองไม่ได้ปรับแต่งค่าให้ล็อก เป็นต้น

อย่างไรก็ตาม โปรแกรมนี้อาจทำอันตรายได้ในบางกรณี เช่น เมื่อทำการล็อกหน้าจอแต่ไม่ปลดล็อกให้ ดังนั้น อาจจะต้องปิดเครื่องคอมพิวเตอร์โดยที่ไม่ได้บันทึกงานไว้ก่อน ทำให้เกิดความเสียหายต่อผู้ใช้งานได้ เป็นต้น ตัวอย่างของโปรแกรมประเภทนี้ เช่น Joke.Train เป็นต้น

3.16 ฟลัดเดอร์ (Flooders)

แฮกเกอร์จะใช้โปรแกรมประเภทนี้ในการโจมตีระบบเครือข่ายเป้าหมายด้วยการส่งข้อมูลในปริมาณมหาศาลเพื่อทำให้เกิดความคับคั่งในระบบเครือข่าย ส่งผลให้เครือข่ายเป้าหมายไม่สามารถให้บริการต่อไปได้ เรียกการโจมตีประเภทนี้ว่า Denial of Service (DoS) ถ้าหากว่ามีเครื่องคอมพิวเตอร์ที่ถูกควบคุมและจะถูกใช้โจมตีแบบ DoS พร้อมกันหลายๆ เครื่องไปยังเป้าหมายเดียวกัน จะเรียกการโจมตีแบบนี้ว่า Distributed Denial of Service (DDoS)

3.17 รูทคิท (Rootkits)

รูทคิท เป็นชุดโปรแกรมเจาะระบบแบบพิเศษที่มักจะถูกใช้หลังจากแฮกเกอร์สามารถเจาะระบบเข้าไปได้สิทธิการควบคุมระบบนั้น จากนั้นก็จะติดตั้งโปรแกรมประเภทนี้โดยการดัดแปลงโปรแกรมใช้งานปกติหรือ Kernel ที่ถูกติดตั้งไว้อยู่แล้ว เพื่อหลอกให้ผู้ดูแลระบบ

ไม่ให้สังเกตเห็นไฟล์ผิดปกติที่ถูกสร้างโดยแฮกเกอร์ มีการทำงานอยู่สองแบบคือ User-Mode และ Kernel-Mode ตัวอย่างรูทคิท เช่น Adore เป็นต้น

ทั้งนี้ เพื่อให้เกิดความสะดวกและง่ายต่อการทำความเข้าใจเกี่ยวกับประเภทและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย จึงขอนำข้อมูลของชุดคำสั่งไม่พึงประสงค์ตามที่ได้กล่าวไปแล้วข้างต้นมาสรุปในรูปแบบของตารางเพื่อแยกแยะว่าชุดคำสั่งไม่พึงประสงค์ประเภทใดบ้างที่เมื่อถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว จะมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรืออาจไม่มีผลกระทบใดต่อข้อมูลคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์เลย เมื่อถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิด ดังรายละเอียดปรากฏตามภาพที่ 2.6 ต่อไปนี้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	การมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้		
	มีผล	ไม่มีผล	หมายเหตุเพิ่มเติม
1. ไวรัสคอมพิวเตอร์ (Computer Virus) เช่น ไวรัสตั้งต้น (Germs), Boot viruses, Program viruses, Multipartite viruses, Stealth viruses, Polymorphic viruses, Macro viruses, Active X เป็นต้น	✓		ไวรัสบางประเภทอาจมีพลานุภาพในการทำลายล้างอย่างมหาศาล แต่ไวรัสบางประเภทอาจเพียงแต่สร้างความรำคาญเล็กๆน้อยๆ ให้กับผู้ใช้เท่านั้น
2. ม้าโทรจัน (Trojan Horses) เช่น โปรแกรมดักข้อมูลผ่านปุ่มคีบอร์ด (Keylogger/Keystroker Generators), โปรแกรมจับรหัสผ่าน (Password Retrievers) เป็นต้น		✓	
3. สปายแวร์ (Spyware)		✓	
4. หนอนคอมพิวเตอร์ (Worm) เช่น Email worms, Instant Messaging worms, Internet worms, IRC worms, File-sharing Networks worms เป็นต้น	✓		
5. แอดแวร์ (Adware)	✓		
6. โปรแกรมทดสอบช่องโหว่ (Exploits)	✓		แม้จะส่งผลกระทบฯ แต่หากการทดสอบช่องโหว่โดยได้รับอนุญาตจากเจ้าของระบบก็ไม่ถือเป็นความผิด
7. โปรแกรมเจาะระบบ (Auto-Rooters)	✓		
8. โปรแกรมดาวน์โหลดไวรัส (Virus Downloaders)	✓		
9. โปรแกรมปล่อยไวรัส (Virus Droppers)	✓		
10. โปรแกรมฉีดไวรัส(Virus Injectors)	✓		
11. โปรแกรมชุดสร้างไวรัส (Kits-Virus Generators)	✓		
12. โปรแกรมสำหรับส่งสแปม (Spammer Programs)	✓		
13. โปรแกรมระเบิด (Bombs Programs)	✓		
14. โปรแกรมโทรศัพท์อัตโนมัติ (Dialers Programs)	✓		
15. โปรแกรมล้อกันเล่น (Joke Programs)	✓		
16. ฟลัดเดอร์ (Flooders)	✓		
17. รูทคิท (Rootkit)	✓		

ภาพที่ 2.6 ตารางสรุปคุณสมบัติของชุดคำสั่งไม่พึงประสงค์และการมีผลกระทบต่อข้อมูลคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เมื่อถูกนำไปใช้ในการกระทำความผิด

จากข้อมูลที่ปรากฏในตารางที่ 2.6 ข้างต้น สามารถสรุปได้ว่า ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายเมื่อถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้วจะไม่มีผลกระทบต่อข้อมูลคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ นั้นได้แก่ ม้าโทรจัน และสปายแวร์

4. วงจรชีวิตของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

เมื่อได้ศึกษาและทราบถึงความหมายและคุณลักษณะ ตลอดจนประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายแล้ว จำเป็นต้องรู้จักวงจรชีวิตของชุดคำสั่งไม่พึงประสงค์ดังกล่าวตั้งแต่ การกำเนิด การแพร่เชื้อ การโจมตีระบบ และการถูกกำจัด เพื่อการรู้จักชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายอย่างลึกซึ้งซึ่งจะนำไปสู่การค้นคว้าและหามาตรการที่เหมาะสมในการจัดการกับชุดคำสั่งไม่พึงประสงค์ต่อไป ทั้งนี้ จากการศึกษาพบว่าชุดคำสั่งไม่พึงประสงค์จะมีวงจรชีวิตเหมือนเฉกเช่นสิ่งมีชีวิตที่เกิดขึ้นเองตามธรรมชาติโดยทั่วไป แต่มีความแตกต่างและข้อจำกัดในเกณฑ์บางประการ โดยชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายมีจรชีวิต ดังนี้

4.1 การกำเนิด

ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายตามที่ได้กล่าวถึงไปแล้วไม่ว่าจะเป็นไวรัสและมัลแวร์ชนิดต่างๆ นั้น ไม่ได้เกิดขึ้นมาเองตามธรรมชาติ แต่เกิดขึ้นมาจากนักเขียนโปรแกรมคอมพิวเตอร์ฝีมือดีที่เขียนโปรแกรมขึ้นมาเพื่อจุดประสงค์ที่แตกต่างกันออกไป เช่น เพื่อลองวิชา เพื่อทดสอบความรู้ของตนเอง เพื่อกลั่นแกล้งแบบสนุกๆ หรือเพื่อมุ่งร้ายต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ เช่น ขโมยข้อมูล ทำลายข้อมูล ทำให้ระบบทำงานช้าลงหรือเพื่อทำให้ระบบทำงานไม่ได้ การเขียนไวรัสคอมพิวเตอร์ในอดีตจะต้องเขียนด้วยภาษาแอสแซมบลีซึ่งเป็นภาษาคอมพิวเตอร์ชั้นต่ำ แต่ปัจจุบันสามารถเขียนด้วยภาษาคอมพิวเตอร์ชั้นสูงหรือเขียนด้วยสคริปต์รวมทั้งมีเครื่องมือช่วยในการพัฒนาไวรัส เป็นต้น ดังนั้น ไวรัสในยุคปัจจุบันจึงมีเป็นจำนวนมากและหลากหลายสายพันธุ์ ตามที่ได้กล่าวถึงโดยละเอียดไปแล้วในข้อ 3 ข้างต้น

4.2 การแพร่เชื้อ

การแพร่เชื้อของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายสามารถแยกได้ตามกลุ่มหรือประเภท กล่าวคือ หนอนสามารถแพร่เชื้อได้เองโดยอัตโนมัติ เช่น หนอนที่ชื่อ “SQL Slammer” ใช้ช่องโหว่ของโปรแกรม SQL Server ส่วนหนอนที่ชื่อ “Sasser” จะใช้ช่องโหว่ของระบบปฏิบัติการวินโดวส์ Windows และพอร์ทหมายเลข 445 เป็นต้น

สำหรับไวรัส ม้าโทรจัน สปายแวร์และแอดแวร์ จะแพร่กระจายได้โดยการที่เหยื่อรันโปรแกรมที่ติดไวรัส เช่น การคลิกรันที่ไฮเปอร์ลิงค์ (Hyper Link หมายถึง เชื่อมโยงหลายมิติ)[70] ต่างๆ โดยตรงเนื่องจากคิดว่าเป็นโปรแกรมที่ไม่มีอันตราย โดยโปรแกรมไวรัสจะได้มาจาก

---

[70] ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 52

โปรแกรมที่ดาวน์โหลดมาจากเว็บไซต์ที่ไม่น่าไว้วางใจ โปรแกรมที่ถูกแนบมากับอีเมล์ หรือโปรแกรมที่สำเนาหรือก๊อปปี้ต่อๆ กันมา นอกจากนั้นการแพร่ของไวรัสอาจจะมาจากการใช้ CD, DVD, แฟลชไดรว์ที่ติดไวรัสและไวรัสก็สามารถรันตัวเองโดยอัตโนมัติผ่านทางระบบ autorun ได้ ซึ่งไวรัสปัจจุบันมักจะใช้เทคนิค autorun นอกจากนั้นไวรัสบางชนิดที่มาในรูปของ ActiveX เช่น เวลาที่เข้าสู่เว็บไซต์บางแห่งแล้วมีข้อความขึ้นมาว่า “Install ActiveX” หากเว็บไซต์นั้นซ่อนไวรัสไว้ในโปรแกรม ActiveX ก็ทำให้เหยื่อติดไวรัสหรือม้าโทรจันได้ ไวรัสบางชนิดพยายามสแกนหาเครื่องเมล์เซิร์ฟเวอร์หรือเครื่องที่เผลอเปิด SMTP (Simple Mail Transfer Protocol หมายถึง เกณฑ์วิธีถ่ายโอนไปรษณีย์อย่างง่าย)[71] พอร์ท 25 ไว้ จากนั้นจึงส่งอีเมล์ไปยังผู้อื่นพร้อมแนบตัวเอง (ไวรัส) ไปด้วย

4.3 การโจมตีระบบ

การโจมตีระบบของชุดคำสั่งไม่พึงประสงค์แต่ละชนิดนั้นจะไม่เหมือนกัน ขึ้นอยู่กับว่าโปรแกรมเมอร์ผู้สร้างชุดคำสั่งไม่พึงประสงค์นั้นจะเขียนโปรแกรมไว้อย่างไร โดยส่วนมากแล้วหากเป็นหนอนจะโจมตีเพื่อทำให้ระบบใช้งานไม่ได้หรือทำงานช้าลงโดยส่งแพ็กเก็ตจำนวนมหาศาลออกไปยังเครือข่าย โดยหนอนจะทำงานเมื่อถึงเวลาที่ตั้งไว้ ส่วนการทำงานของม้าโทรจันจะมีการเปิดพอร์ทเพื่อรอรับคำสั่งจากแฮกเกอร์เพื่อเข้ามาควบคุมเครื่องที่ติดม้าโทรจันนั้นในภายหลังและเพื่อให้แฮกเกอร์ทำกิจกรรมบางอย่าง เช่น การค้นหาไฟล์สำคัญ การขโมยไฟล์ หรือการเปลี่ยนแปลงข้อมูลในไฟล์ต่างๆ เป็นต้น และหากเป็นสปายแวร์ก็จะเน้นไปที่การขโมยข้อมูลกลับไปยังเจ้าของ ส่วนแอดแวร์นั้นก็จะแสดงหน้าจอโฆษณา เป็นต้น ส่วนไวรัสหรือหนอนบางชนิดจะโจมตีโดยใช้โปรโตคอล ARP[72] โดยส่งแพ็กเก็ต ARP Poision ไปทั่วทั้งเน็ตเวิร์กเพื่อให้เครื่องไคลเอนต์[73]สร้างตาราง ARP ที่ผิดพลาดทำให้ไม่สามารถติดต่อกับเกตเวย์ได้ ซึ่งคล้ายกับการทำงานของโปรแกรม Netcut ที่จะทำให้ไม่สามารถใช้งานหรือออกสู่ระบบอินเทอร์เน็ตได้ จึงส่งผลให้เครื่องไคลเอนต์ไม่สามารถใช้งานอินเทอร์เน็ตได้ เป็นต้น

---

71 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 90

72 เป็นโปรโตคอลชนิดหนึ่งที่เป็นตัวกลางในการสื่อสารที่ทำหน้าที่หาแอดเดรสและจับคู่ระหว่างไอพีแอดเดรส ที่เชื่อมโยงเครือข่ายของระบบการขอหมายเลขไอพีแอดเดรสมาใช้บริการเพื่อให้สามารถสื่อสารกันระหว่างระบบเครือข่ายต่างๆได้ สามารถส่งข้อมูลระหว่างคอมพิวเตอร์ที่ติดต่อกัน โดยมีฮาร์ดแวร์สร้างเฟรมข้อมูลแล้วโปรโตคอล ARP จะนำข้อมุลเหล่านั้นเข้าที่เครื่อง host ในระบบเครือข่ายต่อไป

73 ไคลเอนต์ (Client) หมายถึง เครื่องคอมพิวเตอร์ที่สามารถใช้ข้อมูลร่วมกับเครื่องอื่นได้ โดยเครื่องจะทำงานเป็นอิสระและใช้โปรแกรมที่อยู่ในเครื่องนั้นเอง

4.4 การถูกกำจัด

กฎเกณฑ์ของธรรมชาติของสิ่งมีชีวิตทั่วไปในเรื่องการเกิด แก่ เจ็บ ตาย จะไม่สามารถนำมาใช้กับชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ได้ ดังนั้น คำกล่าวที่ว่า “เมื่อไวรัสแก่ตัวไปจนครบอายุขัย ก็จะตายไปเองตามธรรมชาติ” นั้นเป็นความคิดที่ผิด เนื่องจากไวรัสไม่ใช่สิ่งมีชีวิตเหมือนกับไวรัสในทางชีววิทยา เป็นต้น อย่างไรก็ตาม ไวรัสบางชนิดก็สามารถสูญพันธุ์ไปได้เอง แม้ว่าไม่ได้ถูกกำจัดหรือฆ่าโดยโปรแกรมแอนตี้และตรวจสอบไวรัส ตัวอย่างเช่น ไวรัสที่รันบน DOS ก็จะสูญพันธุ์ไปพร้อมกับระบบปฏิบัติการ DOS ที่ปัจจุบันไม่มีใครใช้งานแล้ว เป็นต้น แต่หากจะรอให้ไวรัสบน Windows ตายไปเองหรือเมื่อมีการเลิกใช้ Windows ก็คงจะต้องรอไปอีกนานแสนนาน ทั้งนี้ วิธีกำจัดหรือป้องกันชุดคำสั่งไม่พึงประสงค์ที่นิยมใช้กันนั้นมีอยู่ 2 วิธี ดังนี้

4.4.1 การกำจัดด้วยมือ

วิธีการจำกัดชุดคำสั่งไม่พึงประสงค์ด้วยมือ จัดเป็นวิธีกำจัดในยุคแรกๆ ที่มีการแพร่กระจายของชุดคำสั่งไม่พึงประสงค์ ซึ่งโดยทั่วไปมักจะใช้อยู่ในหมู่ผู้ที่มีความรู้หรือความเชี่ยวชาญทางคอมพิวเตอร์เป็นอย่างดี วิธีการกำจัดด้วยมือก็ เช่น การเข้าไปแก้ไขค่าในรีจิสทรีย์ (Registry)[74] ให้กลับคืนเหมือนเดิม และลบไฟล์ของชุดคำสั่งไม่พึงประสงค์โดยตรง เป็นต้น

อย่างไรก็ตาม เนื่องจากภัยคุกคามจากชุดคำสั่งไม่พึงประสงค์ในทุกวันนี้มีการเปลี่ยนแปลงและมีจำนวนของชุดคำสั่งไม่พึงประสงค์เพิ่มขึ้นอย่างรวดเร็ว โดยในเดือนมกราคม 2007 มีการตรวจพบชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ที่ไม่ซ้ำชนิดกันถึง 250,000 รายการ และในปี 2010 จำนวนมัลแวร์ใหม่ได้พุ่งขึ้นมาอยู่ที่ 286 ล้านรายการ[75] จึงอาจกล่าวได้ว่าอัตราการเพิ่มของมัลแวร์ชนิดใหม่ๆ ภายในรอบสามปีที่ผ่านมานั้นเพิ่มขึ้นเป็นพันเท่า ซึ่งเท่ากับว่ามีภัยคุกคามจากมัลแวร์เกิดขึ้นใหม่ในทุกๆ 9 วินาที เลยทีเดียว ด้วยเหตุนี้ จึงทำให้วิธีการกำจัดด้วยมือแม้จะถือว่าเป็นวิธีการที่ได้ผลดีแต่ก็ไม่คล่องตัวและไม่ทันการ จำเป็นต้องใช้วิธีตรวจจับที่รวดเร็วและสามารถทำได้ง่ายขึ้น นั่นก็คือการใช้โปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์

---

74 Registry คือฐานข้อมูลส่วนกลางที่ระบบปฏิบัติการวินโดวส์ใช้เพื่อเก็บค่าทุกอย่างของวินโดวส์ และโปรแกรมทั้งหมดที่อยู่บนเครื่องคอมพิวเตอร์ข้อมูลที่เก็บอยู่ในเครื่องจะมีตั้งแต่ค่าอุปกรณ์ฮาร์ดแวร์ไปจนถึงซอฟท์แวร์ทั้งหมด รวมถึงค่าที่กำหนดไว้ของผู้ใช้แต่ละคน เมื่อใดก็ตามที่มีการเปลี่ยนอุปกรณ์ หรือติดตั้งโปรแกรมใหม่ ข้อมูลในRegistry จะถูกเรียกใช้และแก้ไขค่าต่างๆ ตามไปด้วย Registryในเครื่องคอมพิวเตอร์จะถูกเก็บไว้ในฮาร์ดดิสก์ ซึ่งมีชื่อเรียกว่า "Registry Hive" Registryไม่ได้เก็บข้อมูลทั้งหมดไว้ในไฟล์ใหญ่ๆเพียงไฟล์เดียวแต่ในทางตรงกันข้ามจะแบ่งข้อมูลเป็นไฟล์ย่อยๆ เพื่อจะทำให้มีความยืดหยุ่นและปลอดภัยในการใช้งานวินโดวส์มากยิ่งขึ้น

75 บริษัท ไซแมนเทค (ประเทศไทย) จำกัด.“การปรับสมรรถนะการป้องกันให้ธุรกิจด้วยตนเอง” หน้า 1

4.4.2 การใช้โปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์

ด้วยเหตุที่จะต้องเผชิญกับภัยคุกคามจากชุดคำสั่งไม่พึงประสงค์ที่เพิ่มจำนวนขึ้นอย่างรวดเร็วและไม่มีวันสิ้นสุดในปัจจุบัน จึงส่งผลให้องค์กรต่างๆ โดยเฉพาะองค์กรในภาคธุรกิจที่กำลังเติบโตหันมาป้องกันภัยคุมคามดังกล่าวโดยการใช้โปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์แทนวิธีการกำจัดด้วยมือ ซึ่งวิธีการนี้นับเป็นวิธีการกำจัดที่ได้ผลดีและเป็นที่นิยมมากที่สุด ซึ่งวิธีการนี้สามารถทำได้โดยการติดตั้งโปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์ แล้วสั่งให้โปรแกรมทำงานตามตารางเวลาที่กำหนดไว้ โดยการสแกนหาและกำจัดชุดคำสั่งไม่พึงประสงค์ ซึ่งวิธีการกำจัดโดยการใช้โปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์นี้นอกจากจะสามารถกำจัดชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ได้แล้ว ยังช่วยป้องกันไม่ให้เครื่องคอมพิวเตอร์ติดมัลแวร์ซึ่งจะมีมาต่อไปได้อีกด้วย

5. เทคนิคและวิธีการตรวจจับชุดคำสั่งไม่พึงประสงค์

สำหรับเทคนิคและวิธีการที่ใช้ในการตรวจจับ เพื่อกำจัดชุดคำสั่งไม่พึงประสงค์โดยทั่วไปแล้วสามารถแบ่งได้เป็น 4 วิธีการ ดังนี้

5.1 การตรวจหา (Scanning)

เป็นการค้นหาไฟล์ที่ถูกชุดคำสั่งไม่พึงประสงค์แฝงตัวอยู่ เช่น ค้นหาในหน่วยความจำ ส่วนเริ่มต้นในการบู๊ต (Boot sector) และไฟล์ที่ถูกเก็บอยู่ในฮาร์ดดิสก์ โดยใช้หลักการเช็คซัม (Checksum)[76] ตัวตรวจตราจะคำนวณหาค่าเช็คซัมของแต่ละไฟล์แล้วนำไปเปรียบเทียบกับค่าเช็คซัมของไฟล์นั้นๆ

5.2 การตรวจสอบความคงอยู่หรือความครบถ้วนสมบูรณ์ (Integrity Checking)

เป็นการตรวจสอบความคงอยู่หรือความครบถ้วนสมบูรณ์ (Integrity Checker) ที่เก็บข้อมูลความคงอยู่ของไฟล์สำคัญไว้สำหรับเปรียบเทียบตัวอย่างข้อมูล เช่น ขนาดไฟล์ เวลาการแก้ไขครั้งล่าสุด เป็นต้น ซึ่งส่วนมากจะใช้ค่าของเช็คซัมในการเปรียบเทียบ เมื่อมีไฟล์เปลี่ยนแปลงที่มีสาเหตุอันเนื่องจากชุดคำสั่งไม่พึงประสงค์ หรือความผิดพลาดใดๆ จนทำให้ข้อมูลความคงอยู่ต่างจากข้อมูลเดิมที่เคยเก็บไว้ ก็จะทำให้ทราบถึงความผิดปกติที่เกิดขึ้น

---

[76] หลักการอย่างหนึ่งในทางพิสูจน์ความคงอยู่ของข้อมูลโดย เมื่อมีการเปลี่ยนแปลงอันอาจมีสาเหตุเนื่องจากไวรัสหรือความผิดพลาดใดๆ จนทำให้ค่าความคงอยู่ของข้อมูลต่างจากข้อมูลเดิมที่เคยเก็บไว้

5.3 การตรวจจับชุดคำสั่งไม่พึงประสงค์ด้วยการวิเคราะห์พฤติกรรม (Heuristic)

เป็นการเปรียบเทียบการทำงานของชุดคำสั่งไม่พึงประสงค์กับกฎ Heuristic (Rules Based System) โดยชุดของกฎ Heuristic ถูกพัฒนาให้สามารถแยกแยะพฤติกรรมการทำงานว่าเป็นการทำงานของชุดคำสั่งไม่พึงประสงค์หรือไม่ โดยเก็บข้อมูลของชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส ที่รู้จักเพื่อใช้ในการจับคู่แพทเทิร์น เป็นต้น ข้อดีของเทคนิคนี้คือ มีความยืดหยุ่นในการตรวจจับ และสามารถรู้จักชุดคำสั่งไม่พึงประสงค์ชนิดใหม่ๆ ได้เอง

5.4 การตรวจจับชุดคำสั่งไม่พึงประสงค์โดยการดักจับ (Interception)

มีลักษณะการทำงานโดยโปรแกรมต่อต้านและตรวจสอบชุดคำสั่งไม่พึงประสงค์จะสร้างเครื่องเสมือนที่มีลักษณะการทำงานเหมือนเครื่องที่กำลังทำงานอยู่ (virtual machine) แต่มีความอ่อนแอในการป้องกันขึ้นมาเพื่อคอยหลอกล่อให้ชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส เป็นฝ่ายโจมตีก่อน เป็นต้น จากนั้นก็จะเฝ้าดูว่ามีไวรัสหรือโปรแกรมใดบ้างที่มีพฤติกรรมน่าสงสัย ตัวอย่างเช่น มีโปรแกรมที่ติดตั้งตัวเอง รวมทั้งมีการส่งคำร้องขอ (request) ที่ผิดปกติออกมา ทำให้ตัวตรวจจับทราบได้ว่าโปรแกรมที่น่าสงสัยนี้เป็นไวรัสหรือชุดคำสั่งไม่พึงประสงค์อื่น เป็นต้น

6. รูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์

เนื่องจากการศึกษาและวิจัยเรื่องนี้จะมุ่งเน้นไปในทางการป้องกันหรือแก้ไขปัญหาจากภัยคุมคามหรือการโจมตีจากชุดคำสั่งไม่พึงประสงค์ ซึ่งเมื่อพิจารณาจากพฤติการณ์ของการกระทำความผิดดังกล่าวแล้วจะเห็นได้ว่ามีลักษณะเป็นการเข้าถึง (access) ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งในเชิงของการบุกรุกทางคอมพิวเตอร์ (computer trespass) หรือการเจาะเข้าไปในระบบ (Hacking or Cracking) และในเชิงของการดักข้อมูล (interception) ซึ่งผู้เขียนเห็นว่าการดักข้อมูลก็เป็นการเข้าถึงอีกรูปแบบหนึ่งด้วยเช่นกัน ทั้งนี้มีวิทยานิพนธ์ฉบับหนึ่งเห็นว่า การดักรับข้อมูลนั้นแท้จริงแล้วเป็นส่วนหนึ่งของการเข้าถึง กล่าวคือเป็นการทำให้ข้อมูลอยู่ในความครอบครองของผู้กระทำความผิด เพียงแต่การกำหนดฐานความผิดดักรับข้อมูลขึ้นมานั้นเป็นแสดงให้เห็นวิธีการกระทำความผิด[77] ดังนั้น รูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ในความเห็นของผู้เขียนจึงมีได้เฉพาะแต่การเข้าถึงทาง

---

77 ชาตรี ส่งสัมพันธ์, “อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ,” (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552), หน้า 70

อิเล็กทรอนิกส์เท่านั้น[78] ผู้เขียนจึงจะขอจำกัดขอบเขตและกล่าวถึงเฉพาะรูปแบบของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ทางอิเล็กทรอนิกส์ ทั้งนี้ จากการศึกษาถึงประเภท คุณลักษณะ ตลอดจนวงจรชีวิตของชุดคำสั่งไม่พึงประสงค์ตามที่ได้กล่าวไปแล้วในข้อ 3 และข้อ 4 ข้างต้น เมื่อนำข้อมูลที่ได้มาวิเคราะห์ถึงรูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ในปัจจุบันแล้วพบว่า ส่วนใหญ่ชุดคำสั่งไม่พึงประสงค์เหล่านั้นจะอาศัยช่องทางการโจมตีผ่านทางเครือข่ายอินเทอร์เน็ตเป็นสำคัญ จึงอาจกล่าวได้ว่าการโจมตีจากชุดคำสั่งไม่พึงประสงค์ในปัจจุบันถือเป็นภัยคุกคามหลักบนเครือข่ายอินเทอร์เน็ตอย่างแท้จริง[79] ซึ่งสามารถสรุปและแยกรูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้เป็น 2 รูปแบบด้วยกัน คือ การกระทำความผิดโดยการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และการกระทำความผิดโดยการดักข้อมูล

---

78 รูปแบบของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ สามารถแยกได้เป็นสองรูปแบบคือ การเข้าถึงทางกายภาพ เช่น การเข้าไป (inside) สัมผัสคอมพิวเตอร์และอุปกรณ์โดยตรง เป็นต้น และการเข้าถึงทางอิเล็กทรอนิกส์ เช่น การเจาะระบบเข้าไปตรงๆ หรือการส่งชุดคำสั่งไม่พึงประสงค์ไปฝังไว้ในระบบเพื่อการแอบขโมยข้อมูลหรือเพื่อประโยชน์ต่อการโจมตีในภายหลัง หรือการทำให้คอมพิวเตอร์มีการตอบสนอง (response) กับคำสั่ง เป็นต้น

79 บทความออนไลน์จาก http://noy198.multiply.com/journal/item/2/2 ซึ่งเป็นข้อมูลจากหนังสือ eLeader Thailand ประจำเดือนกุมภาพันธ์ 2551 ที่ได้สรุปภัยทางอินเทอร์เน็ตไว้เป็น 10 ประเภท แต่ผู้เขียนได้สรุปและเรียบเรียงเฉพาะภัยที่เกิดจากมัลแวร์แยกได้เป็น 4 ประเภท

6.1 การกระทำความผิดโดยการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

6.1.1 การขโมยเอกลักษณ์บุคคล (Identity Theft) ด้วยมัลแวร์[80]

ปัจจุบันการขโมยเอกลักษณ์บุคคล (Identity Theft) ด้วยมัลแวร์ได้เกิดขึ้นจริงแล้ว แต่ไม่รวมถึงการขโมยเอกลักษณ์บุคคลในรูปแบบการปลอมแปลงบัตรเครดิตหรือบัตรเอทีเอ็มซึ่งเป็นความผิดตามประมวลกฎหมายอาญา (ซึ่งจะได้กล่าวถึงต่อไปในบทที่ 4) อยู่แล้ว ทั้งนี้ ตามที่ปรากฏเป็นข่าวในรอบสองถึงสามปีที่ผ่านมานั้นพบว่า ประเทศไทยมีประชาชนได้รับความเสียหายเนื่องจากการขโมยเงินจากระบบอินเทอร์เน็ตแบงค์กิ้งหรือระบบการให้บริการธนาคารผ่านทางอินเทอร์เน็ตซึ่งส่วนใหญ่จะมีระบบเพื่อตรวจสอบการเข้าถึงโดยใช้เพียงชื่อผู้ใช้และรหัสผ่าน (User name and Password) เท่านั้น และแม้ว่าปัจจุบันธนาคารแห่งประเทศไทยในฐานะหน่วยงานของรัฐที่ทำหน้าที่กำกับดูแลธุรกิจธนาคารพาณิชย์จะได้ออกกฎหรือระเบียบเพื่อให้ธนาคารพาณิชย์ทุกธนาคารจะต้องมีกระบวนการในการตรวจสอบความปลอดภัยของระบบให้บริการแบบออนไลน์ของตนเองด้วยการทดสอบเจาะระบบของตนที่เรียกว่า "Penetration Testing" ก่อนการให้บริการกับประชาชนซึ่งถือว่าเป็นการบริหารความเสี่ยง (Risk Management) ที่ถูกต้องตามหลักวิชาการเพื่อป้องกันปัญหาการถูกขโมยเอกลักษณ์บุคคลหรือการถูกโจมตีระบบอินเทอร์เน็ตแบงค์กิ้งแล้วก็ตาม แต่ก็ยังปรากฏว่ามีการขโมยเอกลักษณ์บุคคลด้วยมัลแวร์ให้เห็นเป็นข่าวอยู่เป็นระยะ นอกจากนี้ยังมีธุรกิจอีกประเภทหนึ่งที่ตกเป็นเป้าหมายของบรรดาแฮกเกอร์โดย

---

[80] การขโมยเอกลักษณ์บุคคล (Identity Theft) คือ การที่ข้อมูลส่วนตัวของบุคคลถูกขโมยและนำไปใช้อย่างผิดกฎหมาย เช่น เพื่อเปิดบัญชีและซื้อสินค้าในชื่อของบุคคลนั้น เป็นต้น และบ่อยครั้งที่การโจรกรรมข้อมูลของบุคคลหรือของธุรกิจอาจถูกนำไปใช้เพื่อก่ออาชญากรรมอื่นๆ ต่อ เช่น การโกงบัตรเครดิต เป็นต้น ทั้งนี้ ศูนย์ Identity Theft Resource Center ซึ่งเป็นองค์กรที่ไม่แสวงหากำไร ได้แบ่งประเภทของการขโมยเอกลักษณ์บุคคลออกเป็น 4 ประเภท คือ

1. การขโมยเอกลักษณ์บุคคลทางการเงิน (Financial Identity Theft) ได้แก่ การใช้ชื่อของผู้อื่นและ SSN80 เพื่อให้ได้มาซึ่งสินค้าและการบริการ

2. การขโมยเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรม (Criminal Identity Theft) โดยทำทีว่าเป็นบุคคลอื่นเมื่อถูกสงสัยว่าได้ก่ออาชญากรรม

3. โคลนนิ่งเอกลักษณ์บุคคลของบุคคลอื่น (Identity Cloning) โดยการใช้ข้อมูลของผู้อื่น เพื่อให้เข้าใจว่าผู้ถูกปลอมแปลงเอกลักษณ์บุคคลนั้นเป็นผู้กระทำการด้วยตนเอง

4. การขโมยเอกลักษณ์บุคคลในทางการค้าและธุรกิจ (Business/Commercial Identity Theft) โดยการใช้ชื่อผู้อื่นเพื่อให้ได้มาซึ่งเครดิตต่าง ๆ

ที่มา https://www.paypal-apac.com/translation/th-s2/security-centre/identity-theft-guide-part1.html และ http://www.idtheftcenter.org/cresources.shtml Retrieved August, 29, 2010

การโจมตีในรูปแบบของการขโมยเอกลักษณ์บุคคลคือ ธุรกิจเกมออนไลน์ซึ่งเมื่อคนร้ายได้ชื่อผู้ใช้และรหัสผ่านของผู้เล่นเกมไปแล้วก็จะเข้าไปในเกมเพื่อขโมยทรัพย์สินภายในเกม เช่น การขโมยไอเท็มซึ่งถือเป็นทรัพย์สินของตัวละครต่างๆ แล้วนำทรัพย์สินดังกล่าวมาขายตามตลาดในโลกจริง ทำให้ผู้เล่นเกมได้รับความเสียหาย[81] เป็นต้น

หากวิเคราะห์ถึงพฤติกรรมในการขโมยเอกลักษณ์บุคคลดังกล่าวในปัจจุบันจะพบว่าแฮกเกอร์มักจะนิยมใช้มัลแวร์ในการกระทำความผิดโดยการเจาะระบบหรือการหลอกล่อด้วยการใช้เทคนิคต่างๆ โดยเฉพาะอย่างยิ่งในปัจจุบันแฮกเกอร์มักจะใช้เทคนิควิศวกรรมทางสังคม (Social Engineering technics)[82] ผ่านทางโปรแกรมเครือข่ายสังคมออนไลน์ (Social Networking) ต่างๆ เช่น Facebook Twitter Hi5 เป็นต้น ซึ่งการเข้าถึงโปรแกรมเครือข่ายสังคมออนไลน์เหล่านั้นก็สามารถเข้าถึงได้ง่ายทั้งทางเครื่องคอมพิวเตอร์และอุปกรณ์ชนิดพกพาต่างๆ ในทุกๆ ที่ และทุกๆ เวลา โดยการทำให้เหยื่อหลงเข้าใจผิดในเรื่องที่แฮกเกอร์ปลอมแปลงหรือปรุงแต่งขึ้นมาตามวัตถุประสงค์ที่จะให้เหยื่อทำตามในสิ่งที่แฮกเกอร์ได้กำหนดไว้ล่วงหน้า เช่น ให้เหยื่อเปิดไฟล์มัลแวร์ที่เป็นโปรแกรมประเภทม้าโทรจันหรือสปายแวร์ เป็นต้น ซึ่งปัจจุบันพบว่าแฮกเกอร์พยายามที่จะมุ่งเป้าหมายการโจมตีไปที่อุปกรณ์ชนิดพกพาและโทรศัพท์เคลื่อนที่มากขึ้น และหากผู้ใช้งานหรือเหยื่อหลงเชื่อโดยคิดว่าโปรแกรมที่ถูกส่งมาให้กับผู้ใช้งานผ่านทางอีเมล์โดยทำเป็นไฮเปอร์ลิงค์มากับอีเมล์หรือผ่านทางการดาวน์โหลดจากเว็บไซต์ต่างๆ ซึ่งส่วนใหญ่มักเป็นไฟล์นามสกุล .ZIP, .SCR และ .PIF รวมทั้งไฟล์นามสกุล .EXE และ .COM ด้วยนั้น เป็นโปรแกรมที่จะเป็นประโยชน์หรือเป็นโปรแกรมที่ผู้ใช้หรือเหยื่อกำลังอยากได้ ผู้ใช้งานหรือเหยื่อก็อาจคลิกไปยังไฮเปอร์ลิงค์หรือทำการดาวน์โหลดโปรแกรมตามที่แฮกเกอร์ได้จัดเตรียมไว้ ซึ่งจะแม้ว่าระบบคอมพิวเตอร์ของผู้ใช้งานหรือเหยื่อจะมีการติดตั้งระบบการรักษาความปลอดภัย เช่น Firewall หรือ

---

81 ผู้เขียนในฐานะนิติกรและนักกฎหมายไอทีของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้มีโอกาสตอบข้อหารือของสำนักงานคณะกรรมการคุ้มครองผู้บริโภคตามข้อร้องเรียนของประชาชนเกี่ยวกับตัวละครหรือไอเท็มในเกมออนไลน์อยู่เป็นระยะตั้งแต่ปี 2551 จนถึงปัจจุบัน ซึ่งส่วนใหญ่เรื่องที่สำนักงานคณะกรรมการคุ้มครองผู้บริโภคส่งมาหารือนั้นจะเป็นปัญหาเกี่ยวกับทรัพย์สินในเกมระหว่างผู้เล่นเกมกับผู้ให้บริการเกมออนไลน์

82 Social Engineering technics ในความหมายของแฮกเกอร์คือ การหลอกล่อและลงมือซึ่งอาศัยหลักการทางจิตวิทยาที่คนหมู่มากในสังคมส่วนใหญ่ให้การยอมรับและไว้วางใจ เมื่อแฮกเกอร์สามารถสร้างแรงจูงใจให้กับเป้าหมายได้ ขั้นต่อไปก็คือการทำให้เป้าหมายรู้สึกคล้อยตามและเอนเอียงจนในที่สุดก็ยอมรับในข้อเสนอที่อยู่ตรงหน้าอย่างง่ายดาย โดยอาศัยเทคโนโลยีเป็นเครื่องมือในการกระทำ

ที่มา http://www.arip.co.th/2006/blogs.php?g1=0&blogger=anantayut&id=406165 Retrieved August, 29, 2010

ชุดโปรแกรมตรวจจับและแอนตี้มัลแวร์ต่างๆ ไว้และถือเป็นการกำหนดให้มีมาตรการป้องกันการเข้าถึงไว้เป็นการเฉพาะแล้วก็ตาม หากผู้ใช้หรือเหยื่อยินยอมให้มัลแวร์ที่เป็นประเภทม้าโทรจันหรือสปายแวร์ฝังตัวลงไปในระบบคอมพิวเตอร์ของตน กรณีดังกล่าวจะถือเป็นการเข้าถึงโดยมิชอบโดยการฝ่าฝืนมาตรการป้องกันโดยเฉพาะที่มิได้มีไว้สำหรับตนหรือไม่ อย่างไร เนื่องจาก การให้ความยินยอมจากผู้ใช้หรือเหยื่อในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามกรณีดังกล่าวคงมิอาจถือได้ว่าเป็นการฝ่าฝืนมาตรการป้องกัน แต่เป็นกรณีของการเข้าถึงโดยความยินยอมของผู้ใช้หรือเหยื่อเอง ประกอบกับคุณสมบัติของมัลแวร์ประเภทม้าโทรจันและสปายแวร์นั้น ภายหลังจากที่เข้าถึงได้แล้วก็จะฝังตัวอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งานหรือเหยื่อโดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นที่อยู่ในระบบคอมพิวเตอร์นั้นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ และภายหลังจากนั้นแฮกเกอร์จะทำอะไรกับเครื่องคอมพิวเตอร์หรืออุปกรณ์ชนิดพกพานั้นก็ได้ เช่น การขโมยข้อมูลเอกลักษณ์บุคคล เป็นต้น ดังนั้น การเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว จึงไม่อาจถือเป็นความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์แต่อย่างใด

มีตัวอย่างคดีการเข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ตามกฎหมาย U.S.C. 1030 Fraud and Related Activity in connection with computers มาตรา (a)(1)-(3), 1030 (a)(5), 1028(7) ของประเทศสหรัฐอเมริกา ซึ่งผู้เขียนเห็นว่า เข้าข่ายเป็นการขโมยเอกลักษณ์บุคคล คดีนี้มีข้อเท็จจริงว่า นาย Vasiliy Gorshkov ชาวรัสเซีย อายุ 27 ปี และนาย Alexey V. Ivanov ชาวรัสเซีย อายุ 23 ปี ถูกจับกุมเมื่อวันที่ 11 พฤศจิกายน 2543 ในประเทศสหรัฐอเมริกาในระหว่างการเดินทางมาสัมภาษณ์เข้าทำงานในบริษัทเกี่ยวกับการรักษาความปลอดภัยด้านคอมพิวเตอร์ซึ่งเป็นบริษัทหน้าฉากที่ FBI ตั้งขึ้น โดยทั้งคู่ได้ทำการเข้าถึงระบบคอมพิวเตอร์ของบริษัทในสหรัฐอเมริกาจำนวนนับไม่ถ้วน ขโมยชื่อผู้ใช้งานและรหัสผ่าน ข้อมูลเกี่ยวกับบัตรเครดิต และข้อมูลการเงินอื่นๆ และทำการกรรโชกทรัพย์เจ้าของข้อมูล โดยขู่ว่าจะทำการเปิดเผยข้อมูลที่มีความสำคัญ ลบข้อมูล ทำลายระบบคอมพิวเตอร์ ซึ่งได้สร้างความเสียหายเป็นมูลค่าประมาณ 25 ล้านเหรียญสหรัฐ โดย นาย Vasiliy Gorshkov ถูกตัดสินจำคุก 36 เดือน และให้ชดใช้ค่าเสียหายเป็นจำนวนเงิน 700,000 เหรียญสหรัฐ และนาย Alexey V. Ivanov ถูกตัดสินจำคุก 48 เดือน

นอกจากนี้ ยังมีคดีตัวอย่างคดีที่เกี่ยวกับการขโมยเอกลักษณ์บุคคลที่เกิดขึ้นในประเทศอังกฤษ คือ คดี R v Seward (2005) EWCA Crim 1941[83] คดีนี้ จำเลยได้กระทำ

---

83 http://www.bailii.org/ew/cases/EWCA/Crim/2005/1941.html Retrieved August, 29, 2010

การในนามของบุคคลอื่นโดยใช้บัตรเครดิตและเอกสารอื่นๆ ที่ได้จากการขโมยไปในการซื้อสินค้า โดยสินค้าที่ซื้อนั้นมีมูลค่ารวมถึง 10,000 ปอนด์ ศาลอุทธรณ์พิจารณาตัดสินว่า การกระทำการหลอกลวงของจำเลยดังกล่าว เป็นการกระทำความผิดเกี่ยวกับการการขโมยเอกลักษณ์บุคคล (Identity Theft) และพิพากษาลงโทษจำคุกจำเลย

6.1.2 การโจมตีเครื่องคอมพิวเตอร์แม่ข่ายผ่านช่องโหว่ (Software flaws)

เนื่องจากข้อมูลขององค์กรส่วนใหญ่ในปัจจุบันจะถูกจัดเก็บในรูปแบบของไฟล์ข้อมูลที่อยู่ในรูปแบบดิจิทัล และถูกจัดเก็บไว้ในฮาร์ดดิสก์หรือสื่อทางด้านดิจิทัลต่างๆ ในเครื่องคอมพิวเตอร์แม่ข่าย จึงมีโอกาสถูกแฮกเกอร์หรือผู้บุกรุกโจมตีเพื่อทำให้เสียหายโดยการแอบทำสำเนาข้อมูลออกไปได้โดยง่าย และกลายเป็นปัญหาด้านความปลอดภัยของข้อมูล (Data Security) ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งปัจจุบันมักให้บริการในรูปแบบของโปรแกรมต่างๆ ผ่านเครือข่ายอินเทอร์เน็ตทั้งในรูปแบบเว็บเซิร์ฟเวอร์ (Web Server)[84] หรือเว็บแอพพลิเคชั่น (Web Application) สาเหตุที่เครื่องคอมพิวเตอร์แม่ข่ายถูกโจมตีจากชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ได้โดยง่ายก็เนื่องมาจากการเขียนโปรแกรมประเภทเว็บแอพพลิเคชั่นที่ไม่ปลอดภัยหรือมีช่องโหว่ ซึ่งอาจเป็นเพราะความรู้เท่าไม่ถึงการณ์หรือการขาดความตระหนักของโปรแกรมเมอร์ที่นิยมใช้ภาษาคอมพิวเตอร์ที่มีช่องโหว่ เช่น ASP (Active Server Pages)[85], JSP (Java Server Pages)[86]

---

84 Web Server หมายถึง เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ให้บริการเว็บ

85 ASP (Active Server Page) เป็นเทคโนโลยีที่ทำงานในฝั่งเซิร์ฟเวอร์โดยถูกออกแบบมาให้ง่ายต่อการพัฒนาแอพพลิเคชั่นผ่านเว็บเซิร์ฟเวอร์ การใช้งาน ASP สามารถกระทำได้โดยเขียนคำสั่งหรือสคริปต์ต่างๆ ในรูปของเท็กซ์ไฟล์ธรรมดาทั่วๆไป แล้วนำมาเก็บไว้ที่เซิร์ฟเวอร์ เมื่อมีการเรียกใช้งานจากบราวเซอร์ไฟล์เอกสาร ASP ก็จะถูกแปลโดยตัวแปลภาษาจากเซิร์ฟเวอร์ (Server Interpreter) แล้วส่งผลที่ได้ส่งกลับไปเป็นภาษา HTML ให้บราวเซอร์แสดงผลต่อไป

86 JSP เป็นภาษาสคริปต์อีกภาษาหนึ่งซึ่งเป็นทางเลือกที่น่าสนใจสำหรับการพัฒนาเว็บแอปพลิเคชั่น จุดเด่นที่สำคัญของ JSP อยู่ที่การใช้ภาษา Java ซึ่งเป็นเชิง OOP (Object Oriented Programming หมายถึงการเขียนโปรแกรมในเชิงวัตถุที่ให้ความสำคัญกับวัตถุ ซึ่งสามารถนำมาประกอบกันและนำมาทำงานรวมกันได้ โดยการแลกเปลี่ยนข่าวสารเพื่อนำมาประมวลผลและส่งข่าวสารที่ได้ไปให้วัตถุอื่นๆที่เกี่ยวข้องเพื่อให้ทำงานต่อไป) ที่ช่วยสามารถพัฒนาแอปพลิเคชั่นขนาดใหญ่และซับซ้อนได้อย่างสะดวกและรวดเร็ว

หรือ PHP (Professional Home Page)[87] โดยไม่มีการเพิ่มเติมมาตรการด้านความปลอดภัย (Application Security) เข้าไปที่ภาษาคอมพิวเตอร์เหล่านั้น ทำให้แฮกเกอร์หรือผู้บุกรุกที่มีความเชี่ยวชาญในการพัฒนาโปรแกรมเหล่านั้นรู้ช่องโหว่หรือปัญหานั้นด้วยเช่นกัน แฮกเกอร์หรือผู้บุกรุกจึงมักจะนิยมใช้ชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ในการเจาะระบบและโจมตีเครื่องคอมพิวเตอร์แม่ข่ายที่มี Web Application ที่เขียนด้วยภาษาดังกล่าวเหล่านั้นจนได้รับความเสียหาย ทั้งนี้ วัตถุประสงค์หลักๆ ของแฮกเกอร์หรือผู้บุกรุกก็คือการได้ไปซึ่งไฟล์ข้อมูลที่ถูกจัดเก็บไว้ในเครื่องคอมพิวเตอร์แม่ข่าย หรือในระบบจัดเก็บข้อมูลขนาดใหญ่ขององค์กรต่างๆ ไม่ว่าจะเป็นข้อมูลใน Database Server หรือในระบบ SAN[88] เป็นต้น

ทั้งนี้ โดยส่วนใหญ่แล้วการจะโจมตีเครื่องคอมพิวเตอร์แม่ข่ายใดๆ ได้สำเร็จย่อมเป็นผลมาจากช่องโหว่เล็กๆ น้อยๆ ที่มีอยู่ในซอฟต์แวร์ที่ใช้งานเป็นระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายนั้น ด้วยเหตุนี้เองแฮกเกอร์หรือผู้บุกรุกจึงเปรียบเสมือนผู้ฉวยโอกาสซึ่งนำช่องทางที่ง่ายและสะดวกที่สุดมาใช้ร่วมกับเครื่องมือโจมตีที่มีประสิทธิภาพและหาได้ทั่วไป

---

87 PHP เกิดในปี 1994 โดย Rasmus Lerdorf โปรแกรมเมอร์ชาวสหรัฐอเมริกาได้คิดค้นสร้างเครื่องมือที่ใช้ในการพัฒนาเว็บส่วนตัวโดยใช้ข้อดีของภาษา C และ Perl เรียกว่า Personal Home Page และได้สร้างส่วนติดต่อกับฐานข้อมูลชื่อว่า Form Interpreter (FI) รวมทั้งสองส่วน เรียกว่า PHP/FI ซึ่งก็เป็นจุดเริ่มต้นของ PHP ต่อมาผู้ขอนำไปพัฒนาต่อในลักษณะของ Open Source และได้รับความนิยมมากขึ้นโดย PHP เป็นภาษาสคริปต์ที่ประมวลผลที่ฝั่งเซิร์ฟเวอร์แล้วส่งผลลัพธ์ไปแสดงผลที่ฝั่งไคลเอ็นต์ผ่านบราวเซอร์เช่นเดียวกับ CGI และ ASP ต่อมาเมื่อมีผู้ใช้มากขึ้นจึงมีการร้องขอให้มีการพัฒนาประสิทธิภาพของ PHP/FI ให้สูงขึ้น Rasmus Lerdorf ได้ผู้ที่มาช่วยพัฒนาอีก 2 คนคือ Zeev Suraski และ Andi Gutmans ซึ่งเป็นชาวอิสราเอลโดยการปรับปรุงโค้ดของ Lerdorf ใหม่โดยใช้ C++ ต่อมาก็มีเพิ่มเข้ามาอีก 3 คน คือ Stig Bakken รับผิดชอบความสามารถในการติดต่อ Oracle, Shane Caraveo รับผิดชอบดูแล PHP บน Window 9x/NT, และ Jim Winstead รับผิดชอบการตรวจ ความบกพร่องต่างๆ และได้เปลี่ยนชื่อเป็น Professional Home Page ในปัจจุบัน ที่มา http://www.mindphp.com/modules.php?name=News&file=article&sid=92 Retrieved September, 11, 2010

88 SAN ย่อมาจาก Storage Attach Network มีที่มาจากแนวคิดที่ว่า ในอดีตนั้นการต่อ Storage (อุปกรณ์จัดเก็บข้อมูล) มีอยู่ 2 รูปแบบ คือ แบบแรกต่อเข้ากับ Network กลางโดยตรง โดยหากมีเครื่องคอมพิวเตอร์ไคลเอนต์ทำงานอยู่ในวงของ Network ด้วย ก็จะสามารถมองเห็น Storage ด้วย หรือ อีกแบบหนึ่งคือ การนำ Storage ต่อเข้าไปกับ Server แล้วจึงนำ Server นั้นต่อเข้าไปกับวงของ Network ซึ่งปัจจุบัน Storage นั้นมีขนาดใหญ่ขึ้นเรื่อยๆ การใช้งาน Network ในองค์กรก็มากขึ้นเรื่อยๆ ทำให้เกิดคอขวดของข้อมูล จึงเกิดแนวคิด ใหม่ขึ้น คือ SAN โดยมีหลักการที่สำคัญว่า ให้แยก Storage ออกมาจากวง Network โดยนำมาต่อไว้ข้างหลัง Server ซึ่ง Server หลายตัวก็จะต่อเข้ากับ Storage ผ่านเทคโนโลยี Fibre Channel (FC) ซึ่งมีความเร็วสูง จึงทำให้สามารถรับส่งข้อมูลผ่าน Network ได้ด้วยความเร็วสูงเหมือนการต่อเข้ากับ Network โดยตรง

อย่างเช่นชุดคำสั่งไม่พึงประสงค์ที่มีให้ดาวน์โหลดกันอย่างง่ายดายในปัจจุบัน เพื่อโจมตีจุดอ่อนของระบบซึ่งเป็นที่รู้จักอย่างแพร่หลาย แฮกเกอร์หรือผู้บุกรุกเหล่านั้นจะค้นหาว่ามีเครื่องคอมพิวเตอร์เครื่องใดยังไม่รับการแก้ไขช่องโหว่ โดยอาศัยการตรวจสอบด้วยการสแกนจากอินเทอร์เน็ตเพื่อหาช่องโหว่ที่ต้องการแล้วเข้าโจมตีโดยไม่สนใจว่า เครื่องคอมพิวเตอร์ดังกล่าวเป็นของใคร ทั้งนี้ กรณีการละเมิดเข้าใช้งานระบบในเหตุการณ์การบุกรุกเครือข่ายของ Solar Sunrise Pentagon ถือเป็นตัวอย่างที่เห็นได้ชัดเจน รวมถึงการแพร่กระจายอย่างรวดเร็วและง่ายดายของหนอนอินเทอร์เน็ตอย่าง Code Red และ NIMDA ซึ่งมีความสามารถในการค้นหาและบุกรุกผ่านช่องโหว่ เป็นต้น โดยสามารถแบ่งช่องโหว่ได้เป็น 2 กลุ่ม ตามชื่อของระบบปฏิบัติการที่ได้รับความนิยมในปัจจุบัน คือ ช่องโหว่สำคัญที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการ Windows และช่องโหว่สำคัญที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการ Unix ดังรายละเอียด ต่อไปนี้[89]

1) ช่องโหว่สำคัญที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการ Windows

ได้แก่

(1) Internet Information Services (IIS)

ก. การไม่สามารถจัดการกับการร้องขอที่ผิดจากธรรมดา (Failure to Handle Unanticipated Requests)

ช่องโหว่ของ IIS มากมายเกิดจากการที่ IIS ไม่สามารถจัดการกับการร้องขอ HTTP (HTTP requests) ที่ไม่ถูกต้อง ตัวอย่างของช่องโหว่ที่เป็นที่รู้จักกันดี คือ ช่องโหว่ Unicode directory traversal ซึ่งถูกใช้โดยหนอน Code Blue ในการเข้าใช้ช่องโหว่เหล่านี้ สิ่งที่ผู้โจมตีจากภายนอกอาจกระทำการ ได้แก่ เปิดดูซอร์สโค้ดของแอพพลิเคชั่น (Application)[90] ที่เป็นแบบสคริปต์, เปิดดูไฟล์ที่นอกเหนือจาก Web document root, เปิดดูไฟล์ที่เว็บเซิร์ฟเวอร์ไม่ได้ให้บริการ, สั่งคำสั่งใดๆ ก็ได้บนเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งทำให้เกิดความเสียหายตามมา เช่น การลบไฟล์สำคัญหรือการติดตั้งประตูหลัง (backdoor) เป็นต้น

ข. แอพพลิเคชั่นตัวอย่าง (Sample Application)

โดยทั่วไปแอพพลิเคชั่นตัวอย่างถูกออกแบบมาเพื่อใช้แสดงหน้าที่การทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและส่วนประกอบอื่นๆ ของเครื่องคอมพิวเตอร์

---

89 เรียบเรียงจากบทความ “20 ช่องโหว่สำคัญที่เป็นอันตรายร้ายแรงต่อความปลอดภัยของอินเทอร์เน็ต” ศิริวรรณ อภิสิริเดช และ มนัชยา ชมธวัช, เอกสารออนไลน์ เผยแพร่เมื่อ 28 ตุลาคม 2546 (กรุงเทพฯ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์, 2546). Retrieved June, 20, 2010

90 Application หมายถึง โปรแกรมหรือซอฟท์แวร์ประยุกต์

แม่ข่าย แต่ไม่ได้ถูกออกแบบมาเพื่อรับมือกับการโจมตีและไม่ได้ตั้งใจไว้ให้บริการเป็นแอพพลิเคชั่นที่ใช้งานจริง ประกอบกับความจริงที่ว่าการที่ค่าที่ตั้งมาโดยอัตโนมัติของแอพพลิเคชั่นนั้นเป็นที่รู้จักแพร่หลายอยู่แล้ว และซอร์สโค้ดก็มีพร้อมสำหรับให้ใครนำไปดูก็ได้ จึงทำให้ช่องโหว่นี้เป็นเป้าหมายหลักของการใช้ในการโจมตี ผลที่ตามมาอาจทำให้เกิดความเสียหายร้ายแรงได้ ตัวอย่าง เช่น แอพพลิเคชั่นตัวอย่างที่ชื่อ newdsn.exe จะอนุญาตให้ผู้โจมตีจากภายนอกสร้างหรือเขียนไฟล์โดยพลการบนเครื่องคอมพิวเตอร์แม่ข่ายได้, แอพพลิเคชั่นบางตัวอนุญาตให้ไฟล์ถูกเปิดได้จากภายนอก ซึ่งผู้โจมตีอาจใช้ในการรวบรวมข้อมูล เช่น ฐานข้อมูลของชื่อผู้ใช้ (userids) และรหัสผ่าน (passwords) ได้ หรือแอพพลิเคชั่น iisadmin ชื่อ ism.dll จะอนุญาตให้มีการเข้าถึงข้อมูลของระบบที่มีความสำคัญได้จากภายนอก รวมถึงรหัสผ่านของผู้ดูแลระบบด้วย

(2) Microsoft Data Access Components (MDAC) และ Remote Data Services (RDS) เป็นคอมโพเน้นต์ (component)[91] ในเวอร์ชั่นเก่าของ Microsoft Data Access Components (MDAC) มีช่องโหว่ที่อนุญาตให้ผู้ใช้จากภายนอกสามารถเรียกคำสั่งบนระบบได้ด้วยสิทธิในระดับของผู้ดูแลระบบ ประกอบกับช่องโหว่ใน Microsoft Jet database engine 3.5 ทำให้ช่องโหว่นี้อาจอนุญาตให้มีการเข้าถึงจากภายนอกแบบปิดบังชื่อ (anonymous external access) เข้าสู่ฐานข้อมูลภายในได้ ช่องโหว่เหล่านี้ได้ถูกค้นพบและมีวิธีแก้ไขเผยแพร่มานานหลายปีแล้ว แต่ระบบที่ได้รับการตั้งค่าผิดหรือล้าสมัยก็ยังคงมีความเสี่ยงต่อการถูกโจมตีได้ ระบบปฏิบัติการที่

---

91 คอมโพเน้นต์ (component) หมายถึง object ต่างๆที่นำมาใช้ประกอบในการสร้างแอพลิเคชั่นซึ่งคอมโพเน้นต์ส่วนใหญ่จะถูกจัดเก็บไว้ใน Component Palette โดยแยกเก็บเป็นหมวดหมู่ สำหรับนำไปประกอบกับแอพพลิเคชั่นที่สร้างขึ้น คอมโพเน้นต์จะถูกแยกออกเป็น 2 ประเภทดังนี้

Visual Component เป็นคอมโพเน้นต์ที่มีส่วนติดต่อกับผู้ใช้โดยจะแสดงให้เห็นในขณะที่รันแอพพลิเคชั่นเช่นข้อความหรือปุ่มต่างๆ

Non-Visual Component เป็นคอมโพเน้นต์ที่ไม่แสดงให้เห็นในขณะที่รันแอพพลิเคชั่น โดยจะเป็นไอคอนขนาดเล็กอยู่บนฟอร์มขณะออกแบบ เช่น MainMenu , PopupMenu

คอมโพเน้นต์ มีส่วนประกอบหลัก 3 ส่วน ได้แก่ Property Event Method โดยมีรายละเอียด ดังนี้

Property คือคุณสมบัติต่างๆ ที่ใช้ในการกำหนดลักษณะและการทำงานของคอมโพเน้นต์ จะมีลักษณะเฉพาะตัวที่เป็น Object เช่น ชื่อ ความกว้าง ความสูง เป็นต้น ใน Object ชนิดเดียวกันนั้นจะมี property อย่างเดียวกัน แต่อาจมีค่าของแต่ละ property แตกต่างกัน โดยผู้ใช้สามารถกำหนดค่าของ property ได้

Event คือเหตุการณ์หรือการกระทำที่เกิดขึ้นกับแต่ละ Object ซึ่งอาจเกิดจากผู้ใช้หรือการทำงานภายในแอพพลิเคชั่นเองก็ได้ เช่นเมื่อคลิกเมาส์ที่ปุ่มจะเกิดอีเวนต์ OnClick กับปุ่มนั้น เป็นต้น

Method คือโพรซีเยอร์หรือฟังชั่นการทำงานของคอมโพเน้นต์ หรืออาจจะกล่าวได้ว่า Method ก็คือความสามารถในการทำงานอย่างใดอย่างหนึ่งของแต่ละ Object

ได้รับผลกระทบ ได้แก่ ระบบ Microsoft Windows NT 4.0 ส่วนใหญ่ที่ใช้โปรแกรม IIS 3.0 หรือ 4.0, Remote Data Services 1.5, หรือ Visual Studio 6.0

(3) Microsoft SQL Server (MSSQL)

Microsoft SQL Server (MSSQL) ประกอบด้วยช่องโหว่อันตรายมากมายที่สามารถช่วยให้แฮกเกอร์หรือผู้โจมตีขโมยข้อมูลสำคัญ หรือเปลี่ยนแปลงข้อมูลในฐานข้อมูล หรือทำลายระบบเซิร์ฟเวอร์ของ SQL และค่าต่างๆ ที่ตั้งไว้ และทำลายเครื่องคอมพิวเตอร์แม่ข่ายได้ และถึงแม้ในปัจจุบันผู้ผลิตจะได้มีการเผยแพร่ให้สาธารณชนได้ทราบถึงช่องโหว่ของ MSSQL เหล่านี้แล้ว แต่ก็ยังมีการโจมตีช่องโหว่เหล่านี้ได้สำเร็จอยู่เสมอ แม้กระทั่งหนอน MSSQL ที่แพร่ระบาดก็ใช้ช่องโหว่ของ MSSQL ที่มีหลากหลายช่องโหว่ในการแพร่ระบาดเครื่องคอมพิวเตอร์แม่ข่ายต่างๆ ที่ถูกโจมตีด้วยหนอนชนิดนี้ได้ทำให้การรับส่งข้อมูลทางเครือข่ายเกิดความเสียหาย โดย Internet Storm Center[92] ได้บันทึกไว้ว่า พอร์ต 1433 (พอร์ตที่ MSSQL ใช้โดยอัตโนมัติ) เป็นหนึ่งในหลายๆ พอร์ตที่ถูกสแกนบ่อยที่สุด

แฮกเกอร์หรือผู้โจมตีสามารถฉวยโอกาสโดยใช้ SQLSnake[93] จากการที่ชื่อบัญชีของผู้ดูแลระบบที่ถูกตั้งมาโดยอัตโนมัติ (ชื่อบัญชี “sa”) ไม่มีรหัสผ่าน ดังนั้น จึงมีความจำเป็นที่จะต้องตั้งค่าให้เหมาะสมและปกป้องระบบใดๆ ให้เชื่อมั่นได้ว่าชื่อบัญชีและรหัสผ่านทั้งหมดของระบบได้รับการปกป้องหรือยกเลิกการใช้งานโดยสมบูรณ์กรณีที่ไม่ได้ใช้งาน นอกจากนี้ แฮกเกอร์หรือผู้โจมตีสามารถฉวยโอกาสโดยใช้ SQL Slammer จากการล้นของบัฟเฟอร์ของบริการ SQL Server Resolution เมื่อหนอนส่งแพ็กเก็ตโจมตีไปที่พอร์ต 1434/UDP ของเครื่องที่เป็นเป้าหมายซึ่งมีช่องโหว่อยู่จะทำให้บัฟเฟอร์ล้นและความปลอดภัยของเครื่องลดลง ถ้าเครื่องใดๆ เปิดบริการ SQL อยู่ก็มีความเสี่ยงที่จะเกิดการล้นของหน่วยความจำและได้รับแพ็กเก็ตดังกล่าว ซึ่งจะทำให้เกิดความเสียหายต่อระบบความปลอดภัยทั้งหมดของระบบและตัวของเครื่องคอมพิวเตอร์แม่ข่ายด้วย ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบ Microsoft Windows ที่ติดตั้ง Microsoft SQL Server 7.0, Microsoft SQL Server 2000 หรือ Microsoft SQL Server Desktop Engine 2000

(4) NETBIOS และ Unprotected Windows Networking Shares

---

92 เป็นโปรแกรมของสถาบัน SANS ซึ่งใช้เพื่อตรวจสอบระดับของกิจกรรมที่เป็นอันตรายบนเครือข่ายอินเทอร์เน็ต

93 SQLSnake เป็นโปรแกรมหรือชุดคำสั่งชนิดหนึ่งที่มีรูปแบบการทำงานตอบสนองกับผู้ใช้ในโหมดกราฟฟิก เพื่อใช้เป็นเครื่องมือในการติดต่อกับ MSSQL และจะมีเครื่องมือต่างๆ ให้เลือกใช้โดยที่ผู้ใช้งานไม่ต้องจดจำหรือพิมพ์คำสั่งของ MSSQL ซึ่งมีความยาวและยากต่อการจดจำ

Microsoft Windows สามารถเปิดให้ผู้ใช้ใช้ไฟล์หรือโฟลเดอร์ร่วมกันผ่านทางเครือข่ายโดยใช้ระบบ Windows network shares การร่วมกันใช้ไฟล์หรือโฟลเดอร์ดังกล่าวนี้กระทำโดยใช้โปรโตคอล Server Message Block (SMB) หรือ Common Internet File System (CIFS) โปรโตคอลเหล่านี้จะอนุญาตให้ผู้ใช้ที่อยู่บนเครื่องหนึ่งสามารถใช้ไฟล์ที่อยู่ในอีกเครื่องหนึ่งโดยเปรียบเสมือนว่าไฟล์นั้นอยู่ในเครื่องของผู้ใช้เอง ถึงแม้ว่าคุณสมบัตินี้จะอำนวยความสะดวกในการทำงานบนวินโดวส์ หากผู้ใช้ตั้งค่าของ network shares ไม่ถูกต้อง อาจจะทำให้มีการเปิดเผยไฟล์ของระบบที่มีความสำคัญได้ หรืออาจจะเป็นการเปิดโอกาสให้ผู้ใช้หรือชุดคำสั่งไม่พึงประสงค์สามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ได้ ซึ่งวิธีหนึ่งที่ไวรัส Sircam และหนอน Nimda ใช้ในการกระจายตัวอย่างรวดเร็วในช่วงฤดูร้อนของปี 2001 ก็คือโดยการค้นหาเครื่องที่ network shares ที่ไม่ได้รับการป้องกันแล้วทำการสำเนาตัวเอง เข้าไว้ในเครื่องนั้น จะเห็นได้ว่าแฮกเกอร์สามารถแอบบุกรุกเข้ามาในเครื่องคอมพิวเตอร์โดยที่เจ้าของไม่รู้ตัวได้ หากเจ้าของเครื่องเปิดบางไดร์ฟให้ผู้ใช้ในเครือข่ายมีสิทธิในการอ่าน (readable) และเขียน (writeable) ได้ แต่ถ้าเจ้าของเครื่องมีความระมัดระวังในการตั้งค่า network shares ให้ถูกต้องก็จะสามารถลดความเสี่ยงลงได้ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ Windows 95, Windows 98, Windows NT, Windows Me, Windows 2000, และ Windows XP ที่ล้วนแต่มีช่องโหว่นี้ทั้งสิ้น

(5) Anonymous Logon และ Null Sessions

การเชื่อมต่อแบบ Null Session เรียกอีกชื่อหนึ่งว่า Anonymous Logon เป็นกลไกที่อนุญาตให้ผู้ใช้ใดๆ สามารถดึงข้อมูล (เช่น ชื่อผู้ใช้และการแชร์) ผ่านทางเครือข่าย หรือสามารถเชื่อมต่อได้โดยไม่มีการพิสูจน์ตัวตน คุณสมบัตินี้ถูกใช้โดยแอพพลิเคชั่น เช่น Windows Explorer เพื่อใช้ระบุรายละเอียดการแชร์ในเครื่องคอมพิวเตอร์แม่ข่ายที่อยู่ต่างเครือข่ายกัน บนระบบ Windows NT, Windows 2000 และ Windows XP มีบริการต่างๆ ที่เปิดอยู่ภายใต้ SYSTEM account หรือที่รู้จักกันในชื่อ Local System บน Windows 2000 และ XP ซึ่ง SYSTEM account นี้ ถูกใช้ในทำงานที่สำคัญของระบบมากมาย เมื่อเครื่องหนึ่งต้องการดึงข้อมูลระบบ (system data) จากอีกเครื่องหนึ่ง SYSTEM account จะทำการเปิด null session ไปยังเครื่องนั้น SYSTEM account มีสิทธิพิเศษที่ไม่จำกัดและไม่มีรหัสผ่านดังนั้นโดยปกติแล้วจะไม่มีการอนุญาตให้สามารถล็อกออน (log on) เป็น System ได้ แต่บางครั้ง SYSTEM account ต้องการเข้าถึงข้อมูลบนเครื่องอื่นๆ เช่น แชร์ที่เปิดไว้ ชื่อ user และอื่นๆ ซึ่งเป็นคุณสมบัติของ Network Neighborhood แต่เนื่องจากไม่สามารถล็อกอินเข้าสู่ระบบอื่นๆ ได้โดยใช้ UserID และรหัสผ่าน จึงต้องใช้ Null session เพื่อเข้าถึงแทน ซึ่งผู้โจมตีก็สามารถล็อกอินเป็น Null Session ได้เช่นกัน

ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการทุกๆ ประเภทของ Microsoft Windows NT, 2000 และ XP

(6) LAN Manager Authentication และ Weak LM Hashing

ถึงแม้ว่าระบบ Windows ส่วนใหญ่ไม่มีความจำเป็นต้องใช้ LAN Manager (LM) แล้ว แต่ Microsoft ก็ได้ติดตั้งระบบ hash ของรหัสผ่านสำหรับ LM (LANMAN hashes) ไว้โดยอัตโนมัติบนระบบ Windows NT, Windows 2000 และ Windows XP เนื่องจาก LM ใช้โครงสร้างการเข้ารหัสที่อ่อนแอกว่าโครงสร้างการเข้ารหัสของ Microsoft ปัจจุบันซึ่งใช้ NTLM และ NTLMv2 จึงทำให้รหัสผ่าน LM สามารถถูกแคร็ก (crack) ได้ในเวลาอันสั้น แม้รหัสผ่านที่แข็งแกร่งก็สามารถถูกแคร็กโดยวิธี brute-force[94] ได้ภายใน 1 สัปดาห์ ทั้งนี้ ความอ่อนแอของ LM hashes เกิดจาก รหัสผ่านถูกตัดเป็น 14 ตัวอักษร หรือรหัสผ่านถูกเพิ่มช่องว่างจนมี 14 ตัวอักษร หรือรหัสผ่านถูกแปลงเป็นตัวอักษรตัวใหญ่ทั้งหมด หรือรหัสผ่านถูกแบ่งเป็น 2 ส่วนที่มี 7 ตัวอักษร

จะเห็นได้ว่ากระบวนการ hash ของ LM ดังที่กล่าวข้างต้นนั้นทำให้ผู้โจมตีต้องการเพียงเพื่อเจาะรหัสผ่านที่มีตัวอักษร 7 ตัว 2 ชุด และเป็นอักษรตัวใหญ่เพื่อเข้าถึงระบบได้โดยไม่ต้องพิสูจน์ตัวตน เนื่องจากความยากในการเจาะ hash จะเพิ่มขึ้นตามความยาวของ hash ดังนั้น กลุ่มตัวอักษร 7 ตัว 2 กลุ่มจะถูกโจมตีโดย brute-force ได้ง่ายกว่ากลุ่มสตริงที่ประกอบด้วยตัวอักษร 14 ตัว และเนื่องจากกลุ่มตัวอักษร 7 ตัว (รวมเว้นวรรคด้วย) นั้นเป็นตัวอักษรใหญ่ทั้งหมด ทำให้การโจมตีโดยใช้คำจากพจนานุกรม (dictionary attack) ก็ทำได้ง่ายเช่นกัน กระบวนการ hash ของ LM จึงทำให้นโยบายการตั้งรหัสผ่านที่ดีอ่อนแอลงได้ นอกจากความเสี่ยงที่เกิดจากการมี LM hashes แล้ว กระบวนการพิสูจน์ตัวตนของ LAN Manager (LAN Manager authentication process) ที่อ่อนแอมักถูกเปิดให้ทำงานบนเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แม่ข่ายจะยอมรับกระบวนการนั้นโดยอัตโนมัติ ผลที่ตามมาคือ เครื่องที่ใช้ hash algorithms ที่แข็งแกร่ง จะส่ง LM hashes ที่อ่อนแอผ่านเครือข่ายออกไปแทน LM hashes ที่แข็งแกร่ง ทำให้การพิสูจน์ตัวตนของเครื่องมีช่องโหว่และถูกดักจับแพ็คเก็ต (packet sniffing)

---

[94] การแคร็ก (crack) รหัสผ่านที่นิยมมีอยู่ 2 วิธี ได้แก่ การแคร็กแบบ Dictionary Attack ซึ่งจะใช้รหัสผ่านจากไฟล์ที่มีคำจำนวนมากจากพจนานุกรมรวมทั้งคำที่นิยมนำมาตั้งเป็นรหัสผ่าน และการแคร็กแบบ Brute force ซึ่งจะมีการส่งรหัสผ่านไปทีละตัวโดยให้รันตัวอักษรของรหัสผ่านตั้งแต่ A ถึง Z และ 0-9 (หรือรวมทั้งอักขณะพิเศษ) โดยบังคับจำนวนความยาวของรหัสผ่านตั้งแต่ 1 ตัวอักษรเรื่อยไปจนถึงความยาวที่กำหนดไว้ (ส่วนมากจะกำหนดไว้ไม่เกิน 8 ตัวอักษร) เช่น การส่งรหัสผ่านตั้งแต่ A,B, …,Z, 0, …,9 AA, AB, …AZ, A0, …,A9 เรื่อยไป เป็นต้น

ดังนั้นจึงทำให้ผู้โจมตีสามารถได้รับรหัสผ่านและสุ่มเดารหัสผ่านของผู้ใช้ได้โดยง่าย ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Microsoft Windows ทุกชนิด

(7) General Windows Authentication และ Accounts with No Passwords or Weak Passwords

รหัสผ่าน วลีรหัสผ่าน (passphrases) และโค้ดที่เกี่ยวข้องกับความปลอดภัยนั้นโดยปกติแล้วจะถูกนำมาใช้ในการสื่อสารกันระหว่างผู้ใช้กับระบบสารสนเทศ ซึ่งโดยทั่วไปแล้วระบบการพิสูจน์ตัวตนผู้ใช้ รวมถึงการเก็บรักษาข้อมูลหรือไฟล์ส่วนใหญ่จะเชื่อมั่นในค่ารหัสผ่านที่ได้รับจากผู้ใช้ เนื่องจากข้อมูลการเข้าถึงระบบโดยผ่านขั้นตอนการพิสูจน์ตัวตนตามที่ระบบกำหนดจะไม่ได้รับการบันทึกไว้เป็นหลักฐาน หรือหากบันทึกก็จะไม่บันทึกละเอียดถึงขั้นที่มีการบันทึกการเข้าถึงระบบที่ผิดพลาดไว้ ดังนั้นจึงอาจมีการนำรหัสผ่านที่ได้รับจากวิธีการที่ไม่ถูกต้องมาใช้ในการเข้าถึงข้อมูลระบบโดยที่ผู้ดูแลระบบไม่สามารถตรวจพบได้ ทั้งนี้ ตัวผู้บุกรุกจะได้สิทธิอย่างสมบูรณ์ในการเข้าใช้งานทรัพยากรที่เจ้าของรหัสผ่านตัวจริงสามารถใช้ได้ทั้งหมด และผู้บุกรุกจะพยายามขยายผลให้สามารถเข้าถึงบัญชีผู้ใช้คนอื่นๆ เครื่องคอมพิวเตอร์ที่อยู่ข้างเคียง รวมถึงพยายามให้ได้รับสิทธิเป็นผู้ดูแลระบบ ถึงแม้ว่าผู้ใช้ทุกคนจะทราบถึงความเสี่ยงนี้ แต่ก็ยังคงมีการใช้รหัสผ่านที่ไม่ดีพอหรือไม่มีการกำหนดรหัสผ่านอยู่

ช่องโหว่ของรหัสผ่านที่พบมากที่สุดได้แก่ บัญชีผู้ใช้ที่มีรหัสผ่านที่อ่อนแอหรือไม่มีรหัสผ่านเลย หรือผู้ใช้มักไม่เก็บซ่อนรหัสผ่านของตนเองไว้เป็นอย่างดี (ในที่นี้ไม่เกี่ยวกับเรื่องความแข็งแกร่งของรหัสผ่าน) หรือระบบปฏิบัติการหรือซอฟต์แวร์ที่ติดตั้งภายหลังสร้างชื่อบัญชีของผู้ดูแลระบบ (administrative accounts) โดยมีรหัสผ่านที่อ่อนแอหรือไม่มีรหัสผ่านเลย หรือลำดับวิธีของ password hashing เป็นที่รู้จักโดยทั่วไปและ hashes มักถูกเก็บไว้ในที่ที่มีผู้รับรู้และเห็นเสมอระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระปฏิบัติการทุกระบบหรือแอพพลิเคชั่นที่ผู้ใช้พิสูจน์ตัวตนโดยใช้ชื่อบัญชี (user ID) และรหัสผ่าน (password)

(8) Internet Explorer

Microsoft Internet Explorer (IE) เป็นโปรแกรมท่องเว็บ (browser) หรือเว็บบราวเซอร์ที่ติดตั้งอยู่แล้วบน Microsoft Windows ทุกๆ เวอร์ชั่นของ IE มีช่องโหว่ที่ร้ายแรง ซึ่งผู้ดูแลเว็บที่มีจุดประสงค์ร้ายสามารถออกแบบหน้าเว็บให้อาศัยช่องโหว่เหล่านี้บน IE ของผู้ใช้ขณะเปิดหน้าเว็บเหล่านี้ได้ช่องโหว่สามารถถูกแบ่งย่อยออกได้เป็นหลายชนิด ได้แก่ การปลอมแปลงหน้าเว็บ (web page spoofing) ช่องโหว่ของ ActiveX control ช่องโหว่ของ Active scripting ช่องโหว่ของการแปลที่ผิดพลาดสำหรับ MIME-type และ content-type และบัฟเฟอร์ล้น (buffer overflows) ผลที่ตามมาอาจทำให้เกิดการเปิดเผย cookies ไฟล์หรือข้อมูล

ภายในเครื่อง การสั่งให้โปรแกรมทำงานภายในเครื่อง การดาวน์โหลด และสั่งชุดคำสั่งไม่พึงประสงค์ให้ทำงานหรือการเข้าควบคุมระบบที่มีช่องโหว่ทั้งระบบ สำหรับระบบปฏิบัติการที่ได้รับผลกระทบช่องโหว่เหล่านี้มักจะพบได้ในระบบ Microsoft Windows ที่ใช้โปรแกรม Microsoft Internet Explorer เวอร์ชั่นใดๆ ก็ตาม สิ่งสำคัญที่ต้องคำนึงถึงคือ IE ถูกติดตั้งมากับซอฟท์แวร์ Microsoft หลากหลายชนิด ดังนั้น จึงปรากฏอยู่ในทุกระบบของ Windows แม้กระทั่งบนเครื่องคอมพิวเตอร์แม่ข่ายซึ่งไม่จำเป็นต้องใช้บราวเซอร์เลย

(9) Remote Registry Access

Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows ME และ Windows XP ใช้ฐานข้อมูลแบบ central hierarchical database หรือเรียกอีกชื่อหนึ่งว่า รีจิสทรีย์ (Registry) เพื่อควบคุมซอฟต์แวร์ การตั้งค่าอุปกรณ์และการตั้งค่าผู้ใช้ในระบบ หากสิทธิ์หรือการตั้งค่าความปลอดภัยที่ไม่เหมาะสมอาจทำให้เกิดการเข้าถึงรีจิสทรีย์จากนอกเครื่องได้ โดยผู้โจมตีสามารถใช้คุณสมบัตินี้ในการทำลายระบบหรือเปลี่ยนค่าการเชื่อมต่อและสิทธิ์การเข้าถึงไฟล์เพื่อการสั่งให้ชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ให้ทำงานได้ ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows ME และ Windows XP ทุกเวอร์ชั่น

(10) Windows Scripting Host (WSH)

ในปี 2000 "The Love Bug" (หรือที่รู้จักในชื่อ "I LOVEYOU") เป็นหนอนที่เกิดจาก Visual Basic script (VBScript) ซึ่งก่อให้เกิดความเสียหายถึงหลายล้านเหรียญสหรัฐ หนอนชนิดนี้และชนิดอื่นที่ออกตามมาได้ฉวยประโยชน์จาก Windows Scripting Host (WSH) ซึ่งอนุญาตให้ไฟล์ที่เป็นตัวหนังสือ (text file) ซึ่งมีนามสกุลเป็น ".vbs" สามารถถูกสั่งให้ทำงานเสมือนเป็น Visual Basic script การใช้ WSH นี้ทำให้หนอนแพร่กระจายโดยการรวมเอา VBScript ไว้เป็นส่วนหนึ่งของไฟล์และเริ่มทำงานเมื่อไฟล์ถูกเปิดหรือถูกพรีวิว (preview) ถึงแม้ว่าผู้ดูแลระบบจะทำการ patch และอัพเดตแอพพลิเคชั่นต่างๆ เช่น โปรแกรมท่องเว็บ (browser) โปรแกรมอ่านเมล์ (mail client) และแอพพลิเคชั่นอื่นๆ ก็ตาม การติดตั้ง patch เหล่านี้เพื่อกำจัดผลกระทบที่เกิดจากหนอนเหล่านี้ถือว่ายังไม่ใช่วิธีแก้ปัญหาความเสี่ยงจากการใช้สคริปต์ที่สมบูรณ์นัก ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ Windows 95, Windows NT, Windows 98, Windows ME, Windows 2000 และ Windows XP

2) ช่องโหว่สำคัญที่เป็นอันตรายต่อบริการบนระบบปฏิบัติการ Unix ได้แก่

(1) Remote Procedure Call (RPC)

Remote Procedure Call (RPC) เป็นบริการที่อนุญาตให้โปรแกรมที่ทำงานบนคอมพิวเตอร์เครื่องหนึ่งสามารถเรียกใช้งานโปรแกรมย่อย (Procedure) ที่คอมพิวเตอร์อีกเครื่องได้ โดยใช้การส่งข้อมูลไปยังเครื่องที่ต้องการและรับค่าผลลัพธ์ที่ได้กลับมา RPC ถูกนำไปใช้งานอย่างแพร่หลายร่วมกับบริการชนิดดิสทริบิวต์เน็ตเวิร์ก (Distribute Network) เช่น การดูแลระบบจากระยะไกล การแชร์ไฟล์ผ่าน NFS (Network File System) หรือ NIS (Network Information System) อย่างไรก็ตาม บริการ RPC มีข้อบกพร่องมากมายที่ผู้บุกรุกสามารถนำไปใช้ในการโจมตีระบบได้ โดยส่วนใหญ่แล้ว บริการ RPC ทำงานภายใต้สิทธิของผู้ดูแลระบบ (root) ผลที่จะตามมาก็คือ ระบบใดก็ตามที่ยังคงเปิดให้ใช้งานบริการ RPC ที่มีช่องโหว่สามารถจะถูกผู้บุกรุกนำไปใช้ในการเข้าถึงจากภายนอกด้วยสิทธิของผู้ดูแลระบบโดยไม่ได้รับอนุญาตได้ มีสถิติที่ชัดเจนแสดงให้เห็นว่า การโจมตีด้วยวิธี distributed denial of service (DDoS) ส่วนใหญ่ที่เกิดขึ้นระหว่างปี 2542 ถึงช่วงต้นปี 2543 เกิดขึ้นจากเครื่องถูกละเมิดการใช้งานผ่านช่องโหว่ของบริการ RPC การโจมตีที่เกิดขึ้นสำเร็จในวงกว้างเกิดขึ้นกับระบบของกองทัพสหรัฐอเมริการะหว่างเหตุการณ์ Solar Sunrise ของ Pentagon ซึ่งเกิดจากข้อบกพร่องของบริการ RPC ที่พบในระบบคอมพิวเตอร์จำนวนมากของกระทรวงกลาโหม ระบบปฏิบัติการที่ได้รับผลกระทบได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทุกเวอร์ชั่นที่ได้รับการติดตั้งบริการ RPC และมีการเปิดใช้งาน

(2) Apache Web Server

บ่อยครั้งที่ผู้ดูแลเว็บเซิร์ฟเวอร์ (Web Server) ลงความเห็นว่าโปรแกรม IIS ของไมโครซอฟท์มีแนวโน้มหรือความเสี่ยงต่อการถูกละเมิดการใช้งานมากกว่าโปรแกรมทั่วไป ในขณะที่ โปรแกรม Apache Web Server ซึ่งเป็นโปรแกรมชนิดโอเพนซอร์ส (Open Source) ที่สามารถทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ได้เช่นกันมีความปลอดภัยอย่างสมบูรณ์ ความคิดนี้อาจถูกต้อง หากนำระดับความปลอดภัยของโปรแกรม Apache ไปเปรียบเทียบกับโปรแกรม ISS ถึงแม้ว่า การทำงานของโปรแกรม Apache จะได้รับการยอมรับอย่างแพร่หลายในเรื่องของความปลอดภัย แต่เมื่อพิจารณาแล้วยังไม่สามารถพิสูจน์ได้ว่าโปรแกรม Apache เป็นโปรแกรมที่ปราศจากช่องโหว่ใดๆ ในอดีต ช่องทางโจมตีส่วนการทำงานหลักของโปรแกรม Apache หรือโมดูลของ Apache มีอยู่น้อยมาก แต่ในปัจจุบัน มีการค้นพบช่องโหว่ของโปรแกรม Apache รวมถึงโมดูลที่เกี่ยวข้องเพิ่มขึ้นอย่างรวดเร็ว และนำไปใช้ในการโจมตี ตัวอย่างล่าสุดได้แก่ Apache/mod_ssl Worm หรือ Apache Chunk Handling Exploit เป็นต้น

นอกจากนี้ ความปลอดภัยของเว็บเซิร์ฟเวอร์ยังต้องพิจารณาจากส่วนประกอบในการทำงานของแอพพลิเคชั่นต่างๆ ที่มีอยู่บนเว็บด้วย โดยเฉพาะโปรแกรม CGI

และฐานข้อมูล โปรแกรม Apache จำนวนมากที่ได้รับการปรับแต่งค่า configuration แล้วยังคงปล่อยให้เกิดการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตได้ผ่านทางสคริปต์ CGI ที่ไม่มีการตรวจสอบหรือการกำหนดการควบคุมการเข้าถึงฐานข้อมูลที่ไม่เหมาะสม การเรียกใช้งานสคริปต์ CGI จะทำด้วยสิทธิเดียวกับการทำงานของเว็บเซิร์ฟเวอร์ ดังนั้น ข้อบกพร่องข้อหนึ่งของโปรแกรม Apache คือทำให้สคริปต์ CGI ที่มีอันตรายต่อระบบหรือถูกเขียนอย่างไม่ถูกต้องสามารถทำอันตรายต่อเว็บเซิร์ฟเวอร์ได้ ซึ่งข้อบกพร่องนี้ยังคงเป็นปัญหามาจนถึงปัจจุบัน

ข้อสำคัญอีกข้อหนึ่งคือ การที่จะสามารถป้องกันไม่ให้ข้อมูลภายในเว็บถูกแก้ไขหรือขโมยได้นั้นจำเป็นต้องเริ่มตั้งแต่การสร้างความปลอดภัยให้กับระบบปฏิบัติการที่ใช้ ในความเป็นจริงแล้ว การสร้างความปลอดภัยให้กับระบบปฏิบัติการของเครื่องที่ทำงานเป็นเซิร์ฟเวอร์เป็นสิ่งจำเป็นไม่ว่าบริการบนเครื่องนั้นเป็นบริการใดก็ตาม แต่บริการของเว็บมักจะเปิดให้ภายนอกเข้าใช้งานซึ่งอาจทำให้เกิดอันตราย ดังนั้น ตัวบริการและข้อมูลต่างๆ ในเว็บควรถูกแยกเป็นอิสระออกจากส่วนอื่นๆ ของระบบ ระบบปฏิบัติการที่ได้รับผลกระทบได้แก่ ระบบปฏิบัติการ Linux เกือบทุกเวอร์ชั่น และระบบปฏิบัติการ Unix หลายเวอร์ชั่นที่ได้รับการติดตั้งโปรแกรม Apache และมีการเปิดใช้งาน

(3) Secure Shell (SSH)

Secure Shell (ssh) เป็นบริการที่นิยมใช้งานเพื่อให้เกิดความปลอดภัยในการล็อกอินเข้าสู่ระบบ การเรียกใช้งานคำสั่ง และการรับส่งไฟล์ข้ามเครือข่าย ระบบปฏิบัติการที่มีพื้นฐานมาจากระบบปฏิบัติการ Unix แทบทั้งหมดสามารถใช้งานได้ทั้ง OpenSSH ซึ่งเป็นแพ็กเก็ตชนิดโอเพนซอร์ส และเวอร์ชั่นทางการค้าของบริษัท SSH Communication Security ถึงแม้ว่าบริการ ssh จะมีความปลอดภัยมากกว่าการใช้งานโปรแกรม telnet, ftp และ R-commands ซึ่งเป็นโปรแกรมที่ ssh ถูกนำมาใช้ทดแทนอยู่มากก็ตาม การนำโปรแกรม ssh ทั้งสองแบบมาใช้งานยังทำให้เกิดจุดอ่อนขึ้นมากมายในระบบ จุดอ่อนเหล่านี้ ส่วนใหญ่เป็นข้อผิดพลาดเล็กๆ น้อยๆ ที่ไม่ส่งผลกระทบอย่างกว้างขวาง แต่มีบางจุดที่เป็นอันตรายต่อความปลอดภัยอย่างรุนแรงซึ่งควรได้รับการแก้ไขทันที อันตรายร้ายแรงที่สุดที่เกิดจากช่องโหว่ของบริการ ssh ที่เปิดใช้งานคือ การปล่อยให้ผู้แฮกเกอร์หรือบุกรุกเข้าโจมตีเพื่อให้ได้รับสิทธิเป็นผู้ดูแลระบบในการเข้าถึงเครื่องจากภายนอก

มีตัวอย่างที่แสดงให้เห็นอยู่ทั่วไปถึงช่องโหว่ที่เกิดขึ้นกับตัวโปรโตคอล SSH เวอร์ชัน 1 (SSH1) ในเรื่องของการเข้ารหัสระหว่างการสร้างการติดต่อ ซึ่งทำให้ผู้บุกรุกสามารถถอดรหัสข้อมูลที่ส่งภายใต้การทำงานที่กำหนดได้ ดังนั้น ผู้ดูแลระบบจึงควรเปลี่ยนมาใช้โปรโตคอล SSH เวอร์ชั่น 2 (SSH2) ซึ่งมีความปลอดภัยมากกว่าทันทีที่สามารถทำได้

นอกจากนั้น ผู้ที่ใช้งานแพ็กเก็ต OpenSSH ควรระลึกอยู่เสมอว่าไลบรารีของแพ็กเก็ต OpenSSL (เป็นแพ็กเก็ตที่ต้องติดตั้งร่วมกับ OpenSSH) อาจส่งผลกระทบต่อความปลอดภัยของ OpenSSH เนื่องจากช่องโหว่ของ OpenSSL เองด้วย และผู้ใช้จะต้องให้ความระมัดระวังถึงแพ็กเก็ต OpenSSH ในบางเวอร์ชั่นที่อาจถูกแฝงไว้ด้วยชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันแล้วนำมาเผยแพร่ในอินเทอร์เน็ต ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux ใดๆ ที่ใช้งานแพ็กเก็ต OpenSSH เวอร์ชั่น 3.3 หรือก่อนหน้านั้น หรือแพ็กเก็ต SSH ของบริษัท SSH Communication Security เวอร์ชั่น 3.0.0 หรือก่อนหน้านั้น

(4) Simple Network Management Protocol (SNMP)

Simple Network Managament Protocol (SNMP) ถูกนำมาใช้งานอย่างแพร่หลายในปัจจุบันเพื่อการเฝ้าตรวจและปรับแต่งค่าอุปกรณ์เกือบทุกชนิดที่สามารถทำงานผ่านโปรโตคอล TCP/IP ได้ โปรโตคอล SNMP ถูกนำไปใช้งานอย่างกว้างขวางและมีการทำงานข้ามแพลตฟอร์ม (Platform) ต่างๆ ของเครือข่าย ประโยชน์หลักของโปรโตคอล SNMP คือสามารถใช้เป็นวิธีการหนึ่งในการปรับแต่งการทำงานและจัดการอุปกรณ์ เช่น เครื่องพิมพ์ (Printer) เราท์เตอร์ (Router)[95] สวิตซ์ (Switch) เป็นต้น หรือใช้ในการส่งค่าอินพุต (Input) ไปยังบริการที่ทำหน้าที่เฝ้าตรวจเครือข่าย

การติดต่อแบบ Simple Network Management ประกอบด้วยการแลกเปลี่ยนข้อความที่มีรูปแบบต่างๆ ระหว่างเครื่องที่ทำหน้าที่บริหาร SNMP (SNMP management station) กับอุปกรณ์เครือข่ายซึ่งมีการเปิดใช้งานซอฟต์แวร์ชนิดที่นิยมเรียกว่าซอฟต์แวร์เอเจนต์ (agent software) วิธีการทำงานของโปรโตคอล SNMP ดังกล่าวนี้ทำให้เกิดช่องโหว่ซึ่งแฮกเกอร์หรือผู้บุกรุกสามารถนำไปใช้โจมตีได้ทั้งจากวิธีการจัดการข้อความที่ถูกส่ง และจากกลไกการพิสูจน์ตัวตนผู้ใช้งานในระหว่างการจัดการข้อความ ช่องโหว่ที่เกิดจากวิธีการซึ่งโปรโตคอล SNMP เวอร์ชั่น 1 จัดการและรอรับข้อความ ช่องโหว่ที่ปรากฏจำนวนหนึ่งเกิดจากวิธีการจัดการและการถอดรหัสในขั้นตอนของการร้องขอข้อมูลและการรอรับข้อความทั้งจากฝั่งเครื่องคอมพิวเตอร์ที่ทำหน้าที่บริหาร SNMP และฝั่งซอฟต์แวร์เอเจนต์ ช่องโหว่เหล่านี้มิได้เกิดขึ้นเมื่อนำโปรโตคอล

---

95 เราท์เตอร์ (router) เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายหลายระบบเข้าด้วยกัน คล้ายกับบริดจ์ แต่มีส่วนการทำงานที่ซับซ้อนมากกว่าบริดจ์มาก โดยเราท์เตอร์จะมีเส้นทางการเชื่อมโยงระหว่าง หรือแต่ละเครือข่ายเก็บไว้เป็นตารางเส้นทาง เรียกว่า Routing Table ทำให้เราท์เตอร์สามารถทำหน้าที่จัดหาเส้นทางและเลือกเส้นทางที่เหมาะสมที่สุดในการเดินทาง เพื่อการติดต่อระหว่างเครือข่ายได้อย่างมีประสิทธิภาพ
ที่มา http://wwwkanyanatcom.blogspot.com/2008/07/hub-router-gateway.html Retrieved September, 15, 2010

SMNP ไปใช้งานรูปแบบใดรูปแบบหนึ่งโดยเฉพาะ แต่ส่งผลกับผลิตภัณฑ์ที่ใช้งานโปรโตคอล SNMP จากหลายผู้ผลิต ผลจากการโจมตีผ่านทางช่องโหว่นี้มีความแตกต่างกันออกไป ตั้งแต่การทำให้ระบบไม่สามารถให้บริการได้จากผลของการ DoS (denial of service) ไปจนถึงการทำให้การจัดการและการทำงานของอุปกรณ์ที่เปิดใช้งานโปรโตคอล SNMP ผิดไปจากที่ต้องการ

กลไกการพิสูจน์ตัวตนผู้ใช้ที่มีใช้งานในโปรโตคอล SNMP เวอร์ชั่นเก่ายังคงถูกรวมไว้ในการทำงานของโปรโตคอล SNMP เวอร์ชั่นต่อๆ มา ทำให้ถูกใช้เป็นช่องโหว่สำคัญของระบบ กลไกการพิสูจน์ตัวตนผู้ใช้ที่มีในโปรโตคอล SNMP เวอร์ชั่น 1 และเวอร์ชั่น 2 คือการใช้ "community string" ที่ไม่มีการเข้ารหัสเท่านั้น การขาดการเข้ารหัสทำให้ระบบเกิดความเสี่ยงที่แฮกเกอร์หรือผู้บุกรุกจะนำไปใช้ในการโจมตีได้ อย่างไรก็ตาม ช่องโหว่ของโปรโตคอล SNMP มิได้มีเพียงที่อธิบายไปแล้วเท่านั้น เนื่องจากค่าดีฟอลต์ (default) ของ community string ที่ถูกกำหนดให้กับอุปกรณ์ที่ใช้งาน SNMP เกือบทั้งหมดคือ "public" และผู้ผลิตอุปกรณ์เครือข่ายบางรายได้พยายามแก้ไขค่า community string ที่ใช้เป็น "private" สำหรับการส่งผ่านข้อมูลที่มีความอ่อนไหวกว่า แฮกเกอร์หรือผู้บุกรุกสามารถใช้ช่องโหว่ของโปรโตคอล SNMP ที่กล่าวมานี้ เพื่อแก้ไขหรือหยุดการทำงานของอุปกรณ์ต่างๆ ได้จากเครือข่ายภายนอก นอกจากนั้น การรอรับข้อความที่ถูกส่งด้วยโปรโตคอล SNMP จะทำให้แฮกเกอร์หรือผู้บุกรุกทราบถึงผังโครงสร้างของเครือข่ายที่ใช้งาน รวมถึงระบบและอุปกรณ์ที่เชื่อมต่อกับเครือข่ายนั้น แฮกเกอร์หรือผู้บุกรุกจะใช้ข้อมูลเหล่านี้เพื่อเลือกเป้าหมายและวางแผนการโจมตี

อนึ่ง โปรโตคอล SNMP ไม่ได้มีใช้งานบนระบบปฏิบัติการ Unix เท่านั้น มีการนำโปรโตคอล SNMP ไปใช้งานอย่างกว้างขวางในระบบปฏิบัติการ Windows ในอุปกรณ์เครือข่าย เครื่องพิมพ์ และอุปกรณ์ชนิดฝังตัว แต่การโจมตีที่เกี่ยวข้องกับการทำงานของโปรโตคอล SNMP ส่วนใหญ่ที่พบเกิดขึ้นกับระบบปฏิบัติการ Unix ที่ค่า configuration ซึ่งกำหนดการทำงานของโปรโตคอล SNMP ที่เปิดใช้งานขาดความปลอดภัย สำหรับระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทั้งหมดที่มีการติดตั้งให้ใช้งานโปรโตคอล SNMP และโดยส่วนใหญ่จะถูกเปิดใช้งานโดยดีฟอลต์ นอกจากนั้น อุปกรณ์เครือข่ายและระบบปฏิบัติการอื่นๆ ที่เปิดใช้งานโปรโตคอล SNMP หลายๆ ระบบก็ได้รับผลกระทบจากช่องโหว่นี้เช่นกัน

(5) File Transfer Protocol (FTP)

บริการ FTP ถูกใช้ในการส่งต่อไฟล์ไปยัง anonymous (เป็นวิธีการที่ทำให้ผู้ใช้สามารถเข้าถึงระบบหรือบริการใดๆ ของระบบได้โดยไม่จำเป็นต้องมีชื่อและรหัสผ่านในบัญชีรายชื่อของระบบ) หรือผู้ใช้ที่ผ่านขั้นตอนการพิสูจน์ตัวตน (อาศัยชื่อผู้ใช้และ

รหัสผ่าน) บริการ FTP แบบ anonymous ไม่จำเป็นต้องใช้รหัสผ่านเฉพาะสำหรับผู้ใช้แต่ละคน (แตกต่างจากการใช้งานแบบอื่นๆ) ผู้ใช้ทุกคนเข้าสู่ระบบด้วยชื่อผู้ใช้ชื่อเดียวกัน (เช่น “anonymous” หรือ “ftp”) ดังนั้น จึงเป็นการอนุญาตให้ใครๆ ก็ตามเข้าถึงบริการที่เปิดไว้นี้ได้

บริการ FTP แบบที่มีการพิสูจน์ตัวตนผู้ใช้บังคับให้ผู้ใช้ใส่ชื่อผู้ใช้และรหัสผ่านก่อนที่จะเข้าใช้งาน แต่ข้อมูลทั้งหมดที่ถูกส่งผ่านข้ามเครือข่ายไม่ได้รับการเข้ารหัสแต่อย่างใด จึงเป็นช่องทางให้บุคคลที่สามดักจับข้อมูลสำคัญที่รับส่งไปมาได้ โดยการขโมยข้อมูลที่ใช้ในการล็อกอินเข้าสู่บริการ FTP ผู้โจมตีจะต้องติดตั้งโปรแกรมดักจับข้อมูลบนเครือข่าย (network sniffer) ไว้ตำแหน่งใดตำแหน่งหนึ่งระหว่างเส้นทางการติดต่อ ตัวอย่าง เช่น ในวงเครือข่ายเดียวกับเครื่อง FTP Server หรือในวงเครือข่ายเดียวกับเครื่องไคลเอ็นต์ที่เข้าใช้งานบริการ FTP เหตุการณ์ความปลอดภัยจำนวนมากที่เกิดขึ้นในปัจจุบันต่างพบว่า แฮกเกอร์หรือผู้บุกรุกใช้วิธีของการดักจับข้อมูลที่เกิดขึ้นในระหว่างการรับส่งระหว่างเครื่อง FTP Server และเครื่องไคลเอ็นต์ปลายทาง

นอกจากวิธีการรับส่งข้อมูลที่ไม่มีความปลอดภัยแล้ว ยังมีการค้นพบจุดอ่อนร้ายแรงในซอฟต์แวร์ที่ทำหน้าที่เป็นเครื่อง FTP Server ทั้งซอฟต์แวร์ที่ได้รับจากผู้ผลิตพร้อมกับการติดตั้งระบบปฏิบัติการ (เช่น Sun และ HP-UX) และซอฟต์แวร์ที่พัฒนาขึ้นโดยกลุ่มผู้พัฒนาแบบโอเพนซอร์ส (เช่น WU-FTPD และ ProFTPD) ช่องโหว่ส่วนใหญ่ที่ค้นพบนี้จะอนุญาตให้ผู้บุกรุกได้รับสิทธิของผู้ดูแลระบบในการเข้าถึงเครื่องที่เปิดให้บริการเป็นเครื่อง FTP Server ส่วนช่องโหว่อื่นทั่วไปจะยินยอมให้เกิดการเรียกใช้คำสั่งภายในเครื่องด้วยสิทธิในระดับของผู้ใช้งาน ตัวอย่าง เช่น ช่องโหว่ที่พบในโปรแกรม WU-FTPD ในปัจจุบันคือเมื่อการโจมตีเป็นผลสำเร็จ ผู้บุกรุกได้รับสิทธิของผู้ดูแลระบบ สามารถอัพโหลดไฟล์ชุดคำสั่งไม่พึงประสงค์เพื่อเป็นเครื่องมือของตน เช่น rootkit และนำไปใช้งานในระบบเพื่อทำอันตรายต่อระบบได้ ส่วนใหญ่แล้วช่องโหว่เหล่านี้จำเป็นต้องอาศัยการเปิดใช้งานการเข้าถึงระบบแบบ anonymous แต่มีบางช่องโหว่ที่สามารถถูกโจมตีได้แม้ว่าจะปิดการเข้าถึงแบบ anonymous แล้วก็ตาม ช่องโหว่ยังคงมีอยู่ในระบบตลอดเวลาตราบใดที่ยังเปิดใช้งานเครื่อง FTP Server ให้รอรับการติดต่อเข้าใช้งานที่พอร์ตใดๆ บนเครือข่าย อีกสิ่งหนึ่งที่ควรให้ความระมัดระวังอยู่เสมอในการเปิดให้บริการเครื่อง FTP Server แม้ว่าจะกำหนดให้ทำงานแบบ chroot() เพื่อจำกัดให้ผู้ที่เข้าใช้งานแบบ anonymous เข้าสู่ไดเร็กทอรีที่กำหนดได้เท่านั้นก็ตาม ช่องโหว่จำนวนหนึ่งยังคงมีอยู่ซึ่งเป็นผลมาจากข้อผิดพลาดที่ส่วนใหญ่เกิดขึ้นในขั้นตอนของการนำไปใช้งาน ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทั้งหมดที่มีการติดตั้งซอฟต์แวร์เพื่อทำงานเป็น FTP Server และโดยส่วนใหญ่จะถูกเปิดใช้งานโดยดีฟอลต์

(6) R-Services - Trust Relationships

คำสั่ง remote shell (rsh), remote copy (rcp), remote login (rlogin) และ remote execution (rexec) เป็นคำสั่งที่รู้จักกันโดยทั่วไปในชื่อของกลุ่มคำสั่ง "R-commands" และถูกใช้งานเป็นประจำในการทำงานกับระบบปฏิบัติการ Unix องค์กรใดที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ระบบปฏิบัติการ Unix หลายเครื่องมักจะกำหนดให้เครื่องเหล่านั้นเปิดใช้งานบริการในกลุ่ม "R-services" (เช่น in.rshd, in.rlogind หรือ in.rexecd) เพื่อใช้เป็นช่องทางให้ผู้ใช้ทำงานผ่านเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ได้โดยไม่จำเป็นต้องใส่ชื่อผู้ใช้และรหัสผ่านทุกครั้ง ในการทำงานบนเครือข่ายที่การกำหนดทรัพยากรให้ผู้ใช้งานแต่ละคนถูกเก็บไว้ที่เครื่องคอมพิวเตอร์แต่ละเครื่อง โดยที่ผู้ดูแลระบบมีหน้าที่ดูแลเครื่องคอมพิวเตอร์จำนวนมาก ดังนั้น การเปิดใช้งาน R-services จึงเป็นการช่วยให้ผู้ดูแลระบบสามารถทำงานสลับไปมาระหว่างเครื่องคอมพิวเตอร์หลายเครื่องได้ ผู้ใช้งานแต่ละคนสามารถใช้งานคำสั่ง rsh, rcp, rlogin หรือ rexec จากเครื่องคอมพิวเตอร์ A เพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ B ได้โดยไม่ต้องผ่านการพิสูจน์ตัวตนอีกครั้ง โดยการเพิ่มชื่อและหมายเลขไอพีแอดเดรสของเครื่องคอมพิวเตอร์ A ลงในไฟล์ .rhosts ที่อยู่ภายในไดเร็กทอรีของตนเอง (~/.rhosts) บนเครื่องคอมพิวเตอร์ B หรือหากผู้ใช้ทุกคนต้องการใช้งานคำสั่ง rsh, rcp, rlogin หรือ rexec จากเครื่องคอมพิวเตอร์ A เพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ B โดยไม่ต้องการผ่านการพิสูจน์ตัวตนอีกครั้งก็สามารถทำได้หากชื่อและหมายเลขไอพีแอดเดรสของเครื่องคอมพิวเตอร์ A ถูกกำหนดไว้ในไฟล์ /etc/hosts.equiv ของเครื่องคอมพิวเตอร์ B

การใช้งาน R-services เพื่อการติดต่อผ่านเครือข่ายทำให้เกิดจุดอ่อนพื้นฐานที่สำคัญสองข้อคือ การขาดการเข้ารหัสข้อมูลและความไม่ปลอดภัยในการพิสูจน์ตัวตนผู้ใช้ที่ต้องการเข้าใช้งานเครื่อง การรับส่งข้อมูลระหว่างเครื่องไคลเอ็นต์ที่เรียกใช้ R-commands กับเครื่องที่เปิดใช้ R-services ในรูปของข้อมูลที่ไม่ได้รับการเข้ารหัสอาจทำให้ข้อมูลหรือค่าที่พิมพ์ผ่านคีย์บอร์ดทั้งหมดถูกดักจับได้ จากรูปแบบการทำงานที่เกิดขึ้นจริง R-services ที่เปิดใช้งานจะยอมให้เครื่องไคลเอ็นต์ใดๆ ติดต่อเข้าใช้งานทันทีที่มีการแสดงชื่อและหมายเลขไอพีแอดเดรส ส่งผลให้อาจมีการปลอมค่าดังกล่าวเพื่อให้สามารถเข้าใช้งานได้ เมื่ออาศัยการทำงานในส่วนที่ไม่มีการสร้างความสัมพันธ์ที่เชื่อถือได้ (trust relationship)[96] ซึ่งผู้ใช้งานทุกคนต้องส่งค่า

---

[96] trust relationship เป็นการทำงานที่อาศัยการเชื่อมั่นกันระหว่างเครื่องคอมพิวเตอร์สองเครื่อง โดยเครื่องคอมพิวเตอร์ B จะยอมให้ผู้ใช้ที่ติดต่อมาจากเครื่องคอมพิวเตอร์ A เข้าใช้งานที่เครื่องได้ทันทีโดยไม่ต้องระบุชื่อผู้ใช้และรหัสผ่าน เนื่องจากมั่นใจว่าผู้ใช้คนดังกล่าวได้รับอนุญาตให้เข้าใช้งานระบบแล้ว จากการพิสูจน์ตัวตนที่เครื่องคอมพิวเตอร์ A

รหัสผ่านของตนผ่านเครือข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่ายโดยปราศจากการเข้ารหัสร่วมกับการทำงานของ trust relationship แฮกเกอร์หรือผู้บุกรุกสามารถค้นหาชื่อผู้ใช้ที่อยู่บนเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งที่มีใช้งานจริงในเครือข่าย แล้วล็อกอินเข้าสู่เครื่องนั้น เพื่อให้สามารถเข้าถึงเครื่องคอมพิวเตอร์เครื่องอื่นๆ ได้โดยผ่านการใช้งาน trust relationship จากเครื่องแรก ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทุกเวอร์ชั่นที่ได้รับการติดตั้งและนิยมเปิดใช้งาน R-services

(7) Line Printer Daemon (LPD)

Line Printer (LPD) ของ Berkeley เป็นบริการที่มีใช้งานมาตั้งแต่อดีตเพื่อให้ผู้ใช้สามารถติดต่อกับเครื่องพิมพ์ที่อยู่ในเครือข่ายจากเครื่องคอมพิวเตอร์ที่อยู่ภายในหรือภายนอกเครือข่ายก็ได้ผ่านทางพอร์ต 515 ของโปรโตคอล TCP ถึงแม้ว่าในปัจจุบันจะมีการนำโปรแกรมที่ใช้ทำหน้าที่เป็นพรินต์เซิร์ฟเวอร์ (Print Server) มาใช้งานแทน LPD อยู่หลายโปรแกรมก็ตาม LPD ยังคงเป็นโปรแกรมที่มีผู้นิยมใช้งานสูงสุดในการทำงานกับระบบปฏิบัติการ Unix และ Linux ดิสทริบิวต์ชั่นต่างๆ อย่างไรก็ตาม บ่อยครั้งที่พบว่าโปรแกรม LPD ที่ใช้งานมีข้อบกพร่องภายในตัวโปรแกรมซึ่งนำไปสู่ปัญหาการเกิด buffer overflow ขึ้นในเครื่อง แล้วส่งผลให้แฮกเกอร์หรือผู้บุกรุกสามารถเรียกใช้งานชุดคำสั่งต่างๆ ที่ต้องการบนเครื่องคอมพิวเตอร์เครื่องดังกล่าวได้ด้วยสิทธิของผู้ดูแลระบบ ช่องโหว่ของ LPD จำนวนหนึ่งเกิดขึ้นกับระบบปฏิบัติการ Unix หลายดิสทริบิวต์ชั่นที่แตกต่างกัน ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix เกือบทั้งหมด และระบบปฏิบัติการ Linux หลายระบบที่มีการติดตั้ง LPD เวอร์ชั่นใดเวอร์ชั่นหนึ่งและถูกเปิดใช้งานโดยค่าดีฟอลต์

(8) Sendmail

Sendmail เป็นโปรแกรมที่ทำหน้าที่ส่งรับและส่งต่ออีเมล์ซึ่งส่วนใหญ่ทำงานบนเครื่องที่มีระบบปฏิบัติการเป็น Unix และ Linux จากความนิยมในการนำโปรแกรม Sendmail ไปใช้งานอย่างแพร่หลายบนเครือข่ายอินเทอร์เน็ตทำให้โปรแกรม Sendmail ถูกใช้เป็นเป้าหมายหลักในการโจมตีของแฮกเกอร์หรือผู้บุกรุกตั้งแต่อดีต และส่งผลให้เกิดการพัฒนาชุดคำสั่งไม่พึงประสงค์ที่อาจใช้ในการโจมตีโปรแกรม Sendmail ขึ้นมากมายมาโดยตลอด

ชุดคำสั่งที่ใช้โจมตีส่วนใหญ่นี้สามารถโจมตีได้สำเร็จเฉพาะกับโปรแกรม Sendmail เวอร์ชั่นเก่าเท่านั้น แม้ปัญหาการถูกโจมตีทั้งหมดที่เกิดขึ้นในอดีตได้ถูกรวบรวมขึ้นเป็นเอกสารซึ่งแสดงรายละเอียดที่เกี่ยวข้องและเผยแพร่ไว้มากมาย รวมถึงได้รับการแก้ไขปรับปรุงในซอฟต์แวร์ Sendmail เวอร์ชั่นถัดมา แต่ในปัจจุบันยังคงมีผู้ใช้งานโปรแกรม

Sendmail ที่ใช้งานซอฟต์แวร์เวอร์ชั่นที่ไม่ได้อัพเดตหรือเวอร์ชั่นที่มีข้อผิดพลาดในการทำงาน ส่งผลให้บริการ Sendmail ยังคงเป็นหนึ่งในหลายบริการที่ถูกโจมตีบ่อยที่สุด

ความเสี่ยงจากการเปิดใช้งานบริการ Sendmail แบ่งออกได้เป็นสองรูปแบบคือ การได้รับเพิ่มสิทธิ์การใช้งานระบบซึ่งเป็นผลจากการเกิด buffer overflow และการใช้งานค่า configuration ของโปรแกรม Sendmail ที่ไม่เหมาะสมซึ่งเป็นสาเหตุให้เครื่องถูกนำไปใช้เป็น relay ในการส่งอีเมล์จากเครื่องคอมพิวเตอร์เครื่องใดๆ ไปยังปลายทางที่ต้องการได้ ปัญหารูปแบบแรกเกิดขึ้นกับระบบที่ยังคงใช้งานซอฟต์แวร์ Sendmail เวอร์ชั่นเก่า ส่วนปัญหาในกลุ่มหลังเกิดจากการปรับแต่งค่าไฟล์ configuration ไม่เหมาะสมหรือไม่มีการแก้ไขใดๆ เลยจากค่าดีฟอลต์ของโปรแกรม และยังเป็นอุปสรรคสำคัญในการยับยั้งการแพร่กระจายของอีเมล์ที่ถูก spam ระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทั้งหมดที่มีการติดตั้งโปรแกรม Sendmail เวอร์ชั่นใดเวอร์ชั่นหนึ่งและถูกเปิดใช้งานโดยค่าดีฟอลต์

(9) BIND / DNS

แพ็กเก็ต Berkeley Internet Name Domain (BIND) ถูกนำไปใช้งานเป็นบริการของโดเมนเนม (Domain Name Service : DNS) อย่างแพร่หลาย บริการดังกล่าวนี้จะอนุญาตให้ผู้ใช้ค้นหาตำแหน่งของเครื่องคอมพิวเตอร์แม่ข่ายบนเครือข่ายอินเทอร์เน็ต (หรือภายในเครือข่ายที่ใช้งาน) โดยอาศัยชื่อเครื่อง (เช่น www.abcdef.org เป็นต้น) ได้โดยไม่จำเป็นต้องทราบหมายเลขไอพีแอดเดรสที่แท้จริงของเครื่องดังกล่าว ความแพร่หลายในการนำ BIND ไปใช้งานส่งผลให้บริการของ BIND ตกเป็นเป้าหมายในการบุกรุกระบบอยู่เป็นประจำ ในขณะที่ทีมผู้พัฒนาแพ็กเก็ต BIND ได้แก้ไขช่องโหว่ที่เกิดขึ้นกับโปรแกรม BIND หลังจากตรวจพบอย่างรวดเร็วมาโดยตลอด แต่ยังคงมีเครื่องคอมพิวเตอร์แม่ข่ายจำนวนมากที่ยังคงไม่ได้รับการอัพเดตหรือทำงานด้วยค่า configuration ที่ไม่ถูกต้อง และเป็นช่องทางให้ถูกบุกรุกได้

ปัจจัยสำคัญที่ทำให้เกิดการบุกรุกประกอบก็คือ ผู้ดูแลระบบซึ่งไม่ตระหนักถึงความจำเป็นของการอัพเกรดเพื่อความปลอดภัย เครื่องคอมพิวเตอร์ที่เปิดใช้งาน BIND (ชื่อว่า “named”) โดยไม่มีความจำเป็น และไฟล์ configuration ที่ไม่ปลอดภัย ปัจจัยใดปัจจัยหนึ่งเหล่านี้อาจส่งผลให้เกิด Dos (denial of service) หรือ buffer overflow ที่เครื่อง หรือเกิด DNS cache poisoning[97] โดยในปัจจุบันพบว่า จุดอ่อนของ BIND ที่ตรวจพบบ่อยที่สุดคือการถูกโจมตี

---

97 DNS cache poisoning เป็นความผิดพลาดในการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็น DNS โดยเกิดจากการที่เครื่องได้รับข้อมูลปลอมหรือข้อมูลที่ไม่ถูกต้องจากเครื่องคอมพิวเตอร์แม่ข่ายอื่นภายนอก แล้วบันทึกข้อมูลที่ได้ (cache) ลงในเครื่อง พร้อมทั้งส่งต่อไปยังโปรแกรมที่ร้องขอข้อมูลดังกล่าว

แบบ denial of service ซึ่งเป็นผลจากการที่ผู้บุกรุกสามารถส่งแพ็กเก็ต DNS เข้ามากระตุ้นให้เกิดการตรวจสอบความถูกต้องภายใน หากระบบใดมีช่องโหว่อยู่ DNS จะถูกสั่งหยุดการทำงาน (shutdown) จุดอ่อนอื่นที่ตรวจพบคือ buffer overflow ในกรณีนี้ผู้โจมตีจะใช้ช่องโหว่จากการทำงานของไลบรารี DNS resolver โดยการส่งค่า DNS response ที่ใช้ทำอันตรายแก่ระบบเพื่อเข้าสู่เครื่องคอมพิวเตอร์ที่ต้องการผ่านทางช่องโหว่นี้ แล้วเรียกใช้งานชุดโปรแกรมต่างๆ ตามที่ต้องการ หรือในบางครั้งอาจจะทำให้เกิด denial of service ได้อีกด้วย สำหรับระบบปฏิบัติการที่ได้รับผลกระทบ ได้แก่ ระบบปฏิบัติการ Unix และ Linux เกือบทั้งหมดที่มีการติดตั้งแพ็กเก็ต BIND เวอร์ชั่นใดเวอร์ชั่นหนึ่งและถูกเปิดใช้งานโดยค่าดีฟอลต์ รวมถึงเวอร์ชั่นไบนารีของโปรแกรม BIND ที่ใช้งานกับระบบปฏิบัติการ Windows

(10) General Unix Authentication - Account with No Passwords or Weak Passwords

รหัสผ่าน วลีรหัสผ่าน และชุดคำสั่งที่เกี่ยวข้องกับความปลอดภัยถูกนำมาใช้งานจนเป็นเรื่องปกติในระหว่างการติดต่อกันของผู้ใช้กับระบบสารสนเทศ รูปแบบของการพิสูจน์ตัวตนผู้ใช้ รวมถึงการเก็บรักษาข้อมูลหรือไฟล์ส่วนใหญ่เชื่อมั่นในค่ารหัสผ่านที่ได้รับจากผู้ใช้ เนื่องจากข้อมูลการเข้าถึงระบบโดยผ่านขั้นตอนการพิสูจน์ตัวตนตามที่ระบบกำหนดจะไม่ถูกบันทึกลงในล็อกไฟล์ (log file) หรือหากบันทึกก็จะไม่แสดงถึงความผิดปกติใดๆ ให้สังเกตเห็นได้ ดังนั้น รหัสผ่านที่ได้รับจากวิธีการที่ไม่ถูกต้องอาจถูกนำมาใช้เพื่อสำรวจข้อมูลของระบบจากภายในเครื่องโดยที่ผู้ดูแลระบบไม่สามารถตรวจพบได้ ทั้งนี้ ตัวแฮกเกอร์หรือผู้บุกรุกจะได้สิทธิ์อย่างสมบูรณ์ในการเข้าใช้งานทรัพยากรที่เจ้าของรหัสผ่านตัวจริงได้รับทั้งหมด และเข้าถึงบัญชีผู้ใช้คนอื่นๆ เครื่องคอมพิวเตอร์ที่อยู่ข้างเคียง รวมถึงได้รับสิทธิ์เป็นผู้ดูแลระบบ ถึงแม้ว่าผู้ใช้ทุกคนจะทราบถึงความเสี่ยงนี้ แต่การใช้งานบัญชีผู้ใช้ร่วมกับรหัสผ่านที่ไม่ดีพอหรือไม่มีการกำหนดรหัสผ่านก็ยังคงมีให้เห็นอยู่

ช่องโหว่ที่เกิดขึ้นจากการใช้งานรหัสผ่านโดยทั่วไปที่ตรวจพบบ่อยได้แก่ บัญชีผู้ใช้มีรหัสผ่านที่ไม่ดีพอหรือไม่มีรหัสผ่าน หรือผู้ใช้ขาดความเอาใจใส่ต่อการเก็บรักษารหัสผ่านให้ปลอดภัยทำให้ละเลยต่อการป้องกันรหัสผ่าน หรือระบบปฏิบัติการหรือซอฟต์แวร์ที่ใช้งานสร้างรหัสผ่านที่ไม่ดีพอให้กับชื่อผู้ใช้ที่เป็นผู้ดูแลระบบหรือสร้างผู้ใช้ดังกล่าวโดยไม่กำหนดรหัสผ่าน และอัลกอริทึมการทำ hashing รหัสผ่านเป็นวิธีที่รู้จักอย่างแพร่หลาย และค่าที่ได้รับมักจะถูกเก็บไว้ในตำแหน่งที่ผู้ใช้บางคนสามารถเข้าอ่านได้ การป้องกันที่ดีและเหมาะสมที่สุดคือ การนำนโยบายเรื่องรหัสผ่านที่ดี ซึ่งรวมถึงคำแนะนำในเรื่องข้อควรปฏิบัติในการใช้งานรหัสผ่านที่ดี และการตรวจสอบความถูกต้องของรหัสผ่านมาใช้ สำหรับระบบปฏิบัติการที่ได้รับ

ผลกระทบระบบปฏิบัติการและแอพพลิเคชั่นใดๆ ที่มีการพิสูจน์ตัวตนผู้ใช้โดยอาศัยค่าหมายเลขผู้ใช้และรหัสผ่าน

มีตัวอย่างคดีการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายผ่านช่องโหว่ คือคดี Mafiaboy ซึ่งเป็นการเข้าถึงระบบคอมพิวเตอร์โดยไม่มีอำนาจ (Unauthorized Access) และรบกวนระบบ (System Interference) อันเป็นความผิดตามประมวลกฎหมายอาญาแคนาดา มาตรา 430 และ 342.1 คดีนี้มีข้อเท็จจริงว่า ผู้กระทำความผิดเป็นเด็กชายอายุ 15 ปี อาศัยอยู่ในมอลทรีออล ประเทศแคนาดา โดยใช้ชื่อในอินเทอร์เน็ตว่า “Mafiaboy” ในระหว่างวันที่ 7 ถึง 12 กุมภาพันธ์ 2543 ผู้กระทำความผิดได้ทำการโจมตีเว็บไซต์ต่างๆ โดยวิธีส่งโปรแกรมเข้าไปยึดเครื่องคอมพิวเตอร์ที่มีช่องโหว่ประมาณ 75 เครื่อง แล้วใช้เครื่องคอมพิวเตอร์ดังกล่าวเป็นเครื่องมือในการส่งการติดต่อไปยังเว็บไซต์ที่ต้องการโจมตีพร้อมๆ กันจนเครื่องคอมพิวเตอร์ที่ถูกโจมตีมีการสื่อสารที่หนาแน่นและไม่สามารถใช้งานได้ในที่สุด เว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะเป็นเว็บไซต์ที่มีชื่อเสียง เช่น Amazon.com, Buy.com, CNN.com และ Yahoo.com ซึ่งเว็บไซต์ที่ได้รับความเสียหายจากการโจมตีดังกล่าวมากที่สุดคือ Yahoo.com ที่ถูกโจมตีในวันที่ 7 กุมภาพันธ์ 2543 มีมูลค่าความเสียหายถึง 1.7 พันล้านเหรียญสหรัฐ โดยศาลแคนาดาตัดสินให้ Mafiaboy ถูกควบคุมตัวไว้ในสถานพินิจเด็กเป็นเวลา 8 เดือน และถูกคุมความประพฤติเป็นเวลา 1 ปี อีกทั้ง ถูกวางข้อกำหนดในการใช้งานอินเทอร์เน็ตอย่างเคร่งครัด

6.1.3 การปล่อยมัลแวร์ผ่านโปรแกรมประเภท Peer-to-Peer (P2P)[98] และโปรแกรมประเภท Instant Messaging (IM)

จากความนิยมในการใช้โปรแกรมดาวน์โหลดภาพยนตร์และบทเพลงต่างๆ ในรูปแบบของไฟล์ DIVX หรือ MP3 ในปัจจุบัน ทำให้โปรแกรมประเภท P2P มีสถิติการใช้

---

98 Peer-to-Peer (P2P) หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน ซึ่งหมายความว่า แต่ละเครื่องต่างก็มีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดเครือข่ายคอมพิวเตอร์แบบนี้ทำให้สามารถใช้ทรัพยากรหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ที่อยู่ในเครือข่าย ซึ่งจะแตกต่างจากวิธีการจัดเครือข่ายคอมพิวเตอร์อีกลักษณะหนึ่ง ที่เรียกว่า client-server ที่เป็นการกำหนดให้คอมพิวเตอร์เครื่องหนึ่งเป็นเครื่องให้บริการ หรือเป็นที่เก็บทรัพยากรและแฟ้มทั้งหมด โดยคอมพิวเตอร์ในเครือข่ายจะเรียกใช้ทรัพยากรหรือแฟ้มข้อมูลจากกันไม่ได้ แต่ต้องเรียกจากเครื่องที่ทำหน้าที่ให้บริการเท่านั้น จึงอาจเรียก P2P ว่าเป็นเทคโนโลยีการสื่อสารข้อมูลบนเครือข่ายคอมพิวเตอร์แบบ client-client ที่มา http://guru.sanook.com/search/peer-to-peer Retrieved September, 15, 2010

แบนด์วิดท์[99] (bandwidth) ของเครือข่ายอินเทอร์เน็ตที่สูงมาก ซึ่งผู้ใช้อินเทอร์เน็ตตามบ้านล้วนนิยมใช้โปรแกรม P2P ซึ่งเป็นช่องทางของแฮกเกอร์หรือผู้บุกรุกในการแอบปล่อยมัลแวร์ที่อยู่ตามเครือข่าย P2P ไปยังเครื่องคอมพิวเตอร์ของเหยื่อโดยจะตั้งชื่อโปรแกรมให้มีความน่าสนใจ เพื่อหลอกล่อให้ผู้อ่านโปรแกรม P2P ทำการ Download ไปใช้งาน โดยที่ผู้ใช้ไม่ทราบว่าโปรแกรมเหล่านั้นถูกเขียนขึ้นมาเพื่อวัตถุประสงค์ในการลักลอบดักข้อมูลหรือเป็นเครือข่ายของบ๊อทเน็ตทำให้แฮกเกอร์สามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้จากระยะไกลโดยเหยื่อไม่รู้ตัว

ตัวอย่างโปรแกรมประเภท Instant Messaging หรือ IM เช่น AIM , YIM และโปรแกรมยอดนิยมอย่าง MSN ก็จัดอยู่ในประเภทเดียวกันกับโปรแกรม P2P ซึ่งผู้ใช้งานโปรแกรม IM ก็มีโอกาสจะติดไวรัสที่ถูกส่งมาจากคู่สนทนาที่กำลังแชท (ย่อมาจาก Chat Room หมายถึงห้องพูดคุย)[100] กันอยู่ เนื่องจากคู่สนทนาอีกฝ่ายหนึ่งติดไวรัสก่อน จึงทำให้เครื่องของคู่สนทนาทำการส่งไวรัสออกไปยังทุกคนที่กำลังออนไลน์อยู่ในระบบ Instant Messaging ด้วยวิธีการนี้ ทำให้ไวรัสหรือมัลแวร์แพร่กระจายได้ด้วยความรวดเร็วเป็นทวีคูณจนสร้าง ความเสียหายให้กับเครือข่ายขององค์กรได้ในที่สุด

6.1.4 การโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) ด้วยมัลแวร์

วัตถุประสงค์หลักของแฮกเกอร์หรือผู้บุกรุกดีส่วนใหญ่หากไม่ใช่เรื่องการขโมยข้อมูลหรือการแอบแก้ไขข้อมูลแล้ว ก็คงหนีไม่พ้นการโจมตีเพื่อให้ระบบเป้าหมายไม่สามารถทำงานได้ตามปกติ ซึ่งโดยปกติแล้วเว็บไซต์ประเภทออนไลน์เซอร์วิสหรือประเภทพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) และระบบเครือข่ายที่มีผู้ใช้เป็นจำนวนมาก (เช่น Twitter ที่เคยถูกโจมตีด้วยวิธีการนี้มาแล้ว) มักตกเป็นเป้าหมายการโจมตีในลักษณะนี้เพื่อทำให้เว็บไซต์ดังกล่าวไม่สามารถให้บริการได้ส่งผลให้ลูกค้าเกิดความไม่พอใจหรือทำให้ธุรกิจขาดรายได้ที่ควรจะได้ตามปกติ ทั้งนี้โดยการใช้มัลแวร์เป็นเครื่องมือในการโจมตี

การโจมตีในลักษณะนี้เป็นที่นิยมของบรรดาผู้ก่อการร้ายไฮเทค (Cyber Terrorism) ซึ่งเรียกได้ว่าเป็นการก่อวินาศกรรมในโลกไซเบอร์แต่มีผลกระทบในโลกของ

---

99 วิกิพีเดีย สารานุกรมเสรี.http://th.wikipedia.org/wiki/ แบนด์วิดท์ (อังกฤษ: bandwidth) เป็นคำที่ใช้วัดความเร็วในการส่งข้อมูลของอินเทอร์เน็ต ซึ่งโดยมากมักวัดความเร็วของการส่งข้อมูลเป็น bps (bit per second), Mbp (bps*1000000) เช่น Bandwidth ของการใช้สายโทรศัพท์ในประเทศไทย เท่ากับ 14.4 Kbps,Bandwidth ของสายส่งข้อมูลของ KSC ที่ใช้ในการเชื่อมต่อกับอเมริกาเท่ากับ 2 Mbps เป็นต้น Retrieved September, 15, 2010

100 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 20

ความเป็นจริง ตัวอย่าง เช่น แฮกเกอร์บุกเข้าโจมตีระบบ SCADA ของการไฟฟ้าหรือการประปาเพื่อให้ไฟฟ้าดับหรือน้ำไม่ไหล หรือโจมตีเขื่อนเพื่อสั่งปล่อยน้ำออกจากเขื่อนโดยไม่ได้รับอนุญาต เป็นต้น

ตัวอย่างการโจมตีก็เช่นในประเทศออสเตรเลีย เคยมีผู้ไม่หวังดีเข้าเจาะระบบ SCADA ด้วยชุดคำสั่งไม่พึงประสงค์ โดยผ่านทางอุปกรณ์ไร้สาย (Wireless LAN) เพื่อเข้ามาสั่งให้ระบบปล่อยน้ำเสียลงในแม่น้ำทำให้สัตว์น้ำต้องเสียชีวิตเป็นจำนวนมาก เป็นต้น

6.2 การกระทำความผิดโดยการดักข้อมูล

การกระทำความผิดโดยการดักข้อมูลคอมพิวเตอร์นี้ แฮกเกอร์หรือผู้บุกรุกมักจะใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ประเภทสนิฟเฟอร์ (Sniffer) หรือหากเป็นการดักข้อมูลในเครือข่ายที่ใช้สายก็จะเรียกว่า “เน็ตเวิร์กไวร์แท๊บ (Network wiretap)” ซึ่งชุดคำสั่งไม่พึงประสงค์ประเภทสนิฟเฟอร์นี้จะทำหน้าที่ดักจับหรือดักรับข้อมูลหรือแพ็กเก็ตในเครือข่ายคอมพิวเตอร์ ตัวอย่าง เช่น โปรแกรม Sniffer, Ethereal, หรือ Wireshark เป็นต้น ทั้งที่ในความเป็นจริงแล้ว สนิฟเฟอร์มักจะถูกนำไปใช้เป็นเครื่องมือในการดักจับหรือดักรับข้อมูลหรือแพ็กเก็ตที่วิ่งอยู่บนเครือข่ายคอมพิวเตอร์เพื่อนำไปตรวจสอบและวิเคราะห์ปัญหาต่างๆ ที่เกิดขึ้น โดยส่วนมากจะมีการใช้โปรแกรมสนิฟเฟอร์อยู่สองรูปแบบคือ ใช้ในการบำรุงรักษาเครือข่าย หรือใช้ในการวิเคราะห์และตรวจสอบการบุกรุก ตัวอย่าง เช่น การวิเคราะห์ปัญหาของเครือข่ายว่าเหตุใดเครื่องที่หนึ่งจึงไม่สามารถติดต่อกับเครื่องที่สองได้ หรืออาจใช้วิเคราะห์ประสิทธิภาพของระบบเพื่อแก้ปัญหาคอขวดของข้อมูลหรือใช้ในการตรวจจับหาผู้บุกรุกระบบ เป็นต้น แต่ด้วยคุณสมบัติในการถอดข้อมูลในแพ็กเก็ตและการเก็บบันทึกไว้ให้ผู้ติดตั้งนำไปใช้งานได้ ดังนั้น สนิฟเฟอร์จึงเป็นชุดคำสั่งไม่พึงประสงค์ที่แฮกเกอร์หรือผู้บุกรุกนิยมใช้ในการเจาะเข้าไปในเครื่องคอมพิวเตอร์ของเหยื่อเพื่อใช้ดักจับข้อมูลโดยเฉพาะอย่างยิ่งชื่อบัญชีและรหัสผ่านเพื่อนำไปใช้ในการกระทำความผิดหรือการเจาะระบบอื่นต่อไป ทั้งนี้ สามารถแยกการดักข้อมูลคอมพิวเตอร์ได้เป็น 2 ลักษณะดังต่อไปนี้

6.2.1 การดักข้อมูลในเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์

หลักในการทำงานของสนิฟเฟอร์เพื่อดักข้อมูลในเครือข่ายคอมพิวเตอร์นั้นมักจะดักข้อมูลที่อยู่ระหว่างการส่งข้อมูลโดยอุปกรณ์รวมสัญญาณต่างๆ ซึ่งในที่นี้จะขอยกตัวอย่างการดักข้อมูลของฮับ (Hub) และสวิทช์ (Switch) เนื่องจากอุปกรณ์ทั้งสองชนิดดังกล่าวมักจะถูกนำมาใช้ในการส่งข้อมูลระหว่างเครือข่ายคอมพิวเตอร์มากที่สุด โดยมีหลักการว่า ในระบบเครือข่ายคอมพิวเตอร์ที่ใช้อุปกรณ์รวมสัญญาณแบบฮับนั้น เมื่อเครื่องคอมพิวเตอร์ต้นทางจะส่ง

ข้อมูลไปยังเครื่องคอมพิวเตอร์ปลายทางจะต้องมีการระบุ MAC Address[101] ที่เครื่องตัวเองและที่เครื่องปลายทางลงไปด้วย จากนั้นจึงกระจายข้อมูลออกไปยังทุกพอร์ตของเครื่องที่อยู่ในเครือข่ายคอมพิวเตอร์เดียวกัน แต่จะมีเพียงเครื่องปลายทางที่มี MAC Address ตรงกับที่ระบุเท่านั้นที่จะรับข้อมูลไปประมวลผล ส่วนเครื่องอื่นๆ ที่มี MAC Address ไม่ตรงกับที่ระบุก็จะปล่อยข้อมูลนั้นผ่านไป จากจุดนี้เองจะเห็นได้ว่าการใช้ฮับมีจุดอ่อนตรงที่มีการกระจายข้อมูลออกไปยังทุกเครื่องที่อยู่ในเครือข่าย ทำให้แฮกเกอร์หรือผู้บุกรุกสามารถใช้โปรแกรมสนิฟเฟอร์ดักจับข้อมูลที่วิ่งเข้ามาทั้งหมดโดยไม่สนใจว่าข้อมูลนั้นจะมี MAC Address ตรงกับเครื่องของตัวเองหรือไม่ จึงเรียกการทำงานแบบนี้ว่า “Promiscuous Mode” ด้วยเหตุที่ฮับมีจุดอ่อนในด้านความปลอดภัยดังกล่าว จึงทำให้ในปัจจุบันไม่เป็นที่นิยมนำฮับมาใช้งานกันมากนัก แต่ได้มีการนำอุปกรณ์รวมสัญญาณอีกชนิดหนึ่งที่เข้ามาแทนที่ฮับก็คือสวิทซ์ (Switch) ทั้งนี้ สวิทซ์ถือเป็นอุปกรณ์ที่มีการทำงานเหมือนฮับทุกประการเพียงแต่สวิทซ์ จะไม่กระจายข้อมูลออกไปยังทุกพอร์ตของคอมพิวเตอร์ที่อยู่ในเครือข่าย แต่สวิทซ์จะทำการตรวจสอบก่อนว่าเครื่องปลายทางที่จะส่งข้อมูลออกไปมี MAC Address ตรงกับข้อมูลที่ระบุหรือไม่ หากพบว่าตรงกันก็จะส่งข้อมูลออกไปยังเครื่องปลายทางนั้นเพียงเครื่องเดียว ไม่มีการกระจายข้อมูลไปยังเครื่องอื่นๆ อีก ทำให้โปรแกรมสนิ๊ฟเฟอร์ไม่สามารถดักจับข้อมูลที่วิ่งอยู่บนเครือข่ายได้

อย่างไรก็ตาม แม้ว่าการใช้สวิทซ์ดูเหมือนจะมีความปลอดภัยมากกว่าฮับ แต่สวิทซ์ก็ยังมีช่องโหว่ กล่าวคือ หลักการทำงานของสวิทซ์ที่จะไม่กระจายข้อมูลออกไปยังทุกเครื่องที่อยู่ในเครือข่ายนั้น เป็นเพราะสวิทซ์สามารถสร้างตาราง MAC Address ที่ระบุได้ว่าแต่ละเครื่องที่อยู่ในเครือข่ายมี MAC Address อะไรบ้าง สวิทซ์จึงสามารถส่งข้อมูลไปยังเครื่องที่มี MAC Address ตรงกันได้อย่างถูกต้อง แต่ในช่วงแรกของการทำงานสวิทซ์จะยังไม่รู้ว่าทุกเครื่องที่อยู่ในเครือข่ายมี MAC Address อะไรบ้าง สวิทซ์จึงต้องทำงานคล้ายกับฮับไปก่อน คือ กระจายข้อมูลออกไปยังทุกเครื่องที่อยู่ในเครือข่ายเพื่อคอยเก็บข้อมูลที่ตอบกลับมาจากเครื่องเหล่านั้น ซึ่งจะมีการระบุว่า MAC Address ของแต่ละเครื่องเป็นหมายเลขอะไร เพื่อนำไปสร้างเป็นตาราง MAC Address ทำให้การส่งข้อมูลครั้งต่อไปสวิทซ์จะสามารถระบุเครื่องเป้าหมายที่จะส่งข้อมูลไปให้ได้อย่างถูกต้อง โดยไม่ต้องกระจายข้อมูลไปยังทุกๆ เครื่องอีก

---

101 MAC Address (Media Access Control Address) คือ หมายเลขประจำอุปกรณ์ในระบบเครือข่าย โดยใช้เลขฐาน 16 จำนวน 6 ชุด ทั้งนี้หมายเลขในแต่ละอุปกรณ์จะไม่ซ้ำกัน

ทั้งนี้ โดยปกติการติดต่อระหว่างเครื่องต้นทางและเครื่องปลายทางในเครือข่ายคอมพิวเตอร์จะต้องอาศัยทั้งหมายเลข IP Address[102] และ MAC Address ในการอ้างอิงที่อยู่ของทั้งสองเครื่อง ซึ่งส่วนใหญ่หมายเลข IP Address นั้น จะทราบกันดีอยู่แล้ว เนื่องจากมีการกำหนดไว้ที่คอมพิวเตอร์แต่ละเครื่อง ทั้งจากการกำหนดด้วยตัวผู้ใช้เองหรือการใช้ดีเฮชซีพี (DHCP)[103] ในการจ่ายหมายเลข IP Address ให้โดยอัตโนมัติ ดังนั้น สิ่งที่เครื่องต้นทางและเครื่อง

---

102 IP Address คือหมายเลขประจำเครื่องคอมพิวเตอร์ ซึ่งประกอบด้วยตัวเลข 4 ชุด มีเครื่องหมายจุดขั้นระหว่างชุด เช่น 192.168.100.1 หรือ 172.16.10.1 เป็นต้น มาตรฐานของ IP Address ปัจจุบันเป็นมาตรฐาน Version 4 หรือที่เรียกกันสั้นๆ ว่า IPv4 ซึ่งกำหนดให้ IP Address มีทั้งหมด 32 bit หรือ 4 byte แต่ละ byte จะถูกคั่นด้วยจุด (.) ภายในหมายเลขที่มองเห็นยังถูกแบ่งออกเป็น 2 ส่วน ดังนี้

1. Network Address หรือ Subnet Address

2. Host Address

ทั้งนี้ บนเครื่องคอมพิวเตอร์ที่ใช้ TCP/IP Protocol จะมีหมายเลข IP Address กำกับอยู่ Address นี้ อยู่ใน Layer 3 ของ OSI model ซึ่งสามารถเปลี่ยนแปลงได้ตลอดเวลา (Logical address) และบนเครื่อง คอมพิวเตอร์ไม่ว่าจะใช้โปรโตคอลใดๆ ก็ตามจะต้องมีหมายเลขที่เรียกว่า MAC Address ประจำอยู่ที่ Network card เสมอ MAC Address นี้เป็น Hardware Address ที่เปลี่ยนแปลงไม่ได้ เว้นแต่จะเปลี่ยน Network card ส่วนการแบ่งขนาดของเครือข่าย สามารถแบ่งขนาดของการแจกจ่าย Network Address ได้ 3 ขนาด คือ

1. Class A nnn.ccc.ccc.ccc (nnn ชุดแรก ตัวเลขอยู่ระหว่าง 1-126) เครือข่าย Class A สามารถแจกจ่าย IP Address ได้มากที่สุดถึง 16 ล้านหมายเลข

2. Class B nnn.nnn.ccc.ccc (nnn ชุดแรก ตัวเลขอยู่ระหว่าง 128-191) เครือข่าย Class A สามารถแจกจ่าย IP Address ได้มากเป็นอันดับสอง คือ 65,000 หมายเลข

3. Class C nnn.nnn.nnn.ccc (nnn ชุดแรก ตัวเลขอยู่ระหว่าง 192-233) เครือข่าย Class A สามารถแจกจ่าย IP Address ได้น้อยที่สุด คือ 256 หมายเลข

หมายเหตุ nnn หมายถึง Network Address และ ccc หมายถึง Computer Address ที่มา http://www.compspot.net/index.php?option=com_content&task=view&id=94&Itemid=46 Retrieved September, 15, 2010

103 DHCP คือ โปรโตคอลที่ใช้ในการกำหนด IP Address อัตโนมัติแก่เครื่องลูกข่ายบนระบบที่ติดตั้ง TCP/IP สำหรับ DHCP Server มีหน้าที่แจก IP Address ในเครือข่ายไม่ให้ซ้ำ เป็นการลดความซ้ำซ้อน เมื่อเครื่องลูกข่ายเริ่มบู๊ตก็จะขอ IP Address, Subnet mark, หมายเลข DNS และ Default gateway ขั้นตอนการเชื่อมต่อของเครื่องลูกข่ายกับ DHCP server มี 4 ขั้นตอน คือ (1) เครื่องลูกค้นหาเครื่อง DHCP server ในเครือข่ายโดยส่ง DHCP discover เพื่อร้องขอ IP address (2) DHCP Server จะค้นหา IP Address ที่ว่างอยู่ในฐานข้อมูล แล้วส่ง DHCP offer กลับไปให้เครื่องลูก (3) เมื่อเครื่องลูกได้รับ IP Address ก็จะส่งสัญญาณตอบกลับ DHCP Request ให้เครื่องแม่ทราบ (4) DHCP Server ส่งสัญญาณ DHCP Ack กลับไปให้เครื่องลูก เพื่อแจ้งว่าเริ่มใช้งานได้ ที่มา http://guru.google.co.th/guru/thread?tid=526b8646975ec951 Retrieved September, 15, 2010

ปลายทางต้องการสอบถามเพื่อให้แน่ใจว่าเป็นเครื่องที่ต้องการติดต่อหรือไม่ก็คือ MAC Address นั่นเอง โดยการใช้โปรโตคอล ARP (Address Resolution Protocol) ในการแปลงหมายเลข IP Address ให้เป็น MAC Address ของเครื่องที่ต้องการติดต่อ

เพื่อประกอบการทำความเข้าใจในการทำงานของอุปกรณ์รวมสัญญาณและการดักรับหรือดักจับข้อมูลของแฮกเกอร์หรือผู้บุกรุก ผู้เขียนจึงขอยกตัวอย่างการทำงานของสวิทซ์ กล่าวคือ ในกรณีที่เครื่องต้นทางและสวิทซ์กระจายข้อมูลไปยังทุกๆ เครื่องในเครือข่าย เพื่อสอบถามว่าหมายเลข IP Address 192.168.1.100 ของเครื่องปลายทางมี MAC Address อะไร จะเรียกว่า “ARP Request” และเมื่อมีการตอบกลับจากเครื่องปลายทางว่า หมายเลข IP Address 192.168.1.100 มี MAC Address อะไร จะเรียกว่า “ARP Reply” ซึ่งการตอบกลับไปมาระหว่าง ARP Request และ ARP Reply นี้เอง ที่ทำให้เกิดช่องโหว่ให้แฮกเกอร์หรือผู้บุกรุกใช้โปรแกรมสนิ๊ฟเฟอร์ดักรับหรือดักจับข้อมูลที่วิ่งอยู่ระหว่างทั้งสองเครื่องนี้ได้ โดยใช้เทคนิค ARP Spoof เพื่อหลอกให้เครื่องต้นทางและเครื่องปลายทางเข้าใจผิด และทำให้ทั้งสองเครื่องนี้ส่งข้อมูลวิ่งผ่านมาที่เครื่องของแฮกเกอร์หรือผู้บุกรุกที่เป็นตัวกลางอยู่ระหว่างเครื่องต้นทางและเครื่องปลายทาง โดยเรียกการกระทำดังกล่าวว่า “Man In The Middle (MITM)”

สำหรับหลักในการทำงานของ ARP Spoof และ MITM นั้น จะเป็นรูปแบบการโจมตีที่มีการทำงานร่วมกันโดย ARP Spoof จะอาศัยช่องโหว่ในการทำงานของสวิทซ์ที่ต้องมีการทำ ARP Request และ ARP Reply ระหว่างเครื่องต้นทางและเครื่องปลายทาง เมื่อเครื่องต้นทางเริ่มทำงานโดยกระจายสัญญาณ ARP Request ออกไปยังทุกเครื่องที่อยู่ในเครือข่าย เพื่อตรวจสอบว่าหมายเลข IP Address 192.168.1.100 ของเครื่องปลายทางมี MAC Address อะไรบ้าง ในขั้นตอนการทำงานปกติ เครื่องปลายทางก็จะส่งสัญญาณ ARP Reply กลับไปยังเครื่องต้นทางเพื่อตอบกลับไปว่าหมาย IP Address นี้ มี MAC Address อะไร ตัวอย่าง เช่น เครื่องปลายทางหมายเลข IP Address 192.1.100 มี MAC Address คือ BB 00 00 00 00 02 ดังนั้น เมื่อเครื่องต้นทางได้รับ APR Reply จากเครื่องปลายทางก็จะระบุข้อมูลที่ได้ไปเก็บไว้ในตาราง MAC Address เพื่อนำไปใช้ในภายหลัง ซึ่งหากมีการติดต่อกันอีกก็จะสามารถติดต่อกันได้โดยตรงไม่จำเป็นต้องทำ ARP Request และ ARP Reply อีกครั้ง แต่ในระหว่างที่มีการทำ ARP Request และ ARP Reply นี้ แฮกเกอร์หรือผู้บุกรุกจะใช้เทคนิค ARP Spoof โดยการส่งแพ็คเก็ตปลอมไปยังเครื่องต้นทางและเครื่องปลายทาง เพื่อทำให้เครื่องทั้งสองเกิดความเข้าใจผิด เพราะแทนที่จะรับส่งข้อมูลกันโดยตรงระหว่างสองเครื่อง กลับต้องมีการส่งข้อมูลนั้นผ่านไปทางเครื่องของแฮกเกอร์หรือผู้บุกรุกที่เป็นตัวกลาง (เรียกว่า “Man In The Middle”) เสียก่อนโดยที่ทั้งเครื่องต้นทางและเครื่องปลายทางไม่รู้ตัว

ซึ่งตรงจุดนี้เองที่แฮกเกอร์หรือผู้บุกรุกจะใช้โปรแกรมสนิ๊ฟเฟอร์ดักรับหรือดักจับข้อมูลที่วิ่งผ่านเข้ามาแล้วนำข้อมูลไปใช้ในการกระทำความผิดอื่นต่อไป

มีตัวอย่างคดีการดักข้อมูลในเครือข่ายคอมพิวเตอร์ คือคดี "c0mrade" ตาม กฎหมาย U.S.C. 2511 Interception and disclosure of wire, oral, or electronic communications prohibited และ U.S.C. 1030 Fraud and Related Activity in connection with computers มาตรา (a) (1)-(3) ของประเทศสหรัฐอเมริกาเกี่ยวกับการห้ามดัก และเปิดเผยข้อมูลในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ และการฉ้อโกงและการกระทำที่เกี่ยวข้องกับคอมพิวเตอร์ คดีนี้มีข้อเท็จจริงว่าผู้กระทำความผิดเป็นเด็กอายุ 16 ปี จากมลรัฐไมอามี่ ประเทศสหรัฐอเมริกา ใช้ชื่อในอินเทอร์เน็ตว่า "c0mrade" โดยในระหว่างวันที่ 23 สิงหาคม 2542 ถึง 27 ตุลาคม 2542 ผู้กระทำความผิดได้บุกรุกเครือข่ายคอมพิวเตอร์ทางทหารของ Defense Threat Reduction Agency (DTRA) ซึ่งเป็นหน่วยงานหนึ่งของกระทรวงกลาโหมของสหรัฐอเมริกา (Department of Defense) ที่ทำหน้าที่ลดภัยคุกคามจากอาวุธนิวเคลียร์ อาวุธชีวภาพ และอาวุธร้ายแรงอื่นๆ ต่อสหรัฐอเมริกา โดยการบุกรุกดังกล่าวผู้กระทำความผิดได้เข้าถึงเครื่องแม่ข่าย (Computer Server) ที่ทำหน้าที่เป็นอุปกรณ์จัดเส้นทาง (Router) ซึ่งตั้งอยู่ในดัลลัส และได้ติดตั้งโปรแกรม Backdoor ไว้ในเครื่องแม่ข่ายดังกล่าว โปรแกรม Backdoor ได้ดักข้อความอิเล็กทรอนิกส์ที่ส่งมาถึงหรือส่งไปจากเจ้าหน้าที่ของ DTRA มากกว่า 3,000 ข้อความ อีกทั้ง ผู้กระทำความผิดยังได้ดักเอาข้อมูลที่เป็นชื่อผู้ใช้ (User Names) และรหัสผ่าน (Passwords) เข้าสู่ระบบคอมพิวเตอร์ทางทหารของเจ้าหน้าที่ DTRA อย่างน้อย 10 รายการ นอกจากนี้แล้ว ระหว่างวันที่ 29 ถึง 30 มิถุนายน 2542 ผู้กระทำความผิดได้เข้าถึงโดยมิชอบด้วยกฎหมาย (Illegally Accessed) ซึ่งเครื่องคอมพิวเตอร์ขององค์การนาซ่า (NASA) จำนวน 13 เครื่อง และโดยการเข้าถึงดังกล่าวผู้กระทำความผิดได้ดาวน์โหลดเอาโปรแกรมคอมพิวเตอร์ของ NASA ที่มูลค่าถึง 1.7 ล้านเหรียญสหรัฐ และด้วยการลักเอาโปรแกรมคอมพิวเตอร์ไปนั้นทำให้ NASA ต้องปิดระบบคอมพิวเตอร์เป็นเวลา 21 วันในเดือนกรกฎาคม 2542 ทำให้ NASA ได้รับความเสียหายประมาณ 41,000 เหรียญสหรัฐอเมริกา ผู้กระทำความผิดถูกศาลตัดสินลงโทษด้วยการถูกควบคุมตัวไว้ในสถานกักขังเป็นเวลา 6 เดือน และต้องเขียนจดหมายไปขอโทษกระทรวงกลาโหมและองค์การนาซ่า อีกทั้งต้องให้ความตกลงในการเปิดเผยรายละเอียดของคดีนี้ต่อสาธารณชน

6.2.2 การดักข้อมูลผ่านปุ่มคีย์บอร์ดด้วยมัลแวร์

การดักข้อมูลคอมพิวเตอร์อีกวิธีหนึ่งก็คือ การดักข้อมูลผ่านปุ่มคีย์บอร์ดด้วยชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์ โดยวิธีการนี้แฮกเกอร์หรือผู้บุกรุกจะนิยมใช้กันมากในปัจจุบัน ซึ่งนอกจากแฮกเกอร์หรือผู้บุกรุกจะได้ทั้งชื่อผู้ใช้และรหัสผ่านแล้ว ก็ยังอาจได้ไปซึ่งข้อมูลอื่นๆ ที่เป็นความลับที่ผู้ใช้ได้พิมพ์ลงไปในโปรแกรมต่างๆ อีกด้วย ทั้งนี้ การดักข้อมูลผ่าน

ปุ่มคีย์บอร์ดสามารถทำได้หลายวิธีแต่ส่วนใหญ่จะใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันที่ชื่อ “คีย์ล็อกเกอร์ (Key Logger)” ในการทำงาน โดยก่อนอื่นแฮกเกอร์หรือผู้บุกรุกจะต้องหาทางเข้าถึงคอมพิวเตอร์ที่เป็นเครื่องเป้าหมายให้ได้เสียก่อน โดยอาจจะใช้วิธีการเจาะระบบเข้าไปตรงๆ หรือใช้วิธีการหลอกล่อเพื่อให้เจ้าของเครื่องหรือเหยื่อให้ความยินยอมเพื่อการเข้าไปในระบบเสียก่อน หลังจากนั้นแฮกเกอร์หรือผู้บุกรุกจึงจะติดตั้งโปรแกรมคีย์ล็อกเกอร์ลงไปแล้วกำหนดค่าการทำงานของโปรแกรมให้อยู่ในโหมด Stealth เพื่อทำงานแบบซ่อนตัวไม่ให้ผู้ใช้เครื่องเป้าหมายรู้ตัว หลังจากแฮกเกอร์หรือผู้บุกรุกติดตั้งโปรแกรมคีย์ล็อกเกอร์บนเครื่องเป้าหมายสำเร็จแล้ว ทุกครั้งที่ผู้ใช้เครื่องเป้าหมายมีการกดปุ่มใดๆ ที่คีย์บอร์ด โปรแกรมก็จะส่งค่าการกดปุ่มเหล่านั้นกลับไปยังแฮกเกอร์หรือผู้บุกรุก หรืออาจมีการเก็บไว้ในรูปแบบของไฟล์เอกสาร (Textfile) หรือไฟล์ HTML แล้วส่งออกไป ซึ่งหากมีการพิมพ์ชื่อผู้ใช้งานหรือรหัสผ่านเพื่อใช้งานในระบบต่างๆ รหัสที่พิมพ์ก็จะถูกเก็บไว้ด้วย

ปัจจุบันโปรแกรมคีย์ล็อกเกอร์มีให้เลือกใช้อยู่มากมายหลายโปรแกรม บางโปรแกรมจะมีความสามารถสูง เช่น นอกจากจะดักจับการกดปุ่มคีย์บอร์ดแล้วยังสามารถจับภาพหน้าจอหรือควบคุมการทำงานในส่วนต่างๆ ของคอมพิวเตอร์ได้อีกด้วย ตัวอย่างโปรมแกรมคีย์ล็อกเกอร์ เช่น Family Keylogger Keystroke Spy เป็นต้น

7. ความเสียหายและผลกระทบจากชุดคำสั่งไม่พึงประสงค์ต่อข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์

จากรูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ตามที่ได้กล่าวไปแล้วในข้อ 6 ข้างต้น ซึ่งได้แก่ การเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ และการดักข้อมูลนั้น ย่อมก่อให้เกิดความเสียหายและส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และระบบเครือข่ายคอมพิวเตอร์ (Computer Network Security) ทั้งต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ทั้งนี้ จะขอกล่าวถึงความเสียหายและผลกระทบจากชุดคำสั่งไม่พึงประสงค์ต่อข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ดังนี้

7.1 ความเสียหายและผลกระทบต่อการรักษาความลับ (Confidentiality)

ความลับของข้อมูลถือเป็นหัวใจสำคัญที่เจ้าของข้อมูลต้องการรักษาไว้มิให้ผู้ใดล่วงรู้ ตัวอย่างข้อมูลที่เจ้าของข้อมูลต้องการเก็บรักษาไว้เป็นความลับ เช่น ข้อมูลส่วนตัว (privacy data) รหัสผ่าน (passwords) หรือความลับทางการค้า (secret trade) เป็นต้น ซึ่งการจะถือว่าเป็นการกระทบต่อการรักษาความลับหรือไม่นั้นอาจพิจารณาได้จากข้อมูลนั้น สามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งสอดคล้องกับประโยคคำถามที่ว่า “ใครที่ได้รับอนุญาตให้ใช้ข้อมูลนั้น?” (Who is authorized to use data?) ตัวอย่าง เช่น ข้อมูลอีเมล์ในเมล์บ๊อกซ์ของผู้ใช้ ผู้ที่มีสิทธิ์เข้าถึงอีเมล์บ๊อกซ์และเปิดอ่านจดหมายได้จะต้องเป็นเจ้าของเมล์บ๊อกซ์นั้น เช่น เมล์บ๊อกซ์ของบัญชีอีเมล์ somchai@mictmail.com ที่เจ้าของคือ สมชายนั้นต้องมีแค่สมชายเพียงคนเดียวเท่านั้นที่เข้าถึงและเปิดอ่านจดหมายในเมล์บ๊อกซ์นี้ได้ ผู้ใช้คนอื่นๆ เช่น somsak@mictmail.com หรือ somkiet@mictmail.com ไม่สามารถเข้าถึงเมล์บ๊อกซ์และเปิดอ่านจดหมายของสมชายได้

การคุกคามต่อข้อมูลที่เป็นความลับถือเป็นเรื่องอันตรายมาก เนื่องจากแฮกเกอร์หรือผู้โจมตีอาจนำข้อมูลเหล่านั้นไปใช้ในการดำเนินการที่ผิดกฎหมายต่อไป และในโลกที่การซื้อสินค้าออนไลน์และระบบธนาคารทางอินเทอร์เน็ตหรือระบบอินเทอร์เน็ตแบงก์กิ้งได้รับความนิยมอย่างแพร่หลาย การคุมคามในลักษณะนี้จึงส่งผลกระทบและทำให้ผู้ใช้เสียเงินเป็นจำนวนมาก โดยเฉพาะอย่างยิ่งถ้ามีการเปิดเผยข้อมูลบัตรเครดิตหรือข้อมูลทางธนาคาร

สำหรับกลไกในการควบคุมรักษาความลับของข้อมูลสามารถทำได้โดยการควบคุมการเข้าถึงระบบ (Access Control) เช่น การล็อกอินโดยใช้บัญชีอีเมล์ (username) และรหัสผ่าน (password) การป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและการป้องกันการเข้าถึงข้อมูลโดยตรง เป็นต้น ในกรณีที่มีการส่งข้อมูลลับผ่านระบบเครือข่ายที่สามารถดักจับและอ่านข้อมูลได้ จะต้องมีการเข้ารหัสข้อมูล (Cryptography & Encryption) ตัวอย่างเช่น เว็บไซต์ e-Commerce ที่มีการรับส่งข้อมูลระหว่างบราวเซอร์กับเว็บเซิร์ฟเวอร์บนช่องทาง SSL โดยใช้โปรโตคอล https ซึ่งมีการเข้ารหัสข้อมูล เป็นต้น

7.2 ความเสียหายและผลกระทบต่อความครบถ้วนสมบูรณ์ (Integrity)

การรักษาความครบถ้วนสมบูรณ์ หมายถึง การป้องกันเพื่อให้ข้อมูลไม่ถูกแก้ไขเปลี่ยนแปลง หรือถูกทำลายได้ สอดคล้องกับประโยคคำถามที่ว่า “ข้อมูลยังอยู่ในสภาพเดิมหรือไม่? (Is data good?)” เป็นการทำให้ข้อมูลนั้นมีความน่าเชื่อถือ (ความน่าเชื่อถือว่าข้อมูลนั้นไม่ได้ถูกแก้ไขหรือเปลี่ยนแปลงจากแหล่งเดิมที่มา และความน่าเชื่อถือของแหล่งที่มา) ตัวอย่าง เช่น ผู้ใช้สมชายส่งไฟล์ถึงผู้ใช้ที่ชื่อสมเกียรติ ไฟล์นั้นจะต้องไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยบุคคลอื่นใน

ระหว่างที่ส่งมาเพื่อให้เชื่อได้ว่าไฟล์ไม่ถูกปลอมแปลง รวมทั้งสามารถเชื่อได้ว่าเป็นไฟล์ที่ส่งโดยสมชายจริง ตัวอย่าง การกระทำความผิดที่ส่งผลกระทบและความเสียหายต่อความครบถ้วนสมบูรณ์จากชุดคำสั่งไม่พึงประสงค์ เช่น การป้อนโปรแกรมที่มีไวรัสทำลายข้อมูลหรือโปรแกรมคอมพิวเตอร์ หรือการป้อนหรือส่งม้าโทรจันเข้าไปฝังไว้ในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์สำหรับใช้เพื่อเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใดๆ อันเป็นการรบกวนข้อมูลในภายหลัง เป็นต้น

นอกจากนั้น การรบกวนหรือขัดขวางหรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกติ ไม่ว่าจะเป็นการกระทำในขั้นตอนใดๆ ตั้งแต่การป้อนข้อมูลเข้าไปในระบบหรือในการส่ง ทำลาย ลบ หรือเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำความผิดอาจก่อให้เกิดความเสียหายที่ร้ายแรงหรือรุนแรงต่อการใช้ระบบดังกล่าวหรือต่อการติดต่อสื่อสารกับระบบอื่น เช่น การทำให้ระบบคอมพิวเตอร์ทำงานช้าลง หรือการรบกวนระบบของผู้รับข้อมูลคอมพิวเตอร์โดยการส่งจดหมายอิเล็กทรอนิกส์จำนวนมหาศาลไปยังผู้รับเพื่อให้ระบบคอมพิวเตอร์ทำงานหนักเกินไปจนในที่สุดก็ไม่สามารถทำงานได้อีกต่อไป ที่รู้จักกันในชื่อ “spamming” ก็ล้วนแต่เป็นการกระทำความผิดที่ก่อให้เกิดความเสียหายและส่งผลกระทบต่อความครบถ้วนสมบูรณ์ทั้งสิ้น

สำหรับวิธีการในการรักษาความถูกต้องครบถ้วนของข้อมูลสามารถทำได้หลายวิธีด้วยกัน เช่น การใช้เช็คซัม (checksum) ตัวอย่างเช่น ตรวจสอบไฟล์ที่ดาวน์โหลดจากเว็บไซต์ว่าตรงกับต้นฉบับหรือไม่ สามารถทำได้ด้วยการตรวจสอบจากค่าเช็คซัม (เช่น การใช้มาตรฐาน MD5 เป็นต้น) ส่วนการตรวจสอบการปลอมแปลงไฟล์บน Linux สามารถตรวจสอบ checksum ได้โดยใช้โปรแกรม Tripwire เป็นต้น ซึ่งทั้งหมดนี้เป็นการประยุกต์ใช้การเข้ารหัสข้อมูล (Cryptography & Encryption)

7.3 ความเสียหายและผลกระทบต่อเสถียรภาพในการใช้งาน (Availability)

เสถียรภาพในการใช้งาน หมายถึง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์จะต้องมีสภาพพร้อมใช้งานอยู่ตลอดเวลา สอดคล้องกับประโยคคำถามที่ว่า “สามารถเข้าถึงและใช้งานข้อมูลได้เมื่อต้องการหรือไม่? (Can access data whenever need it?)”

การทำให้เกิดความเสียหายและส่งผลกระทบต่อเสถียรภาพในการใช้งาน จึงหมายถึง การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เสื่อมค่าหรือไร้ประโยชน์ เช่น การลบหรือทำลายข้อมูลคอมพิวเตอร์ หรือกระทำการใดๆ ให้ไม่สามารถเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้นได้ เป็นต้น

ตัวอย่างของความเสียหายและผลกระทบต่อเสถียรภาพในการใช้งาน เช่น เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นเมล์เซิร์ฟเวอร์ที่ชื่อ mictmail.com ถูกโจมตีจากแฮกเกอร์เพื่อให้เกิดการปฏิเสธการให้บริการ (denail of service) เมื่อเมล์เซิร์ฟเวอร์นี้ล่มและไม่สามารถให้บริการผู้ใช้ได้ต้องรอจนกว่าผู้ดูแลระบบจะแก้ไขเพื่อให้ระบบสามารถกลับมาใช้งานได้เหมือนเดิม เป็นต้น ทั้งนี้ หากระบบเมล์นี้ถูกออกแบบให้มีระบบ Mail Backup ที่สามารถทำงานแทนเมล์เซิร์ฟเวอร์ตัวหลักได้ทันทีหากเมล์เซิร์ฟเวอร์ตัวหลักไม่สามารถให้บริการได้ ผู้ใช้ก็จะสามารถเข้าถึงข้อมูลในเมล์บ๊อกซ์เพื่อเปิดอ่านอีเมล์ได้ตลอด

สำหรับการป้องกันเพื่อให้เกิดความพร้อมใช้งานข้อมูล มักจะต้องคำนึงถึงเกี่ยวกับ Load Balanzing, Fail Over, Back Up, ระบบไฟฟ้าสำรอง, การ Hardening เพื่อทำให้เครื่องแม่ข่ายและระบบเครือข่ายมีความแข็งแกร่งและมีความทนทานต่อการโจมตีแบบ DoS

8. ความเสียหายและผลกระทบจากชุดคำสั่งไม่พึงประสงค์ต่อความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชน

ในชีวิตประจำวันของประชาชนผู้ใช้งานอินเทอร์เน็ตเพื่อการติดต่อสื่อสารไม่ว่าจะเป็นการติดต่อสื่อสารกันในเรื่องส่วนตัว หรือในเชิงของธุรกิจต่างๆ อาจมีความจำเป็นต้องบอกข้อมูลส่วนตัวให้ผู้อื่นได้รับทราบจนเป็นเรื่องปกติ เช่น ข้อมูลส่วนตัวที่ให้ในระหว่างการจ่ายเงินค้างชำระ การเตรียมการเดินทาง การใช้บัตรเครดิตในการจับจ่ายใช้สอยเป็นต้น ข้อมูลที่ให้ไปนี้อาจถูกส่งต่อไปให้กับผู้อื่นต่อไปซึ่งทำให้ผู้ให้ข้อมูลขาดความมั่นใจว่าผู้รับจะนำข้อมูลของตนไปเผยแพร่ต่อหรือไม่ และมีบางกลุ่มที่ถึงขนาดมองว่าความเสี่ยงของข้อมูลส่วนตัวในเครือข่ายอินเทอร์เน็ตนั้นมีมากกว่าในโลกแห่งความเป็นจริงในทางกายภาพ ตัวอย่าง เช่น ในขั้นตอนของการสั่งซื้อสินค้า ผู้ซื้ออาจจำเป็นต้องให้ข้อมูลส่วนตัวและหมายเลขบัตรเครดิตกับผู้ขายหรือร้านนั้นโดยผ่านทางอินเทอร์เน็ตซึ่งหากระบบการสั่งซื้อของร้านค้านั้นไม่มีความปลอดภัยอย่างเพียงพอก็อาจมีผู้อื่นแอบดักข้อมูลดังกล่าวไปได้ แม้ว่าปัจจุบัน ฝ่ายผู้ขายหรือร้านค้าที่ทำธุรกิจผ่านทางเว็บไซต์จะให้ความสำคัญและมีนโยบายเกี่ยวกับความเป็นส่วนตัว (Privacy Policy) และพยายามบอกแก่ลูกค้าผู้เข้ามาใช้บริการเว็บไซต์ของตนว่าทางเว็บไซต์มีนโยบายและแนวปฏิบัติเกี่ยวกับการเก็บรวบรวม การประมวลผล การใช้ และการเปิดเผยข้อมูลส่วนบุคคลของลูกค้าที่เข้ามาเยี่ยมชมหรือใช้บริการเว็บไซต์อย่างไรบ้าง แต่ปัญหาที่สำคัญประการหนึ่งที่มักจะเกิดขึ้นกับการจัดให้มีนโยบายความเป็นส่วนตัวก็คือ จะทราบได้อย่างไรว่านโยบายที่จัดแสดงไว้นั้นเพียงพอต่อการก่อให้เกิดความ

น่าเชื่อถือแก่ตัวลูกค้าที่เข้ามาใช้บริการเว็บไซต์ หรือแม้กระทั่งจะทราบได้อย่างไรว่านโยบายความเป็นส่วนตัวดังกล่าวได้มาตรฐานตามที่เจ้าของเว็บไซต์ต้องการแล้ว

ตัวอย่างในต่างประเทศจะมีการส่งอีเมล์แอบอ้างว่ามาจากกรมสรรพากรของประเทศนั้นๆ เพื่อหลอกล่อให้เหยื่อกรอกข้อมูลส่วนตัวที่สำคัญเพื่อนำไปใช้หาผลประโยชน์ต่อไป เป็นต้น นอกจากนี้ ยังมีความเสียหายอื่นๆ อันเป็นพลพวงมาจากการใช้งานอินเทอร์เน็ตที่อาจเกิดขึ้นและส่งผลกระทบต่อความเป็นอยู่ส่วนตัวในการสื่อสารของประชาชน เช่น การละเมิดทรัพย์สินทางปัญญา การหลอกลวงทางอีเมล์ การถูกติดตามบนเครือข่าย เป็นต้น

อย่างไรก็ตาม เพื่อให้อยู่ในการประเด็นการวิจัย ผู้เขียนจึงจะขอกล่าวถึงเฉพาะความเสียหายและผลกระทบต่อความเป็นอยู่ส่วนตัวในการสื่อสารของประชาชน (the right of privacy of data communication) ที่เกิดจากชุดคำสั่งไม่พึงประสงค์เท่านั้น โดยมีตัวอย่างของการนำมัลแวร์มาใช้และมีผลกระทบอย่างรุนแรง ได้แก่ โปรแกรม “Storm Worm” หรือ “Nuwar@MM Worm” ซึ่งมาในรูปแบบของจดหมายลูกโซ่ที่กล่าวถึงผู้เสียชีวิตชาวยุโรปจากพายุ โดยอาศัยชื่อพายุดึงความสนใจคนอ่านเมล์พบว่าคนยุโรปตกเป็นเหยื่อสูงสุด ขณะที่ชาวอเมริกันและเอเชียพบว่าตกเป็นเหยื่อน้อยกว่า เนื่องจากถือเป็นเหตุไกลตัวจึงมีความสนใจน้อยกว่า แต่หากมีการเปลี่ยนชื่ออีเมล์เป็น “สึนามิ” ก็อาจมีคนเอเชียติดหนอนดังกล่าวมากกว่านี้ก็เป็นไปได้ อนึ่ง โปรแกรม “Storm Worm” นั้น ไม่ใช่มัลแวร์ธรรมดาแต่เป็นมัลแวร์ที่ทำการยึดเครื่องของผู้ใช้หรือเหยื่อให้กลายเป็นบ๊อท (BOT ย่อมาจาก Robot ซึ่งเป็นการเปรียบเทียบว่าเหมือนหุ่นยนต์ซึ่งถูกควบคุม) โดยมีชื่อในเครือข่ายตามที่เรียกกันทั่วไปว่า “บ๊อทเน็ต” (BOTNET ย่อมาจาก Robot Network ซึ่งเป็นการเปรียบเทียบว่าเหมือนหุ่นยนต์ซึ่งถูกควบคุมผ่านเครือข่ายอินเทอร์เน็ต) ของแฮกเกอร์อีกด้วย การเป็นบ๊อทเน็ตดังกล่าวจะทำให้แฮกเกอร์สามารถเข้าควบคุมเครื่องคอมพิวเตอร์ของเหยื่อได้จากระยะไกล ซึ่งขณะนี้มีการตรวจพบบ๊อทที่เกิดจากไวรัส “Storm Worm” แล้วทั่วโลกกว่า 50 ล้านเครื่องที่ถูกโจมตี นับว่าเป็นการโจมตีครั้งใหญ่อีกครั้งหนึ่งของแฮกเกอร์

อนึ่ง ยังมีการโจมตีด้วยมัลแวร์บนโทรศัพท์มือถือที่ตรวจพบเมื่อปี พ.ศ. 2547 คือ ไวรัส SymbOS.Cabir ซึ่งถือเป็นมัลแวร์ชนิดแรกบนโทรศัพท์มือถือ แต่ก็ไม่ได้สร้างความเสียหายหรือส่งผลกระทบที่รุนแรงมากนัก อย่างไรก็ตาม ได้มีการค้นพบหนอนที่ชื่อ Cabir.A ซึ่งทำงานภายใต้ระบบปฏิบัติการ Sysbian ของโทรศัพท์มือถือที่ส่งผลกระทบต่อเครื่องโทรศัพท์มือถือตระกูล 60 ของยี่ห้อ Nokia ค่อนข้างรุนแรง หนอนชนิดนี้มีขนาดเพียง 15,104 ไบต์ สามารถแพร่กระจายบน

ระบบปฏิบัติการ Symbian เท่านั้น ซึ่งจะส่งตัวเองในรูปแบบของ SIS[104] ที่ชื่อว่า CARIBE.SIS โดยจะทำการติดตั้งตัวมันเองลงบนโฟลเดอร์ APPS และจะทำการฝังตัวลงที่หน่วยความจำตำแหน่ง 0x101F6F88 และแพร่กระจายผ่านเทคโนโลยี Bluetooth นอกจากนี้ในปัจจุบันยังพบการแพร่กระจายของมัลแวร์ผ่านทางระบบ SMS หรือ MMS อีกด้วย

ทั้งนี้ ยังมีความเสียหายและผลกระทบต่อความเป็นอยู่ส่วนตัวในการสื่อสารของประชาชนที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทสปายแวร์หรือแอดแวร์ที่ควรกล่าวถึงอีกด้วย สาเหตุก็เพราะความนิยมในการใช้งานอินเทอร์เน็ตในปัจจุบัน จึงทำให้อินเทอร์เน็ตกลายเป็นแหล่งโฆษณาสินค้าและบริการแหล่งใหญ่ ซึ่งบ่อยครั้งที่เครื่องคอมพิวเตอร์เกิดปัญหาขึ้น ก็มักจะพบว่ามีสาเหตุมาจาก สปายแวร์หรือแอดแวร์ที่เข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้งานหรือเจ้าของเครื่องไม่รู้ตัว เช่น อาจมีหน้าต่างโฆษณาเล็กๆ แบบ Pop-up ปรากฏขึ้นมาขณะที่เจ้าของกำลังใช้งานเครื่องคอมพิวเตอร์อยู่ หรือเมื่อมีการเปิดเว็บบราวเซอร์ๆ อาจจะทำการติดต่อไปยังเว็บไซต์หลักของตัวสปายแวร์ที่ถูกตั้งค่าไว้ และสปายแวร์อาจทำการติดตามเว็บไซต์ที่มีการเข้าไปเยี่ยมชมบ่อยๆ ก็ได้

สำหรับสปายแวร์บางชนิดจะมีลักษณะรุกรานระบบโดยจะทำการติดตามเพื่อค้นหาคีย์หรือรหัสผ่านที่ผู้ใช้งานพิมพ์ลงไป เมื่อสปายแวร์ได้แอบเข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์แล้วก็จะพยายามรันหรือประมวลผลแบบพิเศษบางอย่างซึ่งจะเป็นผลทำให้เครื่องคอมพิวเตอร์ทำงานช้าลงหรืออาจทำการเข้าสู่เว็บไซต์ต่างๆ ได้ช้า หรืออาจเข้าสู่เว็บไซต์ที่ต้องการไม่ได้

อาการที่แสดงว่าเครื่องคอมพิวเตอร์ติดสปายแวร์หรือแอดแวร์ เช่น จะพบว่ามีหน้าต่างเล็กๆ ที่เป็นโฆษณาแบบ Pop-up ขึ้นมาเองบ่อยครั้งจนนับไม่ถ้วน หรือเมื่อต้องการเข้าสู่เว็บไซต์ใดเว็บไซต์หนึ่งและพิมพ์ URL ลงไปอย่างถูกต้องแล้วแต่เว็บบราวเซอร์จะเข้าสู่เว็บไซต์ที่สปายแวร์ได้ตั้งไว้และจะแสดงหน้าเว็บเหล่านั้นแทนที่จะเข้าไปยังเว็บไซต์ที่ต้องการ หรือจะสังเกตเห็นว่ามีแถบเครื่องมือใหม่ๆ ที่ไม่เคยเห็นหรือไม่คุ้นเคยเกิดขึ้นบนเว็บบราวเซอร์ หรืออาจปรากฏแถบแสดงเครื่องมือหรือไอคอนที่ไม่เคยเห็นมาก่อน หรือฟังก์ชั่นบนปุ่มคีย์บอร์ดบางอย่างที่เคยใช้งานจะเกิดอาการผิดปกติ เช่น เคยกดปุ่ม tab เพื่อเลื่อนไปยังช่องกรอกข้อความในฟิลด์ถัดไปบนหน้าเว็บจะไม่สามารถใช้ในการเลื่อนตำแหน่งได้เหมือนเดิม เป็นต้น

---

104 SIS เป็นนามสกุลของไฟล์ที่ใช้ในระบบปฏิบัติการของโทรศัพท์มือถือซึ่งคล้ายๆ กับไฟล์ที่มีนามสกุล .zip หรือ .rar ในระบบปฏิบัติการของคอมพิวเตอร์ ซึ่งเป็นวิธีการที่ทำให้ไฟล์มีขนาดเล็กลงเพื่อความสะดวกสำหรับการพกพา การส่งต่อ หรือการนำไปใช้

ผลกระทบที่ตามมาเมื่อเครื่องคอมพิวเตอร์ติดสปายแวร์หรือแอดแวร์ ได้แก่ ข้อความแสดงความผิดพลาดของซอฟต์แวร์จะเริ่มปรากฏบ่อยมากขึ้น และเครื่องคอมพิวเตอร์จะทำงานช้าลงอย่างเห็นได้ชัดเมื่อสั่งเปิดโปรแกรมหลายโปรแกรมหรือทำงานหลายอย่าง โดยเฉพาะในระหว่างการบันทึกแฟ้มข้อมูล จนอาจถึงขั้นทำให้เครื่องคอมพิวเตอร์ไม่สามารถตอบสนองการทำงานได้ และต้องทำการติดตั้งระบบปฏิบัติการหรือซอฟท์แวร์อื่นๆ ใหม่ อันเป็นที่มาของการสิ้นเปลืองค่าใช้จ่ายตามมา

บทที่ 3
มาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศ

ในปัจจุบันมีหลายประเทศได้บัญญัติกฎหมายเพื่อใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ เนื่องจากกฎหมายที่มีอยู่เดิมไม่สามารถใช้บังคับกับการก่ออาชญากรรมทางคอมพิวเตอร์หรือการใช้คอมพิวเตอร์ในทางมิชอบได้ โดยบางประเทศได้บัญญัติเป็นกฎหมายพิเศษ หรือในบางประเทศอาจต้องปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่ให้ทันต่อการกระทำความผิดดังกล่าว หรือในบางประเทศอาจใช้ทั้งสองวิธีคือทั้งการปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่และบัญญัติเป็นกฎหมายพิเศษเพื่อการกำหนดฐานความผิดและบทกำหนดโทษขึ้นมาเป็นการเฉพาะเป็นเรื่องๆ ไป ภายใต้ความเหมาะสมของแต่ละประเทศ ทั้งนี้ก็เพื่อให้กฎหมายที่มีอยู่สามารถบังคับใช้และทันต่อการกระทำความผิดดังกล่าวได้ โดยกฎหมายของต่างประเทศตามที่ปรากฏใน A Global Survey of Cybercrime Legislation[105] ซึ่งสำรวจข้อมูลโดย Chief Judge Stein Schjolberg, Moss tingrett (Moss District Court), Norway. นั้นพบว่า กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในโลกนี้มีอยู่หลายประเภทแต่ส่วนใหญ่มักจะบัญญัติให้อยู่ในรูป กฎหมายอาชญากรรมทางคอมพิวเตอร์ (Computer Crime Law) กฎหมายเกี่ยวกับการใช้คอมพิวเตอร์ในทางมิชอบ (Computer Misuse Law) หรือกฎหมายด้านโทรคมนาคม (Telecommunication Ordinance or The Electronic Communications and Transactions Act) โดยรูปแบบของการพัฒนากฎหมายในแต่ละประเทศอาจจะหลากหลายแตกต่างกันไปบ้าง แต่ในส่วนของกฎหมายสารบัญญัติเพื่อการกำหนดฐานความผิดหลักมักจะมีความคล้ายคลึงกัน ทั้งนี้โดยคำนึงถึงลักษณะหรือพฤติการณ์ที่กระทำต่อคอมพิวเตอร์และการใช้คอมพิวเตอร์ในการกระทำความผิดเป็นสำคัญ ซึ่งส่วนใหญ่กฎหมายเหล่านั้นล้วนมีการกำหนดฐานความผิดหรือมาตรการเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่ครอบคลุมหรือใกล้เคียงกับฐานความผิดหลักที่สำคัญ 7 ฐานตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของคณะมนตรีแห่งยุโรป (Council of Europe) ได้แก่ (1) การเข้าถึงโดยมิชอบ (Illegal access) (2) การลักลอบดักข้อมูล (Illegal interception) (3) การรบกวนข้อมูล (Data interference) (4) การรบกวนระบบ (System interference) (5) การใช้อุปกรณ์

---

105 อ่านรายละเอียดและสืบค้นข้อมูลเพิ่มเติมได้ที่ http://www.cybercrimelaw.net

ในทางมิชอบ (Misuse of devices) (6) การปลอมแปลงทางคอมพิวเตอร์ (Computer related-forgery) และ (7) การฉ้อโกงทางคอมพิวเตอร์ (Computer-related fraud)[106]

อย่างไรก็ตาม หากจะพิจารณาเฉพาะฐานความผิดที่อาจใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรปแล้ว จะพบว่ามีเพียง 4 ฐานความผิดเท่านั้น คือ (1) การเข้าถึงโดยมิชอบ (2) การลักลอบดักข้อมูล (3) การรบกวนข้อมูล และ (4) การรบกวนระบบ ส่วนฐานความผิดในการใช้อุปกรณ์ในทางมิชอบ การปลอมแปลงทางคอมพิวเตอร์ และการฉ้อโกงทางคอมพิวเตอร์นั้น โดยพฤติการณ์แล้วมิอาจใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดโดยการเข้าถึงได้ (การเข้าถึงในที่นี้หมายความถึงเฉพาะการเข้าถึงทางอิเล็กทรอนิกส์เท่านั้น) และเมื่อพิจารณาถึงรูปแบบหรือวิธีการกระทำความผิดของทั้ง 4 ฐานความผิดที่อาจใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดดังกล่าวแล้วจะพบว่า มีอยู่เพียง 2 รูปแบบ คือรูปแบบของการเข้าถึง (access) และรูปแบบของการดักรับ (interception) ดังนั้น ชุดคำสั่งไม่พึงประสงค์จึงมีความสัมพันธ์และเกี่ยวข้องกับการเข้าถึงในฐานะที่ชุดคำสั่งไม่พึงประสงค์ถูกใช้เป็นเครื่องมือในการเข้าถึง จึงมีประเด็นปัญหาที่น่าสนใจว่า การกำหนดนิยามและความหมายของการเข้าถึงไว้ในกฎหมายของต่างประเทศในแต่ละประเทศนั้น สามารถจัดการหรือครอบคลุมถึงการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้อย่างไร

สำหรับประเทศไทยแล้ว ปัญหาการบังคับใช้กฎหมายที่เกิดขึ้นในปัจจุบันนั้นเกิดจากรูปแบบของการเข้าถึง ดังนั้น การพิจารณาถึงมาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในกฎหมายต่างประเทศ จึงจะมุ่งศึกษาและพิจารณาไปที่มาตรการป้องกันการกระทำความผิดโดยการเข้าถึงเป็นสำคัญ เนื่องจากหากปราศจากการเข้าถึงแล้วชุดคำสั่งไม่พึงประสงค์ประเภท ม้าโทรจัน หนอนคอมพิวเตอร์บางชนิด แอดแวร์ และสปายแวร์ ก็คงจะถูกส่งและนำไปฝัง

---

106 นอกเหนือจากฐานความผิดที่สำคัญทั้ง 7 ฐานแล้ว ยังมีบทบัญญัติในฐานความผิดที่เกี่ยวกับเนื้อหาสาระ ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง การพยายามและการสนับสนุนการกระทำความผิดที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป ได้แนะนำไว้ให้แต่ละประเทศนำไปบัญญัติเพิ่มเติม โดยในส่วนของบทบัญญัติความผิดที่เกี่ยวกับเนื้อหาสาระ ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง การพยายามและการสนับสนุนการกระทำความผิดได้ถูกบัญญัติไว้ในประมวลกฎหมายอาญาและกฎหมายทรัพย์สินทางปัญญาของประเทศไทยแล้ว ดังนั้นการปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยในส่วนที่พระราชบัญญัตินี้มิได้บัญญัติไว้เป็นการเฉพาะก็ต้องปรับใช้ร่วมกับประมวลกฎหมายอาญาด้วย โดยเฉพาะอย่างยิ่งในส่วนของเจตนา ตัวการ การพยายามและการสนับสนุนการกระทำความผิด เป็นต้น

ไว้ในระบบคอมพิวเตอร์ของผู้อื่นไม่ได้ โดยจะได้พิจารณามาตรการในการกำหนดนิยามและความหมายของคำว่า “เข้าถึง (access)” ในกฎหมายต่างประเทศพร้อมกับยกตัวอย่างกฎหมายของต่างประเทศที่มีการกำหนดคำนิยามดังกล่าวไว้ ต่อจากนั้นจะเป็นการพิจารณาและกล่าวถึงในรายละเอียดและองค์ประกอบของการเข้าถึงโดยมิชอบ (Illegal access) ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป พร้อมกับยกตัวอย่างมาตรการทางกฎหมายในการป้องกันการเข้าถึงโดยมิชอบของต่างประเทศด้วย

1. มาตรการกำหนดนิยามและความหมายของการเข้าถึงให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์

นอกจากมาตรการป้องกันการเข้าถึงโดยมิชอบ (Illegal access) แล้ว ในกฎหมายต่างประเทศยังมีการบัญญัติความหมายของคำว่า “เข้าถึง (access)” ไว้เพื่อให้การปรับใช้กฎหมายเป็นไปอย่างชัดเจนอีกด้วย ซึ่งถือว่าเป็นความแตกต่างที่เป็นนัยสำคัญเกี่ยวกับเทคนิคการบัญญัติกฎหมายในส่วนที่เกี่ยวกับความหมายของชุดคำสั่งไม่พึงประสงค์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยกับกฎหมายของต่างประเทศตรงที่ กฎหมายไทยพยายามจะบัญญัติความหมายของชุดคำสั่งไม่พึงประสงค์ให้มีความทันสมัยและสามารถรองรับกับอนาคตของเทคโนโลยีที่เปลี่ยนแปลงไปได้ตามยุคสมัย กล่าวคือ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยจะใช้วิธีการให้ความหมายแก่บรรดาไวรัสคอมพิวเตอร์ ม้าโทรจัน หนอนคอมพิวเตอร์ สปายแวร์ หรือมัลแวร์ชนิดต่าง ๆ เหล่านั้น โดยเรียกรวมเป็นชื่อเดียวกันว่า “ชุดคำสั่งไม่พึงประสงค์ (malicious software หรือ undesirable sets of instructions)”[107] แล้วใช้เทคนิคการอธิบายเพื่อขยายความหมายชุดคำสั่งไม่พึงประสงค์เหล่านั้นในวรรคสอง ของมาตรา 21 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งอยู่ในส่วนของกฎหมายวิธีสบัญญัติ นอกจากนี้ยังเปิดโอกาสให้มีการเพิ่มเติมเพื่อการขยาย

---

107 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฉบับภาษาอังกฤษเรียกชุดคำสั่งไม่พึงประสงค์ว่า “undesirable sets of instructions” ซึ่ง หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ทั้งนี้ความหมายดังกล่าวก็ตรงกับความหมายในมุมมองของนักคอมพิวเตอร์และหลักสากลที่เรียกชุดคำสั่งไม่พึงประสงค์ว่า “malicious code หรือ malicious program หรือ malicious software” ที่หมายถึงบรรดาไวรัสคอมพิวเตอร์ ม้าโทรจัน หนอนคอมพิวเตอร์ สปายแวร์ หรือมัลแวร์ชนิดต่าง ๆ นั่นเอง

ขอบเขตและความหมายของชุดคำสั่งไม่พึงประสงค์ที่จะเกิดขึ้นในอนาคตโดยการตราเป็นกฎกระทรวงซึ่งเป็นกฎหมายในลำดับรองได้อีกด้วย ส่วนในฝั่งของต่างประเทศนั้น จะไม่ใช้เทคนิคการบัญญัติความหมายของชุดคำสั่งไม่พึงประสงค์รวมไว้เป็นชื่อเดียวกันเหมือนดังประเทศไทย แต่จะใช้วิธีการบัญญัติกฎหมายเป็นสองวิธี ดังนี้

วิธีที่หนึ่ง โดยการเรียกชื่อและกำหนดนิยามความหมายของชุดคำสั่งไม่พึงประสงค์ตามแต่ละประเภทของชุดคำสั่งไม่พึงประสงค์ที่นักคอมพิวเตอร์และที่สากลนิยมเรียกกัน ซึ่งทำให้สามารถสื่อความหมายและเข้าใจได้โดยตรงตามแต่ละประเภทของชุดคำสั่งไม่พึงประสงค์ ตัวอย่างของการเรียกหรือนิยามชุดคำสั่งไม่พึงประสงค์ที่ปรากฏในกฎหมายต่างประเทศ เช่น ประมวลกฎหมายอาญาแห่งมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา (Computer Crimes - Texas Penal Code) ใน Title 7 Chapter 33 ได้ให้นิยามความหมายของไวรัสคอมพิวเตอร์ว่า[108] หมายถึง “โปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์หรือชุดคำสั่งอื่นใดหรือโปรแกรมที่ถูกสร้างขึ้นเฉพาะซึ่งเมื่อบันทึกลงในหน่วยความจำของเครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมอื่นแล้ว สามารถสร้างหรือทำสำเนาตนเองหรือติดตั้งตนเองไปกับโปรแกรมอื่นหรือไฟล์อื่น” แล้วจึงกำหนดความผิดฐานเข้าถึงโดยมิชอบด้วยไวรัสคอมพิวเตอร์ตามนิยามดังกล่าว เป็นต้น

วิธีที่สอง โดยการพิจารณาจากพฤติการณ์และองค์ประกอบของความผิดฐานการเข้าถึงโดยมิชอบเป็นสำคัญ ทั้งนี้ มีทั้งการกำหนดนิยามของการเข้าถึงไว้ และมิได้กำหนดนิยามของการเข้าถึงไว้แต่จะกำหนดเป็นพฤติการณ์และองค์ประกอบในฐานความผิดนั้นๆ ไว้ โดยไม่คำนึงว่าจะใช้ชุดคำสั่งไม่พึงประสงค์ประเภทใดในการเข้าถึงซึ่งหากเข้าข่ายตามพฤติการณ์และองค์ประกอบของฐานความผิดที่กำหนดไว้แล้ว ก็จะถือว่าเป็นการกระทำความผิดฐานเข้าถึงโดยมิชอบ ซึ่งกฎหมายในต่างประเทศส่วนใหญ่มักจะใช้วิธีที่สองนี้เป็นองค์ประกอบในการบัญญัติฐานความผิดการเข้าถึงโดยมิชอบ

ทั้งนี้ จะขอยกตัวอย่างกฎหมายของต่างประเทศที่มีการกำหนดนิยามและความหมายของคำว่า “เข้าถึง (access)” ไว้ ดังต่อไปนี้

---

108 “Computer virus” means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

1.1 ประเทศออสเตรเลีย

ประเทศออสเตรเลียได้กำหนดนิยามการเข้าถึงไว้ใน Cybercrime Act 2001[109] ดังนี้

"เข้าถึง" หมายความว่า

(1) การแสดงผลข้อมูลคอมพิวเตอร์โดยระบบคอมพิวเตอร์ หรือข้อมูลอื่นใดจากระบบคอมพิวเตอร์ หรือ

(2) การทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ

(3) กระทำการใดๆ เพื่อให้ชุดคำสั่งปฏิบัติการ

เมื่อพิจารณาความหมายของคำว่า "เข้าถึง" ใน Cybercrime Act 2001 แล้ว ผู้เขียนเห็นว่า คำนิยามดังกล่าวสามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภททั้งชุดคำสั่งไม่พึงประสงค์ที่มีอยู่ในปัจจุบันและที่จะเกิดขึ้นในอนาคตด้วย เหตุผลที่ผู้เขียนเห็นเช่นนั้นก็เพราะ อย่างน้อยที่สุดแล้วหากมีการใช้ชุดคำสั่งไม่พึงประสงค์ใดในการเข้าถึงก็จะทำให้เกิดการกระทำใดๆ เพื่อให้ชุดคำสั่งนั้นปฏิบัติการหรือประมวลผล

1.2 ประเทศนิวซีแลนด์

ประเทศนิวซีแลนด์ได้กำหนดนิยามการเข้าถึงไว้ใน Crimes Amendment Act 2003 No 39 Part 1 s 15, of July 7th [110] ดังนี้

"เข้าถึง" หมายความว่า การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการ เพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์ หรือได้รับข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ดังกล่าว ตลอดการกระทำการอื่นใดเพื่อแสวงหาประโยชน์จากระบบคอมพิวเตอร์นั้น

---

109 476.1 Definitions

(1) In this Part :

access to data held in a computer means :

(a) the display of the data by the computer or any other output of the data from the computer ; or

(b) the copying or moving the data to any other place in the computer or to a data storage device; or

(c) in the case of a program – the execution of the program.

110 248 Interpretation

''access, in relation to any computer system, means instruct, communicate with, store data in, receive data from, or otherwise make use of any of the resources of the computer system

เมื่อพิจารณาความหมายของคำว่า “เข้าถึง” ใน Crimes Amendment Act 2003 No 39 Part 1 s 15, of July 7th แล้ว ผู้เขียนเห็นว่า คำนิยามดังกล่าวสามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภท เหตุผลที่ผู้เขียนเห็นเช่นนั้นก็เพราะ อย่างน้อยที่สุดแล้วหากมีการใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจัน หรือสปายแวร์ในการเข้าถึง (ผู้เขียนเห็นว่าหากเข้าถึงโดยม้าโทรจัน หรือสปายแวร์แล้วมีปัญหาในการตีความและการบังคับใช้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทย เนื่องจากม้าโทรจัน หรือสปายแวร์ไม่มีคุณสมบัติที่จะทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้เมื่อถูกนำไปใช้ในการกระทำความผิด ดังนั้น ม้าโทรจัน หรือสปายแวร์จึงไม่อยู่ในความหมายของชุดคำสั่งไม่พึงประสงค์ตามกฎหมายของประเทศไทย) ก็จะเป็นการแสวงหาผลประโยชน์จากระบบคอมพิวเตอร์นั้น

1.3 ประเทศอินเดีย

ประเทศอินเดียได้กำหนดนิยามการเข้าถึงไว้ใน The Information Technology Act 2000[111] ดังนี้

“เข้าถึง” หมายความว่า การสั่งการให้คอมพิวเตอร์ปฏิบัติการ หรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลหรือหน่วยบันทึกผลของระบบคอมพิวเตอร์ได้

ทั้งนี้ ได้กำหนดโทษสำหรับการทำความเสียหายกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ไว้ใน มาตรา 43[112] แห่ง The Information Technology Act 2000 และความผิดฐาน

---

111 Section 2 Definitions

(a) “access” with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

112 Section 43. Penalty for damage to computer, computer system , etc.

If any person without permission of the owner or any other person who is incharge of a computer computer, computer system or computer network, - (a) accesses or secures access to such computer, computer system or computer network;

(b) downloads , copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

กระทำการแฮกด้วยคอมพิวเตอร์ซึ่งถือเป็นการเข้าถึงโดยมิชอบไว้ใน มาตรา 66[113] แห่ง The Information Technology Act 2000 ด้วย

เมื่อพิจารณาความหมายของคำว่า “เข้าถึง” ใน The Information Technology Act 2000 แล้ว ผู้เขียนเห็นว่า เป็นตัวอย่างของการกำหนดนิยามคำว่า “เข้าถึง” ได้เป็นอย่างดี และสมควรนำมาเป็นตัวอย่างสำหรับการปรับปรุงกฎหมายของประเทศไทย ทั้งนี้ คำนิยามดังกล่าวสามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภท โดยสามารถอ่านและเข้าใจความหมายของนิยามได้โดยง่ายจนแทบไม่ต้องตีความ เหตุผลที่เป็นเช่นนั้นก็เพราะ นิยามดังกล่าวสอดคล้องกับหลักการทำงานของระบบคอมพิวเตอร์ กล่าวคือ การทำงานของระบบคอมพิวเตอร์จะประกอบด้วยส่วนของการทำงานสำคัญแยกได้เป็น 3 ส่วนใหญ่ๆ คือ ส่วนของการนำเข้า (Input) ส่วนของการประมวล (Process) และส่วนของการแสดงผล (Output)

นอกจากนี้ การกำหนดโทษสำหรับการทำความเสียหายกับคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ไว้ใน มาตรา 43 และการกำหนดฐานความผิดในกระทำการแฮกด้วยคอมพิวเตอร์ซึ่งถือ

(c) introduces or causes to be introduced any computer contaminant or computer virus in to any computer , computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data , computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer , computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tempering with or manipulating any computer , computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

113 Section 66. Hacking with computer system.-

(*1*) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(*2*) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

เป็นการเข้าถึงโดยมิชอบไว้ใน มาตรา 66 เมื่อนำความหมายของนิยามคำว่าการเข้าถึงดังกล่าวมาปรับใช้ด้วยแล้ว ก็จะยิ่งทำให้การตีความและปรับใช้กฎหมายมีความชัดเจนและสามารถขจัดปัญหาในการบังคับใช้กฎหมายได้

1.4 ประเทศสหรัฐอเมริกา[114]

กฎหมายระดับรัฐบาลกลางของประเทศสหรัฐอเมริกามิได้กำหนดนิยามการเข้าถึงไว้โดยตรง แต่ได้กำหนดหลักการของการเข้าถึงโดยมิชอบไว้ใน 18 USC 1030. Fraud and Related Activity in Connection with Computers ว่า “หมายความรวมถึงการเข้าถึงเกินกว่าอำนาจที่ตนมีด้วย (having knowingly accessed a compute without authorization or exceeding authorized access)” อย่างไรก็ตามในกฎหมายระดับมลรัฐก็ได้มีการกำหนดนิยามการเข้าถึงไว้ ดังนี้

1.4.1 รัฐแคลิฟอร์เนีย (CALIFORNIA)[115]

“เข้าถึง” หมายความว่า การทำให้สามารถเข้าสู่ระบบคอมพิวเตอร์ การสั่งการให้คอมพิวเตอร์ปฏิบัติการ หรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลของคอมพิวเตอร์ของระบบคอมพิวเตอร์หรือของเครือข่ายคอมพิวเตอร์ได้

---

114 มีกฎหมายของสหรัฐอเมริกา (United Stated Code) หลายฉบับที่สามารถนำมาปรับใช้กับการก่ออาชญากรรมทางคอมพิวเตอร์ เช่น 15 USC 1644, prohibiting fraudulent use of credit cards, 18 USC 1029, prohibiting fraudulent acquisition of telecommunications services, 18 USC 1030, prohibiting unauthorized access to any computer operated by the U.S. Government, financial institution insured by the U.S. Government, federally registered securities dealer, or foreign bank., 18 USC 1343, prohibiting wire fraud, 18 USC 1361-2, prohibiting malicious mischief, 18 USC 1831, prohibiting stealing of trade secrets, 18 USC 2314, prohibiting interstate transport of stolen, converted, or fraudulently obtained material; does apply to computer data files *U.S. v. Riggs*, 739 F.Supp. 414 (N.D.Ill 1990)., 18 USC 2319 and 17 USC 506, criminal violations of copyright law, 18 USC 2701, prohibiting access to communications stored on a computer (i.e., privacy of e-mail), 47 USC 223, prohibiting interstate harassing telephone calls เป็นต้น แต่ไม่พบการกำหนดนิยามคำว่า “เข้าถึง (access)” ไว้ในกฎหมายเหล่านั้น แต่อย่างใด

115 Computer Crimes - California Penal Code

Section 502. Unauthorized access to computers, computer systems and computer data

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

เมื่อพิจารณาความหมายของคำว่า “เข้าถึง” ใน Computer Crimes - California Penal Code แล้ว ผู้เขียนเห็นว่า เป็นตัวอย่างของการกำหนดนิยามคำว่า “เข้าถึง” ได้ดีมาก และสมควรนำมาเป็นตัวอย่างสำหรับการปรับปรุงกฎหมายของประเทศไทยเป็นอย่างยิ่ง ทั้งนี้ คำนิยามดังกล่าวสามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภท และสามารถอ่านและเข้าใจความหมายของนิยามได้โดยง่ายจนไม่ต้องตีความ เหตุผลที่เป็นเช่นนั้นก็เพราะ นิยามดังกล่าวสอดคล้องกับหลักการทำงานของระบบคอมพิวเตอร์ กล่าวคือ การทำงานของระบบคอมพิวเตอร์จะประกอบด้วยส่วนของการทำงานสำคัญแยกได้เป็น 3 ส่วนใหญ่ๆ คือ ส่วนของการนำเข้า (Input) ส่วนของการประมวล (Process) และส่วนของการแสดงผล (Output) โดยเฉพาะอย่างยิ่งการเน้นที่ส่วนของการประมวลผลของคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ ซึ่งหากมีการใช้ชุดคำสั่งไม่พึงประสงค์เพื่อการเข้าถึงแล้วก็จะต้องมีการประมวลผลโดยหน่วยประมวลผลของคอมพิวเตอร์ ของระบบคอมพิวเตอร์ หรือของเครือข่ายคอมพิวเตอร์ด้วยเสมอ

1.4.2 รัฐแมริแลนด์ (MARYLAND)[116]

“เข้าถึง” หมายความว่า การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการ หรือสื่อสารกับระบบคอมพิวเตอร์ และหมายความรวมถึงการจัดเก็บข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ หรือค้นคืนข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ ตลอดจนการใช้ประโยชน์ใด ๆ จากระบบคอมพิวเตอร์ด้วย เช่น การใช้เพื่อประมวลผลข้อมูล เป็นต้น

อนึ่ง ยังมีอีกหลายมลรัฐที่ได้กำหนดนิยามและความหมายคำว่า “เข้าถึง” ไว้ในทำนองเดียวกันกับมลรัฐแมริแลนด์ ได้แก่ รัฐแอละแบมา รัฐฮาวาย รัฐแอริโซนา รัฐคอนเนตทิคัต รัฐเดลาแวร์ รัฐไอดาโฮ รัฐอิลลินอยส์ รัฐอินดีแอนา รัฐไอโอวา รัฐนิวเจอร์ซีย์ รัฐนอร์ทแคโรไลนา และรัฐออริกอน

เมื่อพิจารณาความหมายของคำว่า “เข้าถึง” ใน Cyber Crime Law-Code of Maryland แล้ว ผู้เขียนเห็นว่า เป็นตัวอย่างของการกำหนดนิยามคำว่า “เข้าถึง” ที่ดีมากและสมควรนำมาเป็นตัวอย่างสำหรับการปรับปรุงกฎหมายของประเทศไทยเป็นอย่างยิ่ง ทั้งนี้ คำนิยามดังกล่าว

---

116 Cyber Crime Law-Code of Maryland

Section 146. Unauthorized access to COMPUTERS prohibited.

(a) Definitions. -- In this section the following words have the meanings indicated.

(9) "Access" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of equipment including, but not limited to, COMPUTERS and other data processing equipment or resources connected therewith.

สามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภท และสามารถอ่านและเข้าใจความหมายของนิยามได้โดยง่ายจนไม่ต้องตีความ เหตุผลที่เป็นเช่นนั้นก็เพราะ นิยามดังกล่าวนอกจากจะสอดคล้องกับหลักการทำงานของระบบคอมพิวเตอร์แล้ว ยังได้เน้นถึงส่วนของการจัดเก็บข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ หรือการค้นคืนข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ ตลอดจนการใช้ประโยชน์ใด ๆ จากระบบคอมพิวเตอร์ซึ่งเป็นสิ่งที่แฮกเกอร์หรือผู้บุกรุกประสงค์และจะต้องกระทำเสมอหากมีการเข้าถึง นอกจากนี้ยังได้ยกตัวอย่างประกอบเพื่อความเข้าใจเพิ่มเติมอีกด้วย

1.4.3 รัฐนิวเม็กซิโก (NEW MEXICO)[117]

"เข้าถึง" หมายความว่า การติดตั้งชุดคำสั่ง หรือการสั่งให้ชุดคำสั่งปฏิบัติการการดักหรือการสื่อสารข้อมูลคอมพิวเตอร์ การจัดเก็บหรือค้นคืนข้อมูลคอมพิวเตอร์

เมื่อพิจารณาความหมายของคำว่า "เข้าถึง" ในกฎหมายของรัฐนิวเม็กซิโกแล้ว ผู้เขียนเห็นว่า เป็นตัวอย่างของการกำหนดนิยามคำว่า "เข้าถึง" ในระดับดี ทั้งนี้ คำนิยามดังกล่าวสามารถครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทุกประเภทเช่นกัน นิยามดังกล่าวนอกจากจะสอดคล้องกับหลักการทำงานของระบบคอมพิวเตอร์แล้ว ยังได้เน้นถึงการจัดเก็บหรือค้นคืนข้อมูลคอมพิวเตอร์ซึ่งก็มีหลักการคล้ายๆ กับนิยามการเข้าถึงในกฎหมายของมลรัฐแมริแลนด์อีกด้วย

2. มาตรการป้องกันการเข้าถึงโดยมิชอบ (Illegal access)[118] ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป

---

117 "access" means to program, execute programs on, intercept, instruct, communicate with, store data in, retrieve data from or otherwise make use of any computer resources, including data or programs of a computer, computer system, computer network or database;

118 Article 2 Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

การกระทำความผิดฐานเข้าถึงโดยมิชอบตามอนุสัญญานี้อาจเกิดขึ้นได้หลายวิธีด้วยกัน เช่น การเจาะระบบ (Hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) เป็นต้น ซึ่งอาจนำไปสู่การขัดขวางการใช้ระบบหรือข้อมูลที่ชอบด้วยกฎหมาย ทั้งนี้ การเข้าถึงระบบคอมพิวเตอร์ดังกล่าวอาจทำให้ได้มาซึ่งข้อมูลที่เป็นความลับ เช่น รหัสผ่าน ข้อมูลเกี่ยวกับระบบคอมพิวเตอร์ที่เป็นเป้าหมายในการโจมตี หรือข้อมูลที่เป็นความลับอื่นใดซึ่งผู้ที่มีข้อมูลเหล่านี้อาจนำข้อมูลไปใช้เพื่อการใช้ประโยชน์ในการกระทำความผิดอื่นต่อไปได้ เช่น การใช้บริการจากระบบโดยไม่ชำระค่าบริการ ตลอดจนการกระทำที่ก่อให้เกิดความเสียหายอย่างร้ายแรงโดยการใช้คอมพิวเตอร์เพื่อฉ้อโกงหรือปลอมเอกสาร เป็นต้น อนุสัญญานี้จึงได้กำหนดให้ความผิดฐานนี้เป็นความผิดในตัวเอง

คำว่า “เข้าถึง (access)” ในที่นี้หมายความว่า[119] การเข้าถึงทั้งในระดับกายภาพด้วย เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายรวมถึงการเข้าระบบคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์ที่ตนต้องการได้ นอกจากนี้ ยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

อนึ่ง “เข้าถึง” ยังหมายถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกันทั่วโลก และยังหมายถึง การเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบเครือข่ายท้องถิ่น (Local Area Network : LAN)

---

119 Convention on Cybercrime (ETS No. 185) Explanatory Report Par. 46

"Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system.

"Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

ระบบอินทราเน็ต (Intranet) ภายในองค์กรเดียวกันโดยไม่ต้องพิจารณาถึงระยะทาง และรูปแบบของการติดต่อสื่อสารว่าใช้วิธีการทางสายหรือไร้สาย

อย่างไรก็ตาม ยังมีข้อสังเกตเพิ่มเติมสำหรับฐานความผิดนี้ คือ ประเทศภาคีอาจกำหนดเงื่อนไขเพิ่มเติมว่า ผู้กระทำความผิดฐานนี้จะต้องละเมิดระบบการรักษาความปลอดภัย (infringing security measures) หรือมีเจตนาเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ หรือเจตนาทุจริตอื่น หรือดำเนินการอื่นใดต่อระบบคอมพิวเตอร์ซึ่งได้เชื่อมต่อเข้ากับระบบคอมพิวเตอร์อื่น

3. มาตรการป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ในกฎหมายต่างประเทศ

กฎหมายของต่างประเทศที่มีมาตรการป้องกันการเข้าถึงโดยมิชอบ โดยการกำหนดเป็นความผิดฐานเข้าถึงโดยมิชอบ (Illegal access) ไว้นั้น สามารถแยกได้เป็น กฎหมายที่ให้การคุ้มครองระบบคอมพิวเตอร์ กฎหมายที่ให้การคุ้มครองข้อมูลคอมพิวเตอร์ และกฎหมายที่ให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ดังต่อไปนี้

3.1 กฎหมายต่างประเทศที่ให้การคุ้มครองระบบคอมพิวเตอร์

ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองระบบคอมพิวเตอร์ เช่น

3.1.1 ประเทศฝรั่งเศส

ประเทศฝรั่งเศสได้บัญญัติมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ไว้ใน Penal Code (Chapter III – Attacks on systems for automated data processing)[120] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดโดยเจตนาทุจริต เข้าถึง ไม่ว่าทั้งหมดหรือบางส่วนของระบบประมวลผลข้อมูลอัตโนมัติ

(2) ต้องระวางโทษจำคุกไม่เกิน… ปี หรือปรับไม่เกิน...ฟรังซ์

---

120 Article 323-1:

The act of fraudulently gaining access to, or maintaining, in all or part of an automated data processing system is punishable by imprisonment not exceeding one year and a fine of up to 100.000 FF.

Whenever this results in the suppression or modification of data contained in the system, or an alteration in the functioning of the system, the act is punished by imprisonment not exceeding two years and a fine up to 200.000 FF.

(3) หากการกระทำข้างต้นก่อให้เกิดผลเป็นการขัดขวางข้อมูล (suppression) การเปลี่ยนแปลงข้อมูล (modification) ซึ่งเก็บอยู่ในระบบ หรือแก้ไขระบบการทำงานของระบบ

(4) ต้องระวางโทษจำคุกไม่เกิน… ปี หรือปรับไม่เกิน… ฟรังซ์

ตามบทบัญญัติดังกล่าว แม้จะไม่ใช้คำว่า “ระบบคอมพิวเตอร์” แต่ใช้คำว่า “ระบบประมวลผลข้อมูลอัตโนมัติ” ก็ย่อมแปลความและหมายถึงระบบคอมพิวเตอร์ที่มีรูปแบบของการทำงานเป็นแบบระบบการประมวลผลข้อมูลแบบอัตโนมัติ จึงเป็นการบัญญัติกฎหมายเพื่อการรองรับกับเทคโนโลยีที่จะเกิดขึ้นในอนาคต ซึ่งเทคโนโลยีใหม่ที่เกิดขึ้นนั้นอาจจะไม่ได้เรียกว่าระบบคอมพิวเตอร์ หรืออาจมีการเรียกชื่อเป็นอย่างอื่นก็ได้ และแม้จะมีการเข้าถึงไม่ว่าทั้งหมดหรือบางส่วนของระบบการประมวลผลอัตโนมัตินั้นก็ถือว่าเป็นความผิดตามกฎหมายนี้แล้ว

นอกจากนี้ ยังมีการลงโทษในบทหนัก หากการเข้าถึงนั้นก่อให้เกิดผลเป็นการขัดขวางข้อมูล การเปลี่ยนแปลงข้อมูล ซึ่งเก็บอยู่ในระบบ หรือแก้ไขระบบการทำงานของระบบ ซึ่งก็คล้ายกับความผิดฐานรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตามมาตรา 9[121] และมาตรา 10[122] แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย

---

121 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 9 ความว่า

“มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

122 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 10 ความว่า

“มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

3.1.2 ประเทศอิตาลี

ประเทศอิตาลีได้บัญญัติมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ไว้ใน Penal Code (Article 615 ter : Unauthorized access into a computer or telecommunication systems)[123] โดยมีองค์ประกอบของความผิดดังนี้

(1) ผู้ใดโดยไม่มีอำนาจ เข้าถึงระบบคอมพิวเตอร์หรือระบบโทรคมนาคม ซึ่งมีมาตรการเพื่อรักษาความปลอดภัย (security measures) หรือ

(2) เข้าไปในระบบดังกล่าวข้างต้นโดยปราศจากการแสดงออกซึ่งความยินยอมทั้งโดยชัดแจ้งและปริยายของผู้มีสิทธิอนุญาต

(3) ต้องระวางโทษจำคุกไม่เกิน… ปี

(4) ผู้กระทำต้องระวางโทษหนักขึ้น โดยต้องถูกระวางโทษจำคุกตั้งแต่… ปี ถึง…ปี หากเข้ากรณีดังต่อไปนี้

---

123 Article 615 ter: Unauthorized access into a computer or telecommunication systems:

Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.

The imprisonment is from one until five years:

1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator.

2) if to commit the crime the culprit uses violence upon things or people, or if he is manifestedly armed.

3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or damage of the data, the information or the programs contained in it. Should the deeds of the 1st and 2nd paragraphs concern computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or whatsoever public interest, the penalty is - respectively- one to five years or three to eight years' imprisonment. In the case provided for in the 1st paragraph, the crime is liable to punishment only after an action by the plaintiff; the other cases are prosecutioned "ex-officio".

ก. หากผู้กระทำผิดเป็นเจ้าหน้าที่ของรัฐ หรือเจ้าหน้าที่ผู้มีหน้าที่ให้บริการสาธารณะ โดยเป็นการใช้อำนาจในทางมิชอบ หรือเป็นการฝ่าฝืนการปฏิบัติตามหน้าที่ หรือเป็นนักสืบเอกชน (private investigator) หรือการปฏิบัติผิดหน้าที่ของผู้ควบคุมระบบ (system operator)

ข. หากในการกระทำผิดนั้น ผู้กระทำได้ก่อความเสียหายต่อทรัพย์สินหรือประชาชน หรือผู้กระทำผิดประสงค์ให้การกระทำของตนมีลักษณะดั่งอาวุธ (or if he is manifestly armed)

ค. หากการกระทำก่อความเสียหาย หรือทำลายระบบไม่ว่าทั้งหมดหรือบางส่วน หรือขัดขวางการทำงานของระบบ หรือทำให้ข้อมูล โปรแกรมที่อยู่ในข้อมูลนั้นถูกทำลายหรือเสียหาย

ตามบทบัญญัติดังกล่าว นอกจากจะเป็นการป้องกันการเข้าถึงระบบคอมพิวเตอร์แล้ว ยังเป็นการป้องกันการเข้าถึงระบบโทรคมนาคมแยกต่างหากอีกด้วย ทั้งนี้จะต้องเป็นการเข้าถึงโดยปราศจากความยินยอมของผู้มีสิทธิอนุญาต และระบบคอมพิวเตอร์หรือระบบโทรคมนาคมนั้นจะต้องมีมาตรการเพื่อรักษาความปลอดภัยด้วยจึงจะถือเป็นความผิด ซึ่งก็คล้ายๆ กับมาตรการป้องกันการเข้าถึงในกฎหมายของประเทศไทย แต่แตกต่างกันตรงที่มาตรการรักษาความปลอดภัยตามกฎหมายของประเทศไทยนั้นจะต้องเป็นมาตรการที่มิได้มีไว้สำหรับตนจึงจะถือเป็นความผิด

นอกจากนี้ ยังมีการลงโทษในบทหนัก หากผู้กระทำผิดเป็นเจ้าหน้าที่ของรัฐ หรือเจ้าหน้าที่ผู้มีหน้าที่ให้บริการสาธารณะ โดยเป็นการใช้อำนาจในทางมิชอบ หรือเป็นการฝ่าฝืนการปฏิบัติตามหน้าที่ หรือเป็นนักสืบเอกชน หรือการปฏิบัติผิดหน้าที่ของผู้ควบคุมระบบ หรือหากในการกระทำผิดนั้น ผู้กระทำได้ก่อความเสียหายต่อทรัพย์สินหรือประชาชน หรือผู้กระทำผิดประสงค์ให้การกระทำของตนมีลักษณะดั่งอาวุธ หรือหากการกระทำก่อความเสียหาย หรือทำลายระบบไม่ว่าทั้งหมดหรือบางส่วน หรือขัดขวางการทำงานของระบบ หรือทำให้ข้อมูล โปรแกรมที่อยู่ในข้อมูลนั้นถูกทำลายหรือเสียหาย ซึ่งก็คล้ายกับการลงโทษในบทหนักตามความผิดฐานรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์แล้วส่งผลกระทบต่อประชาชนหรือประโยชน์สาธารณะ หรือกระทบกับความมั่นคงแห่งรัฐ ตามมาตรา 12[124] แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย

---

124 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 12 ความว่า “มาตรา 12 ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10

3.1.3 ประเทศเนเธอร์แลนด์

ประเทศเนเธอร์แลนด์ได้บัญญัติมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ไว้ใน Criminal Code (Article 138a:)[125] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดโดยเจตนา กระทำการเข้าถึงโดยมิชอบด้วยกฎหมายเพื่อเข้าถึงระบบอัตโนมัติไม่ว่าทั้งหมดหรือบางส่วนที่ใช้สำหรับจัดเก็บ (storage) หรือประมวลผลข้อมูล

(2) ต้องระวางโทษจำคุกไม่เกิน… เดือน หรือปรับไม่เกิน… guilder

(3) หากเป็นการกระทำโดย

ก. เข้าถึงโดยฝ่าฝืนระบบรักษาความปลอดภัย (Breaks through a security system) หรือ

ข. เข้าถึงโดยการรบกวนทางเทคนิค (obtains access by technical intervention) ฯ

ตามบทบัญญัติดังกล่าว แม้จะใช้คำว่าเป็นการป้องกันการเข้าถึง “ระบบอัตโนมัติ” แต่ระบบดังกล่าวเป็นระบบที่ใช้สำหรับจัดเก็บหรือประมวลผลข้อมูล ซึ่งก็คงหมายถึงระบบคอมพิวเตอร์เหมือนดังเช่นกฎหมายของประเทศอื่นๆ นั่นเอง นอกจากนี้ ยังมีการลงโทษในบทหนักหากเป็นการเข้าถึงโดยฝ่าฝืนระบบรักษาความปลอดภัย หรือเป็นการเข้าถึงโดยการรบกวนทางเทคนิค ซึ่งการรบกวนทางเทคนิคนี้อาจแปลความได้อย่างกว้างขวางในอนาคตอีกด้วย

---

(1) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(2) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (2) เป็นเหตุให้ผู้อื่นถึงแก่ความตายต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี”

125 Criminal Code Article 138a:

Any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, shall be liable, as guilty of breach of computer peace, to term of imprisonment not exceeding six months or a fine of 10.000 guilders if he:

(a). Breaks through a security system, or

(b). obtains access by a technical intervention, with the help of false signals or a false key or by acting in a false capacity.

3.1.4 ประเทศโปรตุเกส

ประเทศโปรตุเกสได้บัญญัติมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ไว้ใน Criminal Information Law of August 17, 1991: (Chapter 1 Article 7:)[126] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดโดยมิชอบ เข้าถึงเพื่อตนเองหรือบุคคลอื่นต่อระบบสารสนเทศ (information system) หรือเครือข่าย (network)

(2) ต้องระวางโทษจำคุกไม่เกิน... ปี หรือ ปรับและจำคุกไม่เกิน… วัน

(3) ผู้กระทำผิดต้องระวางโทษหนักขึ้นเป็นจำคุกไม่เกิน…ปี หรือปรับ หากการเข้าถึงดังกล่าวเป็นการเข้าถึงโดยการละเมิดมาตรการรักษาความปลอดภัย (security rules)

(4) ผู้กระทำผิดต้องระวางโทษหนักขึ้นเป็นจำคุกไม่เกิน... ปีหาก

ก. การกระทำนั้นเป็นการเข้าถึงเพื่อให้ได้มาซึ่งข้อมูลด้านความลับทางการค้า

ข. หรือข้อมูลที่ต้องเก็บรักษาเป็นความลับตามกฎหมาย

ตามบทบัญญัติดังกล่าว นอกจากจะเป็นการเข้าถึงเพื่อตนเองแล้วแม้จะเป็นการเข้าถึงเพื่อบุคคลอื่นก็ถือเป็นความผิดด้วยเช่นกัน ทั้งนี้ แม้จะใช้คำว่าเข้าถึงต่อระบบสารสนเทศหรือเครือข่าย แต่ก็ครอบคลุมและมีความหมายในทำนองเดียวกันกับการเข้าถึงต่อระบบคอมพิวเตอร์ นอกจากนี้ ยังมีการลงโทษในบทหนักหากการกระทำนั้นเป็นการเข้าถึงเพื่อให้ได้มาซึ่งข้อมูลด้านความลับทางการค้า หรือข้อมูลที่ต้องเก็บรักษาเป็นความลับตามกฎหมาย

---

126 Chapter 1 Article 7:

1 - Any person who, without authorization obtains for himself or another person an unlawful gain or use by any manner accessing an information system or network, shall be sentenced to imprisonment not exceeding one year, or to a fine and imprisonment not exceeding 120 days.

2 - Imprisonment not exceeding three years or a fine if the person concerned obtains access to information by breaking the security rules.

3 - Imprisonment for a term of one year not exceeding five years when:

(a) the person concerned by obtaining access to information acquires knowledge of trade secrets or confidential data protected by law,

(b) the gain or use results in comprehensive values.

3.1.5 ประเทศสวิตเซอร์แลนด์

ประเทศสวิตเซอร์แลนด์ได้บัญญัติมาตรการเพื่อคุ้มครองระบบคอมพิวเตอร์ไว้ใน Penal Code (Article 143 bis: Unauthorized access to data processing system)[127] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดโดยมิชอบเข้าถึงซึ่งระบบประมวลผลข้อมูลซึ่งถูกป้องกันการเข้าถึงด้วยวิธีการเฉพาะโดยอุปกรณ์อิเล็กทรอนิกส์

(2) ต้องระวางโทษจำคุกหรือปรับ (ไม่ระบุอัตราโทษ)

ตามบทบัญญัติดังกล่าว มีความคล้ายกับมาตรการป้องกันการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทย กล่าวคือ ระบบประมวลผลข้อมูลนั้นจะต้องถูกป้องกันด้วยวิธีการเฉพาะจึงจะถือเป็นความผิด อย่างไรก็ตาม หลักการตามหมายไทยได้เพิ่มเติมว่า มาตรการป้องกันนั้นจะต้องมิได้มีไว้สำหรับตนจึงจะถือเป็นความผิด

3.2 กฎหมายต่างประเทศที่ให้การคุ้มครองข้อมูลคอมพิวเตอร์

ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองข้อมูลคอมพิวเตอร์ เช่น

3.2.1 ประเทศเยอรมัน

ประเทศเยอรมันได้บัญญัติมาตรการเพื่อคุ้มครองข้อมูลคอมพิวเตอร์ไว้ใน Criminal Law (Section 202a)[128] โดยมีองค์ประกอบของความผิด ดังนี้

---

127 Article 143 bis: Unauthorized access to data processing system

Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.

128 Sec. 202a - Data spying

1) Anybody who without authority procures himself or another data which are not meant for him and which are specially secured against unauthorised access shall be sentenced to imprisonment not exceeding 3 years or to a fine.

(2) Data within the meaning of Subsection (1) shall be deemed to be only those which are stored or transmitted electronically, magnetically, or in any other not directly perceptible way.

(1) บุคคลใดโดยไม่มีอำนาจ กระทำการเพื่อเข้าถึงข้อมูล[129] ซึ่งมิได้มีไว้เพื่อตน และ

(2) การกระทำดังกล่าวเป็นการละเมิดระบบการรักษาความปลอดภัยโดยเฉพาะ

(3) ต้องระวางโทษจำคุกไม่เกิน... ปี หรือปรับ (ไม่ระบุจำนวนเงิน)

ตามบทบัญญัติดังกล่าว มีความคล้ายกับมาตรการป้องกันการเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทย แต่แตกต่างกันตรงที่ตามกฎหมายของประเทศเยอรมันข้อมูลที่เข้าถึงจะต้องเป็นข้อมูลที่มิได้มีไว้สำหรับตนจึงจะถือเป็นความผิด นอกจากนี้ หมายไทยยังได้เพิ่มเติมอีกว่า มาตรการป้องกันนั้นจะต้องมิได้มีไว้สำหรับตนจึงจะถือเป็นความผิด

3.2.2 ประเทศอังกฤษ

ประเทศอังกฤษได้บัญญัติมาตรการเพื่อคุ้มครองข้อมูลคอมพิวเตอร์ไว้ใน Computer Misuse Act 1990 (section 1)[130] โดยมีองค์ประกอบของความผิด ดังนี้

(1) บุคคลจะมีความผิด หาก

---

129 ข้อมูลซึ่งจะเป็นวัตถุในการกระทำความผิดฐานนี้ จะต้องเป็นข้อมูลที่ถูกจัดเก็บ (stored) หรือส่งผ่าน (transmitted) ด้วยวิธีการทางอิเล็กทรอนิกส์ (electronically) หรือแม่เหล็กไฟฟ้า (magnetically) หรือวิธีการอย่างอื่นซึ่งไม่เปิดเผยโดยชัดแจ้ง (not directly perceptible way)

130 Section 1 Unauthorised access to computer material.

1.—(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

ก. ใช้เครื่องคอมพิวเตอร์ในการดำเนินการเพื่อเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลซึ่งเก็บในคอมพิวเตอร์

ข. บุคคลดังกล่าวกระทำไปโดยปราศจากอำนาจให้กระทำได้ และ

ค. บุคคลดังกล่าวทราบว่าในขณะที่ตนได้ดำเนินการอยู่นั้นว่าเป็นการกระทำไปเพื่อเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูล

(2) เจตนาในการกระทำความผิดข้างต้น ไม่จำต้องเป็นการกระทำโดยตรงต่อ

ก. โปรแกรมหรือข้อมูลชนิดใดชนิดหนึ่ง

ข. โปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง

(3) ผู้กระทำความผิดตามมาตรานี้ต้องระวางโทษจำคุกไม่เกิน… เดือน หรือปรับไม่เกินระดับ 5 ของบัญชีแนบท้าย (standard scale) หรือทั้งจำทั้งปรับ

ตามบทบัญญัติดังกล่าว จะเน้นไปที่การตั้งใจหรือจงใจเพื่อการเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลโดยปราศจากอำนาจให้กระทำได้ ไม่ว่าจะเป็นการกระทำโดยตรงหรือโดยอ้อม กล่าวคือ หากมีการกระทำผิดโดยการเข้าถึงผ่านทางโปรแกรมหรือข้อมูลที่เก็บอยู่ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่ง แล้วมีผลทำให้เป็นการเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลซึ่งเก็บในคอมพิวเตอร์ที่ตนต้องการได้ ก็ถือเป็นความผิดด้วยเช่นกัน ทั้งนี้ ในการฟ้องร้องผู้กระทำความผิดฐานนี้ โจทก์จะต้องพิสูจน์ให้ศาลเห็นถึงสาระสำคัญ 2 ประการคือ ประการที่หนึ่ง จำเลยมีเจตนาเข้าสู่ระบบ และประการที่สอง จำเลยได้รู้ในขณะที่เขากระทำให้คอมพิวเตอร์แสดงผลหรือแสดงการทำงานใดๆ ว่า เขาได้เข้าไปสู่ระบบด้วยความจงใจโดยปราศจากอำนาจ ซึ่งการพิสูจน์ทั้งสองประการที่เป็นเรื่องของจิตใจของผู้กระทำนั้นถือเป็นหลักในการที่จะลงโทษผู้นั้น[131]

3.3 กฎหมายต่างประเทศที่ให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์

ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ มีดังนี้

---

131 พิญดา เลิศกิตติกุล, “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์,” (วิทยานิพนธ์นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2550), หน้า 97

3.3.1 ประเทศฟิลิปปินส์

ประเทศฟิลิปปินส์ได้บัญญัติมาตรการเพื่อคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ใน Electronic Commerce Act 2000 (section 33)[132] โดยมีองค์ประกอบของความผิด ดังนี้

(1) การเจาะระบบ (Hacking or cracking) โดยปราศจากอำนาจเข้าไป หรือรบกวนระบบการทำงานของระบบคอมพิวเตอร์ เครื่องให้บริการ (server) หรือระบบสารสนเทศและการสื่อสาร (information and communication system) หรือ

(2) ทำการเข้าถึงเพื่อเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ให้ด้อยค่าลง (corrupt) การเปลี่ยนแปลง (alter) การขโมย (steal) หรือทำลาย (destroy) ข้อมูลหรือระบบคอมพิวเตอร์ โดยใช้คอมพิวเตอร์ หรืออุปกรณ์ด้านสารสนเทศและการสื่อสารใดๆ ซึ่งปราศจากการรู้เห็นและความยินยอมจากเจ้าของ (owner) ของคอมพิวเตอร์ หรือระบบสารสนเทศและการสื่อสาร และให้รวมถึงการแพร่ไวรัสคอมพิวเตอร์หรือสิ่งอื่นในทำนองเดียวกัน อันเป็นผลให้ข้อมูลอิเล็กทรอนิกส์ (electronic data messages) หรือเอกสารอิเล็กทรอนิกส์ (electronic document) ถูกทำลาย (destruction) เปลี่ยนแปลง สูญหายหรือเสียหาย (theft or loss)

(3) ต้องระวางโทษปรับไม่เกิน... เปรโซหรือจำคุกตั้งแต่...เดือน ถึง... ปี

ตามบทบัญญัติดังกล่าว ผู้เขียนเห็นว่า เป็นมาตรการทางกฎหมายที่สามารถจัดการกับปัญหาการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ดีที่สุดในบรรดากฎหมายที่ยกมาเป็นตัวอย่าง แม้จะมิได้มีการกำหนดนิยามของการเข้าถึงไว้ ก็ตาม โดยเฉพาะอย่างยิ่งใน (2) ที่มีการบัญญัติไว้โดยชัดเจนเกี่ยวกับการเข้าถึงโดยชุดคำสั่งไม่พึงประสงค์ไม่ว่าจะเป็นไวรัสคอมพิวเตอร์หรือสิ่งอื่นในทำนองเดียวกัน ซึ่งจะสามารถใช้เป็นแนวทางอันชัดเจนสำหรับผู้ที่อยู่ในกระบวนการยุติธรรมตั้งแต่พนักงานสอบสวน อัยการ และศาล ในการประกอบการพิจารณาและใช้

---

132 Sec. 33. Penalties. - The folowing Acts shall be penalized by fine and/or imprisonment, as follows:

Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years.

ดุลพินิจเพื่อการตัดสินใจและการดำเนินคดีกับผู้กระทำผิดภายใต้กรอบของกฎหมายที่มีความชัดเจนเพียงพอ

3.3.2 ประเทศอินเดีย

ประเทศอินเดียได้บัญญัติมาตรการเพื่อคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ใน The Information Technology Act 2000 (section 66)[133] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดโดยเจตนา หรือรู้อยู่ว่าการกระทำของตนจะก่อให้เกิดความสูญหาย หรือเสียหาย หรือเกิดการเปลี่ยนแปลงของข้อมูลในคอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์เพื่อกิจการสาธารณะ หรือกระทำการอื่นใดอันเป็นการทำให้เสื่อมค่า (diminished it value) หรือประโยชน์ในการใช้งานระบบคอมพิวเตอร์ ผู้นั้นมีความผิดฐาน Hacking

(2) ผู้กระทำผิดต้องระวางโทษจำคุกไม่เกิน... ปี หรือปรับไม่เกิน... lakh rupees หรือทั้งจำทั้งปรับ

ตามบทบัญญัติดังกล่าว ผู้เขียนเห็นว่า ยังไม่มีความชัดเจนเพียงพอที่จะจัดการกับปัญหาการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ กล่าวคือ ความผิดฐาน Hacking ดังกล่าว แม้จะตีความได้ว่าการ Hacking เป็นการเข้าถึง แต่ก็ยังไม่ครอบคลุมถึงการขโมยข้อมูล หรือการทำสำเนาข้อมูลที่เกิดจากม้าโทรจัน หรือสปายแวร์ และแม้จะมีประโยคที่ว่า “หรือกระทำการอื่นใดอันเป็นการทำให้เสื่อมค่าหรือประโยชน์ในการใช้งานระบบคอมพิวเตอร์” ก็ตาม ประโยคดังกล่าวก็ยังมีความกำกวมเกินกว่าที่จะตีความให้ครอบคลุมถึงการกระทำดังกล่าวได้

---

133 Section 66. Hacking with computer system.-

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

3.3.3 ประเทศฟินแลนด์

ประเทศฟินแลนด์ได้บัญญัติมาตรการเพื่อคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ใน Penal Code (Chapter 38 Section 8)[134] โดยมีองค์ประกอบของความผิด ดังนี้

(1) ผู้ใดใช้รหัสในการแสดงตนของบุคคลอื่น หรือเข้าถึงระบบซึ่งมีการป้องกันโดยไม่มีเหตุอันจะอ้างได้ (unjustifiable) หรือ

(2) เข้าถึงระบบคอมพิวเตอร์ซึ่งใช้ในการประมวลผลข้อมูล จัดเก็บข้อมูล หรือส่งผ่านข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการทางเทคนิคอื่นใด หรือ

(3) เข้าไปในระบบคอมพิวเตอร์ที่มีการป้องกันไว้แล้ว (separately protected part of such a system)

(4) ต้องระวางโทษจำคุกไม่เกิน... ปี

อนึ่ง ความผิดฐานนี้ยังได้กำหนดให้ลงโทษแก่บุคคลที่แม้ไม่ได้เข้าถึงคอมพิวเตอร์แต่กระทำโดยวิธีการทางเทคนิคอื่นใดเพื่อให้ได้มาซึ่งข้อมูลในระบบคอมพิวเตอร์ด้วย

ตามบทบัญญัติดังกล่าว ผู้เขียนเห็นว่า ยังมิอาจแปลความให้ครอบคลุมถึงการขโมยข้อมูล หรือการทำสำเนาข้อมูลที่เกิดจากม้าโทรจัน หรือสปายแวร์ได้ กล่าวคือ เป็นเพียงการบัญญัติถึงการเข้าถึงระบบคอมพิวเตอร์ซึ่งใช้ในการประมวลผลข้อมูล จัดเก็บข้อมูล หรือส่งผ่านข้อมูลด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการทางเทคนิคอื่นใด ว่าเป็นความผิด แต่ภายหลังจากการเข้าถึงแล้วหากมีการขโมยข้อมูล หรือสำเนาข้อมูลไป ก็มิอาจแปลความให้ครอบคลุมถึงการกระทำดังกล่าวได้

---

134 Penal Code Chapter 38 Section 8: Data trespass.

Any person who, by using an identification code that does not belong to him or by breaking through a corresponding protective system unjustifiable, breaks into a computer system where data are processed, stored or transmitted by electronical or other technical methods or into a separately protected part of such a system, shall be sentenced for data trespass to fines or imprisonment not exceeding one year.

For data trespass is also sentenced any person without breaking into a computer system or a part thereof, uses a special technical device to unjustifiably obtain information that is stored in such a computer system.

Attempt is also punishable.

This Section will only be applied if the act is not punishable as a more severe offense.

3.3.4 ประเทศสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาได้บัญญัติมาตรการเพื่อคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ใน 18 U.S.C. 1030. Fraud and Related Activity in Connection with Computers[135] โดยมีหลักการและองค์ประกอบของความผิดว่า การเข้าถึง

---

135 1030. Fraud and Related Activity in Connection with Computers

(a) Whoever

(1) having knowingly accessed a computer without authorization or exceeding authorized access…

(2) intentionally accesses a computer without authorization or exceeds authorized access…

(A) information contained in a financial record of a financial institution…or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access…

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

โดยมิชอบหมายถึง “การเข้าถึงโดยไม่มีอำนาจและหมายความรวมถึงการเข้าถึงเกินกว่าอำนาจที่ตนมีด้วย (having knowingly accessed a compute without authorization or exceeding authorized access)” นอกจากนี้ ยังมีบทบัญญัติในการคุ้มครองเป็นพิเศษ (Protected Computer) สำหรับคอมพิวเตอร์ที่ใช้เพื่อการดำเนินงานในสถาบันการเงินหรือหน่วยงานของรัฐ หรือคอมพิวเตอร์ที่ใช้เพื่อการพาณิชย์ การสื่อสารระหว่างมลรัฐหรือระหว่างประเทศซึ่งหมายความรวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกราชอาณาจักรที่ถูกใช้งานเพื่อกิจการดังกล่าวด้วย ซึ่งอาจสรุปเป็นภาพรวมได้ ดังนี้[136]

1. การเข้าถึงโดยปราศจากอำนาจที่จะเป็นความผิดตามกฎหมายนี้ สามารถเกิดขึ้นได้ไม่ต้องคำนึงถึงว่าจะเป็นคอมพิวเตอร์ที่มีการป้องกันหรือไม่ โดยจะเห็นได้ว่า หากเป็นสิ่งที่สำคัญที่กฎหมายมุ่งคุ้มครองเป็นหลักโดยเฉพาะข้อมูลของรัฐหรือสถาบันการเงิน แม้ไม่เป็นคอมพิวเตอร์ที่มีการป้องกันถ้าเข้าไปโดยปราศจากอำนาจก็เป็นความผิด

อย่างไรก็ตาม คำว่าคอมพิวเตอร์ที่มีการป้องกันในความหมายของประเทศสหรัฐอเมริกานั้น มีความแตกต่างจากคำว่าระบบคอมพิวเตอร์ที่มีการป้องกันการเข้าถึงโดยเฉพาะของไทย เนื่องจากคำว่าคอมพิวเตอร์ที่มีการป้องกันในความหมายของประเทศสหรัฐอเมริกาหมายถึงคอมพิวเตอร์ที่ (1) ใช้โดยเฉพาะในสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา หรือใน

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

…

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of the section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e) (8) (A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under section 1030 (a) (5) of Title 18, United States Code.

Similar special penal legislation in numerous states in the United States.

136 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 80-81

กรณีที่คอมพิวเตอร์ไม่ได้ใช้ในกรณีดังกล่าว แต่ถูกใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา และมีผลเป็นความผิดในการใช้หรือสำหรับสถาบันการเงินหรือรัฐบาลของสหรัฐอเมริกา (2) ซึ่งถูกใช้ในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกประเทศสหรัฐอเมริกาซึ่งถูกใช้จัดการในการค้าพาณิชย์หรือติดต่อสื่อสารระหว่างมลรัฐหรือระหว่างประเทศของสหรัฐอเมริกา ไม่ได้หมายความถึงระบบคอมพิวเตอร์ที่มีระบบป้องกันการเข้าถึงแต่อย่างใด

2. การเข้าถึงโดยปราศจากอำนาจโดยปกติแล้วไม่เป็นความผิดทางอาญาโดยเฉพาะเมื่อพิจารณาจากกฎหมายนี้ จะต้องมีองค์ประกอบอื่นนอกเหนือจากการเข้าไปโดยปราศจากอำนาจด้วยจึงจะเป็นความผิด เช่น ตามอนุมาตรา (a) (1) เป็นการเข้าไปโดยปราศจากอำนาจเพื่อเอาไปซึ่งข้อมูลเกี่ยวกับความมั่นคงของประเทศสหรัฐอเมริกา หรือแม้ในอนุมาตรา (a) (3) ที่เป็นการบุกรุกเข้าไปในคอมพิวเตอร์ของรัฐแม้จะไม่มีองค์ประกอบอื่นหากแต่การกระทำดังกล่าวก็ต้องส่งผลกระทบต่อสหรัฐอเมริกา จึงจะเป็นความผิดตามกฎหมายนี้

3. การคุ้มครองการเข้าถึงโดยปราศจากอำนาจของประเทศสหรัฐอเมริกาตามกฎหมายนี้ ไม่มีลักษณะเป็นการคุ้มครองโดยทั่วไป หากแต่มีรายละเอียดเฉพาะเจาะจงว่าเป็นการคุ้มครองเพื่อจุดประสงค์ใด เช่น คอมพิวเตอร์หรือข้อมูลของรัฐ สถาบันการเงิน

4. โดยหลักแล้วกฎหมายนี้จะคุ้มครองคอมพิวเตอร์หรือข้อมูลของรัฐเป็นหลัก เนื่องจากเริ่มแรกกฎหมายนี้บัญญัติขึ้นเพื่อคุ้มครองรัฐ แต่ต่อมาได้มีการขยายขอบเขตไปยังคอมพิวเตอร์ของเอกชนในการแก้ไขเพิ่มเติมกฎหมายในภายหลัง

5. จากบทบัญญัติของอนุมาตรา (g) แม้กฎหมายนี้จะเป็นกฎหมายอาญาเกี่ยวกับการกระทำผิดทางด้านคอมพิวเตอร์ แต่จากการแก้ไขกฎหมายเพิ่มเติมสหรัฐอเมริกาได้เพิ่มเติมหลักเกณฑ์ทางกฎหมายโดยเปิดช่องให้ผู้เสียหายสามารถฟ้องร้องทางแพ่งได้ด้วย

6. นอกเหนือจากความผิดที่เกี่ยวข้องกับการเข้าถึงคอมพิวเตอร์โดยตรงแล้วยังมีความผิดที่เกี่ยวข้องคือ ความผิดในการซื้อขายรหัสผ่านเพื่อฉ้อโกง ซึ่งแม้ไม่ใช่ความผิดโดยตรงหากแต่ก็เป็นความผิดที่สนับสนุนการกระทำผิดในการเข้าถึงโดยปราศจากอำนาจ

7. การให้คำนิยามทางกฎหมายนั้น กฎหมายนี้ในอนุมาตรา (e) ได้มีการให้คำนิยามคำว่า คอมพิวเตอร์ คอมพิวเตอร์ที่ถูกปกป้อง การเข้าถึงเกินขอบอำนาจ แต่ไม่มีคำนิยามว่าการเข้าถึงโดยปราศจากอำนาจหมายถึงอะไร

4. ความไม่ลงรอยของแนวความคิดเกี่ยวกับความรับผิดทางกฎหมายในความผิดฐานเข้าถึงโดยไม่มีอำนาจ

สิ่งที่จะกล่าวถึงต่อไปนี้ จะเป็นการแสดงให้เห็นถึงความไม่ลงรอยของแนวความคิดเกี่ยวกับความรับผิดทางกฎหมายในความผิดฐานเข้าถึงโดยไม่มีอำนาจ สำหรับประเทศที่มีทั้งการกำหนดนิยามของคำว่า “เข้าถึง” และมิได้กำหนดนิยามของคำว่า “เข้าถึง” ไว้ในกฎหมาย จึงทำให้เกิดความแตกต่างหรือความไม่ลงรอยกันในคำตัดสินของศาลในความผิดฐานเข้าถึงโดยไม่มีอำนาจทั้งๆ ที่ข้อเท็จจริงของคดีมีความคล้ายคลึงกันหรืออาจเรียกได้ว่าเป็นแบบเดียวกัน กรณีดังกล่าวจึงเป็นภาระหรือหน้าที่ของผู้ที่อยู่ในกระบวนการยุติธรรมในการที่จะตีความกฎหมายเพื่อนำไปสู่การวินิจฉัยและการปรับใช้กฎหมายให้เกิดความยุติธรรมมากที่สุด ซึ่งจะขอยกตัวอย่างคำตัดสินของศาลในประเทศสหรัฐอเมริกา ซึ่งเป็นประเทศที่มีทั้งการกำหนดนิยามของคำว่า “เข้าถึง” และมิได้กำหนดนิยามของคำว่า “เข้าถึง” ไว้ในกฎหมาย กล่าวคือ ในกฎหมายของรัฐบาลกลางมิได้มีการกำหนดนิยามของคำว่า “เข้าถึง” ไว้ แต่ในกฎหมายระดับมลรัฐในบางมลรัฐได้กำหนดนิยามของคำว่า “เข้าถึง” ไว้ในกฎหมายด้วย

เนื่องจากคำว่า “เข้าถึง (access)” สามารถที่จะให้ความหมายได้ทั้งแบบแคบและแบบกว้าง ดังนั้น ศาลในประเทศสหรัฐอเมริกาจึงมีความไม่ลงรอยกันในการตีความของคำดังกล่าว โดยมีตัวอย่างของคำตัดสินของศาลที่แตกต่างกัน ดังนี้[137]

คดีของศาลสูงแคนซัสในปี 1996 ในคดี State V. Allen โดยคดีนี้ Allen ได้ใช้คอมพิวเตอร์ของเขาในการทำซ้ำเพื่อทำให้คอมพิวเตอร์ของบริษัท Southwestern Bell Telephone ที่ควบคุมการเปิด-ปิด การโทรศัพท์ทางไกลทำให้ผู้ใช้ใช้โทรศัพท์ทางไกลฟรี โดย Allen ต่อสู้ว่าไม่มีหลักฐานว่าตนได้เข้าไปยังคอมพิวเตอร์ของบริษัท Southwestern Bell Telephone ศาลเห็นว่าการตีความคำว่า “เข้าถึง” อย่างกว้างขวางตามที่กฎหมายบัญญัติ จะทำให้การกระทำทางกายภาพที่ไม่ได้รับอนุญาตทั้งหมดเป็นความผิดทางอาญา ซึ่งไม่ถูกต้องและเห็นว่าควรใช้ความหมายพื้นฐานตามปกติ ดังนั้น ความหมายของคำว่า “เข้าถึง” จึงเป็นความหมายที่คล้ายคลึงกับความหมายทางกายภาพ โดยหมายถึงการใส่ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องและทำให้ผู้ใช้ได้เข้าไปใน (inside) เครื่องคอมพิวเตอร์อย่างแท้จริงเพื่อหาข้อมูลข้างใน ดังนั้น เขาจึงไม่ได้เข้าถึงคอมพิวเตอร์ของบริษัทดังกล่าว

---

137 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 83-84

ศาลของรัฐบาลกลางได้ตัดสินคล้ายคลึงกันในคดี Moulton V. VC3 ซึ่งเป็นคดีแพ่งระหว่างบริษัทรักษาความปลอดภัยของคอมพิวเตอร์ โดยคดีเกิดขึ้นในปี 1994 บริษัทแรกฟ้องบริษัทที่สองเมื่อลูกจ้างของบริษัทที่สองได้ทำ port scan คอมพิวเตอร์ของบริษัทแรก โดยศาลได้ตัดสินว่าการ scan port ของบริษัทที่สองไม่ใช่การเข้าถึงคอมพิวเตอร์ของบริษัทแรก เนื่องจากไม่มีการเข้า (inside) เกิดขึ้น

ขณะที่คดีของ State V. Allen และคดี Moulton V. VC3 ได้มองว่าการเข้าถึงคอมพิวเตอร์มีขีดจำกัด โดยต้องมีการเข้าไปในคอมพิวเตอร์จึงจะถือว่าเป็นการเข้าถึง แต่ก็มีคดีที่ตัดสินแตกต่างออกไปโดยให้คำนิยามคำว่า “เข้าถึง” ที่กว้างขวางกว่า

ในคดีของศาลสูงวอชิงตัน State V. Riley ข้อเท็จจริงของคดีคล้ายคลึงกับคดี State V. Allen โดย Riley ได้ใช้คอมพิวเตอร์ของเขาในการทำซ้ำเพื่อหมุนคอมพิวเตอร์ของบริษัท Northwest Telco และเดารหัสผ่านทำให้ผู้ใช้ใช้โทรศัพท์ทางไกลฟรี โดย Riley ได้ต่อสู้ว่าเขาไม่ได้เข้าไปในคอมพิวเตอร์ของบริษัทดังกล่าว แต่ศาลวอชิงตันได้อธิบายคำว่า “เข้าถึง” แตกต่างจากศาลแคนซัสในคดี Allen โดยศาลวอชิงตันได้ถือเอาคำนิยามของคำว่า “เข้าถึง” อย่างกว้าง ซึ่งรวมถึงการสื่อสารกับคอมพิวเตอร์ด้วย และตัดสินว่าการกระทำของ Riley เป็นการเข้าถึงคอมพิวเตอร์แล้ว

เมื่อได้ศึกษาถึงแนวความคิดเกี่ยวกับความรับผิดทางกฎหมายซึ่งไม่ลงรอยกันข้างต้นแล้วผู้เขียนเห็นว่า สาเหตุที่ทำให้เกิดความไม่ลงรอยกันในคำตัดสินของศาลทั้งๆ ที่ข้อเท็จจริงในคดีมีความคล้ายคลึงกันนั้น อาจเป็นเพราะในคดีที่ตัดสินโดยศาลระดับมลรัฐนั้น ได้มีการกำหนดนิยามคำว่า “เข้าถึง” ไว้ในกฎหมายของมลรัฐ จึงทำให้มีบรรทัดฐานที่เพียงพอในการวินิจฉัยของศาลถึงความหมายของคำว่า “เข้าถึง” ว่า มีความหมายเพียงใด ซึ่งแตกต่างจากศาลของรัฐบาลกลางที่ไม่มีการกำหนดนิยามคำว่า “เข้าถึง” ไว้ในกฎหมายของรัฐบาลกลาง จึงขึ้นอยู่กับดุลพินิจและการวินิจฉัยของศาลที่จะวินิจฉัยความหมายของคำว่า “เข้าถึง” เอง จนทำให้เกิดความแตกต่างในคำตัดสินข้างต้น

บทที่ 4
มาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในประเทศไทย

1. ชุดคำสั่งไม่พึงประสงค์ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จากการสืบค้นและตรวจสอบที่มาของการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่า ในชั้นการยกร่างตั้งแต่ปี พ.ศ. 2541 กฎหมายดังกล่าวมีชื่อเดิมว่าร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ที่ยกร่างโดยคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee : NITC)[138] โดยในเบื้องต้นหรือในวาระเริ่มแรกของการยกร่างนั้น ได้คำนึงถึงเพียงแต่ลักษณะของการกระทำความผิดที่ได้กระต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ซึ่งอาจสรุปความผิดสำคัญได้ 3 ฐานความผิด คือ การเข้าถึงโดยไม่มีอำนาจ (unauthorized access) การใช้คอมพิวเตอร์โดยมิชอบ (computer misuse) ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (Computer related crime) โดยแบ่งการกระทำความผิดออกเป็นสองหมวดด้วยกัน คือ หมวดที่ว่าด้วยความผิดเกี่ยวกับการักษาความลับความครบถ้วนและการทำงานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ และหมวดที่ว่าด้วย

---

138 ในปี 2535 รัฐบาลนายอานันท์ ปันยารชุน ได้ออกระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศ พ.ศ. 2535 (ฉบับที่ 1) ให้มีการแต่งตั้งคณะกรรมการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee : NITC) เพื่อทำหน้าที่ในการให้ข้อเสนอแนะแผนพัฒนาเทคโนโลยีสารสนเทศแห่งชาติต่อคณะรัฐมนตรี ส่งเสริมการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศเสริมสร้างบรรยากาศให้มีการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงานต่างๆ การพัฒนาโครงสร้างพื้นฐานด้านโทรคมนาคม ปรับปรุงกฎหมาย ระเบียบข้อบังคับให้สอดคล้องกับการดำเนินการธุรกิจสมัยใหม่โดยสื่ออีเล็กทรอนิกส์ ส่งเสริมการผลิต การบริการ การวิจัยและพัฒนาให้มีเทคโนโลยีสารสนเทศขึ้นในประเทศไทย ส่งเสริมผู้ประกอบการขนาดกลางและขนาดเล็ก ส่งเสริมและสนับสนุนการผลิตการบริการและการใช้เทคโนโลยีสารสนเทศของประเทศ รวมถึงการให้ข้อเสนอแนะในการแก้ไขปัญหาอุปสรรคในการพัฒนาเทคโนโลยีสารสนเทศ

ความผิดเกี่ยวกับคอมพิวเตอร์[139] ต่อมา เมื่อมีการตรวจพิจารณาจากผู้ทรงคุณวุฒิโดยสำนักงานคณะกรรมการกฤษฎีกา และผ่านการรับฟังความคิดเห็นจากภาคประชาชน รวมทั้งได้ผ่านการพิจารณาจากคณะกรรมาธิการวิสามัญ สภานิติบัญญัติแห่งชาติ จนกระทั่งได้รับการลงพระปรมาภิไธยและมีผลบังคับใช้เมื่อวันที่ 18 กรกฎาคม พ.ศ. 2550 ภายใต้ชื่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทำให้มีมาตราทั้งสิ้น 30 มาตรา โดยมีเจตนารมณ์เพื่อกำหนดฐานความผิดและบทลงโทษรวมทั้งการกำหนดเกี่ยวกับพนักงานเจ้าหน้าที่ โดยมีข้อพึงสังเกตว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยนี้จัดอยู่ในประเภทกฎหมายสารบัญญัติและวิธีสบัญญัติอยู่ในตัวซึ่งแตกต่างจากในชั้นการยกร่างที่มิได้แยกส่วนของกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติออกจากกันอย่างชัดเจน ทั้งนี้ ก็อาจเนื่องมาจากในชั้นการตรวจพิจารณาได้มีการคำนึงถึงหลักการสำคัญของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[140] (Convention on Cybercrime : ETS. No. 185) ซึ่งมีวัตถุประสงค์ที่สำคัญ 3 ประการ ได้แก่ (1) เพื่อให้กฎหมายสารบัญญัติภายในประเทศต่างๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีความสอดคล้องและเป็นไปในทิศทางเดียวกัน (2) เพื่อให้กฎหมายวิธีพิจารณาความอาญาตามกฎหมายภายในให้อำนาจที่จำเป็นเพื่อการสืบสวนสอบสวนและฟ้องร้องการกระทำความผิดที่ได้กระทำโดยใช้ระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ และ (3) เพื่อเร่งให้เกิดความร่วมมือระหว่างประเทศที่รวดเร็วและบรรลุเป้าหมายของอนุสัญญา

อย่างไรก็ตาม หากพิจารณาโครงสร้างของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วจะประกอบด้วยสองส่วน คือ ส่วนทั่วไปซึ่งมี 4 มาตรา ได้แก่ มาตรา 1 ชื่อกฎหมาย, มาตรา 2 วันบังคับใช้กฎหมาย, มาตรา 3 คำนิยาม, มาตรา 4 ผู้รักษาการ และส่วนที่เป็นเนื้อหาของกฎหมายอีกสองหมวดคือ หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งถือเป็นส่วนของกฎหมายสารบัญญัติเพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และหมวด 2 พนักงานเจ้าหน้าที่ซึ่งถือเป็นส่วนของกฎหมายวิธีสบัญญัติเพื่อกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่เกี่ยวกับวิธีพิจารณาความอาญาเฉพาะคดีอาญาความผิด

---

139 เอกสารคำอธิบายร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... เพื่อเป็นข้อมูลประกอบการนำเสนอ หัวข้อ “จะไล่ล่าอาชญากรอย่างไรเมื่อไม่มีประจักษ์พยานและกฎหมายวิธีพิจารณาความที่จำเป็นในคดีอาชญากรรมทางคอมพิวเตอร์” ในการสัมมนาหัวข้อ “กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์” ซึ่งจัดทำโดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) เมื่อวันที่ 16 ธันวาคม 2546 เวลา 13.30 – 16.00 น. ณ ห้องพิมานเมฆ แกรนด์บอลรูม ชั้น 3 โรงแรม เดอะแกรนด์ กรุงเทพฯ

140 อนุสัญญาและคำอธิบาย สืบค้นได้ที่ http://conventions.coe.int/Treaty/ EN/cadreprincipal.htm

เกี่ยวกับคอมพิวเตอร์ โดยสามารถสรุปสาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ดังนี้

1.1 ส่วนของกฎหมายสารบัญญัติเพื่อกำหนดฐานความผิดและบทกำหนดโทษ

สำหรับส่วนของกฎหมายสารบัญญัติเพื่อกำหนดฐานความผิดและบทกำหนดโทษในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น อยู่ในหมวดหนึ่ง ความผิดเกี่ยวกับคอมพิวเตอร์ มีทั้งสิ้น 12 มาตรา โดยเริ่มตั้งแต่มาตรา 5 ถึงมาตรา 16 ส่วนมาตรา 17 นั้น เป็นการกำหนดขึ้นเพื่อรองรับสภาพของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ผู้กระทำผิดจะอยู่ที่ใดในโลกก็ได้ ซึ่งหากมีการกระทำผิดแล้วเข้าเงื่อนไขแม้ความผิดที่ได้กระทำผิดนั้นจะเกิดขึ้นนอกราชอาณาจักรก็จะต้องรับโทษในราชอาณาจักรด้วย

สำหรับส่วนของกฎหมายสารบัญญัติเพื่อกำหนดฐานความผิดและบทกำหนดโทษนี้สามารถแยกได้เป็นสองส่วนที่สำคัญคือ ส่วนที่หนึ่งเป็นการกระทำที่กระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ กล่าวคือ เป็นการกระทำความผิดที่กระทบต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ซึ่งส่วนใหญ่นิยมใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดจึงอาจกล่าวได้ว่า ความผิดส่วนนี้จัดเป็นความผิดที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์ และส่วนที่สองเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือการกระทำความผิดที่มิได้เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์ โดยกฎหมายกำหนดไม่ให้การกระทำความผิดในหมวดหนึ่งนี้เป็นความผิดอันยอมความได้ เนื่องจากผลของการกระทำความผิดหรือการก่อให้เกิดความเสียหายใดๆ ขึ้นนั้น อาจไม่ได้กระทบต่อบุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจง แต่อาจกระทบต่อสังคม ต่อความมั่นคงของประเทศ หรืออาจก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจในวงกว้าง รวมทั้งการหาตัวผู้กระทำความผิดและการแสวงหาพยานหลักฐานก็กระทำได้ยาก หรือในบางครั้งก็อาจไม่รู้ด้วยซ้ำว่าใครเป็นผู้เสียหาย เว้นเสียแต่มาตรา 16 ซึ่งเป็นความผิดเกี่ยวกับการตัดต่อหรือดัดแปลงภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัด ต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอายเท่านั้นที่กฎหมายกำหนดให้เป็นความผิดอันยอมความได้ ทั้งนี้ก็เนื่องจากความเสียหายนั้นมักเกิดขึ้นกับบุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงและเพื่อเป็นการให้โอกาสที่คู่ความจะสามารถหาข้อยุติและเยียวยาความเสียหายหรือตกลงกันได้เอง โดยภาพรวมของหมวด 1 แล้วมีฐานความผิดครอบคลุมในเรื่อง ดังต่อไปนี้

มาตรา 5	การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ
มาตรา 6	การล่วงรู้มาตรการป้องกันการเข้าถึงโดยมิชอบ
มาตรา 7	การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 8	การดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 9	การรบกวนข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 10	การรบกวนระบบคอมพิวเตอร์โดยมิชอบ
มาตรา 11	การทำสแปมเมล์ (Spam Mail)
มาตรา 12	การกระทำความผิดที่ก่อให้เกิดความเสียหายแก่ประชาชนหรือกระทบต่อความมั่นคงของประเทศ
มาตรา 13	การจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ เพื่อใช้ในการกระทำความผิด
มาตรา 14	การนำเข้าและเผยแพร่ข้อมูลคอมพิวเตอร์ปลอม ข้อมูลคอมพิวเตอร์อันเป็นเท็จ ข้อมูลคอมพิวเตอร์ที่มีลักษณะอันลามก หรือเผยแพร่เนื้อหาอันไม่เหมาะสมจนก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกในหมู่ประชาชน
มาตรา 15	ความรับผิดของผู้ให้บริการที่สนับสนุนการกระทำตามมาตรา 14
มาตรา 16	การเผยแพร่ภาพจากการตัดต่อหรือดัดแปลงให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรืออับอาย
มาตรา 17	การกระทำความผิดนอกราชอาณาจักรซึ่งต้องรับโทษในราชอาณาจักร

ทั้งนี้ หากนำฐานความผิดและบทกำหนดโทษข้างต้นมาแยกเป็นประเภทความผิดในมุมมองของผู้เขียนแล้ว สามารถแยกได้ ดังนี้

1.1.1 ฐานความผิดและตัวอย่างการกระทำความผิดที่อาจเกิดจากชุดคำสั่งไม่พึงประสงค์ ได้แก่

1) การเข้าถึงโดยมิชอบ ตามมาตรา 5 และมาตรา 7

การกระทำความผิดฐานเข้าถึงโดยมิชอบหรือโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมายนี้ อาจเกิดขึ้นได้หลายวิธี เช่น การเจาะระบบ (hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) เพื่อทำลายระบบคอมพิวเตอร์หรือเปลี่ยนแปลงแก้ไขข้อมูล หรือการเข้าถึงข้อมูลที่เก็บรักษาไว้เป็นความลับ (secret) การส่งชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจัน (Trojan Horses) สปายแวร์ (spyware) ผ่านช่องโหว่ต่างๆ โดยเข้าไปฝังตัวในระบบ

คอมพิวเตอร์เพื่อขโมยข้อมูลรหัสผ่านหรือข้อมูลส่วนบุคคลของผู้อื่นเพื่อใช้บุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้นั้น หรือนำข้อมูลดังกล่าวไปก่ออาชญากรรมอื่นต่อไป เป็นต้น จนอาจเป็นที่มาของการกระทำความผิดฐานอื่นและอาจก่อให้เกิดความเสียหายต่อเนื่องเป็นมูลค่ามหาศาล ซึ่งสามารถเรียกวิธีการเข้าถึงประเภทนี้ว่า “การเข้าถึงทางอิเล็กทรอนิกส์ หรือ การเข้าถึงทางดิจิทัล” ซึ่งอาจเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ไม่ว่าทั้งหมดหรือแต่บางส่วนก็ได้ เช่น การเข้าถึงถึงฮาร์ดแวร์ซึ่งเป็นส่วนประกอบต่างๆ ของคอมพิวเตอร์หรือข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง หรือข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น นอกจากนี้ยังหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ที่แม้ว่าตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ไม่ว่าจะเข้าถึงนั้นจะผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น หรือโดยผ่านทางระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network หมายถึง เครือข่ายคอมพิวเตอร์โดยการเชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้เคียงเข้าด้วยกัน) เป็นต้น

นอกจากจะมีการเข้าถึงทางอิเล็กทรอนิกส์แล้ว หากพิจารณาถึงความหมายและเจตนารมณ์ของกฎหมายแล้ว ย่อมหมายความรวมถึง “การเข้าถึงในระดับกายภาพ” ด้วย เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ แล้วผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้น เป็นต้น

อย่างไรก็ตาม ยังมีประเด็นที่ต้องพิจารณาเกี่ยวกับการกระทำความผิดฐานนี้อีกว่า หากเพียงแค่มีการเข้าถึงโดยไม่ได้รับอนุญาตจะถือว่าเป็นการก่ออาชญากรรมได้หรือไม่ หรือผู้กระทำจะต้องมีมูลเหตุจูงใจที่จะกระทำให้เกิดความเสียหายด้วยจึงจะถือเป็นการก่ออาชญากรรม เช่น บุคคลซึ่งมิได้มีมูลเหตุจูงใจดังกล่าวแต่มีความอยากรู้อยากเห็นหรืออยากทดลองจึงทดลองเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยมิได้มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย กรณีดังกล่าวควรกำหนดให้ต้องรับผิดและมีบทลงโทษหรือไม่ และกรณีที่มีการเข้าถึงแม้โดยไม่มีมูลเหตุจูงใจที่จะก่อให้เกิดความเสียหาย เช่น การเข้าไปในระบบคอมพิวเตอร์ของสายการบินแล้วทำการเปลี่ยนแปลงระบบจองตั๋วเครื่องบินและสลับตารางการบินของลูกค้าที่จองไว้ จนเกิดความเสียหายต่อสายการบินและตัวลูกค้า กรณีดังกล่าวนี้จะกำหนดขอบเขตในการพิจารณาว่าเป็น

ความผิดอย่างไร เป็นต้น ประเด็นนี้มีนักกฎหมายเห็นว่า[141] การเข้าถึงโดยมิชอบตามมาตรา 5 และมาตรา 7 นี้ ถือเป็นความผิดในตัวเอง (mala inse) กล่าวคือ แม้ว่าผู้กระทำจะมิได้มีมูลเหตุจูงใจเพื่อก่อให้เกิดความเสียหาย หรือการกระทำดังกล่าวจะยังมิได้ก่อให้เกิดความเสียหายก็ตาม ทั้งนี้ เพราะเห็นว่าการกระทำดังกล่าวนั้นสามารถก่อให้เกิดการกระทำผิดฐานอื่นหรือฐานที่ใกล้เคียงค่อนข้างง่ายและอาจก่อให้เกิดความเสียหายร้ายแรงทั้งการพิสูจน์มูลเหตุจูงใจทำได้ค่อนข้างยาก และที่สำคัญจะต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะจึงจะเป็น ซึ่งผู้เขียนก็เห็นด้วยกับแนวความเห็นนี้

2) การดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 8

ในปัจจุบันข้อมูลได้ถูกจัดเก็บในรูปแบบอิเล็กทรอนิกส์และมีการโอนข้อมูลทางอิเล็กทรอนิกส์กันมากขึ้น โอกาสที่จะถูกดักรับหรือล่วงรู้ข้อมูลนั้นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์จึงมีมากขึ้นตามไปด้วย ดังนั้น การลักลอบดักข้อมูลโดยฝ่าฝืนกฎหมาย (Illegal interception) จึงเป็นปัญหาสำคัญอีกปัญหาหนึ่งที่อาจส่งผลกระทบต่อความเป็นส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชนในทำนองเดียวกับการให้ความคุ้มครองสิทธิความเป็นส่วนตัวในการติดต่อสื่อสารรูปแบบเดิมที่ห้ามดักฟังโทรศัพท์ การลักลอบดักข้อมูลในที่นี้หมายถึงการลักลอบดักข้อมูลโดยใช้วิธีการทางเทคนิค (technical means) เพื่อลักลอบดักฟัง ตรวจสอบหรือติดตามเนื้อหาสาระของข้อมูลข่าวสารที่สื่อสารถึงกันระหว่างบุคคล หรือกรณีเป็นการกระทำอันเป็นการล่อลวงหรือจัดหาข้อมูลดังกล่าวให้กับบุคคลอื่นรวมทั้งการแอบบันทึกข้อมูลที่สื่อสารถึงกันนั้นด้วย ตัวอย่าง เช่น การใช้ชุดคำสั่งไม่พึงประสงค์ประเภทสนิฟเฟอร์ (sniffer) แอบดักแพ็คเกต (packet) ซึ่งเป็นชุดของข้อมูลที่เล็กที่สุดที่อยู่ระหว่างการส่งไปให้ผู้รับ เป็นต้น ทั้งนี้ วิธีการทางเทคนิคก็หมายถึงอุปกรณ์ที่มีสายเชื่อมต่อกับระบบเครือข่ายต่างๆ และหมายรวมถึงอุปกรณ์ประเภทไร้สายด้วย เช่น การติดต่อผ่านทางโทรศัพท์มือถือหรืออุปกรณ์ชนิดพกพาต่างๆ เป็นต้น อย่างไรก็ตาม การกระทำที่จะถือเป็นความผิดฐานลักลอบดักข้อมูลนั้นข้อมูลที่ส่งจะต้องมิใช่ข้อมูลที่อาจเปิดเผยให้สาธารณชนสามารถรับรู้ได้ (non-public transmissions) การกระทำความผิดฐานนี้จึงจำกัดเฉพาะแต่เพียงวิธีการส่งที่ผู้ส่งข้อมูลประสงค์จะส่งข้อมูลนั้นให้แก่บุคคลหนึ่งบุคคลใดโดยเฉพาะเจาะจงเท่านั้นจึงจะได้รับความคุ้มครองแม้จะเป็นการส่งข้อมูลผ่านทางเครือข่ายสาธารณอย่างอินเทอร์เน็ตก็ตาม ดังนั้น จึงไม่ต้องพิจารณาถึงเนื้อหาสาระของข้อมูลที่ส่งด้วยแต่อย่างใด เพราะเนื้อหาสาระของข้อมูลที่ส่งนั้นอาจมีเนื้อหาสาระที่หาได้โดยทั่วไป

---

141 แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) , พ.ศ. 2546 หน้า 22

หรือมีอยู่ทั่วไป รวมทั้งข้อมูลที่เป็นความลับทางการค้า หรือเป็นข้อมูลส่วนบุคคลที่เจ้าของข้อมูลประสงค์จะปกปิดเป็นความลับก็ได้[142]

อนึ่ง หากพิจารณาถึงลักษณะหรือพฤติการณ์แห่งการกระทำความผิดฐานลักลอบดักรับข้อมูลคอมพิวเตอร์และฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบแล้ว จะเห็นได้ว่าความผิดทั้งสองฐานดังกล่าวมีลักษณะหรือพฤติการณ์แห่งการกระทำที่ใกล้เคียงกันอย่างยิ่ง แต่มีความแตกต่างกันที่เจตนาภายใน กล่าวคือ การกระทำความผิดฐานลักลอบดักรับข้อมูลต้องเป็นการกระทำโดยมีมูลเหตุจูงใจเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ ส่วนการกระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบนั้น แม้จะกระทำโดยมิได้มีเจตนาหรือมีมูลเหตุจูงใจหรือมิได้ประสงค์ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ใดโดยเฉพาะเจาะจง และแม้จะมิได้มีความเสียหายใดๆ เกิดขึ้น ผู้กระทำก็ต้องรับผิดในการกระทำดังกล่าว

3) การเปิดเผยมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะโดยมิชอบ ตามมาตรา 6

การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ไม่ว่าจะล่วงรู้โดยชอบหรือมิชอบก็ตาม ตัวอย่างการล่วงรู้โดยมิชอบ เช่น การใช้ชุดคำสั่งไม่พึงประสงค์ประเภทโปรแกรมดักข้อมูลผ่านปุ่มคีย์บอร์ด (Keylogger หรือ Keystroker) แอบบันทึกการกดรหัสผ่านของผู้อื่นแล้วนำไปเปิดเผยต่อ เป็นต้น เพียงแค่นี้ก็ถือว่าเป็นการนำมาตรการป้องกันหรือรหัสผ่านนั้นไปเปิดเผยโดยมิชอบซึ่งเข้าองค์ประกอบของความผิดฐานนี้แล้ว ไม่ว่าบุคคลที่สามซึ่งล่วงรู้มาตรการป้องกันหรือรหัสผ่านนั้นจะนำไปใช้เพื่อเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นหรือไม่ก็ตาม

4) การรบกวนข้อมูลคอมพิวเตอร์และรบกวนระบบคอมพิวเตอร์ ตามมาตรา 9 และมาตรา 10

ความผิดฐานรบกวนหมายถึงการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์โดยจงใจก่อให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมทั้งระบบคอมพิวเตอร์และระบบการสื่อสารด้วย ทั้งนี้ประโยชน์ที่กฎหมายมุ่งประสงค์จะคุ้มครองคือความครบถ้วนสมบูรณ์ของข้อมูลและเสถียรภาพในการใช้งานหรือการใช้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่บันทึกเก็บไว้บนสื่อคอมพิวเตอร์ได้เป็นไปโดยปกติสุข โดยไม่ต้องการให้มีการทำให้เสียหาย หรือทำให้ข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์เสื่อมค่าหรือไร้ประโยชน์ รวมถึงการลบหรือทำลายข้อมูลคอมพิวเตอร์ หรือกระทำการใดๆ ให้ไม่สามารถเข้าถึง

---

142 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค), อ้างแล้วในเชิงอรรถที่ 141 หน้า 25-27

ข้อมูลคอมพิวเตอร์หรือใช้โปรแกรมคอมพิวเตอร์นั้นได้รวมทั้งการเปลี่ยนแปลงข้อมูลใดๆ ที่มีอยู่ด้วย

ตัวอย่างของการกระทำความผิดในฐานนี้ ได้แก่ การป้อนโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ เช่น ไวรัส เพื่อทำลายข้อมูลคอมพิวเตอร์ หรือการป้อนชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันเข้าไปในระบบเพื่อขโมยรหัสผ่านของผู้ใช้คอมพิวเตอร์ สำหรับนำไปใช้ในการกระทำความผิดอื่นต่อไป เช่น การนำรหัสผ่านที่เกี่ยวกับธุรกรรมทางการเงินบนอินเทอร์เน็ตหรืออินเทอร์เน็ตแบงก์กิ้งของผู้ใช้คอมพิวเตอร์ไปก่ออาชญากรรมทางการเงิน หรือการเข้าไปลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใดๆ อันเป็นการรบกวนข้อมูลคอมพิวเตอร์ เป็นต้น นอกจากนั้น กฎหมายยังมุ่งคุ้มครองการทำงานของระบบคอมพิวเตอร์และระบบการติดต่อสื่อสารให้เป็นไปตามปกติสุขซึ่งรูปแบบหรือวิธีการรบกวนหรือขัดขวางหรือทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานได้เป็นปกติสุขนั้นอาจเกิดขึ้นได้ในขั้นตอนต่างๆ ตั้งแต่การป้อนข้อมูลเข้าไปในระบบหรือในการส่ง ทำลาย ลบ หรือเปลี่ยนแปลงแก้ไขข้อมูลคอมพิวเตอร์ ซึ่งผลของการกระทำจะก่อให้เกิดความเสียหายที่ร้ายแรงหรือรุนแรงต่อการใช้ระบบดังกล่าวหรือต่อการติดต่อสื่อสารกับระบบอื่น เช่น การโจมตีจากชุดคำสั่งไม่พึงประสงค์เพื่อทำให้ระบบทำงานหนักและปฏิเสธการทำงาน (denial of service) หรือทำให้ระบบทำงานช้าลง เป็นต้น

5) การรบกวนการใช้ระบบคอมพิวเตอร์โดยปกติสุข ตามมาตรา 11

การรบกวนการใช้งานระบบคอมพิวเตอร์โดยปกติสุขในที่นี้ก็คือ การทำสแปมเมล์ (Spam Mail) ซึ่งเป็นรูปแบบการโจมตีระบบคอมพิวเตอร์ด้วยการใช้โปรแกรมสำหรับส่งสแปม (Spammer Programs) ส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่างๆ เป็นจำนวนมหาศาลผ่านทางอีเมล์หรือโปรแกรมสนทนา (Instant Messaging) รวมทั้งอีเมล์และ SMS ในโทรศัพท์มือถือโดยปกปิดแหล่งที่มา เช่น ไม่ปรากฏหมายเลข IP address หรือชื่อของผู้ส่งไม่ว่าจะเป็นชื่อเล่นหรือชื่อจริง เป็นต้น ซึ่งการโจมตีของพวกสแปมเมอร์นี้จึงไม่ใช่ปัญหาเล็กๆ ที่เป็นแค่ทำให้เกิดความรำคาญแก่ผู้ใช้คอมพิวเตอร์ทั่วไป แต่กำลังกลายเป็นปัญหาใหญ่ที่ส่งผลกระทบและสร้างความเสียหายในเชิงเศรษฐกิจ กล่าวคือ สแปมเมล์มักก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการใช้ทรัพยากรของระบบคอมพิวเตอร์ รวมทั้งระบบคอมพิวเตอร์และระบบการสื่อสาร จนอาจต้องเสียค่าใช้จ่ายในการซื้อซอฟต์แวร์สำหรับใช้กำจัดสแปมเมล์ หรืออาจถึงขั้นทำให้เครื่องเมล์เซิร์ฟเวอร์ (เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ในการให้บริการจดหมายอิเล็กทรอนิกส์) ของฝ่ายผู้รับอีเมล์ต้องทำงานหนักจนไม่สามารถทำงานต่อไปได้และหยุดให้บริการในที่สุดซึ่งมักจะมีค่าใช้จ่ายในการซ่อมแซมหรือการดูแลรักษาตามมา ทั้งนี้ โดยภาพรวมแล้วโปรแกรมสำหรับส่งสแปมเมล์ดังกล่าวถือเป็นชุดคำสั่งไม่พึงประสงค์อีกประเภทหนึ่งด้วย

เพราะการส่งอีเมล์จำนวนมากๆ ในคราวเดียวกันหรือต่อเนื่องกันเป็นจำนวนมหาศาลนั้นมนุษย์คงไม่สามารถกระทำได้ จึงต้องใช้โปรแกรมสำหรับส่งสแปมเป็นเครื่องมือพิเศษช่วยในการส่งดังกล่าว

อย่างไรก็ตาม มีข้อน่าสังเกตว่า ผลกระทบจากการรบกวนด้วยการทำสแปมเมล์ที่ถึงขั้นทำให้เครื่องเมล์เซิร์ฟเวอร์ของฝ่ายผู้รับอีเมล์ต้องทำงานหนักจนไม่สามารถทำงานต่อไปได้และหยุดให้บริการในที่สุดนั้น อาจคล้ายคลึงกับการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตามมาตรา 9 และ มาตรา 10 แต่แตกต่างกันที่วิธีการ เจตนา และการประสงค์ต่อผลหรือย่อมเล็งเห็นผลของการกระทำ กล่าวคือ ในการส่งสแปมเมล์นั้นผู้ส่งอีเมล์อาจเพียงแต่ต้องการก่อให้เกิดความรำคาญแก่ผู้รับอีเมล์หรือต้องการโฆษณาเชิญชวนเพื่อให้ทำการอย่างใดอย่างหนึ่งหรือหลอกให้ตกเป็นเหยื่อเท่านั้น แต่หากผลที่เกิดจากการกระทำนั้นถึงขั้นที่ทำให้เครื่องเมล์เซิร์ฟเวอร์ของฝ่ายผู้รับอีเมล์ไม่สามารถทำงานต่อไปได้และหยุดให้บริการนั้น ย่อมเป็นการทำให้ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของเครื่องเมล์เซิร์ฟเวอร์ฝ่ายผู้รับอีเมล์ได้รับความเสียหายและเข้าข่ายเป็นการรบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ด้วย

6) การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายต่อประชาชนหรือสาธารณะ ตามมาตรา 12

การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ก่อให้เกิดความเสียหายต่อประชาชนหรือกระทบต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ ตามมาตรา 12 นี้ ปัจจุบันเป็นปัญหาการกระทำความผิดทางคอมพิวเตอร์ที่ประเทศส่วนใหญ่วิตกกังวล กล่าวคือ การใช้โปรแกรมหรือชุดคำสั่งเจาะเข้าไปในระบบคอมพิวเตอร์และแอบเติมหรือทำลายข้อมูลคอมพิวเตอร์ หรือแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ อันอาจส่งผลกระทบต่อระบบสาธารณูปโภคหรือระบบการเงินของประเทศ หรือแม้กระทั่งเป็นที่มาของการทำสงครามข้อมูลข่าวสาร (Information Warfare) ที่กำลังเกิดขึ้นกับสังคมไทยอยู่ในปัจจุบันโดยผ่านทางโปรแกรมเครือข่ายสังคมออนไลน์อย่าง Facebook[143] เป็นต้น ทั้งนี้จากงานวิจัยชิ้นหนึ่งที่ได้รับการเผยแพร่โดยบริษัทโซโฟส (Sophos) ระบุว่าผู้ใช้เกือบร้อยละ 60 มีความเห็นว่าเว็บไซต์ Facebook เป็นเครือข่ายสังคมออนไลน์ที่มีภัยคุกคาม

---

143 Facebook คือ เครือข่ายสังคมออนไลน์ที่ได้รับความนิยมสูงสุดในปัจจุบันและจากผลสำรวจพบว่ามีจานวนผู้สมัครใช้งานเว็บไซต์ดังกล่าวถึง 350 ล้านรายชื่อ เมื่อศึกษาถึงจานวนของผู้สมัครใช้งานในประเทศไทย พบว่ามีจานวนผู้สมัครใช้งานกว่า 1,632,880 คน นอกจากนั้นประเทศไทยติดอันดับที่ 2 ของประเทศที่มีอัตราการเติบโตของผู้ใช้งานสูงที่สุด (10.96%) ซึ่งเป็นรองเพียงประเทศโปแลนด์ซึ่งมีอัตราการเติบโตของผู้ใช้งานที่ 12.46%

ด้านความปลอดภัยมากที่สุด (อันดับ 2 คือ MySpace ที่ ร้อยละ 18, อันดับ 3 คือ Twitter ที่ร้อยละ 17 และอันดับที่ 4 คือ LinkedIn ที่ร้อยละ 4) แม้ว่าทีมงานของ Facebook จะพยายามแก้ไขหรือป้องกัน แต่ก็เป็นเรื่องที่ยากลำบาก เนื่องจากจานวนผู้สมัครใช้งานเว็บไซต์ดังกล่าวกว่า 350 ล้านคน จึงมีความจำเป็นที่ผู้ใช้เครือข่ายสังคมออนไลน์ จะต้องรู้เท่าทันถึงภัยคุกคามต่างๆ ที่มากับ Facebook ตลอดจนวิธีป้องกันตัวจากภัยคุกคามดังกล่าว[144]

7) การจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ ตามมาตรา 13

แม้ถ้อยคำในตัวบทของมาตรา 13[145] จะมิได้ใช้คำว่า “ชุดคำสั่งไม่พึงประสงค์” ในการบัญญัติฐานความผิด แต่ใช้คำว่า “ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะ” ก็ย่อมแปลความหรืออนุมานได้ว่า ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะดังกล่าวหมายถึงชุดคำสั่งไม่พึงประสงค์นั่นเอง ซึ่งมาตรา 13 นี้เป็นการกำหนดฐานความผิดและบทลงโทษสำหรับการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์เพื่อนำไปใช้ในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 แต่ก็มีข้อที่น่าสังเกตเพิ่มเติมว่า การมีไว้เพื่อการจำหน่ายจะเป็นความผิดตามมาตรานี้หรือไม่ ซึ่งผู้เขียนเห็นว่าการมีไว้เพื่อการจำหน่ายไม่เข้าองค์ประกอบและไม่เป็นความผิดตามมาตรานี้ เพราะหากพิจารณาจากถ้อยคำในตัวบทที่ใช้คำว่า “การจำหน่ายหรือเผยแพร่” แล้ว กฎหมายน่าจะมุ่งคุ้มครองเฉพาะในขั้นตอนของการจำหน่ายหรือการเผยแพร่เท่านั้น และคงจะเป็นเรื่องที่พิสูจน์ได้ยากในทางปฏิบัติว่า อย่างไรจึงจะถือว่าเป็นการมีไว้เพื่อการจำหน่าย เว้นแต่จะมีการตรวจพบว่าชุดคำสั่งเหล่านั้นถูกจัดเก็บไว้ในสื่อบันทึกข้อมูลที่มีลักษณะทางกายภาพที่ชัดเจน เช่น อาจถูกเก็บไว้ในแผ่นซีดีหรือแผ่นดิจิทัลอเนกประสงค์และแผ่นบันทึกนั้นมีปริมาณมากเกินกว่าการใช้งานตามปกติ เป็นต้น สำหรับตัวอย่างของชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะก็ เช่น ชุดคำสั่งไม่พึงประสงค์ที่ใช้สำหรับการเจาะระบบ (hacker tools) เป็นต้น นอกจากนี้ยังรวมถึงรหัสผ่าน

---

144 นิพนธ์ นาชิน,ประธาน พงศ์ทิพย์ฤกษ์, อนันต์ โซนี่ Edited by ปริญญา หอมอเนก. “เรียนรู้และทำความเข้าใจภัยจากการใช้งานโปรแกรมประเภท Social Networking Understand How Hacker attack Social Networking by using Social Engineering” เอกสารประกอบการสัมมนา Social Networking Secutiry Conference 2010 : SNS CON 2010 จัดโดย เขตอุตสาหกรรมซอฟร์แวร์ ศูนย์บริหารจัดการเทคโนโลยี ภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยความร่วมมือกับสมาคมความมั่นคงปลอดภัยสารสนเทศ (Thailand Information Security Association–TISA) และ บริษัท เอซิสโปรเฟสชั่นนัล เซ็นเตอร์ (ACIS Professional Center) จำกัด วันที่ 21 กรกฎาคม 2553 ณ ห้องแกรนด์บอลลูม ชั้น 3 โรงแรม อโนมา กรุงเทพฯ

145 มาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

คอมพิวเตอร์ (computer password) รหัสในการเข้าถึง (access code) หรือข้อมูลอื่นที่มีลักษณะคล้ายคลึงกันที่ได้จากการ Crack / Key Gen / Serial No.[146] ทั้งนี้ ไม่รวมถึงชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายที่สร้างขึ้นเพื่อใช้ในการปกป้องระบบหรือทดสอบระบบ และจะนำชุดคำสั่งเหล่านั้นมาใช้ทดสอบหรือปกป้องระบบได้ก็แต่เพียงเท่าที่อยู่ภายใต้เงื่อนไขว่าต้องมีอำนาจหรือได้รับอนุญาตให้กระทำได้เท่านั้น

อนึ่ง สำหรับความหมายของการเผยแพร่นั้น หมายความรวมถึงการส่งข้อมูลที่ได้รับให้ผู้อื่นอีกทอดหนึ่ง (forward) หรือการเชื่อมโยงฐานข้อมูลเข้าด้วยกัน (hyperlinks) เพื่อให้สามารถเข้าถึงชุดคำสั่งไม่พึงประสงค์ดังกล่าวได้โดยสะดวกด้วย

1.1.2 ฐานความผิดเนื่องจากการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์โดยมิชอบ

ส่วนของกฎหมายสารบัญญัติในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ นอกจากจะกำหนดฐานความผิดและบทกำหนดโทษเกี่ยวกับการใช้ชุดคำสั่งไม่พึงประสงค์ตามที่ได้กล่าวไปแล้วในข้อ 1.1.1 ข้างต้นแล้ว ยังมีการกำหนดฐานความผิดเพื่อห้ามมิให้มีการจำหน่ายและเผยแพร่ชุดคำสั่งไม่พึงประสงค์ที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 ถึงมาตรา 11 อีกด้วย โดยกำหนดไว้ในมาตรา 13 ทั้งนี้ก็เพื่อเป็นการป้องปรามมิให้มีการนำชุดคำสั่งไม่พึงประสงค์ไปใช้ในการกระทำความผิดอีกทางหนึ่ง

อย่างไรก็ตาม ยังมีมาตรการในการป้องปรามชุดคำสั่งไม่พึงประสงค์โดยพนักงานเจ้าหน้าที่อีกหนึ่งมาตรการซึ่งกำหนดไว้ในมาตรา 21 โดยมีใจความว่า

“มาตรา 21 ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับ

---

146 Crack คือโปรแกรมที่จะเข้าไปแก้ไขในส่วนของการตั้งเวลาหมดอายุการใช้งานซอฟท์แวร์หรือทำให้ฟังก์ชั่น (function) ต่าง ๆ ของซอฟท์แวร์ที่ไม่อนุญาตให้ใช้งานสามารถใช้งานได้ วิธีการ crack ส่วนใหญ่จะคล้ายกัน กล่าวคือ ให้ทำการสำเนาไฟล์ crack ใส่ไว้ใน folder เดียวกันกับที่เก็บซอฟท์แวร์นั้นและเรียกใช้งานไฟล์ crack แทนไฟล์เดิมของซอฟท์แวร์ ส่วน Key Gen คือโปรแกรมสำหรับการลงทะเบียนรหัสใช้งาน (Register Code) หรือหมายเลขลำดับ (Serial No.) ของซอฟท์แวร์ต่าง ๆ ที่ยังไม่ได้ลงทะเบียนเพื่อใช้งาน (Un register Version) จากเจ้าของซอฟท์แวร์ โดย Key Gen จะให้ผู้ใช้งาน (user name) ป้อนชื่อผู้ใช้งานที่จะลงทะเบียน จากนั้นก็จะแจ้งรหัส (Code) มาให้สำหรับนำไปเติมในช่อง Register Code เพื่อให้ซอฟท์แวร์กลายเป็นเวอร์ชั่นที่ลงทะเบียนแล้ว (Register Version)

การใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา"

ทั้งนี้ มีข้อน่าสังเกตว่า กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยที่เป็นทั้งกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติในตัวเองนั้น ได้ให้ความสำคัญกับการป้องกันและปราบปรามชุดคำสั่งไม่พึงประสงค์เป็นอย่างมาก จนถึงขั้นมีการบัญญัติเกี่ยวกับมาตรการป้องปรามชุดคำสั่งไม่พึงประสงค์ไว้ทั้งในส่วนของกฎหมายสารบัญญัติตามมาตรา 13 และในส่วนของกฎหมายวิธีสบัญญัติตามมาตรา 21 ซึ่งจะได้กล่าวถึงต่อไป

1.1.3 ฐานความผิดที่มิได้เกิดจากชุดคำสั่งไม่พึงประสงค์ ได้แก่

1) การนำเข้าหรือเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะที่ไม่เหมาะสม ตามมาตรา 14 และมาตรา 15

การนำเข้าข้อมูลคอมพิวเตอร์ตามมาตรา 14 และมาตรา 15 นี้ เป็นลักษณะอันเกิดจากการนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นเท็จหรือมีเนื้อหาไม่เหมาะสมในรูปแบบต่างๆ โดยในมาตรา 14 นั้น กำหนดไว้ให้ครอบคลุมทั้งการปลอมแปลงข้อมูลคอมพิวเตอร์หรือทำข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือก่อให้เกิดความเสียหายหรือก่อให้เกิดความตื่นตระหนกกับประชาชน หรือเนื้อความที่กระทบต่อความมั่นคงของประเทศหรือการก่อการร้าย รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลาย และรวมถึงการส่งข้อมูลที่ได้รับให้ผู้อื่นอีกทอดหนึ่งด้วย

อย่างไรก็ตาม นอกจากการกำหนดโทษสำหรับผู้กระทำความผิดตามมาตรา 14 แล้ว ยังมีการกำหนดโทษของผู้ให้บริการที่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ไว้ในในมาตรา 15 ด้วย โดยผู้ให้บริการที่สนับสนุนหรือให้ความยินยอมดังกล่าวต้องรับโทษเช่นเดียวกับผู้กระทำความผิดด้วย

2) การนำเข้าภาพของผู้อื่นที่เกิดจากการตกแต่ง ตามมาตรา 16

การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดซึ่งอาจเรียกโดยง่ายว่า "การตกแต่งภาพ" อันอาจทำให้ผู้อื่นเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ตามมาตรา 16 นี้ มีความใกล้เคียงอย่างยิ่งกับความผิดฐาน

หมิ่นประมาทซึ่งกำหนดไว้ในประมวลกฎหมายอาญา หากแต่การแพร่กระจายและความเสียหายในลักษณะดังกล่าวมักเป็นไปอย่างรวดเร็วและขยายวงกว้างมากกว่า อย่างไรก็ตาม หากเป็นการนำเข้าโดยสุจริตก็ไม่มีความผิด ซึ่งก็เทียบเคียงได้กับบัญญัติในประมวลกฎหมายอาญา มาตรา 326 ที่บัญญัติว่า "ผู้ใดแสดงความคิดเห็นหรือข้อความโดยสุจริต...ผู้นั้นไม่มีความผิดฐานหมิ่นประมาท"[147]

1.2 ส่วนของกฎหมายวิธีสบัญญัติเพื่อกำหนดอำนาจดำเนินการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ให้กับพนักงานเจ้าหน้าที่

ในชั้นการดำเนินกระบวนพิจารณาและการดำเนินการของพนักงานเจ้าหน้าที่ซึ่งถือเป็นต้นทางของกระบวนการยุติธรรมทางอาญาในคดีความผิดเกี่ยวกับคอมพิวเตอร์นั้น นอกจากกฎหมายจะกำหนดอำนาจดำเนินการเป็นการทั่วไปให้กับพนักงานเจ้าหน้าที่ ได้แก่ อำนาจในการระงับการเผยแพร่หรือปิดกั้น (block) เว็บไซต์ที่มีเนื้อหากระทบต่อความมั่นคงหรือขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนตามมาตรา 20 หรืออำนาจทั่วไปของพนักงานเจ้าหน้าที่ตามมาตรา 18 อนุมาตรา (1) ที่ให้พนักงานเจ้าหน้าที่สามารถส่งหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดนั้นมาให้ถ้อยคำหรือชี้แจงได้ อนุมาตรา (2) ให้เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการได้ อนุมาตรา (3) สั่งให้ส่งมอบข้อมูลของผู้ใช้บริการที่ผู้ให้บริการต้องจัดเก็บได้ ซึ่งทั้งสามอนุมาตราดังกล่าวพนักงานเจ้าหน้าที่สามารถกระทำได้เอง (4) การทำสำเนาข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ (5) การสั่งให้ผู้ซึ่งครอบครองข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ (6) การตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ (7) การถอดรหัสลับข้อมูลคอมพิวเตอร์ และ (8) การยึดหรืออายัดระบบคอมพิวเตอร์นั้น พนักงานเจ้าหน้าที่จะกระทำได้เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดของผู้กระทำความผิดโดยต้องมีการขออนุญาตจากศาลเสียก่อนแล้ว

นอกจากนี้ กฎหมายยังได้ให้อำนาจดำเนินการพิเศษแก่พนักงานเจ้าหน้าที่เพื่อเป็นการป้องกันและปราบปรามชุดคำสั่งไม่พึงประสงค์ไว้อีกด้วย กล่าวคือ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้อง

---

147 พรเพชร วิชิตชลชัย "คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550", เอกสารอิเล็กทรอนิกส์ หน้า 27 Retrieved July, 21, 2010

ต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

สำหรับความเป็นมาของการกำหนดอำนาจดำเนินการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ให้กับพนักงานเจ้าหน้าที่ตามมาตรา 21 นั้น เดิมทีในชั้นการยกร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... โดยคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (NITC) มีมาตรารวมทั้งสิ้น 17 มาตรา[148] และมิได้มีบทบัญญัติในเรื่องที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ไว้แต่อย่างใด ต่อมาในชั้นการตรวจพิจารณาร่างกฎหมายดังกล่าวโดยคณะกรรมการกฤษฎีกา (คณะพิเศษ) ได้มีการเพิ่มเติมมาตราทั้งสิ้นเป็น 28 มาตรา โดยได้ปรากฏบทบัญญัติและหลักการเกี่ยวกับการกำหนดมาตรการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ขึ้นโดยเป็นการกำหนดหลักการเพื่อให้พนักงานเจ้าหน้าที่มีอำนาจเฉพาะในการสั่งห้ามการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้น หรือกำหนดเงื่อนไขการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ (ร่างมาตรา 19)[149] นอกจากนี้ คณะกรรมการกฤษฎีกา (คณะพิเศษ) ยังได้เปลี่ยนชื่อกฎหมายนี้ จาก “ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ....”

---

148 ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ที่ เสนอโดยคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ ปรากฏตามบันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เรื่องเสร็จที่ 257/2548 มีทั้งสิ้น 17 มาตรา

149 ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ที่ สำนักงานคณะกรรมการกฤษฎีกาตรวจพิจารณาแล้ว ปรากฏตามบันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เรื่องเสร็จที่ 257/2548 ความว่า

“มาตรา 19 ในกรณีที่พนักงานเจ้าหน้าที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่มีอำนาจสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครองครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีกำหนดโดยประกาศในราชกิจจานุเบกษา”

เป็น "ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...."[150] อีกด้วย และในชั้นการพิจารณาของสภาได้มีผู้ขอแปรญัตติร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 19 เพียงคนเดียวคือ นายไพศาล พืชมงคล ที่ขอแปรญัตติแก้ไขเพิ่มเติมความในวรรคหนึ่งและวรรคสอง ของร่าง มาตรา 19 ดังนี้

"มาตรา 19 ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์ที่ใช้กระทำความผิดรวมอยู่ด้วย พนักงานเจ้าหน้าที่มีอำนาจสั่งห้ามจำหน่ายหรือเผยแพร่หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ที่ใช้กระทำความผิดดังกล่าวก็ได้"

ทั้งนี้ นายไพศาล พืชมงคล ได้ขอแปรญัตติแก้ไขเพิ่มเติมความในวรรคสองของมาตรา 19 ดังนี้

"ชุดคำสั่งไม่พึงประสงค์ที่ใช้ในการกระทำความผิดตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ตามปกติหรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีกำหนดโดยประกาศในราชกิจจานุเบกษา"

ผลจากการแปรญัตติดังกล่าว มิได้ส่งผลให้เนื้อหาสาระของชุดคำสั่งไม่พึงประสงค์ตามร่างมาตรา 19 ที่ผ่านการตรวจพิจารณาของคณะกรรมการกฤษฎีกา (คณะพิเศษ) มีผลเปลี่ยนแปลงไปจากเดิมแต่อย่างใด และท้ายที่สุดสภาก็เห็นชอบโดยคงเนื้อหาในร่างมาตรา 19 ไว้ตามเดิม จึงมีผลทำให้บทบัญญัติในร่างมาตรา 19 ซึ่งผ่านการตรวจพิจารณาของคณะกรรมการกฤษฎีกา (คณะพิเศษ) กลายมาเป็น มาตรา 21 ในปัจจุบันตามที่ได้กล่าวไปแล้ว ดังนั้น จึงอาจกล่าว

---

150 เหตุผลในการเปลี่ยนชื่อกฎหมายนี้ปรากฏตามบันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เรื่องเสร็จที่ 257/2548 หน้าที่ 11 ข้อ 32 ว่า โดยที่สาระสำคัญของร่างพระราชบัญญัตินี้เป็นการกำหนดฐานความผิดสำหรับบุคคลที่กระทำความผิดต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยตรง มิได้มุ่งถึงกรณีที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดตามประมวลกฎหมายอาญา อีกทั้งชื่อของร่างพระราชบัญญัติที่เสนอมานั้นไม่สะท้อนถึงเจตนารมณ์ของร่างกฎหมายนี้เท่าที่ควร จึงได้แก้ไขชื่อของร่างพระราชบัญญัติจาก "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ...." เป็น "ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ...." เพื่อให้เกิดความชัดเจน และสอดคล้องกับเจตนารมณ์และสาระสำคัญของกฎหมาย

ได้ว่าชุดคำสั่งไม่พึงประสงค์ที่ประกาศใช้ตามกฎหมายนี้เป็นผลผลิตที่เกิดขึ้นจากแนวคิดในขณะการตรวจพิจารณาร่างโดยคณะกรรมการกฤษฎีกา (คณะพิเศษ) โดยแท้

สาเหตุที่ได้บัญญัติมาตรการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ไว้เช่นนั้นก็อาจเนื่องมาจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยการใช้ชุดคำสั่งไม่พึงประสงค์เพื่อกระทำความผิดตามพระราชบัญญัตินี้ในรูปแบบต่างๆ มีโอกาสเกิดขึ้นได้โดยง่ายและบ่อยครั้ง จึงได้ให้อำนาจกับพนักงานเจ้าหน้าที่ในการห้ามจำหน่ายหรือห้ามเผยแพร่ชุดคำสั่งเหล่านั้นเสียตั้งแต่ต้นทางเพื่อให้สามารถระงับการใช้ หรือให้ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์นั้น ทั้งนี้อาจกำหนดเงื่อนไขใดๆ ในการใช้ มีไว้ในความครอบครอง หรือเผยแพร่ชุดคำสั่งนั้นได้อีกด้วย โดยให้พนักงานเจ้าหน้าที่ร้องขอต่อศาลในการดำเนินการดังกล่าว

อนึ่ง เพื่อให้กฎหมายมีความยืดหยุ่นในการบังคับใช้และสามารถปรับใช้ให้ทันต่อยุคสมัยตามพัฒนาการทางเทคโนโลยี จึงมีการเปิดช่องทางให้มีการกำหนดรายละเอียดเพิ่มเติมของชุดคำสั่งที่มีลักษณะดังกล่าวไว้ในกฎกระทรวง เว้นเสียแต่เป็นชุดคำสั่งทำนองเดียวกันแต่มีไว้สำหรับเพื่อใช้ในการนำไปทำลายชุดคำสั่งดังกล่าว เช่น โปรแกรมหรือชุดคำสั่งแอนตี้ไวรัสทั้งหลาย เป็นต้น ก็ให้รัฐมนตรีเพียงแต่ประกาศกำหนดในราชกิจจานุเบกษาเพื่อให้ประชาชนได้รับทราบโดยทั่วกัน

อย่างไรก็ตามยังมีข้อน่าสังเกตอีกว่า เหตุใดจึงไม่บัญญัติมาตรานี้ไว้ในหมวดของความผิดเกี่ยวกับคอมพิวเตอร์แต่ใช้วิธีการบัญญัติเป็นมาตรการต่างหากโดยให้อำนาจแก่พนักงานเจ้าหน้าที่ในการจัดการกับชุดคำสั่งไม่พึงประสงค์ได้เองภายใต้คำสั่งของศาล ประเด็นนี้ผู้เขียนขอตั้งข้อสันนิษฐานว่า หากมีการบัญญัติมาตรานี้ไว้ในหมวดของความผิดเกี่ยวกับคอมพิวเตอร์ก็จะทำให้เกิดความยุ่งยากในทางปฏิบัติ กล่าวคือ ชุดคำสั่งไม่พึงประสงค์มีอยู่ด้วยกันสองกลุ่มใหญ่ๆ คือ กลุ่มแรก เป็นชุดคำสั่งในทางทำให้เกิดความเสียหายเพื่อมุ่งผลในการทำลายชุดคำสั่งอื่น และกลุ่มที่สองเป็นชุดคำสั่งในทางต่อต้านหรือแก้ไขชุดคำสั่งในกลุ่มแรก ดังนั้น ในทางปฏิบัติจึงยากที่จะแยกแยะและวินิจฉัยในเบื้องต้นได้ว่าชุดคำสั่งไม่พึงประสงค์ใดจะจัดอยู่ในกลุ่มใดเพราะต้องอาศัยผู้ที่มีความรู้และความเชี่ยวชาญด้านคอมพิวเตอร์เป็นอย่างมากในการวินิจฉัยและแยกแยะดังกล่าว ซึ่งจะเป็นปัญหาและอุปสรรคต่อการบังคับใช้กฎหมายของเจ้าพนักงานเจ้าหน้าที่ในกระบวนการยุติธรรมที่จะวินิจฉัยฐานความผิด และข้อสันนิษฐานอีกประการหนึ่งก็คือ ถ้าบัญญัติไว้ในหมวดความผิดเกี่ยวกับคอมพิวเตอร์ก็จะทำให้มีผลกระทบและเกิดความปั่นป่วนต่อวงการและอุตสาหกรรมอันเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ที่อยู่ในกลุ่มที่สอง เช่น อุตสาหกรรมโปรแกรมแอนตี้ไวรัส เป็นต้น เพราะในความเป็นจริงแล้วโปรแกรมแอนตี้ไวรัสก็ทำงานเหมือนเป็นไวรัสชนิดหนึ่งด้วยเหมือนกัน

2. ความหมายและสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์กับความรับผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา

เหตุที่ต้องกล่าวและศึกษาถึงสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ เนื่องจากข้อมูลคอมพิวเตอร์เป็นเป้าหมายสำคัญของอาชญากรรมทางคอมพิวเตอร์ที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดตามที่ได้กล่าวไปแล้วในความนำและจากบทวิเคราะห์เกี่ยวกับรูปแบบของการโจมตีจากจากชุดคำสั่งไม่พึงประสงค์ ไม่ว่าจะเป็นการกระทำความผิดโดยการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ได้แก่ การขโมยเอกลักษณ์บุคคล (Identity Theft) ด้วยมัลแวร์, การโจมตีเครื่องคอมพิวเตอร์แม่ข่ายผ่านช่องโหว่ (Software flaws), การปล่อยมัลแวร์ผ่านโปรแกรมประเภท Peer-to-Peer (P2P) และ Instant Messaging (IM), การโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) ด้วยมัลแวร์ รวมทั้งการกระทำความผิดโดยการดักรับข้อมูล ได้แก่ การดักรับข้อมูลในเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ และการดักข้อมูลผ่านปุ่มคีย์บอร์ดด้วยมัลแวร์ ก็ล้วนแล้วแต่เพื่อให้ได้ไปซึ่งข้อมูลที่สามารถใช้ระบุเอกลักษณ์บุคคลหรือข้อมูลสำคัญขององค์กร ตัวอย่างเช่น การนำสปายแวร์ หรือม้าโทรจันไปฝังไว้ในระบบคอมพิวเตอร์เพื่อเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ ภายในเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งอยู่ หรือการใช้โปรแกรมดักข้อมูลผ่านปุ่มคีย์บอร์ด (Keylogger หรือ Keystroke) เพื่อแอบบันทึกการกดรหัสผ่านของผู้อื่นหรือการบันทึกเว็บไซต์ที่เคยเข้าเยี่ยมชมมาและการเข้าถึงไฟล์ข้อมูลต่างๆ เป็นต้น โดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นที่อยู่ในระบบคอมพิวเตอร์ของเจ้าของข้อมูลที่ชุดคำสั่งไม่พึงประสงค์ตามตัวอย่างดังกล่าวฝังตัวอยู่นั้น มิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด จึงไม่อาจถือได้ว่าการกระทำดังกล่าวเป็นความผิดฐานเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามมาตรา 5 และมาตรา 7 และไม่เป็นการรบกวนทางคอมพิวเตอร์ตามมาตรา 9 และมาตรา 10 อีกด้วย

อาจกล่าวได้ว่า เมื่อมีการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดตามตัวอย่างข้างต้นแล้วจะไม่เป็นความผิดฐานใดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และไม่เป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญาด้วยเพราะขาดซึ่งองค์ประกอบของความผิดสำคัญที่ว่าข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ตามนิยามและความหมายใน

ประมวลกฎหมายแพ่งและพาณิชย์[151] และมิอาจปรับรูปแบบของการกระทำความผิดนี้เข้ากับฐานความผิดตามพระราชบัญญัติที่มีโทษทางอาญาใดได้เลย จึงทำให้นำไปสู่ประเด็นปัญหาหรือช่องว่างของกฎหมายที่กระทบต่อการปฏิบัติงานของผู้เกี่ยวข้องในการดำเนินคดีกับผู้กระทำผิดในทุกขั้นตอนของกระบวนการยุติธรรมทางอาญา ไม่ว่าจะเป็นการสืบสวน สอบสวน พิจารณา และพิพากษาคดี ซึ่งจำเป็นที่จะต้องแสวงหาแนวทางในการแก้ไขโดยเร็ว

เกี่ยวกับความหมายและสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์นี้ พันตำรวจเอก ดร.มาโนช ตันตระเธียร ได้ศึกษาและวินิจฉัยไว้แล้วในระดับหนึ่งซึ่งพอสรุปได้ว่า[152] ข้อมูลคอมพิวเตอร์ซึ่งอยู่ในของประจุคลื่นแม่เหล็กไฟฟ้า (Electromagnetic Impulse) ที่ไม่มีคุณสมบัติทางกายภาพและไม่สามารถจับต้องได้ไม่เข้าลักษณะเป็น “ทรัพย์” ตามกฎหมายแพ่งและพาณิชย์ มาตรา 137 ที่บัญญัติให้ทรัพย์หมายถึงเฉพาะ “วัตถุมีรูปร่าง” เท่านั้น แต่ข้อมูลคอมพิวเตอร์อาจเข้าลักษณะเป็น “ทรัพย์สิน” ตามประมวลกฎหมายแพ่งและพาณิชย์

นอกจากนี้ พรทิพย์ ตัณฑวนันท์ ยังได้ให้ความเห็นเกี่ยวกับประเด็นข้อมูลคอมพิวเตอร์มิใช่ทรัพย์และมิใช่เอกสารไว้ว่า[153] “ระบบคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์มิได้รับการคุ้มครองทางอาญา เนื่องจากหลักการดั้งเดิมของกฎหมายอาญามุ่งคุ้มครองแก่วัตถุที่มีรูปร่าง

---

151 คำพิพากษาศาลฎีกาที่ 5161/2547 ตัดสินว่าข้อมูล ตามพจนานุกรมให้ความหมายว่า ข้อเท็จจริง หรือ สิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักอนุมานหาความจริงหรือการคำนวณ ส่วนข้อเท็จจริง หมายความว่า ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่จริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุมีรูปร่าง สำหรับตัวอักษร ภาพ แผนผัง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อ ป.พ.พ. มาตรา 137 บัญญัติว่า ทรัพย์ หมายความว่า วัตถุมีรูปร่าง ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์

152 พ.ต.อ. ดร. มโนช ตันตระเธียร บทความทางวิชาการ เรื่อง “อาชญากรรมคอมพิวเตอร์ : กระบวนการยุติธรรมไทยพร้อมหรือยัง ?” ซึ่งได้ถูกนำออกเผยแพร่ครั้งแรกเป็นเอกสารประกอบการสัมมนาทางวิชาการเรื่อง “กฎหมายพาณิชย์อิเล็กทรอนิกส์ (E-Commerce Laws): นวัตกรรมทางกฎหมายที่จำเป็นและเร่งด่วนแห่งสังคมไทย” จัดโดยกองทุนศาสตราจารย์สัญญา ธรรมศักดิ์, คณะนิติศาสตร์ มหาวิทยาธรรมศาสตร์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สภาทนายความ, ชมรมนักข่าวสายเทคโนโลยีสารสนเทศ เมื่อวันที่ 6-7 พฤษภาคม 2542 ณ หอประชุมมหิศร อาคารไทยพาณิชย์ ปาร์ค พลาซ่า กรุงเทพมหานคร. และถูกนำออกตีพิมพ์ในวารสารทางวิชาการอีกหลายเล่ม

153 พรทิพย์ ตัณฑวนันท์, “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ (Crime Related to Data Message),” (วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 82

ระบบคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์เป็นสิ่งที่ไม่มีรูปร่าง ยังไม่มีสถานะที่แน่นอนในทางกฎหมายอาญา" ซึ่งในชั้นการพิจารณาของศาลก็ได้มีคำพิพากษาฎีกาได้วินิจฉัยไว้อย่างชัดเจนว่า "ข้อมูลมิใช่ทรัพย์ ข้อมูลไม่นับเป็นวัตถุที่มีรูปร่าง ตัวอักษร ภาพ แผนผังและตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึกข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล การนำแผ่นบันทึกข้อมูลคัดลอกข้อมูลออกมาจึงมิใช่การลักทรัพย์ และข้อมูลอิเล็กทรอนิกส์ก็มิใช่เอกสารแม้ว่าข้อมูลอิเล็กทรอนิกส์จะต้องมีวัตถุที่รองรับหรือบันทึกก็ตาม แต่การทำให้ข้อความที่ถูกบันทึกปรากฏขึ้นได้นั้นต้องอาศัยอุปกรณ์คอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ โดยมีบุคคลเป็นตัวเชื่อมโยงการทำงาน นอกจากนั้น ข้อความที่ปรากฏขึ้นนั้นก็ปรากฏขึ้นบนอุปกรณ์คอมพิวเตอร์มิได้ปรากฏอยู่บนวัตถุที่รองรับแตกต่างจากเอกสาร ทั้งยังเป็นการปรากฏขึ้นเป็นเพียงชั่วคราว เมื่อปิดเครื่องคอมพิวเตอร์ข้อความนั้นก็หายไปด้วย นิยามคำว่าเอกสารตามประมวลกฎหมายอาญาจึงไม่ครอบคลุมถึงข้อมูลคอมพิวเตอร์"

3. มาตรการทางกฎหมายเกี่ยวกับการขโมยเอกลักษณ์บุคคล (Identity Theft) ในรูปแบบของการปลอมแปลงบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา

สำหรับมาตรการทางกฎหมายของประเทศไทยในความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในประเด็นการขโมยเอกลักษณ์บุคคล (Identity theft) นั้น ประมวลอาญาได้บัญญัติความผิดไว้ โดยแบ่งออกเป็น 2 กลุ่ม กล่าวคือ

กลุ่มแรก ความผิดเกี่ยวกับการปลอมและแปลงบัตรอิเล็กทรอนิกส์ ตามมาตรา 269/1 ถึงมาตรา 269/4

กลุ่มที่สอง ความผิดฐานใช้หรือมีไว้เพื่อใช้ซึ่งบัตรอิเล็กทรอนิกส์ที่แท้จริงของผู้อื่นโดยมิชอบ ตามมาตรา 269/5 และมาตรา 269/6

โดยมีรายละเอียดเกี่ยวกับองค์ประกอบของฐานความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์ในประเด็นการขโมยเอกลักษณ์บุคคล ตามที่ประมวลกฎหมายอาญาบัญญัติไว้ ดังต่อไปนี้

3.1 มาตรา 269/1 การปลอมและแปลงบัตรอิเล็กทรอนิกส์

"มาตรา 269/1 ผู้ใดทำบัตรอิเล็กทรอนิกส์ปลอมขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด เติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนถ้าได้กระทำเพื่อให้ผู้หนึ่งผู้ใดหลงเชื่อว่า

เป็นบัตรอิเล็กทรอนิกส์ที่แท้จริงหรือเพื่อใช้ประโยชน์อย่างหนึ่งอย่างใด ผู้นั้นกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงห้าปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนบาท”

ข้อพิจารณาสำหรับมาตรานี้ คือ สิ่งที่กฎหมายประสงค์จะคุ้มครองสำหรับความผิดฐานนี้ คือ ความมั่งคงและความน่าเชื่อถือของบัตรอิเล็กทรอนิกส์ในฐานะที่เป็นพยานหลักฐานสำคัญ หรือเป็นเงื่อนไขแห่งการเข้าถึงสินค้า บริการ หรือทรัพย์สินของผู้อื่น ทั้งนี้ ความผิดในส่วนการกระทำตามมาตรานี้แยกเป็น 2 กรณี คือ

กรณีแรก เป็นการกระทำความผิดโดยการปลอมบัตรอิเล็กทรอนิกส์ขึ้นทั้งฉบับหรือแต่ส่วนหนึ่งส่วนใด ส่วนกรณีที่สอง เป็นการกระทำความผิดโดยการแปลงบัตรอิเล็กทรอนิกส์ด้วยการเติมหรือตัดทอนข้อความ หรือแก้ไขด้วยประการใดๆ ในบัตรอิเล็กทรอนิกส์ที่แท้จริง ซึ่งทั้งสองกรณีถือได้ว่าเป็นการกระทำความผิดฐานปลอมบัตรอิเล็กทรอนิกส์ทั้งสิ้น

สำหรับความหมายของการปลอมบัตรอิเล็กทรอนิกส์คือ การทำเลียนแบบบัตรที่แท้จริง การปลอมบัตรเทียบได้กับการกระทำความผิดฐานปลอมเอกสารสิทธิตามประมวลกฎหมายอาญา มาตรา 265 โดยมีคำพิพากษาศาลฎีกาที่ 5598/2540 วินิจฉัยว่า จำเลยปลอมบัตรเครดิตธนาคารแล้วใช้บัตรเครดิตดังกล่าวรูดกับเครื่องรูดบัตรเครดิตซึ่งธนาคารให้ไว้แก่จำเลยและปลอมสลิปของบุคคลหลายคนเพื่อแสดงว่าผู้เป็นเจ้าของบัตรได้ซื้อหรือใช้บริการด้วยบัตรเครดิต เป็นการปลอมเอกสารสิทธิและใช้เอกสารสิทธิปลอม

ส่วนวิธีการการปลอมบัตรอิเล็กทรอนิกส์นั้น สามารถทำได้หลายวิธี เช่น การนำข้อมูลที่แท้จริงของบัตรอิเล็กทรอนิกส์มาพิมพ์ข้อมูลลงบนแถบแม่เหล็กบันทึกข้อมูลของบัตรโดยเครื่องมือที่เรียกว่า “Embossing Machine” ข้อมูลที่ถูกบันทึกได้แก่ หมายเลขบัญชี หมายเลขบัตร ชุดตัวเลขธนาคารซึ่งออกบัตรอิเล็กทรอนิกส์ได้เข้ารหัสไว้ หลังจากนั้นผู้กระทำผิดจะลงลายมือชื่อในบัตร แล้วนำไปซื้อสินค้าและบริการ โดยร้านค้าจะไม่ทราบว่าเป็นบัตรปลอมเนื่องจากลายมือชื่อตรงกับในบัตร

3.2 มาตรา 269/4 การใช้หรือมีไว้ซึ่งบัตรอิเล็กทรอนิกส์อันได้มาโดยการปลอมหรือแปลง

“มาตรา 269/4 ผู้ใดใช้หรือมีไว้ใช้ซึ่งสิ่งใดๆ ตามมาตรา 269/1 อันได้มาโดยรู้ว่าเป็นของที่ทำปลอมหรือแปลงขึ้น ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี หรือปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือมีไว้เพื่อจำหน่ายซึ่งสิ่งใดๆ ที่ทำปลอมหรือแปลงขึ้นตามมาตรา 269/1 ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี หรือปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ

ถ้าผู้กระทำความผิดตามวรรคแรกหรือวรรคสองเป็นผู้ปลอมซึ่งบัตรอิเล็กทรอนิกส์ตามมาตรา 269/1 ให้ลงโทษตามมาตรานี้แต่กระทงเดียว"

ข้อพิจารณาสำหรับมาตรานี้คือ สิ่งที่กฎหมายประสงค์จะคุ้มครองในความผิดฐานนี้เป็นเช่นเดียวกับมาตรา 261/1 กล่าวคือ เพื่อความมั่นคงและความน่าเชื่อถือของบัตรอิเล็กทรอนิกส์ในฐานะที่เป็นพยานหลักฐานอันสำคัญ หรือเป็นเงื่อนไขสำคัญในการเข้าถึงสินค้า บริการ หรือทรัพย์สินของผู้อื่น แต่มาตรานี้จะมุ่งลงโทษผู้ใช้หรือมีไว้เพื่อใช้ และผู้จำหน่ายหรือมีไว้เพื่อจำหน่ายบัตรอิเล็กทรอนิกส์ที่ปลอมหรือแปลงขึ้นตามมาตรา 269/1 โดยรู้ว่าเป็นบัตรอิเล็กทรอนิกส์ที่ได้มาจากการปลอมหรือแปลงขึ้น

3.3 มาตรา 269/5 การใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ

"มาตรา 269/5 ผู้ใดใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบ ในประการที่น่าจะก่อให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ"

ข้อพิจารณาสำหรับมาตรานี้คือ สิ่งที่กฎหมายประสงค์ก็เพื่อลงโทษผู้ยึดถือ หรือครอบครองหรือผู้เก็บได้ซึ่งบัตรอิเล็กทรอนิกส์อันแท้จริงของผู้อื่นแล้วนำออกใช้โดยมิชอบ

3.4 มาตรา 269/7 การกำหนดบทหนัก

"มาตรา 269/7 "ถ้าการกระทำดังกล่าวในหมวดนี้ เป็นการกระทำเกี่ยวกับบัตรอิเล็กทรอนิกส์ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ เพื่อประโยชน์ในการชำระค่าสินค้า ค่าบริการหรือหนี้อื่นแทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด ผู้กระทำต้องระวางโทษหนักกว่าที่บัญญัติไว้ในมาตรานั้นๆ กึ่งหนึ่ง"

ข้อพิจารณาสำหรับมาตรานี้คือ บทบัญญัติดังกล่าวมีวัตถุประสงค์ที่จะคุ้มครองความมั่นคงและความน่าเชื่อถือของการชำระราคาด้วยบัตร ซึ่งวิธีการชำระราคาโดยบัตร หมายถึงผู้รับชำระราคาได้รับสิทธิเรียกร้องที่จะได้รับการชำระหนี้โดยลูกหนี้ที่อยู่ในฐานะจะชำระหนี้ได้

เป็นผู้ให้ประกันสิทธิเรียกร้องดังกล่าว ลักษณะของการให้ประกันดังกล่าวจึงทำให้การชำระราคาโดยบัตรมีลักษณะในทำนองเดียวกันกับวิธีการชำระราคาด้วยเงินสด

3.5 ปัญหาและช่องว่างของมาตรการทางกฎหมายเกี่ยวกับการขโมยเอกลักษณ์บุคคล (Identity Theft) ในรูปแบบของการปลอมแปลงบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญา

ประมวลกฎหมายอาญา มาตรา 1 (14) กำหนดนิยามคำว่า "บัตรอิเล็กทรอนิกส์" ไว้ ดังนี้

"บัตรอิเล็กทรอนิกส์" หมายความว่า

(ก) เอกสารหรือวัตถุอื่นใดไม่ว่าจะมีรูปลักษณะใดที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ ซึ่งจะระบุชื่อหรือไม่ก็ตาม โดยบันทึกข้อมูลหรือรหัสไว้ด้วยการประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน ซึ่งรวมถึงการประยุกต์ใช้วิธีการทางแสงหรือวิธีการทางแม่เหล็กให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข รหัส หมายเลขบัตร หรือสัญลักษณ์อื่นใดทั้งที่สามารถมองเห็นและมองไม่เห็นด้วยตาเปล่า

(ข) ข้อมูล รหัส หมายเลขบัญชี หมายเลขชุดทางอิเล็กทรอนิกส์หรือเครื่องมือทางตัวเลขใดๆ ที่ผู้ออกได้ออกให้แก่ผู้มีสิทธิใช้ โดยมิได้มีการออกเอกสารหรือวัตถุอื่นใดให้ แต่มีวิธีการใช้ในทำนองเดียวกับ (ก) หรือ

(ค) สิ่งอื่นใดที่ใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของ

เมื่อพิจารณาความหมายจากนิยามข้าง จะเห็นได้ว่าเป็นการขยายกรอบของกฎหมายให้กว้างมากขึ้นโดยระบุไว้ใน (ข) และ (ค) โดยให้มีเนื้อหารองรับกับพัฒนาการทางเทคโนโลยีที่จะเกิดขึ้นในอนาคต เพื่อให้ครอบคลุมถึงสิ่งอื่นใดที่มิใช่บัตรและสิ่งที่สามารถระบุตัวบุคคลได้ ซึ่งเมื่อพิจารณาประกอบกับฐานความผิดแล้วพบว่า สิ่งที่ถือว่าเป็นบัตรอิเล็กทรอนิกส์ตาม (ข) และ (ค) นั้น ไม่สามารถปรับเข้ากับฐานความผิดต่างๆ ตามที่บัญญัติไว้ในมาตรา 269/1 ถึงมาตรา 269/7 ได้ ทั้งนี้เนื่องจากองค์ประกอบของความผิดจะสามารถปรับใช้ได้แต่เฉพาะกรณีที่ต้องมีการออกบัตรที่อยู่ในรูปของวัตถุที่มีรูปร่างทั้งสิ้น กรณีดังกล่าวจึงอาจก่อให้เกิดช่องว่างในการบังคับใช้กฎหมายได้ เช่น การแอบจดจำรหัสที่สามารถตั้งหรือกำหนดขึ้นเองหรือนำข้อมูลของบุคคลอื่นหลายๆ ข้อมูลมาประกอบกัน (การได้มาซึ่งข้อมูลของบุคคลอื่นอาจใช้ชุดคำสั่งไม่พึงประสงค์หรือมัลแวร์เป็นเครื่องมือในการขโมย หรืออาจได้มาโดยวิธีการอื่นก็ได้) เพื่อนำรหัสหรือข้อมูลดังกล่าวไปใช้เพื่อแสวงหาประโยชน์โดยมิชอบ เป็นต้น ซึ่งการกระทำดังกล่าวมิได้มีการทำปลอมหรือแปลงรหัสหรือข้อมูลตามความหมายและนิยามที่กำหนดไว้แต่อย่างใด จึงทำให้มิอาจนำบทบัญญัติตั้งแต่มาตรา 269/1 ถึง มาตรา 269/7 มาปรับใช้กับกรณีตัวอย่างดังกล่าวได้

ทั้งนี้ เกี่ยวกับปัญหาจากการขโมยเอกลักษณ์บุคคลดังตัวอย่างข้างต้นนั้น นายสราวุธ เบญจกุล นักกฎหมายและผู้พิพากษาของประเทศไทยก็ได้กล่าวไว้ว่า[154] “Identity theft ถือเป็นการกระทำความผิดทางอาญาประเภทหนึ่ง ที่เกิดจากการที่ผู้กระทำผิด กระทำการโดยมิชอบเพื่อให้ได้มาหรือใช้ข้อมูลส่วนตัวของบุคคลอื่นโดยฉ้อฉล เพื่อที่จะให้ได้มาซึ่งผลประโยชน์ทางการเงิน สิ่งของหรือบริการต่างๆ โดยปราศจากการได้รับอนุญาต” และในฝั่งต่างประเทศก็เห็นว่าการขโมยเอกลักษณ์บุคคลเป็นความผิดฐานหนึ่งซึ่งเป็นการนำสิ่งซึ่งเป็นเอกลักษณ์หรือสามารถระบุตัวบุคคลไปใช้เพื่อแสวงหาประโยชน์แก่ตนเองหรือผู้อื่น และกำหนดให้เป็นฐานความผิดไว้ต่างหากในรูปแบบของกฎหมายเฉพาะ ตามที่ได้ยกตัวอย่างและกล่าวถึงไปแล้วในบทที่ 2 ข้อ 6.1.1 (การขโมยเอกลักษณ์บุคคล (Identity theft) ด้วยมัลแวร์)

4. มาตรการทางกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในรูปแบบข้อมูลคอมพิวเตอร์

เมื่อศึกษาและวิเคราะห์ถึงรูปแบบการละเมิดข้อมูลส่วนบุคคลส่วนใหญ่ในปัจจุบัน พบว่า มิได้มีสาเหตุหรือเกิดจากผู้ที่มีส่วนเกี่ยวข้องในการเก็บ รวบรวม ประมวลผลหรือควบคุมข้อมูลส่วนบุคคลที่ได้มาจากเจ้าของข้อมูลเป็นผู้ทำการละเมิด แต่เกิดจากการละเมิดข้อมูลส่วนบุคคลโดยการใช้เทคโนโลยีสารสนเทศและการสื่อสารหรือคอมพิวเตอร์เป็นเครื่องมือในการกระทำการละเมิดโดยที่บุคคลเจ้าของข้อมูลมิได้ยินยอมหรือมอบข้อมูลส่วนบุคคลของตนให้และเป็นลักษณะของอาชญากรรมทางคอมพิวเตอร์ โดยที่เจ้าของข้อมูลมักจะไม่รู้ตัว ซึ่งมูลเหตุจูงใจหลักของการละเมิดข้อมูลดังกล่าวก็เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลอันเกี่ยวกับการเงินของเจ้าของข้อมูลเพื่อประโยชน์สำหรับก่ออาชญากรรมด้านการเงิน หรือเพื่อก่อความเดือดร้อนรำคาญหรือความเสียหายต่อเจ้าของข้อมูลต่อไป และต้องยอมรับกันว่าข้อมูลส่วนบุคคลส่วนใหญ่ในปัจจุบันจะถูกจัดเก็บอยู่ในรูปแบบข้อมูลคอมพิวเตอร์ จึงทำให้โอกาสที่จะถูกละเมิดมีมากขึ้นและกำลังกลายเป็นปัญหาใหญ่ของสังคมอยู่ในขณะนี้ สาเหตุเป็นเพราะกระแสความนิยมในสังคมออนไลน์แบบ Social networking ที่มีมากขึ้นไม่ว่าจะเป็น Facebook Twitter หรือ Hi5 ซึ่งโปรแกรมเหล่านี้สามารถเข้าถึงทางเครื่องคอมพิวเตอร์และอุปกรณ์พกพาชนิดต่างๆ ได้โดยง่ายและสะดวก

---

154 สราวุธ เบญจกุล, “E-crime” อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่, บทความออนไลน์พิเศษในเว็บไซต์ผู้จัดการออนไลน์ http://www.manager.co.th/Daily/ViewNews.aspx?NewsID=9500000078831 เผยแพร่เมื่อ 6 กรกฎาคม 2550 Retrieved August, 13, 2011

รวดเร็วในทุกๆ ที่ และทุกๆ เวลา จึงทำให้มีจำนวนผู้ใช้งานมากขึ้นทุกๆ ขณะ ซึ่งส่งผลให้เกิดปัญหาอื่นๆ ตามมามิใช่เฉพาะปัญหาการละเมิดข้อมูลส่วนบุคคลเท่านั้นแต่อาจมีภัยคุมคามอื่นแอบแฝงมาในรูปแบบต่างๆทั้งนี้ภัยคุกคามดังกล่าวมักจะใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิด จึงหลีกเลี่ยงไม่ได้ที่จะต้องมีการศึกษาและกล่าวถึงการคุ้มครองข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บในรูปแบบของข้อมูลส่วนบุคคล เนื่องจากกฎหมายอาชญากรรมทางคอมพิวเตอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลมีเนื้อหาเกี่ยวข้องกันโดยเฉพาะอย่างยิ่งในประเด็นการบุกรุกหรือทำลายข้อมูลที่ถูกจัดเก็บในรูปแบบของ “ข้อมูลส่วนบุคคล” ใน ระบบคอมพิวเตอร์[155] ที่สมควรได้รับการแก้ไขโดยเร็วแม้ว่าจะไม่สามารถทำให้ปัญหาดังกล่าวหมดสิ้นไป แต่ก็ควรได้รับการบรรเทาและเยียวยาความเสียหายลงได้บ้าง หากได้รับการคุ้มครองโดยกฎหมายตรงจุดและตรงประเด็น

อย่างไรก็ตาม หากจะกล่าวถึงกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลในประเทศไทยที่มีบัญญัติให้ความคุ้มครองไว้อยู่แล้วพบว่ามีอยู่หลายฉบับด้วยกัน เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2550[156] ประมวลกฎหมายอาญา[157] ประมวล

---

155 ข้อความบางส่วนในระเบียบวาระที่ 1 (เรื่องที่แจ้งให้ที่ประชุมทราบ) จากเอกสารสรุปการประชุมคณะอนุกรรมการเฉพาะกิจยกร่างกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ครั้งที่ 6 (1/2544) เมื่อวันพฤหัสบดี ที่ 8 มีนาคม 2544 เวลา 14.00-17.00 น. ณ ห้องประชุม ชั้น 4 อาคารกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม

156 รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550

“มาตรา 35 สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง

การกล่าวหาหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง หรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่กรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน”

157 ประมวลกฎหมายอาญา

“มาตรา 322 ผู้ใดเปิดผนึกหรือเอาจดหมาย โทรเลขหรือเอกสารใด ๆ ซึ่งปิดผนึกของผู้อื่นไปเพื่อล่วงรู้ข้อความก็ดี เพื่อนำข้อ ความในจดหมาย โทรเลขหรือเอกสารเช่นว่านั้นออกเปิดเผยก็ดี ถ้าการกระทำนั้นน่าจะเกิดความเสียหายแก่ผู้หนึ่งผู้ใด ต้องระวางโทษ...”

กฎหมายแพ่งและพาณิชย์[158] พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544[159] พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545[160] เป็นต้น โดยกฎหมายส่วนใหญ่เหล่านั้นบัญญัติขึ้นเพื่อรองรับเรื่องใดเรื่องหนึ่งโดยเฉพาะ อีกทั้งยังมีข้อจำกัดอยู่ในตัวเองและมักจะใช้มาตรการ “เยียวยา” ความเสียหายมากกว่ามาตรการ “ป้องกัน” ซึ่งขัดแย้งกับหลักการคุ้มครองข้อมูลส่วนบุคคลของอารยประเทศที่มุ่งให้ความคุ้มครองในลักษณะการป้องกันเป็นสำคัญ

อนึ่ง แม้ว่าปัจจุบันร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....[161] ซึ่งเป็นกฎหมายกลางเพื่อวางหลักเกณฑ์ในการคุ้มครองข้อมูลส่วนบุคคลจะอยู่ในระหว่างการพิจารณาของสภานิติบัญญัติ โดยร่างกฎหมายดังกล่าวมีหลักการว่า ให้ผู้ที่มีส่วนเกี่ยวข้องในการเก็บ รวบรวม

---

158 ประมวลกฎหมายแพ่งและพาณิชย์

“มาตรา 420 ผู้ใดจงใจหรือประมาทเลินเล่อ ทำต่อบุคคลอื่นโดยผิดกฎหมายให้เขาเสียหายถึงแก่ชีวิตก็ดี แก่ร่างกายก็ดี อนามัยก็ดี เสรีภาพก็ดี ทรัพย์สินหรือสิทธิอย่างหนึ่งอย่างใดก็ดี ท่านว่าผู้นั้นทำละเมิดจำต้องใช้ค่าสินไหมทดแทนเพื่อการนั้น”

159 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

“มาตรา 50 ให้คณะกรรมการกำหนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับ ข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม

ให้ผู้รับใบอนุญาตมีหน้าที่ปฏิบัติตามมาตรการที่คณะกรรมการกำหนดตามวรรคหนึ่ง

เมื่อพบว่ามีบุคคลใดกระทำการละเมิดสิทธิของผู้ใช้บริการตามวรรคหนึ่ง ให้ผู้รับใบอนุญาตหรือคณะกรรมการดำเนินการเพื่อระงับการกระทำดังกล่าว และแจ้งให้ผู้ใช้บริการทราบโดยเร็ว

มาตรา 74 ผู้ใดกระทำด้วยประการใด ๆ เพื่อดักรับไว้ใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสารหรือข้อมูลอื่นใดที่มีการสื่อสารทางโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย ต้องระวางโทษ...”

160 พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545

“มาตรา 3 ข้อมูล หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงของข้อมูลเครดิต ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือผ่านวิธีใด ๆ และไม่ว่าจะได้ทำในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

ข้อมูลห้ามจัดเก็บ หมายความว่า ข้อมูลของบุคคลธรรมดาที่ไม่เกี่ยวกับการบริการ การขอสินเชื่อ หรือที่มีผลกระทบต่อความรู้สึก หรืออาจก่อให้เกิดความเสียหาย หรือมีผลกระทบต่อสิทธิเสรีภาพของผู้เป็นเจ้าของข้อมูลอย่างชัดเจน ดังต่อไปนี้...”

161 ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... ณ วันที่ 14 กรกฎาคม 2551 ได้บัญญัติมาตรการคุ้มครองข้อมูลส่วนบุคคลไว้ในหมวด 2 ตั้งแต่มาตรา 15 ถึงมาตรา 39

ประมวลผลหรือควบคุมข้อมูลส่วนบุคคลที่ได้มาจากบุคคลซึ่งเป็นเจ้าของข้อมูลจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลเหล่านั้นด้วย หากฝ่าฝืนก็จะได้รับโทษทั้งทางปกครองและทางอาญาตามที่ได้บัญญัติไว้ ซึ่งอาจจะเป็นไปตามหลักการคุ้มครองข้อมูลส่วนบุคคลของอารยประเทศที่มุ่งให้ความคุ้มครองในลักษณะการป้องกันเป็นสำคัญ แต่ก็ยังไม่เป็นที่แน่นอนว่ากฎหมายดังกล่าวจะสามารถประกาศใช้ได้เมื่อใด หรือหากมีการประกาศใช้กฎหมายดังกล่าวแล้วหลักการต่าง ๆ เหล่านั้นจะยังคงอยู่เหมือนเดิมหรือไม่

ดังนั้น กฎหมายที่ให้ความคุ้มครองแก่ข้อมูลส่วนบุคคลของประเทศไทยดังกล่าวข้างต้นจึงยังไม่ครอบคลุมและยังไม่สามารถปรับใช้กับลักษณะการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ ตัวอย่างที่เห็นได้ชัดเจนคือ กฎหมายอาญามีบทบัญญัติเรื่องการคุ้มครองข้อมูลส่วนบุคคลเฉพาะเรื่องที่เกี่ยวกับเสรีภาพและชื่อเสียงเท่านั้น แต่ไม่รวมถึงข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์ด้วย เช่น การเปิดผนึกจดหมายของผู้อื่นแล้วนำข้อความที่รับทราบไปเผยแพร่ทำให้เจ้าของจดหมายได้รับความเสียหาย ถือเป็นความผิดตามกฎหมายอาญา แต่ไม่สามารถนำมาปรับใช้กับการกระทำที่เป็นการละเมิดต่อข้อมูลที่จัดเก็บในระบบคอมพิวเตอร์ได้ เป็นต้น เนื่องจากกฎหมายอาญาต้องตีความโดยเคร่งครัดซึ่งยังไม่มีบทบัญญัติที่กำหนดให้การกระทำละเมิดต่อข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์เป็นความผิดตามกฎหมายอาญา[162]

กล่าวโดยสรุปแล้ว มาตรการทางกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ในปัจจุบันยังไม่สามารถแก้ไขปัญหาได้ตรงจุด เนื่องจากรูปแบบการละเมิดข้อมูลส่วนบุคคลที่เกิดจากชุดคำสั่งไม่พึงประสงค์เมื่อเปรียบเทียบกับหลักการในการคุ้มครองข้อมูลส่วนบุคคลตามร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... แล้ว เป็นคนละหลักการกัน กล่าวคือ หลักการของร่างกฎหมายดังกล่าวมุ่งเน้นให้ผู้ที่มีส่วนเกี่ยวข้องในการเก็บรวบรวม ประมวลผลหรือควบคุมข้อมูลส่วนบุคคลที่ได้มาจากบุคคลซึ่งเป็นเจ้าของข้อมูลจะต้องมีมาตรการในการคุ้มครองข้อมูลส่วนบุคคลเหล่านั้นด้วย หากฝ่าฝืนก็จะได้รับโทษทั้งทางปกครองและทางอาญาตามที่ได้บัญญัติไว้ ส่วนการคุกคามและละเมิดข้อมูลส่วนบุคคลที่ถูกจัดเก็บในระบบคอมพิวเตอร์ด้วยชุดคำสั่งไม่พึงประสงค์นั้น มีลักษณะเป็นการละเมิดโดยที่เจ้าของข้อมูลมิได้ยินยอมมอบข้อมูลให้และในขณะเดียวกันการกระทำละเมิดนั้นก็ไม่เข้าข่ายเป็นความผิดทางอาญาตามกฎหมายที่มีโทษทางอาญาใดเลย ตัวอย่างที่เห็นได้ชัดเจนที่สุดคือ การขโมยเอกลักษณ์บุคคล

---

162 น้ำทิพย์ บุญเกิด, “ความรับผิดทางอาญากรณีละเมิดข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์ (Criminal Liability for the Transgression of Personal Data : Particularly Study about Personal Data which be Kept in the Computer System.),” (สารนิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 28

(Identity Theft) ด้วยมัลแวร์โดยที่มัลแวร์นั้นมิได้มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นที่อยู่ในระบบคอมพิวเตอร์ของเจ้าของข้อมูลนั้นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด กรณีจึงไม่เข้าข่ายเป็นความผิดฐานบุกรุกหรือเข้าถึงโดยมิชอบตามความหมายของมาตรา 5 มาตรา 7 หรือการรวบกวนข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตามความหมายของมาตรา 9 และ มาตรา 10 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อีกด้วย

บทที่ 5
วิเคราะห์ปัญหาเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. ความสัมพันธ์ระหว่างชุดคำสั่งไม่พึงประสงค์กับการเข้าถึง

เหตุที่ต้องกล่าวถึงความสัมพันธ์ระหว่างชุดคำสั่งไม่พึงประสงค์กับการเข้าถึงนั้น ก็เนื่องมาจากการกระทำความผิดโดยใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือนั้น ถือได้ว่าเป็นการกระทำความผิดต่อคอมพิวเตอร์โดยแท้ที่จะต้องผ่านกระบวนการเข้าถึง (การเข้าถึงในที่นี้หมายความถึงเฉพาะการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลเท่านั้น) ก่อนเสมอจึงจะสามารถนำไปสู่การกระทำที่จะก่อให้เกิดความเสียหายและส่งผลกระทบอื่นๆ ตามมา ไม่ว่าจะเป็นความเสียหายหรือผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) และระบบเครือข่ายคอมพิวเตอร์ (Computer Network Security) ทั้งต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตามที่ได้กล่าวไปแล้วในบทที่ 2 ทั้งนี้ หากปราศจากการเข้าถึงเสียแล้ว ความเสียหายและผลกระทบต่างๆ ก็คงมิอาจเกิดขึ้นได้ จึงอาจกล่าวได้ว่าการเข้าถึงเป็นบ่อเกิดหรือเป็นต้นธารแห่งการกระทำความผิดต่อคอมพิวเตอร์โดยแท้

เมื่อพิจารณาถึงเป้าประสงค์หรือวัตถุแห่งการกระทำที่ผู้กระทำผิดต้องการเนื่องจากการใช้ชุดคำสั่งไม่พึงประสงค์แล้วก็คือ ความเสียหายหรือผลกระทบต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ปรากฏออกมาในรูปแบบต่างๆ ได้หลายๆ รูปแบบ เช่น ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เป็นต้น นอกจากนี้ ยังมีความเสียหายหรือผลกระทบในรูปแบบอื่นๆ อันสืบเนื่องมาจากการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดอีกโดยเฉพาะอย่างยิ่งความเสียหายและผลกระทบต่อความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชน และความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับไม่ว่าจะเป็นความลับต่อส่วนตัว หรือความลับในทางการค้า ซึ่งผู้กระทำผิดมักจะได้ข้อมูลที่เป็น

ความลับเหล่านั้นไปโดยการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิด แล้วนำข้อมูลที่ได้ไปก่ออาชญากรรมอื่นต่อไป

อย่างไรก็ตาม หากพิจารณามาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศ จะมิได้มีแต่เฉพาะมาตรการป้องกันหรือแก้ไขปัญหาที่เกิดจากการที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้เท่านั้น แต่มาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศนั้น สามารถครอบคลุมถึงความเสียหายหรือผลกระทบ และพฤติการณ์จากชุดคำสั่งไม่พึงประสงค์ได้อย่างครบถ้วนในทุกรูปแบบซึ่งรวมถึงความเสียหายและผลกระทบต่อความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชน และความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับด้วย จนทำให้การกระทำความผิดโดยการใช้ชุดคำสั่งไม่พึงประสงค์ทุกๆ ประเภทไม่ว่าจะเป็นไวรัสคอมพิวเตอร์ ม้าโทรจัน สปายแวร์ และแอดแวร์ ในบางประเทศนั้นสามารถปรับเข้ากับฐานความผิดในกฎหมายที่มีอยู่ได้แทบทุกกรณีที่เกิดขึ้น โดยไม่เกิดความคลุมเครือในการบังคับใช้กฎหมาย สาเหตุที่เป็นเช่นนั้นก็เพราะในกฎหมายของต่างประเทศได้มีการกำหนดนิยามและความหมายของการ “เข้าถึง (access)” ไว้โดยชัดแจ้งเพื่อให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดได้ในทุกๆ รูปแบบและใช้เป็นบรรทัดฐานสำหรับผู้ที่ต้องปรับใช้กฎหมายได้เป็นอย่างดีนั่นเอง

2. องค์ประกอบภายนอกของความรับผิดทางอาญาที่เกิดจากชุดคำสั่งไม่พึงประสงค์

องค์ประกอบภายนอกของความรับผิดทางอาญาแทบทุกฐานแยกออกได้เป็น ผู้กระทำ การกระทำ และวัตถุแห่งการกระทำ เช่น ความผิดฐานฆ่าคนตายโดยเจตนาตามประมวลกฎหมายอาญามาตรา 288 ได้แก่ ผู้ใด (ผู้กระทำ) ฆ่า (การกระทำ) ผู้อื่น (วัตถุแห่งการกระทำ) เป็นต้น ทั้งนี้ในการวินิจฉัยความรับผิดทางอาญาของบุคคลนั้น มีหลักเกณฑ์ในการวินิจฉัยที่สำคัญที่สุดประการแรกคือ ต้องพิจารณาเสียก่อนว่าบุคคลนั้นมี “การกระทำ” หรือไม่ เพราะประมวลกฎหมายอาญามาตรา 59 บัญญัติว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำโดยเจตนา เว้นแต่จะได้กระทำโดยประมาท ในกรณีที่กฎหมายบัญญัติให้ต้องรับผิดเมื่อได้กระทำโดยประมาท หรือเว้นแต่ในกรณีที่กฎหมายบัญญัติไว้โดยชัดแจ้งให้ต้องรับผิด แม้ได้กระทำโดยไม่มีเจตนา” จากบทบัญญัติดังกล่าวในตอนต้นที่ว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำ...” แสดงว่าการกระทำเป็นเงื่อนไขประการแรกของความรับผิดในทางอาญา ทั้งนี้ สำหรับองค์ประกอบภายนอกของความรับผิดทางอาญาในอาชญากรรมพื้นฐาน (Conventional Crimes) นั้น จะพิจารณาการกระทำจากการ

เคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึก กล่าวคือ การเคลื่อนไหวร่างกายนั้นต้องอยู่ภายใต้บังคับของจิตใจ แต่สำหรับอาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ที่ใช้ชุดคำสั่งไม่ถึงประสงค์เป็นเครื่องมือในกระทำผิดโดยการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลนั้น การพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึกเพียงอย่างเดียวคงไม่เพียงพอที่จะถือว่าบุคคลนั้นมี “การกระทำ” หรือไม่ ทั้งนี้จะต้องพิจารณาจากลักษณะหรือผลที่ปรากฏออกมา ซึ่งได้แก่ การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ประกอบด้วยเสมอ ส่วนวัตถุแห่งการกระทำสำหรับความผิดนี้ก็คือ ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นนั่นเอง ทั้งนี้ จะต้องพิจารณาถึงองค์ประกอบภายในซึ่งเป็นส่วนของเจตนาตามมาตรา 59 ประกอบด้วย

ต่อไปนี้ จะเป็นการวิเคราะห์ถึงปัญหาความรับผิดทางอาญาจากชุดคำสั่งไม่พึงประสงค์โดยจะเป็นการพิจารณาองค์ประกอบภายนอกว่า ชุดคำสั่งไม่พึงประสงค์ใดบ้างที่เมื่อถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดโดยการเข้าถึงทางดิจิทัลแล้ว มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ โดยจะแยกพิจารณาเป็น 2 ลักษณะด้วยกัน คือ

2.1 การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม

อย่างไรจึงจะเรียกว่าเป็น “การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม” ลักษณะดังกล่าวนี้เป็นการใช้ถ้อยคำซึ่งเป็นองค์ประกอบความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญามาตรา 358 คือคำว่า “ทำให้เสียหาย” และ “ทำลาย” แต่ในส่วนที่เกี่ยวกับการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมนั้น ไม่ได้ยกองค์ประกอบของความผิดฐานปลอมเอกสารมา[163] อาจเป็นเพราะชุดคำสั่งไม่พึงประสงค์จะอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์หรือดิจิทัลจึงนำลักษณะของการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมในข้อมูลอิเล็กทรอนิกส์ไปเปรียบเทียบกับความผิดฐานปลอมเอกสารไม่ได้ ทั้งนี้คำว่า “การแก้ไข เปลี่ยนแปลง เพิ่มเติม” จัดได้ว่าเป็นคำสามัญที่มีความชัดเจนเพียงพอและพึงเข้าใจได้

---

163 พรเพชร วิชิตชลชัย , อ้างแล้วในเชิงอรรถที่ 147 หน้า 13

สำหรับในทางคอมพิวเตอร์นั้น การรักษาความครบถ้วนสมบูรณ์ (Integrity) หมายถึง การป้องกันเพื่อให้ข้อมูลไม่ถูกแก้ไข เปลี่ยนแปลง เพิ่มเติม หรือถูกทำลายได้ ซึ่งวิธีการในการรักษาความถูกต้องครบถ้วนของข้อมูลสามารถทำได้หลายวิธีด้วยกัน เช่น การใช้เช็คซัม (checksum) ซึ่งเป็นการตรวจสอบความคงอยู่หรือความครบถ้วนสมบูรณ์ (Integrity Checker) ที่เก็บข้อมูลความคงอยู่ของไฟล์สำคัญไว้สำหรับเปรียบเทียบ ตัวอย่างข้อมูล เช่น ขนาดไฟล์ เวลาการแก้ไขครั้งล่าสุด เป็นต้น ซึ่งส่วนมากจะใช้ค่าของเช็คซัมในการเปรียบเทียบ เมื่อมีไฟล์เปลี่ยนแปลงที่มีสาเหตุอันเนื่องจากชุดคำสั่งไม่พึงประสงค์ หรือความผิดพลาดใดๆ จนทำให้ข้อมูลความคงอยู่ต่างจากข้อมูลเดิมที่เคยเก็บไว้ ก็จะทำให้ทราบถึงความผิดปกติที่เกิดขึ้น

ตัวอย่างของการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม เช่น การป้อนโปรแกรมที่มีไวรัสที่มีคุณสมบัติในการทำลายล้างข้อมูลหรือโปรแกรมคอมพิวเตอร์ เข้าไปในระบบเพื่อลบ เปลี่ยนแปลงแก้ไขข้อมูลหรือกระทำการใดๆ อันเป็นการรบกวนข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เป็นต้น

2.2 การทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้

การทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้นั้น สามารถพบได้ในสองลักษณะ คือ การที่ระบบคอมพิวเตอร์เกิดความขัดข้อง หรือการที่ระบบคอมพิวเตอร์ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ สำหรับประเด็นที่ว่าอย่างไรจึงจะเรียกว่าเป็นการ “ขัดข้องหรือการปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้” นั้น ย่อมพิจารณาได้จากการที่ระบบคอมพิวเตอร์นั้นไม่สามารถทำงานได้โดยสมบูรณ์ ดังนั้น ถึงแม้ว่าระบบคอมพิวเตอร์จะทำงานได้ แต่เป็นการทำงานที่ไม่สมบูรณ์หรือผิดปกติไป (malfunctioning) ก็ย่อมอยู่ในความหมายของถ้อยคำดังกล่าวแล้ว[164]

ตัวอย่างของการทำให้ระบบคอมพิวเตอร์ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น การป้อนโปรแกรมที่ทำให้ระบบคอมพิวเตอร์ปฏิเสธการทำงาน (denial of service) หรือทำให้ระบบคอมพิวเตอร์ทำงานได้ช้าลงโดยการป้อนไวรัสคอมพิวเตอร์เพื่อให้เกิดผลชะลอการทำงานของระบบ เป็นต้น ส่วนการกระทำทางกายภาพ (physical) โดยเข้าไปยุ่งเกี่ยวกับระบบคอมพิวเตอร์ เช่น การวางระเบิด การก่อวินาศกรรมเพื่อให้มีผลทำลายการทำงานของระบบ

---

164 พรเพชร วิชิตชลชัย, อ้างแล้วในเชิงอรรถที่ 147 หน้า 15

คอมพิวเตอร์นั้น แม้จะถือเป็นการทำให้ระบบคอมพิวเตอร์ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ แต่ก็ไม่อยู่ในประเด็นวิจัยของวิทยานิพนธ์ฉบับนี้ ผู้เขียนจึงไม่ขอกล่าวถึงรายละเอียดในส่วนของการกระทำทางกายภาพนี้

ทั้งนี้ ผลจากการรวบรวม ศึกษาและพิเคราะห์เกี่ยวกับคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายในบทที่ 2 ซึ่งสามารถจัดและแยกประเภทชุดคำสั่งดังกล่าวได้ทั้งหมดเป็น 17 ประเภทนั้นพบว่า ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ได้แก่ ไวรัส หนอน แอดแวร์ โปรแกรมทดสอบช่องโหว่ โปรแกรมเจาะระบบ โปรแกรมดาวน์โหลดไวรัส โปรแกรมปล่อยไวรัส โปรแกรมฉีดไวรัส โปรแกรมชุดสร้างไวรัส โปรแกรมสำหรับส่งสแปม โปรแกรมระเบิด โปรแกรมโทรศัพท์อัตโนมัติ โปรแกรมล้อกันเล่น ฟลัดเดอร์ รูทคิท

สำหรับม้าโทรจันและสปายแวร์นั้น ผู้เขียนเห็นว่าไม่มีคุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด สาเหตุที่เป็นเช่นนั้นก็เพราะเมื่อม้าโทรจันและสปายแวร์ถูกนำไปติดตั้งหรือฝังไว้ในระบบคอมพิวเตอร์ที่ตกเป็นเหยื่อแล้วจะมิได้ก่อให้เกิดความเสียหายใดๆ ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น ทั้งนี้ สามารถพิจารณาได้จากการที่ระบบคอมพิวเตอร์นั้นยังสามารถทำงานได้โดยสมบูรณ์อยู่นั่นเอง (ส่วนความเสียหายเนื่องจากการดักจับเอารหัสผ่านต่างๆ หรือข้อมูลจากปุ่มคีย์บอร์ดที่ถูกกดในเครื่อง หรือการเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ แล้วส่งข้อมูลออกไป เพื่อการเข้าไปใช้หรือโจมตีระบบในภายหลัง หรือการนำข้อมูลนั้นไปเปิดเผยหรือนำไปก่ออาชญากรรมอื่นต่อไปนั้น ก็ยังไม่อาจจัดได้ว่าเป็นความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์หรือชุดคำสั่งอื่นตามความหมายในมาตรา 21 ของกฎหมายนี้ แต่อย่างใด) โดยจะขอกล่าวถึงคุณสมบัติของชุดคำสั่งไม่พึงประสงค์เหล่านั้นในเชิงการขยายความเพื่อชี้ให้เป็นถึงการมีผลและไม่มีผลต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น ดังรายละเอียดปรากฏตามภาพที่ 5.1 ต่อไปนี้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
1. ไวรัสคอมพิวเตอร์ (Computer Virus) เช่น ไวรัสตั้งต้น (Germs), Boot viruses, Program viruses, Multipartite viruses, Stealth viruses, Polymorphic viruses, Macro viruses, Active X เป็นต้น	ไวรัสสามารถสร้างความรำคาญเล็กๆ น้อยๆไปจนถึงการทำลายหรือล้างข้อมูลในฮาร์ดดิสก์ แต่ไวรัสบางชนิดไม่ได้ออกแบบมาเพื่อที่จะทำลายล้างแต่ออกแบบมาอย่างง่ายๆ และแพร่กระจายไปเรื่อยๆ เพื่อก่อกวนหรืออาจสร้างปัญหาให้ถึงขึ้นที่ระบบคอมพิวเตอร์ล่มหรือปฏิเสธการทำงานได้ ดังนั้น นอกจากไวรัสจะมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมแล้ว ไวรัสยังมีผลทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้อีกด้วย
2. ม้าโทรจัน (Trojan Horses) เช่น โปรแกรมดักข้อมูลผ่านปุ่มคีบอร์ด (Keylogger/Keystroker Generators), โปรแกรมจับรหัสผ่าน (Password Retrievers) เป็นต้น	ม้าโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ แต่ถูกออกแบบมาให้สอดคล้องและแฝงตัวเองเข้าไปในระบบคอมพิวเตอร์และจะทำงานโดยการดักจับเอารหัสผ่านต่างๆ หรือข้อมูลจากปุ่มของคีย์บอร์ดที่ถูกกดในเครื่องคอมพิวเตอร์ที่ถูกม้าโทรจันฝังตัวไว้ แล้วส่งข้อมูลนั้นออกไป เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ดังนั้น ด้วยคุณสมบัติดังกล่าวของม้าโทรจัน จึงมิได้มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
3. สปายแวร์ (Spyware)	สปายแวร์เป็นโปรแกรมที่มีจุดมุ่งหมายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ ภายในเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งอยู่ และเทคนิคที่ใช้นั้นได้แก่ การดักข้อมูลที่ถูกกดปุ่มคีย์บอร์ด การบันทึกเว็บไซต์ที่เคยเข้าเยี่ยมชมมา หรือไฟล์เอกสารต่างๆ ที่อยู่ภายในเครื่องโดยไม่ทำอันตรายใดๆต่อเครื่อง ดังนั้น สปายแวร์จึงมิได้มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
4. หนอนคอมพิวเตอร์ (Worm) เช่น Email worms, Instant Messaging worms, Internet worms, IRC worms, File-sharing Networks worms เป็นต้น	หนอนสามารถแพร่กระจายตัวเองผ่านระบบเครือข่ายได้อย่างอัตโนมัติและรวดเร็วโดยทำความเสียหายรุนแรงกว่าไวรัสมาก ดังนั้น หนอนจึงมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงได้โดยตรง

5. แอดแวร์ (Adware)	แอดแวร์มีการทำงานและการติดเชื้อคล้ายกับสปายแวร์มาก ต่างกันตรงที่สปายแวร์จะเน้นไปที่การขโมยข้อมูล ส่วนแอดแวร์จะเน้นที่การโฆษณา โดยจะแสดงหรือดาวน์โหลดโฆษณามายังเครื่องคอมพิวเตอร์หลังจากที่ถูกติดตั้งโปรแกรมนี้แล้ว หรือจะสร้างหน้าจอ Pop-up หรือการ์ตูนน่ารักต่างๆ เพื่อหลอกล่อให้เหยื่อเผลอคลิกเข้าไปยังเว็บไซต์ขายสินค้าในขณะที่มีการเรียกใช้งาน เช่น เว็บไซต์ขายภาพหรือวีดีโอโป๊ เว็บไซต์ของธุรกิจขายตรง เป็นต้น นอกจากนี้ แอดแวร์มักจะถูกแนบมากับอีเมล์ขยะหรือโปรแกรมประเภทพักหน้าจอ โดยแอดแวร์สามารถทำงานได้โดยอัตโนมัติเมื่อเหยื่อเริ่มใช้งานหรือเข้าสู่อินเทอร์เน็ต ดังนั้น แอดแวร์จึงมีผลทำให้ระบบคอมพิวเตอร์เพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
6. โปรแกรมทดสอบช่องโหว่ (Exploits)	เมื่อมีการเจาะระบบผ่านทางช่องโหว่แล้วก็จะทำให้มีการได้มาซึ่งสิทธิ์เพื่อควบคุมระบบ ดังนั้น โปรแกรมทดสอบช่องโหว่จึงมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ตามไปด้วย ซึ่งส่วนใหญ่มักจะถูกนำไปใช้โดยได้รับอนุญาตในการทดสอบเจาะระบบ
7. โปรแกรมเจาะระบบ (Auto-Rooters)	โปรแกรมเจาะระบบจะถูกใช้ในการเจาะระบบคอมพิวเตอร์ผ่านทางช่องโหว่ และทำให้ได้มาซึ่งสิทธิ์และการเป็นผู้ดูแลระบบและสามารถควบคุมเครื่องคอมพิวเตอร์หรือเซิร์ฟเวอร์ที่เป็นเป้าหมายจากระยะไกลได้ ดังนั้น โปรแกรมเจาะระบบจึงมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ตามไปด้วย
8. โปรแกรมดาวน์โหลดไวรัส (Virus Downloaders)	โปรแกรมดาวน์โหลดไวรัส เมื่อถูกติดตั้งและถูกเอ็กซิคิวต์แล้วจะดาวน์โหลดโปรแกรมอื่นๆ ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์และระบบเครือข่ายจากเว็บไซต์หรือแหล่งอื่นๆ แล้วทำการรันโปรแกรมนั้นโดยอัตโนมัติ จึงเป็นการทำให้ระบบคอมพิวเตอร์ถูกเพิ่มเติมโดยโปรแกรมที่ดาวน์โหลดมา
9. โปรแกรมปล่อยไวรัส (Virus Droppers)	เป็นโปรแกรมที่ใช้ในการปล่อยไวรัสจากโปรแกรมไวรัสเอง จึงเป็นการทำให้ระบบคอมพิวเตอร์ถูกเพิ่มเติมโดยไวรัสที่ปล่อยออกมา
10. โปรแกรมฉีดไวรัส (Virus Injectors)	โปรแกรมฉีดไวรัสทำงานคล้ายกับโปรแกรมปล่อยไวรัส แตกต่างกันที่โปรแกรมประเภทนี้จะทำการติดตั้งและโหลดส่วนของไวรัสไปไว้ในหน่วยความจำได้ เหมือนกับการฉีดไวรัสเข้าไปสู่หน่วยความจำ นอกจากนี้อาจจะฉีดไวรัสเข้าไปกับข้อมูลที่เคลื่อนที่

	อยู่ในระบบเครือข่ายคอมพิวเตอร์ได้ จึงเป็นการทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลง
11. โปรแกรมชุดสร้างไวรัส (Kits-Virus Generators)	แม้โปรแกรมชุดสร้างไวรัสจะถูกใช้เพื่อสร้างไวรัสตัวใหม่ๆ โดยอัตโนมัติ แต่หากมีการสร้างไวรัสนั้นในระบบคอมพิวเตอร์ก็จะมีผลทำให้ระบบคอมพิวเตอร์นั้นถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลงตามไปด้วย
12. โปรแกรมสำหรับส่งสแปม (Spammer Programs)	โปรแกรมสำหรับส่งสแปมมักจะถูกใช้เพื่อส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่างๆ ผ่านทางอีเมล์ โปรแกรมสนทนา รวมทั้งอีเมล์และ SMS ในโทรศัพท์มือถือ จึงมีผลทำให้ระบบคอมพิวเตอร์นั้น ถูกเพิ่มเติมข้อความนั้นลงไปด้วย
13. โปรแกรมระเบิด (Bombs Programs)	โปรแกรมระเบิดเป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใดๆ เกิดขึ้น ลักษณะที่พบ เช่น โปรแกรมจะถูกลบเองเมื่อถูกรันไปแล้ว 2-3 ครั้ง จึงอาจส่งผลทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีอยู่เสียหาย หรือถูกทำลายตามไปด้วย
14. โปรแกรมโทรศัพท์อัตโนมัติ (Dialers Programs)	หากมีการติดตั้งโปรแกรมประเภทนี้ในเครื่องคอมพิวเตอร์ จะมีการต่อโทรศัพท์อัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อที่จะให้เหยื่อนั้นต้องจ่ายค่าโทรศัพท์ในอัตราที่แพงที่สุดหรือทำให้เสียค่าโทรศัพท์ระหว่างประเทศ จึงเป็นการทำให้ระบบคอมพิวเตอร์ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
15. โปรแกรมล้อกันเล่น (Joke Programs)	เป็นโปรแกรมที่ไม่ได้ตั้งใจทำอันตรายต่อเครื่องหรือระบบโดยตรง หากเพียงแค่ต้องการก่อกวนหรือสร้างความรำคาญให้แก่ผู้ใช้งาน โดยการเข้าไปเปลี่ยนพฤติกรรมปกติของเครื่องคอมพิวเตอร์ เช่น หากโปรแกรมนี้เป็นสกรีนเซฟเวอร์ก็อาจจะทำการล็อกหน้าจอได้เองทั้งๆ ที่ผู้ใช้งานเองไม่ได้ปรับแต่งค่าให้ล็อก อย่างไรก็ตาม โปรแกรมนี้อาจทำอันตรายได้ในบางกรณี เช่น เมื่อทำการล็อกหน้าจอแต่ไม่ปลดล็อกให้ ดังนั้น อาจจะต้องปิดเครื่องคอมพิวเตอร์โดยที่ไม่ได้บันทึกงานไว้ก่อน ทำให้เกิดความเสียหายต่อผู้ใช้งานได้ เป็นต้น กรณีดังกล่าวจึงเป็นการทำให้ระบบคอมพิวเตอร์ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
16. ฟลัดเดอร์ (Flooders)	แฮกเกอร์จะใช้โปรแกรมประเภทนี้ในการโจมตีระบบเครือข่ายเป้าหมายด้วยการส่งข้อมูลในปริมาณมหาศาล เพื่อทำให้เกิดความคับคั่งในระบบเครือข่าย ส่งผลให้เครือข่ายเป้าหมายไม่สามารถ

	ให้บริการต่อไปได้ เรียกการโจมตีประเภทนี้ว่า Denial of Service (DoS) ถ้าหากว่ามีเครื่องคอมพิวเตอร์ที่ถูกควบคุมและจะถูกใช้โจมตีแบบ DoS พร้อมกันหลายๆ เครื่องไปยังเป้าหมายเดียวกัน จะเรียกการโจมตีแบบนี้ว่า Distributed Denial of Service (DDoS) ดังนั้น ฟลัดเดอร์จึงมีผลทำให้ระบบคอมพิวเตอร์ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
17. รูทคิท (Rootkit)	หลังจากแฮกเกอร์สามารถเจาะระบบเข้าไปจนได้สิทธิการควบคุมระบบแล้ว จากนั้นก็จะติดตั้งโปรแกรมรูทคิทโดยการดัดแปลงโปรแกรมที่ถูกติดตั้งไว้อยู่แล้ว เพื่อหลอกให้ผู้ดูแลระบบไม่ให้สังเกตเห็นไฟล์ผิดปกติที่ถูกสร้างโดยแฮกเกอร์ จึงมีผลทำให้ระบบคอมพิวเตอร์นั้นถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลงตามไปด้วย

ภาพที่ 5.1 ตารางแสดงคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

จากข้อมูลในตารางข้างต้น จึงทำให้เห็นถึงความแตกต่างในคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายว่า ม้าโทรจันและสปายแวร์มิได้มีคุณสมบัติหรือมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เมื่อขณะถูกนำไปใช้ในการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ แต่อย่างใด

อนึ่ง เมื่อนำถ้อยคำในมาตรา 21 วรรคสอง ซึ่งเป็นเสมือนถ้อยคำที่เป็นการให้ความหมายหรือเป็นการกำหนดนิยามหรือเป็นการบอกให้ทราบว่า “ชุดคำสั่งไม่พึงประสงค์” ตามความหมายในกฎหมายนี้จะต้องมีความหมายถึง “ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้” แล้ว ก็จะทำให้ม้าโทรจันและสปายแวร์มิได้อยู่ในความหมายของคำว่า “ชุดคำสั่งไม่พึงประสงค์” ตามมาตรา 21 วรรคสอง นี้แต่อย่างใด ทั้งที่จริงแล้วในศาสตร์ทางคอมพิวเตอร์ย่อมถือว่าม้าโทรจันและสปายแวร์เป็นชุดคำสั่งในทางทำให้เกิดความเสียหายตามที่ได้กล่าวไว้อย่างละเอียดแล้วในบทที่ 2

ดังนั้น จึงทำให้เกิดปัญหาในประเด็นองค์ประกอบภายนอกของความรับผิดทางอาญาว่าการดักจับเอารหัสผ่านต่างๆ หรือข้อมูลจากปุ่มคีย์บอร์ดที่ถูกกดในเครื่องคอมพิวเตอร์ หรือการเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่างๆ โดยม้าโทรจันและสปายแวร์ แล้วส่งข้อมูลเหล่านั้นออกไป

จะถือเป็น “การกระทำ” ในทางอาญาหรือไม่ ซึ่งผู้เขียนจะได้วิเคราะห์ถึงปัญหา โดยการเชื่อมโยงกับความหมายของ “การเข้าถึง” ในความผิดฐานการเข้าถึงโดยมิชอบใน ข้อ 3 ข้อ 4 และข้อ 5 ต่อไป

3. ปัญหาในการบังคับใช้กฎหมาย

จากผลการศึกษาพบว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จัดอยู่ในประเภทกฎหมายพิเศษในเชิงเทคนิคเฉพาะ ที่มีทั้งส่วนของกฎหมายสารบัญญัติ (หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์) เพื่อกำหนดฐานความผิดและบทกำหนดโทษ และในส่วนของกฎหมายวิธีสบัญญัติ (หมวด 2 พนักงานเจ้าหน้าที่) เพื่อกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ในการดำเนินกระบวนพิจารณาทางอาญาเฉพาะคดีความผิดเกี่ยวกับคอมพิวเตอร์ รวมทั้งการกำหนดหน้าที่ของผู้ให้บริการที่จะต้องมีการเก็บข้อมูลจราจรทางคอมพิวเตอร์เพื่อใช้สำหรับการเป็นพยานหลักฐานตั้งแต่ชั้นการสอบสวน การสั่งฟ้องหรือไม่ฟ้องของพนักงานอัยการ และการพิจารณาพิพากษาคดีของศาล ซึ่งนับว่าเป็นสิ่งที่ดีที่กฎหมายดังกล่าวเป็นทั้งกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติอยู่ในตัว ทำให้สามารถอ้างอิงและปรับใช้ได้โดยง่ายและเป็นไปตามวัตถุประสงค์แห่งอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของคณะมนตรีแห่งยุโรป (Council of Europe) ทั้ง 3 ประการ ที่ว่า (1) เพื่อให้กฎหมายอาญาสารบัญญัติภายในประเทศต่าง ๆ ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์มีความสอดคล้องและเป็นไปในทางเดียวกัน (2) เพื่อให้กฎหมายวิธีพิจารณาความอาญาตามกฎหมายภายในให้อำนาจที่จำเป็นเพื่อการสืบสวน สอบสวน และฟ้องร้องการกระทำความผิดที่ได้กระทำโดยใช้ระบบคอมพิวเตอร์ ตลอดจนการรวบรวมพยานหลักฐานที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ และ (3) เพื่อเร่งให้เกิดความร่วมมือระหว่างประเทศที่ค่อนข้างรวดเร็วและบรรลุเป้าหมายของอนุสัญญา

อย่างไรก็ตาม ด้วยความเป็นมาของการบัญญัติมาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์มิได้ปรากฏขึ้นในชั้นการยกร่างกฎหมาย แต่ได้มีการเพิ่มเติมขึ้นโดยการกำหนดเป็นมาตรการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์เป็นการเฉพาะและให้อำนาจพิเศษแก่พนักงานเจ้าหน้าที่ในการจัดการกับชุดคำสั่งไม่พึงประสงค์ภายใต้คำร้องขอและคำสั่งอนุญาตของศาล ซึ่งการบัญญัติให้เป็นอำนาจพิเศษของพนักงานเจ้าหน้าที่ดังกล่าวได้ถูกกำหนดขึ้นในชั้นการตรวจพิจารณาร่างกฎหมายโดยคณะกรรมการกฤษฎีกา (คณะพิเศษ) ที่อาจมิได้มีการศึกษาข้อเท็จจริงให้ละเอียดถี่ถ้วนเสียก่อนว่า ในทางปฏิบัติจะประสบกับปัญหาใดได้บ้าง ซึ่งอันที่จริงแล้วก่อนออกกฎหมายนี้ก็ต้องมีการพิจารณากลั่นกรองโดยสภาอีกชั้นหนึ่ง (คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....) แต่ก็มิได้มีการกลั่นกรอง

ในเรื่องที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ แต่ประการใด[165] สาเหตุอาจเป็นเพราะคณะกรรมาธิการวิสามัญในการพิจารณากฎหมายฉบับนี้มีปัญหาและข้อจำกัดในหลายประการ กล่าวคือ ปัญหาและอุปสรรคส่วนใหญ่ของคณะกรรมาธิการพิจารณาร่างพระราชบัญญัติฯนั้น เป็นเรื่องของความเห็นที่ไม่ตรงกันเกี่ยวกับตัวบทกฎหมายเพราะหากนำคนที่มีความรู้พื้นฐานไม่เท่ากันและประสบการณ์ที่แตกต่างกันมาปฏิบัติงานร่วมกันก็ย่อมเกิดความแตกต่างทางความคิดได้เป็นธรรมดา เนื่องจากคณะกรรมาธิการร่างพระราชบัญญัติฯ ประกอบด้วยกลุ่มนักกฎหมายที่ไม่มีความรู้ด้านเทคโนโลยีสารสนเทศในเชิงเทคนิคและกลุ่มผู้เชี่ยวชาญด้านเทคนิคที่มีความรู้ด้านเทคโนโลยีสารสนเทศดีเยี่ยมแต่ไม่มีความรู้ด้านกฎหมายเพียงพอ

ดังนั้น ความเห็นบางอย่างอาจไม่ตรงกันโดยบทลงโทษในกฎหมายบางครั้งก็ถูกตัดออกไปโดยไม่จำเป็น หรือในตัวบทกฎหมายในบางข้อความก็มีบ้างที่ไม่จำเป็นต้องนำมาเขียนไว้ แต่ผู้ปฏิบัติตามกฎหมายต้องสามารถอธิบายกับพนักงานเจ้าหน้าที่ได้เวลาที่เกิดเหตุการณ์ไม่พึงประสงค์โดยเริ่มจากการศึกษาตัวบทกฎหมายให้รู้แจ้งเห็นจริงเสียก่อน จึงจะสามารถตอบสนองความต้องการของพนักงานเจ้าหน้าที่ในฐานะผู้บังคับใช้กฎหมาย (Law Enforcement) ตลอดจน Auditor และ Regulator รวมทั้งตอบสนองต่อความต้องการของลูกค้า หรือผู้ใช้งานคอมพิวเตอร์ทั่วไป (Users) ได้อย่างถูกต้องตามกฎหมาย[166] หรืออาจเป็นเพราะต้องการรีบผลักดันให้กฎหมายซึ่งได้ยกร่างมาตั้งแต่ปี พ.ศ. 2541 ออกจากสภาโดยเร็วที่สุดเนื่องจากขณะที่พิจารณาเพื่อออกกฎหมายนี้โดยสภานั้นอยู่ในช่วงของการปฏิวัติรัฐประหาร (ยุคคณะมนตรีความมั่นคงแห่งชาติ : คมช.)[167] ที่

---

165 พิจารณาได้จากรายงานการประชุมคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....ที่มีผู้ขอแปรญัตติร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... มาตรา 19 เพียงคนเดียวคือ นายไพศาล พืชมงคล ที่ขอแปรญัตติแก้ไขเพิ่มเติมความในวรรคหนึ่งและวรรคสอง แต่ก็ไม่มีผลเปลี่ยนแปลงหลักการของร่างมาตรา 19 แต่อย่างใด ทั้งนี้ ตามที่ได้กล่าวไปแล้วในข้อ 1.2 (ส่วนของกฎหมายวิธีสบัญญัติเพื่อกำหนดอำนาจดำเนินการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ให้กับพนักงานเจ้าหน้าที่)

166 ปริญญา หอมอเนก,“The Latest Update Computer Crime Law Implementation Status in Thailand สรุปความเคลื่อนไหวเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550หลังมีผลบังคับใช้” ที่มา http://www.acisonline.net/article/?p=9 เผยแพร่เมื่อวันศุกร์ที่ 27 มีนาคม 2552 Retrieved September, 30, 2010

167 วิกิพีเดีย สารานุกรมเสรี.http://th.wikipedia.org/wiki/ คณะมนตรีความมั่นคงแห่งชาติ ชื่อย่อ คมช. (Council of National Security - CNS) เป็นคณะบุคคลที่แปรสภาพมาจากคณะปฏิรูปการปกครองในระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข ซึ่งได้กระทำการยึดอำนาจการปกครองประเทศไทยสำเร็จเมื่อวันที่ 19 กันยายน พ.ศ. 2549 คณะมนตรีฯ บัญญัติขึ้นตามมาตรา 34 ของ รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2549 มีหน้าที่ในการรักษาความสงบเรียบร้อย และความมั่นคงแห่งชาติแทรก คมช.

มีสภาอยู่ในรูปของสภานิติบัญญัติแห่งชาติซึ่งมิได้เป็นสภาในยุคบ้านเมืองปกติซึ่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ถูกสภานิติบัญญัติแห่งชาติผลักดันให้ออกเป็นกฎหมายฉบับแรกๆ ของสภานี้

ด้วยเหตุนี้ จึงทำให้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีปัญหาหลายจุดว่ากันตั้งแต่ “นิยามคำศัพท์ที่ไม่ครอบคลุมพอ” “ฐานความผิดที่มีไม่ครบและบางฐานซ้ำซ้อนกันเอง” “ภาระหน้าที่ของผู้ให้บริการอินเทอร์เน็ต” แต่ที่หนักๆ เห็นจะเป็นประเด็น “อำนาจเจ้าพนักงานของรัฐ” ในอันที่จะสั่งดำเนินการใดๆ กับสิ่งที่เกิดขึ้น[168] ทั้งนี้ เกี่ยวกับประเด็นความเป็นห่วงดังกล่าวนี้ นายสิทธิชัย โภไคยอุดม รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารในขณะนั้นในฐานะประธานคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... ได้แสดงความเห็นไว้ว่า “ในขั้นตอนการแปรญัตติในชั้นคณะกรรมาธิการตนยืนยันจะทำให้ดีที่สุด เพื่อแก้ไขความไม่สมบูรณ์ของร่างพระราชบัญญัตินี้ให้หมดความแคลงใจ โดยเฉพาะเรื่องการใช้อำนาจของเจ้าหน้าที่ตามร่างพระราชบัญญัติฯ นี้ จะไม่เปิดโอกาสให้ใช้อำนาจ โดยมิชอบและที่สำคัญคือ จะเน้นการปกป้องสิทธิเสรีภาพของประชาชน โดยเฉพาะสิทธิส่วนบุคคล อย่างไรก็ตาม ต้องยอมรับว่าแม้จะมีกฎหมายฉบับนี้ออกมาแล้วคงไม่สามารถควบคุมปัญหาที่เกิดขึ้นได้ร้อยเปอร์เซ็นต์ แต่จะทำให้ดีที่สุด”[169]

จากข้อเท็จจริงเกี่ยวกับขั้นตอนการออกกฎหมายดังกล่าวประกอบกับการไม่ได้รับการพิจารณาอย่างรอบคอบในมาตรการเพื่อจัดการเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ จึงกลายเป็นปัญหาและภาระอันหนักอึ้งของพนักงานเจ้าหน้าที่ทั้งในภาคปฏิบัติเพื่อการบังคับใช้กฎหมาย หรืออาจถูกมองไปในทางลบในสายตาของประชาชนในการใช้อำนาจหรือการดำเนินการใดเพื่อให้เป็นไปตามเจตนารมณ์ของกฎหมาย หรืออาจเกิดความเสียหายแก่ประชาชนและประเทศชาติตามมาหากพนักงานเจ้าหน้าที่ใช้อำนาจในทางมิชอบในการดำเนินการกับชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 ทั้งนี้ สามารถสรุปประเด็นปัญหาและข้อบกพร่องในการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ดังนี้

---

168 ความเห็นจากเจ้าของบทความ “กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบๆ (ตอน 1)” จากบล็อก (Blog) กฎหมาย ในเว็บไซต์ http://www.BioLawCom.De Retrieved June, 14, 2010

169 คำให้สัมภาษณ์ของนายสิทธิชัย โภไคยอุดม ภายหลังจากการอภิปรายของ สนช. เมื่อวันที่ 16 พฤศจิกายน 2549 จากเว็บไซต์สมาคมผู้ดูแลเว็บไทย http://www.webmaster.or.th/news/

3.1 ความไม่ชัดเจนและไม่สอดคล้องกับทางปฏิบัติของส่วนกฎหมายวิธีสบัญญัติตามมาตรา 21

ประเด็นความไม่ชัดเจนและความไม่สอดคล้องกับทางปฏิบัติของส่วนกฎหมายวิธีสบัญญัติตามมาตรา 21 นี้ ผู้เขียนเห็นว่าเป็นปัญหาที่สำคัญที่สุดที่ทำให้มาตรการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ยังไม่ได้ผล ทั้งนี้เมื่อพิจารณาถึงบทบัญญัติของมาตรา 21 วรรคหนึ่ง ที่บัญญัติไว้ว่า “ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้” แล้ว ผู้เขียนเห็นว่า เป็นการบัญญัติกฎหมายที่มิได้มีความชัดเจนเพียงพอและมิได้มีความสอดคล้องกับหลักการในทางปฏิบัติที่เกิดขึ้นจริง จึงทำให้เกิดปัญหาในการบังคับใช้กฎหมายในมาตรา 21 วรรคหนึ่ง นี้ อยู่สองประการ คือ

ประการแรก ในทางปฏิบัติพบว่าโอกาสที่พนักงานเจ้าหน้าที่จะตรวจพบชุดคำสั่งไม่พึงประสงค์ที่แอบแฝงหรือปะปนอยู่กับข้อมูลคอมพิวเตอร์อื่นเป็นไปได้ยากมาก เพราะหากพนักงานเจ้าหน้าที่เข้าไปตรวจโดยไม่ได้รับอนุญาตหรือยังมิได้เกิดอำนาจในการสืบสวนสอบสวนคดีก่อนแล้ว ก็จะกลายเป็นว่าพนักงานเจ้าหน้าที่จะเป็นผู้กระทำผิดกฎหมายเสียเอง (โดยการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ) ซึ่งอาจทำให้เกิดภาพในทางลบในสายตาประชาชนเกี่ยวกับการใช้อำนาจซึ่งไม่มีกฎหมายบัญญัติให้กระทำเช่นนั้นได้ หรือหากพนักงานเจ้าหน้าที่แจ้งเจ้าของข้อมูลคอมพิวเตอร์ก่อนเข้าไปตรวจ เจ้าของข้อมูลคอมพิวเตอร์ก็คงจะโยกย้าย ทำลาย หรือสับเปลี่ยนที่อยู่ของข้อมูลคอมพิวเตอร์หรือหาหนทางหลีกเลี่ยงการตรวจก่อนที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจ นอกจากนี้ในความเป็นจริงยังพบอีกว่า ชุดคำสั่งไม่พึงประสงค์นอกจากจะถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์แล้ว ยังถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลอื่นอีกมากมาย เช่น แฟลชไดรว์ (Flash Drive), แผ่นซีดี (Compact Disc : CD), แผ่นดิจิทัลอเนกประสงค์ (Digital Versatile Disc : DVD), External Hard Disk เป็นต้น แต่กฎหมายมิได้มีฐานอำนาจรองรับเพื่อให้พนักงานเจ้าหน้าที่เข้าไปตรวจเพื่อหาชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลเหล่านั้นได้

ทั้งนี้ ผู้เขียนเห็นว่า สาเหตุที่ทำให้เกิดปัญหาเช่นนั้นก็เพราะในกฎหมายฉบับนี้ได้บัญญัติเกี่ยวกับการพบชุดคำสั่งไม่พึงประสงค์ขึ้นมาลอยๆ เพียงว่า “ในกรณีที่พนักงานเจ้าหน้าที่พบว่า...” โดยไม่มีฐานอำนาจมารองรับว่าจะสามารถพบชุดคำสั่งไม่พึงประสงค์ได้อย่างไร ซึ่งหาก

เป็นกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามกฎหมายนี้และเป็นไปเพื่อประโยชน์ในการสืบสวนและสอบสวนตามที่บัญญัติไว้ในมาตรา 18 พนักงานเจ้าหน้าที่ก็คงมีอำนาจที่จะตรวจและพบชุดคำสั่งไม่พึงประสงค์ที่อยู่ในสื่อบันทึกข้อมูลอื่นได้ แต่หากเป็นกรณีที่ยังไม่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด พนักงานเจ้าหน้าที่ก็คงไม่มีอำนาจในการตรวจชุดคำสั่งไม่พึงประสงค์เหล่านั้นได้ การบัญญัติกฎหมายที่สวนทางกับวิธีปฏิบัติจริงเช่นนี้ย่อมเป็นการไร้ผล จึงทำให้เกิดความสับสนแก่พนักงานเจ้าหน้าที่ผู้ซึ่งต้องบังคับใช้กฎหมายเป็นอย่างมาก

ประการที่สอง หากมีการเผยแพร่หรือจำหน่ายหรือใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ในการกระทำความผิดแล้ว ก็จะทำให้พนักงานเจ้าหน้าที่มิอาจอาศัยอำนาจตามมาตรา 21 วรรคหนึ่ง ในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ที่มีม้าโทรจันและสปายแวร์ติดตั้งหรือฝังอยู่ได้ หรือจะขอให้ศาลมีคำสั่งเพื่อกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวนั้นก็ไม่ได้อีกเช่นกัน สาเหตุที่เป็นเช่นนั้นก็เพราะ เมื่อพิจารณาถึงความหมายของชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคสอง ที่บัญญัติว่า “ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา” แล้ว ยังมิอาจแปลความได้ว่าม้าโทรจันและสปายแวร์จัดเป็นชุดคำสั่งไม่พึงประสงค์ตามความหมายดังกล่าว เนื่องจาก คุณสมบัติของม้าโทรจันและสปายแวร์มิได้มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด (สามารถดูข้อมูลสรุปคุณสมบัติของชุดคำสั่งไม่พึงประสงค์และการมีผลกระทบต่อข้อมูลคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เมื่อถูกนำไปใช้ในการกระทำความผิดได้ที่ ภาพ 2.6 ตามที่ได้กล่าวไปแล้วในบทที่ 2 ข้อที่ 3 (ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย))

เพื่อประกอบการทำความเข้าใจในประเด็นปัญหานี้ ผู้เขียนจะยกตัวอย่างและข้อเท็จจริงประกอบ คือ หากมีกรณีการแพร่ระบาดของม้าโทรจันและสปายแวร์ผ่านทางอีเมล์ และมีประชาชนที่ได้รับความเสียหายแจ้งและร้องเรียนปัญหาดังกล่าวมายังพนักงานเจ้าหน้าที่เพื่อขอให้ดำเนินการกำจัดหรือปราบปรามม้าโทรจันและสปายแวร์ดังกล่าว แต่ประชาชนผู้ได้รับความ

เสียหายนั้นไม่ยอมมาแจ้งความหรือร้องเรียนด้วยตนเอง ซึ่งจะทำให้พนักงานเจ้าหน้าที่ไม่เกิดอำนาจในการดำเนินการสืบสวน สอบสวน เพราะถือว่าเป็นกรณีที่มิได้มีการแจ้งความร้องทุกข์[170] กรณีดังกล่าวนี้จะทำให้พนักงานเจ้าหน้าที่มิอาจใช้อำนาจใดๆ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดำเนินการกับปัญหานี้ได้เลย แต่หากมีการแจ้งความร้องทุกข์ก็จะทำให้พนักงานเจ้าหน้าที่เกิดอำนาจในการสืบสวน สอบสวน และอาจใช้อำนาจตามมาตรา 18 (1) ที่ให้พนักงานเจ้าหน้าที่สามารถส่งหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดนั้นมาให้ถ้อยคำหรือชี้แจงได้ (2) ให้เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการได้ (3) สั่งให้ส่งมอบข้อมูลของผู้ใช้บริการที่ผู้ให้บริการต้องจัดเก็บได้ ซึ่งทั้งสามอนุมาตราดังกล่าวพนักงานเจ้าหน้าที่สามารถกระทำได้เอง หรือใช้อำนาจตาม (4) การทำสำเนาข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ (5) การสั่งให้ผู้ซึ่งครอบครองข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ (6) การตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ (7) การถอดรหัสลับข้อมูลคอมพิวเตอร์ และ (8) การยึดหรืออายัดระบบคอมพิวเตอร์นั้น พนักงานเจ้าหน้าที่จะกระทำได้เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดของผู้กระทำความผิด แต่การดำเนินการตามสี่อนุมาตรานี้พนักงานเจ้าหน้าที่ไม่สามารถกระทำได้เองแต่ต้องมีการขออนุญาตจากศาลก่อน

อย่างไรก็ตาม ไม่ว่าประชาชนผู้ได้รับความเสียหายเนื่องจากการแพร่ระบาดของม้าโทรจันและสปายแวร์ดังกล่าว จะแจ้งความหรือไม่แจ้งความร้องทุกข์ แต่ในที่สุดแล้ว ก็จะต้องติดกับประเด็นปัญหาที่ว่า คุณสมบัติของมาโทรจันและสปายแวร์ไม่เข้าข่ายและอยู่ในความหมายของชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคสอง ที่พนักงานเจ้าหน้าที่จะสามารถดำเนินการใดๆ ต่อไปได้ ไม่ว่าจะเป็นการดำเนินคดีกับผู้ที่ปล่อยให้ม้าโทรจันและสปายแวร์แพร่ระบาด หรือการยื่นคำร้องต่อศาลเพื่อขอให้ศาลมีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ หรือสั่งให้เจ้าของ

---

170 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 29 บัญญัติเพื่อให้อำนาจในการสืบสวน สอบสวน คดีความผิดเกี่ยวกับคอมพิวเตอร์แก่พนักงานเจ้าหน้าที่ไว้ ความว่า

"มาตรา 29 ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์ หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตาม

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป"

หรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ที่มีม้าโทรจันและสปายแวร์ติดตั้งหรือฝังตัวอยู่ได้ หรือจะขอให้ศาลมีคำสั่งเพื่อกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวนั้นก็ไม่ได้อีกเช่นกัน สาเหตุที่ดำเนินคดีไม่ได้นี้ มิใช่เพราะไม่มีพยานหลักฐาน[171] ที่จะสามารถประกอบการดำเนินคดีได้ แต่เป็นเพราะม้าโทรจันและสปายแวร์ไม่จัดอยู่ในชุดคำสั่งไม่พึงประสงค์ตามนัยแห่งมาตรา 21 วรรคสอง และยังมีปัญหาในการใช้และการตีความกฎหมายอื่นๆ อีกหลายประเด็น ได้แก่ ปัญหาที่กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง ปัญหาที่กฎหมายอาญาต้องตีความโดยเคร่งครัด และปัญหาความสัมพันธ์ระหว่างการกระทำและผล ซึ่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยไม่มีความชัดเจนในประเด็นเหล่านั้นอย่างเพียงพอ ซึ่งผู้เขียนจะได้กล่าวถึงและวิเคราะห์ประเด็นปัญหาเหล่านั้นอย่างละเอียด ต่อไป

3.2 การมิได้แยกแยะประเภทของชุดคำสั่งไม่พึงประสงค์

นับแต่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้เรื่อยมาจนถึงปัจจุบันนั้น ยังมิได้มีการแยกแยะประเภทของชุดคำสั่งไม่พึงประสงค์ หรือมีการประกาศรับรองชุดคำสั่งไม่พึงประสงค์ที่ถือเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่น ตามความหมายและเจตนารมณ์ของมาตรา 21 วรรคสอง แต่อย่างใด จึงส่งผลทำให้ชุดคำสั่งใดก็ตามที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ถูกสันนิษฐานโดยผลของกฎหมายไว้ก่อนว่า เป็นชุดคำสั่งไม่พึงประสงค์ จึงเท่ากับว่าปัจจุบันยังไม่มีชุดคำสั่งไม่พึงประสงค์ใดที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันและแก้ไขชุดคำสั่งอื่นเลย ทั้งที่ในความเป็นจริงแล้วยังมีชุดคำสั่งอีกหลายประเภทที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์อื่นที่ถูกพบเห็นและนำมาใช้ในชีวิตประจำวันของประชาชนทั่วไป เช่น โปรแกรมต่อต้านและตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ หรือม้าโทรจัน โปรแกรมต่อต้านการส่งสแปมเมล์ เป็นต้น

---

171 ในเชิงเทคนิคและเชิงวิชาการของศาสตร์ด้านการพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ (Computer Forensics) นั้น สามารถที่จะหาพยานหลักฐานมาดำเนินคดีกับผู้กระทำผิดได้ โดยอาศัยอำนาจตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในมาตรา 18 ประกอบมาตรา 25 และมาตรา 26 ซึ่งพยานหลักฐานทางคอมพิวเตอร์หรือทางอิเล็กทรอนิกส์นี้ เป็นศาสตร์อีกหนึ่งศาสตร์ที่มีรายละเอียดอย่างกว้างขวาง ซึ่งผู้เขียนจะไม่ขอกล่าวถึงรายละเอียดในวิทยานิพนธ์ฉบับนี้

ด้วยเหตุที่มิได้มีการแยกแยะและประกาศรับรองชุดคำสั่งไม่พึงประสงค์ดังกล่าว จึงทำให้พนักงานเจ้าหน้าที่และประชาชนเกิดความสับสนและความไม่แน่ใจในทางปฏิบัติและมิได้เป็นไปตามเจตนารมณ์ที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่บัญญัติให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารซึ่งอยู่ในฐานะผู้รักษาการกฎหมายฉบับนี้เป็นผู้ประกาศเพื่อรับรองชุดคำสั่งคอมพิวเตอร์ไม่พึงประสงค์ที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าว จุดนี้เองได้กลายเป็นปัญหาและอุปสรรคสำคัญที่พนักงานเจ้าหน้าที่ยังไม่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นในกรณีที่พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วยได้ กล่าวคือ ตราบใดที่ยังมิได้มีประกาศดังกล่าวของรัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร พนักงานเจ้าหน้าที่ก็จะไม่อาจทราบได้เลยว่าชุดคำสั่งไม่พึงประสงค์ใดเป็นชุดคำสั่งที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่น จึงทำให้การบังคับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในมาตรา 21 ที่มีเจตนารมณ์ในการป้องกันและปราบปรามปัญหาเกี่ยวกับการใช้ชุดคำสั่งไม่พึงประสงค์ยังไม่สมบูรณ์และไม่สามารถบรรลุวัตถุประสงค์ตามเจตนารมณ์ของกฎหมายได้อย่างแท้จริง

4. ปัญหาในการบัญญัติกฎหมาย

หากย้อนไปเมื่อประมาณปี พ.ศ.2541 ซึ่งเป็นปีที่มีการยกร่างกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งในขณะนั้นอาชญากรรมทางคอมพิวเตอร์ถือเป็นเรื่องใหม่มากสำหรับประเทศไทย ดังนั้น ข้อบกพร่องในการบัญญัติกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็ย่อมต้องมีหรือเกิดขึ้นได้บ้าง ซึ่งก็ถือเป็นเรื่องปกติธรรมดาที่ย่อมต้องเกิดขึ้นกับกฎหมายที่มีการบัญญัติขึ้นมาใหม่เสมอ ทั้งนี้มาตรการสำหรับดำเนินการในส่วนที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ตามที่ปรากฏในมาตรา 21 นั้น ก็มิได้ปรากฏขึ้นในชั้นการยกร่างกฎหมาย แต่ได้มีการเพิ่มเติมขึ้นในชั้นการตรวจพิจารณาร่างกฎหมายโดยสำนักงานคณะกรรมการกฤษฎีกา ที่อาจจะมิได้มีการศึกษาข้อเท็จจริงให้ละเอียดลึกซึ้งเพียงพอเสียก่อนว่า ในทางปฏิบัติและการบังคับใช้กฎหมายจะประสบกับปัญหาใดได้บ้าง และในชั้นการพิจารณาของสภาก็มิได้มีการกลั่นกรองในกรณีดังกล่าวด้วยเช่นกัน ดังนั้นรูปร่างหน้าตาและมาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ทั้งในส่วนของกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงปรากฏออกมาเป็นอย่างที่เห็นและได้กล่าวถึงในรายละเอียดไป

แล้วในบทที่ 4 สำหรับในส่วนนี้ จะขอกล่าวถึงในเชิงการวิเคราะห์ปัญหาทางกฎหมายที่เกิดจากการบัญญัติกฎหมายเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ ซึ่งสามารถสรุป ได้ดังนี้

4.1 การกำหนดนิยามและความหมายทางเทคนิค

การกำหนดฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ไว้ตั้งแต่มาตรา 5 ถึงมาตรา 13 นั้น ก็เพื่อให้ครอบคลุมถึงลักษณะของการกระทำความผิดที่จะส่งผลกระทบและเกี่ยวข้องโดยตรงกับคอมพิวเตอร์ซึ่ง ได้แก่ การส่งผลกระทบต่อการรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และเสถียรภาพในการใช้งาน (Availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เช่น การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ การดักรับข้อมูลคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ความผิดเกี่ยวกับสแปมเมล์ การรบกวนระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่กระทบต่อความมั่นคงของประเทศ ความปลอดภัยของสาธารณะ ความมั่นคงในทางเศรษฐกิจ และการบริการสาธารณะ เป็นต้น นอกจากนี้ยังต้องการให้ครอบคลุมถึงการนำคอมพิวเตอร์ไปใช้เป็นเครื่องมือในการกระทำความผิดซึ่งอาจเรียกได้ว่าเป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ (ความผิดฐานการล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบนี้หากมีการเข้าถึงโดยมิชอบเพื่อการล่วงรู้ก็จะจัดอยู่ในประเภทความผิดที่กระทำต่อคอมพิวเตอร์โดยแท้ด้วย) การเผยแพร่ชุดคำสั่งไม่พึงประสงค์ที่ใช้ในการกระทำความผิด การเผยแพร่เนื้อหาอันไม่เหมาะสมหรือเป็นเท็จ รวมทั้งข้อมูลคอมพิวเตอร์อันลามกทั้งหลาย เป็นต้น

อย่างไรก็ตาม การบัญญัติกฎหมายเพื่อให้ครอบคลุมถึงลักษณะของการกระทำความผิดดังกล่าว ยังมิอาจครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์ได้ทั้งหมด กล่าวคือ ปัจจุบันมีการก่ออาชญากรรมทางคอมพิวเตอร์โดยใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดโดยการจัดทำและเผยแพร่โปรแกรมหรือชุดคำสั่งที่ไม่พึงประสงค์ผ่านทางเครือข่ายคอมพิวเตอร์อย่างแพร่หลายเพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ ความครบถ้วน และเสถียรภาพในการใช้งานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชน โดยเฉพาะอย่างยิ่งการนำข้อมูลเอกลักษณ์บุคคลที่ได้ไปก่ออาชญากรรมทางด้านการเงินหรือด้านอื่นๆ ต่อไป โดยชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์ที่เมื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดแล้ว จะไม่มีผลทำให้

ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ตามความหมายในมาตรา 21 วรรคสอง จึงมิอาจปรับบทฐานความผิดใดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้เข้ากับพฤติการณ์ดังกล่าวได้ และไม่ถือเป็นความผิดตามพระราชบัญญัติอื่นที่มีโทษทางอาญาเลยตามที่ได้กล่าวถึงไปแล้วในบทที่ 4

หากพิจารณาถึงองค์ประกอบของฐานความผิดข้างต้นแล้วจะพบว่า ลักษณะและพฤติการณ์ของการกระทำความผิดที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำนั้น มีลักษณะเป็นการเข้าถึง (access) ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ด้วยวิธีการทางอิเล็กทรอนิกส์หรือทางดิจิทัลทั้งในเชิงของการบุกรุกทางคอมพิวเตอร์ (computer trespass) หรือการเจาะเข้าไปในระบบ (Hacking or Cracking) และในเชิงของการดักข้อมูล (interception) ซึ่งผู้เขียนเห็นว่าการดักข้อมูลก็เป็นการเข้าถึงอีกรูปแบบหนึ่งด้วยเช่นกัน

ทั้งนี้ จากการศึกษาพบว่าความหมายของการเข้าถึงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทย มีความแตกต่างกับความหมายของการเข้าถึงในกฎหมายของต่างประเทศอย่างมีนัยสำคัญ กล่าวคือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้กำหนดนิยามความหมายของคำว่า “เข้าถึง (access)” ไว้โดยตรง จึงเป็นหน้าที่ของผู้ปรับใช้กฎหมายที่จะต้องใช้ดุลพินิจในการตีความเอาเองว่าจะให้ความหมายของคำว่า “เข้าถึง” นี้ มีความหมายเพียงใด ซึ่งเมื่อได้อ่านและอนุมานจากความหมายในมาตรา 5 และมาตรา 7 ในความผิดฐานการเข้าถึงโดยไม่มีอำนาจซึ่งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนแล้ว ทำให้เข้าใจความหมายของคำว่า “เข้าถึง” ได้ว่า หมายถึง เป็นการกระทำด้วยวิธีการใดๆ ไม่ว่าทั้งทางดิจิทัลหรือทางกายภาพเพื่อให้สามารถเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ผู้กระทำประสงค์จะเข้าถึง และเมื่อสามารถเข้าถึงได้แล้ว ก็ย่อมจะถือว่าการกระทำการเข้าถึงดังกล่าวได้สำเร็จลงแล้ว แต่ภายหลังจากนั้นไม่ว่าจะเกิดอะไรขึ้น เช่น มีการทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ หรือทำการรบกวนต่างๆ จนทำให้ระบบคอมพิวเตอร์หยุดทำงานนั้นก็ยังอยู่ในความหมายของการเข้าถึงนี้อยู่ แต่หากมีกรณีการได้ใช้ประโยชน์อื่นใดภายหลังจากการเข้าถึงที่ไม่เข้ากรณีดังกล่าว เช่น (1) มีการทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ (2) การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการเพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์หรือได้รับข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ดังกล่าว หรือ (3) การสั่งการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วย

ประมวลผลหรือหน่วยบันทึกผลของระบบคอมพิวเตอร์อื่นได้ (การสั่งการตาม (2) และ (3) นี้เป็นการกระทำในเชิงของการใช้คอมพิวเตอร์ของเหยื่อเป็นฐานทัพหรือเป็นเครื่องมือสำหรับการเข้าถึงระบบคอมพิวเตอร์อื่นต่อไป) ตลอดจนการกระทำการอื่นใดเพื่อแสวงหาประโยชน์จากระบบคอมพิวเตอร์ที่ถูกเข้าถึงโดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้นั้น

ดังนั้น ความหมายของคำว่า “เข้าถึง” ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยคงบังคับและตีความไปไม่ถึงการกระทำดังกล่าวได้ เพราะหลักการตีความกฎหมายอาญาต้องตีความโดยเคร่งครัดและเป็นไปตามหลักสากลที่ว่า “ไม่มีกฎหมาย ไม่มีความผิด” และรัฐธรรมนูญแห่งราชอาณาจักรไทย ฉบับปัจจุบัน (พ.ศ. 2550) ก็ได้รับรองหลักดังกล่าวโดยบัญญัติไว้ในหมวด 3 สิทธิและเสรีภาพของชนชาวไทย ส่วนที่ 4 สิทธิในกระบวนการยุติธรรม ว่า "มาตรา 39 ...บุคคลไม่ต้องรับโทษอาญา เว้นแต่ได้กระทำการอันกฎหมายที่ใช้อยู่ในเวลาที่กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแก่บุคคลนั้นจะหนักกว่าโทษที่กำหนดไว้ในกฎหมายที่ใช้อยู่ในเวลาที่กระทำความผิดมิได้" ในขณะที่ประมวลกฎหมายอาญาก็ได้บัญญัติไว้ทำนองเดียวกันว่า "มาตรา 2 บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะ กระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้ และโทษที่จะลงแต่ผู้กระทำความผิดนั้น ต้องเป็นโทษที่บัญญัติไว้ในกฎหมาย”[172]

เมื่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยมิได้กำหนดนิยามหรือความหมายของการเข้าถึงไว้ จึงทำให้ความหมายของคำว่า “เข้าถึง” ตามกฎหมายไทยเป็นไปในเชิงที่แคบกว่าคำว่า “เข้าถึง” ในกฎหมายของต่างประเทศ จนกลายเป็นช่องว่างของกฎหมายไทยและเป็นอุปสรรคสำคัญในการบังคับใช้กฎหมายดังกล่าว

---

172 หลักการตีความกฎหมายอาญาต้องตีความโดยเคร่งครัดนี้ ศาสตราจารย์จิตติ ติงศภัทิย์ ได้อธิบายไว้ในหนังสือกฎหมายอาญาภาค 1 ซึ่งพิมพ์โดยสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา พ.ศ. 2536 หน้า 39 ว่า “หลักที่ว่าจะลงโทษบุคคลในทางอาญาได้ ต่อเมื่อกฎหมายบัญญัติว่า การกระทำเช่นนั้นเป็นความผิดมีผลอยู่ในตัวเองว่า กฎหมายที่บัญญัติความผิดเช่นนั้น จะต้องบัญญัติโดยชัดแจ้งว่าการกระทำอย่างใดเป็นความผิด การตีความในกฎหมายนั้นจึงต้องพิจารณาตามตัวอักษร จะขยายความในบทกฎหมายออกไปถึงกรณีที่ไม่ระบุไว้ให้ชัดว่าเป็นความผิดด้วยย่อมไม่ตรงกับหลักที่กล่าวนั้น”

เพื่อประกอบความเข้าใจในความแตกต่างระหว่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยกับกฎหมายของต่างประเทศในประเด็นปัญหาการกำหนดนิยามและความหมายทางเทคนิคของการเข้าถึงในทางคอมพิวเตอร์ ผู้เขียนจึงจะขอเปรียบเทียบความหมายของคำว่า “เข้าถึง (access)” ตามกฎหมายของประเทศไทยกับกฎหมายของต่างประเทศ และตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป ดังนี้

4.1.1 เปรียบเทียบความหมายคำว่า “เข้าถึง (access)” ในกฎหมายต่างประเทศกับกฎหมายไทย

หากพิจารณาถึงความหมายคำว่า “เข้าถึง (access)” ในกฎหมายต่างประเทศตามที่ได้กล่าวไปแล้วใน บทที่ 3 ข้อ 1 (มาตรการกำหนดนิยามและความหมายของการเข้าถึง (access) ให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์) จะพบว่า มีความแตกต่างจากความหมายตามกฎหมายว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยและอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรปอย่างมีนัยสำคัญ กล่าวคือ ความหมายของคำว่า “เข้าถึง” ในกฎหมายต่างประเทศตามที่ยกตัวอย่างมา ได้แก่ ประเทศออสเตรเลีย ประเทศนิวซีแลนด์ ประเทศอินเดีย และประเทศสหรัฐอเมริกา นั้น มิได้มีขอบเขตครอบคลุมแต่เฉพาะเมื่อการเข้าถึงที่ได้กระทำให้สำเร็จลงแล้วเท่านั้น แต่ยังมีความหมายครอบคลุมไปถึงการกระทำที่จะเกิดขึ้นต่อไปอีกด้วย เช่น หากมีการทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือมีการสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการเพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์ หรือได้รับข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ดังกล่าว หรือมีการสั่งการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลหรือหน่วยบันทึกผลของระบบคอมพิวเตอร์อื่นได้ เป็นต้น

ดังนั้น เมื่อเปรียบเทียบความหมายคำว่า “เข้าถึง” ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยกับกฎหมายต่างประเทศแล้ว จึงทำให้เกิดปัญหาทางกฎหมายและกลายเป็นช่องว่างของกฎหมายไทย ที่ไม่สามารถปรับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยให้ครอบคลุมถึงพฤติการณ์และข้อเท็จจริงที่จะเกิดขึ้นต่อไปภายหลังจากที่การเข้าถึงสำเร็จลงแล้วได้ ตามที่ได้ยกเป็นตัวอย่างไปข้างต้น

อนึ่ง สำหรับมาตรการทางกฎหมายเกี่ยวกับการขโมยเอกลักษณ์บุคคล (Identity Theft) และกรณีตัวอย่างคดีในต่างประเทศตามที่ได้กล่าวถึงไปในบทที่ 2 หัวข้อที่ 6.1.1 (การขโมยเอกลักษณ์บุคคล (Identity theft) ด้วยมัลแวร์) นั้น อาจกล่าวได้ว่าเป็นมาตรการทาง

กฎหมายที่สามารถนำมาป้องกันและแก้ไขปัญหาที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์โดยการขโมยข้อมูลที่แสดงถึงตัวตนหรือเอกลักษณ์ของบุคคลและเป็นข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ได้เป็นอย่างดี เพราะไม่ว่าจะมีการกระทำความผิดในลักษณะใดก็ตาม หากการกระทำความผิดนั้นทำให้ได้ไปซึ่งข้อมูลเอกลักษณ์บุคคลก็จะสามารถปรับเข้ากับหลักกฎหมายดังกล่าวได้

อย่างไรก็ตาม ในปัจจุบันประเทศไทยยังไม่มีแนวคิดหรือมาตรการทางกฎหมายที่คล้ายคลึงหรือใกล้เคียงกับมาตรการทางกฎหมายเกี่ยวกับการขโมยเอกลักษณ์ตามกฎหมายของต่างประเทศ จะมีก็เพียงแต่มาตรการทางกฎหมายเกี่ยวกับการขโมยเอกลักษณ์บุคคล (Identity theft) ในรูปแบบของการปลอมแปลงบัตรอิเล็กทรอนิกส์ตามประมวลกฎหมายอาญาที่ได้กล่าวไปแล้วใน บทที่ 4 ข้อ 3 ซึ่งได้กล่าวถึงและเปรียบเทียบไปแล้วว่า บทบัญญัติในประมวลกฎหมายอาญาตั้งแต่มาตราที่ 269/1 ถึงมาตรา 269/7 (ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์) มิอาจนำมาปรับใช้กับการขโมยข้อมูลด้วยชุดคำสั่งไม่พึงประสงค์ได้ ซึ่งความเป็นจริงและปัญหาสำหรับประเทศไทยในวันนี้ก็คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิอาจแก้ไขปัญหาหรือภัยคุกคามที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ครอบคลุมทุกกรณี ดังนั้น จะมีวิธีการเช่นไรที่จะสามารถปรับใช้กฎหมายที่มีอยู่ให้ทันต่อความผิดและปัญหาที่เกิดขึ้น ซึ่งสมควรที่จะหาทางแก้ไขโดยการปรับแก้หรือเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อรับมือกับภัยดังกล่าวนี้ให้ดียิ่งขึ้น

4.1.2 เปรียบเทียบความหมายคำว่า “เข้าถึง (access)” ในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์กับกฎหมายไทย

จากการศึกษาและค้นคว้าเอกสารรายงานคำอธิบายเกี่ยวกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป ส่วนที่ 46 ได้อธิบายความหมายของคำว่า “เข้าถึง (access)” ไว้ว่า “เข้าถึง หมายความว่า การเข้าสู่ระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วน ไม่ว่าจะเป็นการเข้าสู่ส่วนอุปกรณ์ ข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บไว้ในระบบการทำงานของระบบคอมพิวเตอร์ สารบบการทำงานของระบบคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลอื่นใดที่เกี่ยวข้อง ทั้งนี้ ให้รวมถึงการเข้าสู่ระบบคอมพิวเตอร์อื่นที่ได้เชื่อมต่อเข้ากับเครือข่าย

โทรคมนาคมสาธารณะ หรือระบบคอมพิวเตอร์ในเครือข่ายเดียวกัน โดยไม่คำนึงว่าการเชื่อมต่อดังกล่าวจะได้กระทำผ่านทางสายสัญญาณสื่อสารหรือไม่"[173]

จากคำอธิบายความหมายคำว่า "เข้าถึง" ดังกล่าวข้างต้น เมื่อเปรียบเทียบกับความหมายคำว่า "เข้าถึง" (ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยที่มิได้กำหนดนิยามความหมายไว้) ตามที่อาจารย์พรเพชร วิชิตชลชัย ได้อธิบายไว้ในคำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ว่า[174] "การเข้าถึง ตรงกับคำภาษาอังกฤษว่า "access" หมายถึง การเข้าถึงทั้งในระดับกายภาพ เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์ แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ นอกจากนั้นยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่างๆ ของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่นข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น ส่วนวิธีการเข้าถึงนั้นรวมทุกวิธีการไม่ว่าจะเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่นอินเทอร์เน็ตอันเป็นการเชื่อมโยงระหว่างเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน และยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN อันเป็นเครือข่ายที่เชื่อมต่อคอมพิวเตอร์ที่ตั้งอยู่ในพื้นที่ใกล้ๆ เข้าด้วยกัน นอกจากนี้ยังหมายความรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สายอีกด้วย" นั้น

ในมุมมองของผู้เขียนเห็นว่า ความหมายคำว่า "เข้าถึง" ทั้งของประเทศไทยและของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ต่างมีความหมายและเป็นไปในทำนองเดียวกันคือ เมื่อการเข้าถึงสำเร็จลงแล้วหากมีเหตุการณ์หรือการกระทำใดเกิดขึ้นต่อไป ก็จะไม่อยู่ใน

---

173 INTERPOL, Convention on Cybercrime (ETS No. 185) *Explanatory Report*., เอกสารรายงานคำอธิบายเกี่ยวกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป ในเว็บไซต์ http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm Retrieved December, 16, 2010

174 พรเพชร วิชิตชลชัย "คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550", เอกสารอิเล็กทรอนิกส์ หน้า 8 ซึ่งได้อ้างอีกชั้นหนึ่งว่า ได้ความหมายคำว่า "เข้าถึง" มาจากเอกสารชี้แจงของสำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ซึ่งใช้อธิบายประกอบเสนอร่างกฎหมายต่อคณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....

ความหมายของการเข้าถึงนี้ เหตุที่เป็นเช่นนั้นก็อาจเนื่องมาจากในชั้นการยกร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... ของประเทศไทยนั้นส่วนใหญ่ได้นำแนวทางจากอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรปมาเป็นแม่แบบในการยกร่างกฎหมายดังกล่าว

4.2 การกำหนดฐานความผิด

ปัญหาทางกฎหมายที่สำคัญอีกประการหนึ่งก็คือ การกำหนดฐานความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ยังไม่ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ทั้งหมด กล่าวคือ แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดฐานความผิดและบทลงโทษสำหรับผู้ที่จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 ถึงมาตรา 11 ให้ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับไว้ในมาตรา 13 (ซึ่งการบัญญัติเช่นนั้นของมาตรา 13 ดังกล่าวถือว่าเป็นการรับรองโดยนัยของกฎหมายว่าชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะหมายถึง ชุดคำสั่งไม่พึงประสงค์ตามความหมายในมาตรา 21 วรรคสองนั่นเอง) และมีมาตรการในการดำเนินการเกี่ยวกับโปรแกรมหรือชุดคำสั่งคอมพิวเตอร์ไม่พึงประสงค์ไว้ในมาตรา 21 แล้วก็ตาม แต่บทบัญญัติในมาตราดังกล่าวยังมีความไม่ชัดเจนในทางปฏิบัติที่จะสามารถเอื้ออำนวยและใช้เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ให้มีประสิทธิภาพและประสิทธิผลได้อยู่สองประการตามที่ได้กล่าวไปแล้วในข้อ 2.1 ข้างต้น

ทั้งนี้ หากพิจารณาความหมายของ “ชุดคำสั่งไม่พึงประสงค์” ตามความในมาตรา 21 วรรคสอง แล้วนั้น ผู้เขียนเห็นว่า ยังไม่ครอบคลุมถึงลักษณะของการกระทำความผิดที่เกิดขึ้นจริงซึ่งกำลังเป็นที่นิยมกระทำกันอย่างแพร่หลายในบรรดาหมู่อาชญากรจนก่อปัญหาและส่งผลเสียหายต่อประชาชนและประเทศชาติอย่างมากในปัจจุบันนี้ กล่าวคือ มีการก่ออาชญากรรมคอมพิวเตอร์โดยใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดโดยการจัดทำและเผยแพร่โปรแกรมหรือชุดคำสั่งที่ไม่พึงประสงค์ผ่านทางเครือข่ายคอมพิวเตอร์อย่างแพร่หลายเพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชนเป็นอย่างมาก โดยเฉพาะอย่างยิ่งการนำข้อมูลที่ได้ไปก่ออาชญากรรมด้านการเงินหรืออาชญากรรมอื่นต่อไป โดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นที่อยู่ในระบบคอมพิวเตอร์ของเจ้าของ

ข้อมูลนั้นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้เมื่อมีการใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดแต่อย่างใด

ตัวอย่างชุดคำสั่งไม่พึงประสงค์เหล่านั้นได้แก่ ม้าโทรจันและสปายแวร์ ที่เมื่อถูกส่งและนำไปฝังไว้ในระบบคอมพิวเตอร์ของผู้อื่นแล้วมักจะมีการแอบส่งข้อมูลคอมพิวเตอร์ หรือแอบดักข้อมูลต่างๆ ผ่านปุ่มคีย์บอร์ด (Keylogger หรือ Keystroke) เพื่อบันทึกการกดรหัสผ่านของผู้อื่น ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลสำคัญที่เป็นเอกลักษณ์บุคคลส่งออกไปยังคนร้ายหรือผู้บุกรุก ทั้งนี้ หากการกระทำความผิดดังกล่าวเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เป็นการเข้าไปทำลาย แก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือเป็นการเข้าไปรบกวนต่อระบบคอมพิวเตอร์โดยการฝ่าฝืนมาตรการป้องกันที่จัดทำไว้เป็นการเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ก็จะถือเป็นความผิดตามมาตรา 5 ถึง มาตรา 11 ได้[175] แต่ประเด็นปัญหาที่จะเกิดขึ้นและเป็นประเด็นของการวิจัยในวิทยานิพนธ์นี้ก็คือ หากการเข้าถึงตามตัวอย่างดังกล่าวนั้นเป็นการเข้าถึงโดยชอบไม่ว่าจะเป็นเพราะความยินยอมของเจ้าของคอมพิวเตอร์นั้น หรือในบางกรณีแฮกเกอร์หรือคนร้ายอาจใช้เทคนิคการหลอกล่อเพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป แล้วต่อมามีการแอบส่งข้อมูลคอมพิวเตอร์ออกไปยังคนร้าย ก็จะทำให้การเข้าถึงในกรณีนี้ไม่เข้าข่ายเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

นอกจากนี้ การกระทำดังกล่าวก็ไม่เป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญาเพราะขาดซึ่งองค์ประกอบของความผิดสำคัญที่ว่าข้อมูลคอมพิวเตอร์ไม่ใช่ทรัพย์ตามนิยามและความหมายในประมวลกฎหมายแพ่งและพาณิชย์ และไม่เป็นความผิดตามพระราชบัญญัติอื่นที่มีโทษทางอาญาเลย ทั้งนี้ประเด็นการขโมยหรือแอบส่งหรือแอบดักข้อมูลด้วยม้าโทรจันหรือสปายแวร์ยังถือเป็นการกระทำละเมิดต่อข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์อีกด้วย ซึ่งปัจจุบันก็ยังไม่มีกฎหมายใดที่จะสามารถปรับใช้เพื่อการป้องกันหรือปราบปรามการกระทำความผิดดังกล่าวได้ ตามที่ได้กล่าวถึงไปแล้วในบทที่ 4 ข้อ 4 (มาตรการทางกฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในรูปแบบข้อมูลคอมพิวเตอร์)

---

175 การปรับบทฐานความผิดตั้งแต่มาตรา 5 ถึงมาตรา 11 ขึ้นอยู่กับว่าเป็นการเข้าถึงต่ออะไร เช่น หากเข้าถึงซึ่งระบบคอมพิวเตอร์ก็เป็นความผิดตามมาตรา 5 แต่หากเป็นการเข้าถึงซึ่งข้อมูลคอมพิวเตอร์ก็จะเป็นความผิดตามมาตรา 7 เป็นต้น

4.2.1 ความหมายคำว่า “โดยมิชอบ”

เนื่องจากองค์ประกอบของความผิดในการเข้าถึงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น มีองค์ประกอบที่สำคัญอีกหนึ่งองค์ประกอบคือ การเข้าถึงนั้นจะต้องเป็นการเข้าถึงโดยมิชอบ ซึ่งผู้เขียนเห็นว่าองค์ประกอบของความผิด “เข้าถึงโดยมิชอบ” เป็นการรวมคำสองคำเข้าด้วยกัน คือ คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” แต่มิได้หมายความว่าเมื่อนำไปปรับใช้กับฐานความผิดการเข้าถึงโดยมิชอบแล้วจะต้องตีความรวมเป็นคำเดียวกัน แต่ในทางตรงกันข้ามผู้เขียนเห็นว่า คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” จะต้องตีความแยกออกจากกัน โดยความหมายของคำว่า “เข้าถึง” นั้น ผู้เขียนได้ศึกษาและวิเคราะห์ไปแล้วว่า มีความหมายและขอบเขตเพียงใดบ้าง โดยเฉพาะการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลโดยใช้ชุดคำสั่งไม่พึงประสงค์ในการเข้าถึง พร้อมทั้งได้ให้ความเห็นและได้ทำการเปรียบเทียบกับกฎหมายของต่างประเทศและได้ชี้ให้เห็นถึงช่องว่างของกฎหมายไทยที่มิได้มีการกำหนดนิยามและความหมายของคำว่า “เข้าถึง” ไว้ จนทำให้เกิดปัญหาในทางกฎหมายและเป็นที่มาของประเด็นการวิจัยตามวิทยานิพนธ์นี้ ตามที่ได้กล่าวไปแล้ว นั้น

ต่อไปนี้ จะเป็นการพิจารณาถึงความหมายและขอบเขตของคำว่า “โดยมิชอบ” ซึ่งคำว่า “โดยมิชอบ” นี้ ได้มีผู้ทำการศึกษาและวิจัยไว้ในระดับหนึ่งแล้ว ซึ่งมีทั้งส่วนที่ผู้เขียนเห็นด้วยและไม่เห็นกับงานวิจัยนั้น โดยงานวิจัยเกี่ยวกับคำว่า “โดยมิชอบ” นี้ มีวิทยานิพนธ์ฉบับแรกได้สรุปเกี่ยวกับคำว่า “โดยมิชอบ” ไว้ ดังนี้[176]

คำว่า “โดยมิชอบ” มีใช้อยู่ในบทบัญญัติที่แตกต่างกันย่อมมีความหมายตามบริบทของบทบัญญัตินั้น ดังนั้นคำว่า “โดยมิชอบ” จึงเป็นคำที่มีลักษณะเป็นกลางแล้วแต่ผู้ใช้กฎหมายจะเป็นผู้ตีความให้เหมาะสมว่า “โดยมิชอบ” นั้น จะหมายถึงลักษณะการกระทำเช่นใด ซึ่งอาจแยกแยะประเภทการกำหนดหลักเกณฑ์ในการแปลความหมายของคำว่า “โดยมิชอบ” ได้ใน 3 ลักษณะใหญ่ๆ คือ ไม่ชอบด้วยกฎหมาย (Illegal) โดยปราศจากอำนาจ (Unauthorized) และไม่เหมาะสม ไม่ถูกต้อง (Improper)

หากคำว่า “โดยมิชอบ” หมายถึง โดยมิชอบด้วยกฎหมาย (Illegal) แล้ว ย่อมหมายความว่า การกระทำนั้นจะเป็นความผิดเมื่อเป็นการฝ่าฝืนข้อห้ามหรือข้อบังคับที่มีกฎหมายห้ามมิให้กระทำไว้ หรือไม่มีอำนาจหน้าที่ตามกฎหมายให้กระทำได้ ซึ่งหากแปลความของคำว่า “โดยมิชอบ” หมายถึงโดยมิชอบด้วยกฎหมายแล้ว ก็จะเป็นการแปลความหมายที่ค่อนข้างแคบเนื่องจากจะหมายความว่าการเข้าถึงนั้นจะต้องไม่มีกฎหมายห้าม หรือเข้าถึงโดยชอบด้วยกฎหมายแล้ว

---

176 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 153-154

การเข้าถึงนั้นก็ย่อมไม่เป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด

การตีความเช่นนี้จะทำให้การกระทำหลายอย่างไม่สามารถลงโทษได้ เนื่องจากกฎหมายไม่ได้บัญญัติว่าการกระทำนั้นเป็นความผิด เช่น กรณีที่ไม่มีกำหนดห้ามแต่ผิดข้อสัญญาหรือข้อตกลงก็จะไม่เป็นความผิดเนื่องจากการกระทำนั้นเพียงแต่ผิดข้อสัญญาเท่านั้นไม่ได้ผิดกฎหมาย หรือกรณีที่ไม่มีอำนาจให้กระทำแต่การกระทำนั้นไม่ถึงขนาดไม่ชอบด้วยกฎหมาย การกระทำนั้นจะไม่เป็นความผิด โดยเฉพาะอย่างยิ่งกรณีที่มีอำนาจกระทำได้ตามอำนาจหน้าที่ หากแต่การกระทำนั้นเป็นไปเพื่อประโยชน์ส่วนตัวก็ไม่เป็นความผิดเช่นเดียวกัน เนื่องจากผู้กระทำมีอำนาจกระทำได้จึงไม่เป็นการไม่ชอบด้วยกฎหมายแต่อย่างใด

แต่ถ้าจะแปลความหมายของคำว่า “โดยมิชอบ” ว่าหมายถึงโดยปราศจากอำนาจ (Unauthorized) แล้ว จะมีความหมายกว้างกว่าที่จะแปลความว่าโดยมิชอบด้วยกฎหมาย โดยคำว่า โดยปราศจากอำนาจนั้นหมายถึง การทำโดยไม่มีอำนาจ หรือทำโดยไม่มีอำนาจอย่างชัดแจ้งหรือโดยปริยาย และการตีความว่าโดยมิชอบว่าหมายถึงโดยปราศจากอำนาจนี้ก็จะเหมือนกับความผิดในการเข้าถึงโดยปราศจากอำนาจในกฎหมายต่างประเทศ โดยในประเทศสหรัฐอเมริกาและอังกฤษ ก็ใช้ความหมายนี้ในการกำหนดว่าการเข้าถึงจะเป็นความผิดก็ต่อเมื่อเป็นการเข้าถึงโดยปราศจากอำนาจ ซึ่งจากการพิจารณาความหมายของคำว่า “โดยปราศจากอำนาจ” ที่ปรากฏอยู่ในกฎหมายต่างประเทศนั้น มีผู้สรุปได้ว่าการเข้าถึงโดยปราศจากอำนาจ อาจเทียบเคียงได้กับการเข้าถึงโดยไม่ได้รับอนุญาตนั่นเอง โดยอาจเกิดจากกฎเกณฑ์หรือสัญญาก็ได้

นอกจากการแปลความหมายคำว่า “โดยมิชอบ” ว่า หมายถึงโดยไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจแล้ว อาจจะสามารถแปลความคำว่าโดยมิชอบได้อีกทางหนึ่งที่มีความหมายครอบคลุมกว่าการแปลความในสองกรณีข้างต้นโดยอาศัยคำพิพากษาศาลฎีกาเป็นเกณฑ์ในการกำหนดหลักเกณฑ์ในการตีความ ซึ่งคำว่า “โดยมิชอบ” อาจตีความตามแนวคำพิพากษาของศาลฎีกาที่เคยพิจารณาคำว่า “โดยมิชอบ” ไว้ และเห็นได้ว่า มีความหมายค่อนข้างกว้างทั้งทางแพ่งและทางอาญา ตามแต่ละคดีที่ศาลเห็นสมควร เช่น ศาลฎีกาเคยตีความคำว่า “โดยมิชอบ” ไว้ว่าหมายถึง ปราศจากสิทธิโดยชอบ ไม่ระมัดระวังตามหน้าที่ ไม่ซื่อสัตย์สุจริต ประพฤติตนไม่สมควร ทุจริตต่อหน้าที่ ฝ่าฝืนต่อกฎระเบียบและคำสั่งของผู้บังคับบัญชา กระทำลงโดยไม่คำนึงถึงความเสียหายใดๆ ไม่ขวนขวายดำเนินการตามหน้าที่และระเบียบข้อบังคับ เบียดบังเวลาและทรัพย์สินของผู้อื่นเพื่อแสวงหาประโยชน์ส่วนตัว ทำให้ผู้อื่นได้รับประโยชน์โดยไม่ควร ละเว้นไม่ตรวจสอบความถูกต้องแท้จริง ฝ่าฝืนคำสั่ง ละเลยไม่ปฏิบัติหน้าที่ กระทำการนอกหน้าที่ ทำโดยปราศจากอำนาจ ขู่เข็ญใช้อำนาจครอบงำผิดคลองธรรม กระทำลงทั้งที่เล็งเห็นผลความเสียหายที่จะเกิดขึ้น

ฝ่าฝืนระเบียบ ใช้ดุลพินิจตามอำเภอใจหรือปราศจากเหตุผล การเลือกปฏิบัติ ใช้ประโยชน์จากทรัพย์สินของผู้อื่นโดยผู้นั้นไม่ยินยอม[177]

ทั้งนี้ วิทยานิพนธ์ฉบับดังกล่าวได้สรุปและเสนอความเห็นไว้ว่า การตีความคำว่าการเข้าถึง “โดยมิชอบ” นั้นไม่ควรที่จะกำหนดกฎเกณฑ์ว่าเป็นการมิชอบด้วยกฎหมายหรือปราศจากอำนาจอย่างเดียว เนื่องจากอาจก่อให้เกิดปัญหาในการลงโทษผู้กระทำผิดได้ เช่น หากการเข้าถึงนั้นชอบแล้ว แม้ต่อมาจะไปทำความผิดได้อีก หากไม่มีกฎหมายบัญญัติความผิดไว้ การกระทำนั้นก็ไม่เป็นความผิดอีก เช่น การขโมยข้อมูล เป็นต้น โดยควรปล่อยให้เป็นหน้าที่ของศาลที่จะตีความให้เหมาะสมกับพฤติกรรมของผู้กระทำผิดว่าเป็นการกระทำที่ไม่ชอบหรือไม่ เพื่อให้เกิดความเป็นธรรมในแต่ละคดี

นอกจากนี้ ยังมีวิทยานิพนธ์อีกฉบับหนึ่งที่ได้สรุปเกี่ยวกับคำว่า “โดยมิชอบ” ไว้ ดังนี้[178]

ประเภทหรือรูปแบบของคำว่า “โดยมิชอบ” อาจแบ่งได้เป็น 6 รูปแบบ คือ

1. โดยมิชอบด้วยกฎหมาย คือ การกระทำที่ไม่ถูกต้องตามกฎหมาย กฎระเบียบ ข้อบังคับ โดยรวมถึงการใช้ดุลพินิจที่ไม่สุจริตด้วย

2. โดยมิชอบด้วยหน้าที่ คือ การกระทำที่ไม่ถูกต้องตามหน้าที่ที่ควรกระทำ ควรละเว้นที่จะกระทำ แต่กลับไม่กระทำ ฝืนกระทำอันเป็นการขัดแย้งต่อหน้าที่ โดยหน้าที่อาจจะเป็นหน้าที่ตามกฎหมาย หรือหน้าที่ตามสัญญาก็ได้

3. โดยมิชอบตามสัญญา คือ การกระทำที่ไม่ถูกต้องตามขอบเขต เนื้อหา และวัตถุประสงค์ของสัญญา

4. โดยมิชอบต่อหลักศาสนา คือ การกระทำที่ไม่ชอบด้วยหลักแห่งศาสนา

5. โดยไม่ชอบด้วยกฎหมาย คือ การกระที่เป็นการฝ่าฝืน กฎ ระเบียบ ข้อบังคับ หรือเป็นการกระทำที่ฝ่าฝืนวัตถุประสงค์ของกฎหมาย ไม่ว่าการกระทำดังกล่าวะกระทำไปโดยสุจริต หรือทุจริตก็ตาม คำว่า “ไม่ชอบด้วยกฎหมาย” เป็นถ้อยคำที่มาจากกฎหมายปกครอง

6. โดยผิดกฎหมาย กระทำโดยไม่ชอบด้วยกฎหมาย ส่วนการกระทำที่เป็นการผิดสัญญานั้นไม่เป็นการผิดกฎหมาย เว้นแต่จะทำให้คู่สัญญาอีกฝ่ายเสียหายต่อสิทธิตามกฎหมายด้วยการกระทำซึ่งมีกฎหมายบัญญัติว่าเป็นความผิด

---

177 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 157-159

178 ชาตรี ส่งสัมพันธ์, อ้างแล้วในเชิงอรรถที่ 77 หน้า 34-35

ทั้งนี้ วิทยานิพนธ์ฉบับที่สองนี้ได้สรุปเกี่ยวกับคำว่า “โดยมิชอบ” อาจมีความหมายอย่างกว้างได้ว่า เป็นการกระทำโดยไม่เหมาะสม ไม่สุจริต ปราศจากสิทธิอันชอบธรรม หรือไม่ได้รับอนุญาต โดยครอบคลุมถึงการกระทำของผู้ที่ได้รับอนุญาตที่กระทำการเกินขอบอำนาจ หรือไม่เกินขอบอำนาจเท่านั้นแต่รวมถึงกระทำโดยไม่สุจริต หรือไม่ถูกต้อง ไม่เหมาะสม จึงมีความหมายกว้างกว่า “โดยมิชอบด้วยกฎหมาย” ในส่วนความหมายของ “โดยมิชอบ” สมควรให้อำนาจศาลมีดุลพินิจในการพิจารณาให้เหมาะสมกับยุคสมัยว่า การกระทำเช่นไรที่มีลักษณะเป็นการอันมิชอบ โดยเสนอให้ศาลพิเคราะห์อย่างลึกซึ้งในรายละเอียดว่า การกระทำดังกล่าวเป็น “การเข้าถึง” หรือไม่ และการกระทำใดสมควรที่จะเป็นความผิดทางอาญา[179]

สำหรับผู้เขียนแล้ว เห็นด้วยกับการให้ความหมายและการแยกประเภทของคำว่า “โดยมิชอบ” ในวิทยานิพนธ์ทั้งสองฉบับ ที่ให้หมายความถึง “โดยไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจ หรืออาจมีความหมายอย่างกว้างได้ว่า เป็นการกระทำโดยไม่เหมาะสม ไม่สุจริต ปราศจากสิทธิอันชอบธรรม หรือไม่ได้รับอนุญาต โดยครอบคลุมถึงการกระทำของผู้ที่ได้รับอนุญาตที่กระทำการเกินขอบอำนาจ หรือไม่เกินขอบอำนาจเท่านั้นแต่รวมถึงกระทำโดยไม่สุจริต หรือไม่ถูกต้อง ไม่เหมาะสม จึงมีความหมายกว้างกว่า “โดยมิชอบด้วยกฎหมาย” ”

แต่อย่างไรก็ตาม ผู้เขียนก็ไม่เห็นด้วยกับแนวคิดของวิทยานิพนธ์ทั้งสองฉบับดังกล่าวที่ให้อาศัยคำพิพากษาศาลฎีกาเป็นเกณฑ์ในการกำหนดหลักเกณฑ์ในการตีความ คำว่า “โดยมิชอบ” และการเสนอให้ปล่อยให้เป็นหน้าที่ของศาลที่จะตีความให้เหมาะสมกับพฤติกรรมของผู้กระทำผิดในแต่ละคดี สาเหตุที่ผู้เขียนไม่เห็นด้วยก็เพราะแนวคำพิพากษาของศาลฎีกานั้นเหล่านั้นมิใช่เป็นคดีหรือความผิดที่เกี่ยวกับคอมพิวเตอร์ แต่เป็นคดีแพ่งและคดีอาญาทั่วไป ซึ่งที่มาของการบัญญัติกฎหมายมีความแตกต่างจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีความเป็นกฎหมายพิเศษและเฉพาะด้านจริง ๆ โดยกฎหมายฉบับนี้เป็นทั้งกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติอยู่ในตัวเอง และตัวผู้พิพากษาที่ตัดสินคดีนั้นก็อาจมิได้เป็นผู้ที่มีความรู้หรือมีความเชี่ยวชาญด้านคอมพิวเตอร์อย่างเพียงพอที่จะสามารถใช้เป็นบรรทัดฐานในการตัดสินคดีความผิดเกี่ยวกับคอมพิวเตอร์ได้ ประกอบกับผู้เขียนเห็นว่า ในการปรับใช้และการตีความกฎหมายตามความเห็นของวิทยานิพนธ์ทั้งสองฉบับดังกล่าวนั้น เป็นการตีความคำว่า “เข้าถึง” และคำว่า “โดยมิชอบ” รวมเข้าเป็นคำเดียวกัน จึงทำให้เกิดปัญหาในการตีความและยากแก่การพิจารณาและทำความเข้าใจ แต่หากเปลี่ยนหลักในการตีความเสียใหม่โดยแยกคำว่า “เข้าถึง”

---

179 ชาตรี ส่งสัมพันธ์, อ้างแล้วในเชิงอรรถที่ 77 หน้า 117-118

กับคำว่า “โดยมิชอบ” ออกจากกันก็จะทำให้ง่ายแก่การทำความเข้าใจความหมายของทั้งสองคำดังกล่าว ซึ่งผู้เขียนจะได้กล่าวถึงประเด็นนี้โดยละเอียดอีกครั้งในบทสรุปและข้อเสนอแนะ

4.2.2 เปรียบเทียบการกำหนดฐานความผิดเพื่อป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ในกฎหมายต่างประเทศกับของไทย

เพื่อประกอบความเข้าใจในความแตกต่างระหว่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยกับกฎหมายของต่างประเทศในประเด็นปัญหาการกำหนดฐานความผิดเพื่อป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ที่อาจเกิดจากชุดคำสั่งไม่พึงประสงค์ ผู้เขียนจึงจะขอเปรียบเทียบการกำหนดฐานความผิดดังกล่าว ดังนี้

จากผลการศึกษามาตรการป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ในกฎหมายต่างประเทศพบว่า มีทั้งกฎหมายที่กำหนดฐานความผิดเพื่อให้การคุ้มครองเฉพาะระบบคอมพิวเตอร์ กฎหมายที่กำหนดฐานความผิดเพื่อให้การคุ้มครองเฉพาะข้อมูลคอมพิวเตอร์ และกฎหมายที่กำหนดฐานความผิดเพื่อให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ทั้งนี้การกำหนดองค์ประกอบของฐานความผิดการเข้าถึงโดยไม่มีอำนาจในกฎหมายต่างประเทศ มีการบัญญัติไว้เป็นสี่รูปแบบด้วยกัน คือ

รูปแบบที่หนึ่ง กำหนดองค์ประกอบของฐานความผิดไว้เพียงว่า หากมีการเข้าถึงโดยไม่มีอำนาจก็ถือเป็นความผิดแล้ว โดยไม่คำนึงว่าจะต้องมีเจตนาพิเศษอื่นใด และไม่ต้องคำนึงว่าผู้กระทำผิดจะต้องกระทำละเมิดหรือฝ่าฝืนต่อมาตรการป้องกันหรือระบบรักษาความปลอดภัย(คล้ายกับกฎหมายของไทยที่กำหนดให้เป็นความผิดในตัวเอง แม้ไม่มีเจตนาทุจริตพิเศษอื่นก็เป็นความผิด)

รูปแบบที่สอง กำหนดองค์ประกอบของฐานความผิดไว้ว่า หากมีการเข้าถึงโดยไม่มีอำนาจและผู้กระทำมีเจตนาทุจริตพิเศษอื่น จึงจะถือเป็นความผิด

รูปแบบที่สาม กำหนดองค์ประกอบของความผิดไว้ว่า หากมีการเข้าถึงโดยไม่มีอำนาจแม้ผู้กระทำผิดไม่มีเจตนาทุจริตพิเศษ แต่ผู้กระทำผิดได้กระทำการละเมิดหรือฝ่าฝืนต่อมาตรการป้องกันหรือระบบรักษาความปลอดภัย ก็ถือเป็นความผิด (ในบางประเทศกำหนดให้การละเมิดหรือฝ่าฝืนต่อมาตรการป้องกันหรือระบบรักษาความปลอดภัยเป็นความผิดบทหนักขึ้นด้วย)

รูปแบบที่สี่ กำหนดองค์ประกอบของฐานความผิดไว้ว่า กรณีจะถือเป็นความผิดจะต้องมีการเข้าถึงโดยไม่มีอำนาจและโดยมีเจตนาพิเศษอื่น และผู้กระทำผิดจะต้องกระทำการละเมิดหรือฝ่าฝืนต่อมาตรการป้องกันหรือระบบรักษาความปลอดภัยด้วย จึงจะถือเป็นความผิด

สำหรับตัวอย่างของเจตนาพิเศษในกฎหมายของต่างประเทศก็เช่น มีเจตนาทุจริตเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ หรือมีเจตนาเพื่อการเปลี่ยนแปลงหรือทำให้ข้อมูลคอมพิวเตอร์

ด้อยค่าลง (corrupt) หรือเพื่อการเปลี่ยนแปลง (alter) หรือเพื่อการขโมย (steal) หรือเพื่อทำลาย (destroy) ซึ่งข้อมูลหรือระบบคอมพิวเตอร์ หรือเพื่อการได้ใช้คอมพิวเตอร์หรืออุปกรณ์ด้านสารสนเทศและการสื่อสารใดๆ โดยไม่มีสิทธิ หรือดำเนินการอื่นใดต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์โดยมิชอบ เป็นต้น

นอกจากนี้ ในบางประเทศยังกำหนดให้ผู้กระทำผิดต้องได้รับโทษหนักขึ้นหากได้กระทำการเข้าถึงซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ส่งผลกระทบต่อประชาชนหรือประโยชน์สาธารณะ หรือหากผู้กระทำผิดเป็นเจ้าหน้าที่ของรัฐหรือเป็นเจ้าหน้าที่ผู้มีหน้าที่ให้บริการสาธารณะ หรือโดยเป็นการใช้อำนาจในทางมิชอบ หรือเป็นการฝ่าฝืนการปฏิบัติตามหน้าที่ หรือหากในการกระทำผิดนั้นผู้กระทำได้ก่อความเสียหายต่อทรัพย์สินหรือประชาชน หรือการกระทำนั้นเป็นการเข้าถึงเพื่อให้ได้มาซึ่งข้อมูลด้านความลับทางการค้าหรือข้อมูลที่ต้องเก็บรักษาเป็นความลับตามกฎหมาย

ส่วนในฝั่งของกฎหมายไทยนั้น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดความผิดฐานเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไว้ในมาตรา 5 และมาตรา 7 โดยมีหลักการและองค์ประกอบของความผิดที่สำคัญว่า จะต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ไม่ว่าทั้งหมดหรือบางส่วน และจะต้องกระทำการละเมิดหรือฝ่าฝืนมาตรการหรือระบบรักษาความปลอดภัยที่จัดทำไว้เป็นการเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน จึงจะถือเป็นความผิด โดยไม่ต้องคำนึงว่าผู้กระทำผิดจะมีเจตนาทุจริตหรือไม่ (เหมือนดังเช่นรูปแบบที่หนึ่งกฎหมายในต่างประเทศที่กำหนดให้เป็นความผิดในตัวเอง) ทั้งนี้ ยังมีการกำหนดความผิดฐานการล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำไว้เป็นการเฉพาะแล้วนำไปเปิดเผยโดยมิชอบ ตัวอย่างการล่วงรู้โดยมิชอบในกรณีนี้ก็ เช่น การใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันที่เป็นโปรแกรมดักข้อมูลผ่านปุ่มคีย์บอร์ด (Keylogger หรือ Keystroker) แอบบันทึกการกดรหัสผ่านของผู้อื่นแล้วนำไปโพสต์ไว้ในกระทู้ต่างๆ เป็นต้น ซึ่งการที่จะกระทำเช่นนั้นได้ก็ย่อมต้องใช้เทคนิคและกระบวนการเข้าถึงทางดิจิทัลด้วยเช่นกัน

นอกจากนี้ กฎหมายไทยยังได้กำหนดฐานความผิดเพื่อป้องกันความเสียหายหรือผลกระทบต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ไม่ว่าจะเป็นการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ซึ่งการที่จะกระทำเช่นนั้นได้ก็ต้องผ่านกระบวนการเข้าถึงทางดิจิทัลก่อนเช่นกัน โดยกำหนดไว้ในมาตรา 9 ถึง มาตรา 10 และยังมีการกำหนดฐานความผิดเพื่อป้องกันการดักรับข้อมูล (ภัยคุมคามหรือการโจมตีจากชุดคำสั่งไม่พึงประสงค์ ซึ่งเมื่อ

พิจารณาจากพฤติการณ์ของการกระทำความผิดดังกล่าวแล้วจะเห็นได้ว่ามีลักษณะเป็นการเข้าถึง (access) ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งในเชิงของการบุกรุกทางคอมพิวเตอร์ (computer trespass) หรือการเจาะเข้าไปในระบบ (Hacking or Cracking) และในเชิงของการดักข้อมูล (interception) ซึ่งผู้เขียนเห็นว่าการดักข้อมูลก็เป็นการเข้าถึงอีกรูปแบบหนึ่งด้วยเช่นกัน) ไว้ในมาตรา 8 อีกด้วย แต่เงื่อนที่จะเป็นความผิดตามมาตราเหล่านั้น จะต้องเป็นการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ไม่ว่าทั้งหมดหรือบางส่วน และจะต้องกระทำการละเมิดหรือฝ่าฝืนมาตรการหรือระบบรักษาความปลอดภัยที่จัดทำไว้เป็นการเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

ดังนั้น จึงมีผลทำให้กฎหมายไทยไม่ครอบคลุมถึงการกระทำความผิดโดยการใช้ชุดคำสั่งไม่พึงประสงค์ในการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มิได้มาตรการป้องกันเป็นการเฉพาะ หรือแม้จะมีมาตรการป้องกันเป็นการเฉพาะแต่เจ้าของระบบได้ให้ความยินยอมในการเข้าถึงคอมพิวเตอร์นั้น หรือในบางกรณีแฮกเกอร์หรือคนร้ายอาจใช้เทคนิคในการหลอกล่อ (Spoof) เพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป และทำให้แฮ๊กเกอร์สามารถนำชุดคำสั่งไม่พึงประสงค์ประเภท ม้าโทรจันหรือสปายแวร์ไปฝังไว้ในระบบแล้วทำการขโมยข้อมูลสำคัญหรือข้อมูลเอกลักษณ์บุคคล (Identity theft) ออกไปได้ในที่สุด ดังนั้น ในประเด็นของการเข้าถึงนี้จึงทำให้กลายเป็นช่องว่างของกฎหมายไทยที่เห็นได้อย่างชัดเจน

5. ปัญหาการใช้และการตีความกฎหมาย

ปัญหาในการใช้และการตีความกฎหมาย ย่อมเกิดขึ้นและอยู่คู่กับผู้ที่มีส่วนในการบังคับใช้กฎหมายเสมอ ไม่ว่าจะเป็นผู้ทำหน้าที่ในการสืบสวน สอบสวน และรวบรวมพยานหลักฐานเพื่อหาตัวผู้กระทำความผิดมาลงโทษอย่างเช่นพนักงานสอบสวน หรือผู้มีหน้าที่ในการวินิจฉัยและพิจารณาว่าจะสั่งฟ้องหรือไม่ฟ้องผู้ต้องหาหรือไม่อย่างเช่นพนักงานอัยการ และผู้ที่มีหน้าที่ในการใช้และตีความกฎหมายในท้ายที่สุดก็คือศาลนั่นเอง

อย่างไรก็ตาม ปัญหาในการใช้และการตีความกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งเป็นกฎหมายที่ว่าด้วยเรื่องของศาสตร์ทางคอมพิวเตอร์และศาสตร์ทางด้านเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีรายละเอียดในทางด้านเทคนิคต่างๆ มากมาย จึงทำให้กฎหมายฉบับนี้มีความเป็นกฎหมายพิเศษและเฉพาะด้านอย่างแท้จริง อีกทั้งยังเป็นเรื่องใหม่สำหรับประเทศไทย จึงอาจทำให้เกิดปัญหาในการใช้และการตีความกฎหมายฉบับนี้มีอยู่มากมายและในหลายแง่มุม แต่สิ่งที่สำคัญที่สุดก็คือ ปัจจุบันยังไม่มีคดีความผิดเกี่ยวกับคอมพิวเตอร์โดยแท้ที่ขึ้นสู่

การพิจารณาของศาลฎีกาอันจะสามารถนำมาเป็นบรรทัดฐานในการใช้และการตีความกฎหมายฉบับนี้ได้อย่างแท้จริง

สำหรับปัญหาในการใช้และการตีความกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามหัวข้อและประเด็นการวิจัยในวิทยานิพนธ์นี้ หลักๆ ก็คงเป็นเรื่องของการตีความเกี่ยวกับความรับผิดในทางอาญาของผู้กระทำผิดว่า พฤติการณ์ที่เขาได้กระทำลงไปนั้นจะถือเป็นความผิดทางอาญาตามที่กฎหมายกำหนดฐานความผิดไว้หรือไม่ ซึ่งประเด็นการตีความก็คงเป็นเรื่องของความผิดฐานการเข้าถึงโดยมิชอบ (Illegal access) ตามที่ผู้เขียนได้วิเคราะห์ไปแล้วว่าความผิดที่ถือเป็นความผิดที่กระทำต่อคอมพิวเตอร์โดยแท้ตามมาตรา 5 ถึง มาตรา 11 นั้น จะต้องผ่านกระบวนการเข้าถึงก่อนเสมอ จึงจะสามารถกระทำให้เกิดความเสียหายและผลกระทบต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ตามมา ซึ่งผู้เขียนเห็นว่า ประเด็นที่เป็นปัญหาและต้องคำนึงถึงเมื่อมีการปรับใช้กฎหมายดังกล่าวก็คือ หลักในการใช้บังคับกฎหมายอาญาซึ่งได้แก่ กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง กฎหมายอาญาต้องมีความโดยเคร่งครัด และหลักของความรับผิดทางอาญาในส่วนของความสัมพันธ์ระหว่างการกระทำและผล โดยจะขอวิเคราะห์ถึงหลักการต่างๆ ดังนี้

5.1 กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง

ในเรื่องความชัดแจ้งของบัญญัติแห่งกฎหมายอาญานี้ สามารถแยกพิจารณาได้เป็น 3 ส่วนที่สำคัญคือ

5.1.1 บทบัญญัติกฎหมายอาญาต้องเป็นลายลักษณ์อักษร

ตามประมวลกฎหมายอาญา มาตรา 2 ที่บัญญัติว่า “บุคคลจักต้องรับโทษในทางอาญาต่อเมื่อได้กระทำการอันกฎหมายที่ใช้ในขณะกระทำนั้นบัญญัติเป็นความผิดและกำหนดโทษไว้...” จึงเป็นการบ่งชัดว่า กฎหมายอาญาจะต้องมีบทบัญญัติเป็นลายลักษณ์อักษรเท่านั้น มิฉะนั้นก็ไม่อาจจะใช้บังคับได้ การใช้บังคับกฎหมายอาญาจึงต่างกับกฎหมายแพ่ง กล่าวคือการใช้บังคับกฎหมายอาญานั้นหากมีช่องว่างในกฎหมายหรือไม่มีกฎหมายบัญญัติเป็นลายลักษณ์อักษรว่าการกระทำใดเป็นความผิดไว้ ผู้กระทำย่อมไม่ต้องรับผิดในทางอาญาสำหรับการกระทำนั้น[180]

---

180 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544) “เอกสารการสอนชุดวิชา กฎหมายอาญา 1 : ภาคบทบัญญัติทั่วไป” พิมพ์ครั้งที่ 13 (นนทบุรี สำนักพิมพ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช) หน้า 100

ดังนั้น แม้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะบัญญัติฐานความผิดเกี่ยวกับคอมพิวเตอร์ไว้อย่างเป็นลายลักษณ์อักษร ทั้งในส่วนที่ถือเป็นความผิดที่กระทำต่อคอมพิวเตอร์โดยแท้ ตั้งแต่มาตรา 5 ถึง มาตรา 11 และส่วนของความผิดที่มิได้กระทำต่อคอมพิวเตอร์โดยแท้ แต่เป็นการใช้คอมพิวเตอร์ในการกระทำความผิดตั้งแต่มาตรา 14 ถึง มาตรา 16 ซึ่งในส่วนของความผิดที่กระทำต่อคอมพิวเตอร์โดยแท้นั้นจะต้องผ่านกระบวนการเข้าถึงก่อนเสมอ จึงจะสามารถทำให้เกิดความเสียหายและส่งผลกระทบต่อระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ได้ แต่กฎหมายดังกล่าวก็มิได้บัญญัติหรือกำหนดความหมายของคำว่า “เข้าถึง” ไว้ ซึ่งหากเป็นการเข้าถึงทางกายภาพก็คงไม่มีปัญหาและไม่ถือเป็นช่องว่างของกฎหมาย เพราะการเข้าถึงทางกายภาพมีความชัดเจนอยู่ในตัวและสามารถเข้าใจได้ดีอยู่แล้ว แต่สำหรับกรณีของการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลโดยเฉพาะอย่างยิ่งการเข้าถึงโดยใช้ชุดคำสั่งไม่พึงประสงค์นั้น จะมีความหมายและขอบเขตของการเข้าถึงเพียงใด จึงเป็นสิ่งที่นักกฎหมายหรือผู้ใช้กฎหมายจะต้องตีความกันเอาเอง

อย่างไรก็ตาม หากเป็นการเข้าถึงทางดิจิทัลโดยใช้ชุดคำสั่งไม่พึงประสงค์ประเภท ไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ แอดแวร์ โปรแกรมทดสอบช่องโหว่ โปรแกรมเจาะระบบ โปรแกรมดาวน์โหลดไวรัส โปรแกรมปล่อยไวรัส โปรแกรมฉีดไวรัส โปรแกรมชุดสร้างไวรัส โปรแกรมสำหรับส่งสแปม โปรแกรมระเบิด โปรแกรมโทรศัพท์อัตโนมัติ โปรแกรมล้อกันเล่น ฟลัดเดอร์ รูทคิท หรือโปรแกรมอื่นใดในอนาคตที่มีคุณสมบัติทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ก็พอที่จะตีความได้ว่าเป็นการเข้าถึงโดยมิชอบตามบทบัญญัติของกฎหมายดังกล่าว

แต่ที่เป็นปัญหาและยากแก่การตีความเพื่อการบังคับใช้กฎหมายก็คือ การตีความให้ผู้กระทำความผิดต้องรับโทษในฐานความผิดการเข้าถึงโดยมิชอบโดยใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์ที่ไม่มีคุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เมื่อถูกนำไปใช้เป็นเครื่องมือในการเข้าถึง ซึ่งผู้เขียนเห็นว่า เป็นเรื่องยากที่จะตีความให้ได้เช่นนั้น เพราะพื้นฐานทางศาสตร์คอมพิวเตอร์และศาสตร์ทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของแต่ละบุคคลนั้นย่อมมีไม่เท่ากัน โดยเฉพาะพนักงานเจ้าหน้าที่ผู้ซึ่งถือว่าเป็นต้นธารแห่งกระบวนการยุติธรรม หากไม่มีความเข้าใจหรือไม่สามารถตีความกฎหมายได้หรือหากตีความผิดพลาดคลาดเคลื่อนไปก็จะทำให้ส่งผลกระทบต่อกระบวนการยุติธรรมและส่งผลกระทบต่อสิทธิและเสรีภาพของประชาชนอย่างหลีกเลี่ยงไม่ได้

หรือแม้แม่ศาลเองซึ่งเป็นบุคคลที่อยู่ท้ายสุดของกระบวนการยุติธรรมก็คงเกิดความยากลำบากในการตีความเกี่ยวกับความผิดฐานเข้าถึงโดยมิชอบโดยใช้ม้าโทรจันหรือสปายแวร์ในการเข้าถึงด้วยเช่นกัน

กรณีดังกล่าวจึงถือเป็นช่องว่างของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งผู้เขียนเห็นว่า ความผิดฐานการเข้าถึงโดยมิชอบโดยใช้ม้าโทรจันหรือสปายแวร์ในการเข้าถึงตามกฎหมายนี้มิได้เป็นไปตามหลักบทบัญญัติโดยชัดแจ้งของกฎหมายอาญา ดังนั้น เมื่อกรณีนี้ถือว่าเป็นช่องว่างในกฎหมายแล้ว ผู้กระทำผิดก็ย่อมไม่ต้องรับผิดในทางอาญาสำหรับการกระทำนี้ ทั้งๆที่จริงแล้วผู้กระทำผิดสมควรจะต้องได้รับโทษฐานการเข้าถึงโดยมิชอบแต่บทบัญญัติของกฎหมายตีความไปไม่ถึง ทำให้ต้องปล่อยตัวผู้ต้องหาหรือจำเลยไปในที่สุด

5.1.2 กฎหมายอาญาต้องมีบทบัญญัติความผิดและโทษไว้ในขณะกระทำ

สำหรับหลักที่ว่ากฎหมายอาญาต้องมีบทบัญญัติความผิดและโทษไว้ขณะกระทำนั้น ก็คงไม่มีประเด็นปัญหาใดสำหรับกฎหมายที่ใช้อยู่ในปัจจุบัน แต่ผู้เขียนมีข้อสังเกตเพียงว่า หากมีการแก้ไขกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ตามข้อเสนอแนะของผู้เขียนโดยการกำหนดนิยามและความหมายของคำว่า “เข้าถึง” เพื่อให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากม้าโทรจันและสปายแวร์แล้ว โทษสำหรับความผิดฐานการเข้าถึงโดยมิชอบดังกล่าว จะสามารถบังคับใช้ตามกฎหมายที่แก้ไขใหม่ได้หรือไม่ กล่าวคือ โดยพฤติการณ์ของม้าโทรจันและสปายแวร์จะยังไม่ก่อให้เกิดความเสียหายหรือส่งผลกระทบใดๆ ต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์จนกว่าม้าโทรจันหรือสปายแวร์ที่ถูกนำไปฝังหรือติดตั้งไว้ในระบบคอมพิวเตอร์นั้นจนกว่าม้าโทรจันหรือสปายแวร์นั้นจะได้ทำการสำเนาหรือส่งข้อมูลหรือดักข้อมูลแล้วส่งไปยังแฮกเกอร์หรือผู้กระทำผิด ซึ่งก็จะมีปัญหาว่า การกระทำเช่นนั้นของม้าโทรจันและสปายแวร์จะถือว่าเป็นการเข้าถึงตามความหมายและนิยามของคำว่า “เข้าถึง” ที่กำหนดขึ้นใหม่หรือไม่ อย่างไร เนื่องจากเป็นการบัญญัติความผิดโดยการเข้าถึงดังกล่าวขึ้นในภายหลัง

5.1.3 บทบัญญัติกฎหมายอาญาต้องชัดเจนปราศจากการคลุมเครือ

กฎหมายอาญานั้นนอกจากจะต้องมีบทบัญญัติเป็นลายลักษณ์อักษร และต้องมีบทบัญญัติความผิดและโทษไว้ในขณะกระทำแล้ว ถ้อยคำในบทบัญญัตินั้นจะต้องชัดเจนปราศจากความคลุมเครือ ทั้งในส่วนของบทบัญญัติ ความผิด และบทกำหนดโทษ ในกรณีที่ถ้อยคำใดเป็นศัพท์เฉพาะที่มิได้มีความหมายอย่างภาษาสามัญธรรมดาก็จะมีคำนิยาม (definition) บัญญัติคำอธิบายศัพท์นั้นไว้เป็นการเฉพาะ อย่างไรก็ตาม บทบัญญัติที่ว่าต้องชัดเจนปราศจากความคลุมเครือนั้น หมายความว่าชัดเจนแน่นอนพอสมควร (reasonable definition) เท่านั้น เพราะจะ

บัญญัติให้ละเอียดถี่ถ้วนลงไปนั้นคงทำได้ยากมาก ซึ่งก็ไม่มีประเทศใดสามารถทำได้ ในกรณีที่ไม่สามารถบัญญัติให้ชัดเจนแน่นอนได้ ก็ย่อมจะต้องอาศัยดุลพินิจของเจ้าพนักงานในการยุติธรรม[181]

อย่างไรก็ตาม ผู้เขียนเห็นว่า กรณีของคำว่า “เข้าถึง” นี้ จัดได้ว่าเป็นศัพท์เฉพาะที่มิใช่ภาษาสามัญธรรมดา จึงจำเป็นต้องกำหนดเป็นคำนิยามไว้ ประกอบกับนานาอารยประเทศก็ได้มีการกำหนดนิยามคำว่า “เข้าถึง” ไว้ในกฎหมายของตนตามที่ได้ยกตัวอย่างและวิเคราะห์เกี่ยวกับคำว่า “เข้าถึง” ของกฎหมายต่างประเทศตามที่ได้กล่าวไปแล้วใน บทที่ 3 ข้อ 1 (มาตรการกำหนดนิยามและความหมายของการเข้าถึง (access) ให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์) ทั้งนี้ ก็เพื่อจะได้เป็นบรรทัดฐานในการบังคับใช้และการตีความกฎหมายของเจ้าพนักงานในการยุติธรรมโดยเฉพาะพนักงานเจ้าหน้าที่

5.2 กฎหมายอาญาต้องตีความโดยเคร่งครัด

แม้กฎหมายอาญาจะต้องมีบทบัญญัติโดยชัดแจ้งตามที่ได้กล่าวไปแล้ว แต่การจะบัญญัติกฎหมายให้ละเอียดและชัดเจนแน่นอนลงไปในทุกกรณีย่อมเป็นไปไม่ได้ ฉะนั้นจึงต้องอาศัยการตีความเช่นเดียวกับกฎหมายอื่นๆ กล่าวคือ จะต้องตีความตามตัวอักษรและตามเจตนารมณ์ (Spirit) ของกฎหมายนั้น ๆ เป็นแต่กฎหมายอาญามีหลักการตีความพิเศษเพิ่มขึ้นอีก นั่นคือ กฎหมายอาญาต้องตีความโดยเคร่งครัด เพื่อเป็นหลักประกันว่าประชาชนผู้อยู่ภายใต้การใช้บังคับกฎหมายจะได้รับความเป็นธรรม[182]

ทั้งนี้ ผู้เขียนมีความเห็นเกี่ยวกับหลักกฎหมายอาญาที่ต้องตีความโดยเคร่งครัดสำหรับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่า ด้วยเหตุที่กฎหมายดังกล่าวยังเป็นเรื่องใหม่สำหรับประเทศไทย จึงทำให้ไม่มีบรรทัดฐานของคดีที่ตัดสินโดยศาลฎีกาเพื่อวางหลักในความผิดฐานการเข้าถึงโดยมิชอบไว้ การตีความจึงต้องอยู่ภายใต้หลักการตีความโดยเคร่งครัดที่ว่า การตีความต้องตีความตามตัวอักษร การตีความต้องตีความตามเจตนารมณ์ ซึ่งหากมีกรณีเป็นที่สงสัยก็ต้องยกผลประโยชน์แห่งความสงสัยให้กับจำเลย ส่วนหลักในการเปรียบเทียบกฎหมายที่ใกล้เคียงอย่างยิ่งและการตีความโดยขยายความนั้นจะนำมาใช้ในทางที่เป็นโทษแก่จำเลยหรือผู้ต้องหาไม่ได้

---

181 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 101

182 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 103

5.2.1 การตีความตามตัวอักษร

ตามประมวลกฎหมายอาญา มาตรา 2 ที่บัญญัติว่า “บุคคลจักต้องรับโทษในทางอาญาก็ต่อเมื่อ...” ซึ่งหมายความว่า กฎหมายอาญาจะต้องตีความอย่างเคร่งครัด ในเมื่อกฎหมายบัญญัติว่าการกระทำใดเป็นความผิดและต้องรับโทษในทางอาญาแล้ว ก็ต้องถือว่าการกระทำนั้นๆ เท่านั้นที่เป็นความผิดและผู้กระทำจะต้องถูกลงโทษ จะรวมถึงการกระทำอื่นๆ ด้วยไม่ได้ นั่นคือ จะต้องตีความตามตัวอักษร หรือตามถ้อยคำในตัวบทกฎหมายอย่างเคร่งครัดนั่นเอง[183]

ทั้งนี้ ในประเด็นการเข้าถึงโดยมิชอบด้วยชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ผู้เขียนได้วิเคราะห์ไปแล้วว่า ความผิดฐานการเข้าถึงดังกล่าวจะถือว่าเป็นความผิดสำเร็จก็เมื่อผ่านการเข้าถึงโดยฝ่าฝืนมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน แต่ต่อจากนั้นหากการติดต่อสื่อสารระหว่างคอมพิวเตอร์ที่ใช้ในการเข้าถึงกับเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อถูกตัดขาดจากกันแล้ว การเข้าถึงในคราวนั้นจึงสิ้นสุดลง หากต่อมาม้าโทรจันหรือสปายแวร์ได้ทำการสำเนาหรือขโมยหรือดักข้อมูลแล้วส่งออกไปยังภายนอก หากจะแปลความว่ามีการติดต่อสื่อสารในขณะที่เครื่องที่ตกเป็นเหยื่อส่งข้อมูลออกไปนั้นเป็นการสื่อสารที่เกิดขึ้นใหม่ก็มิได้หมายความว่าเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายถูกเข้าถึงอีกครั้ง แต่ในทางตรงกันข้ามเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายเข้าถึงเครื่องที่ใช้ในการโจมตีในครั้งก่อน กรณีจึงเป็นเรื่องยากที่จะตีความได้ว่าเครื่องที่ตกเป็นเหยื่อเป็นฝ่ายถูกเข้าถึง เพราะไม่มีถ้อยคำใดในกฎหมายฉบับนี้ที่บัญญัติไว้ให้ตีความได้เช่นนั้น

5.2.2 การตีความตามเจตนารมณ์

ในบางกรณีการตีความกฎหมายอาญาตามตัวอักษรแต่เพียงอย่างเดียวยังไม่อาจทำให้เข้าใจความหมายที่แท้จริงของบทบัญญัติแห่งกฎหมายได้ ด้วยเหตุนี้ จึงจำเป็นต้องพิจารณาเจตนารมณ์ของกฎหมายด้วย หรือในกรณีที่หากการตีความโดยเคร่งครัดตามตัวอักษรจะทำให้เกิดผลประหลาด ก็จะต้องตีความตามเจตนารมณ์ของกฎหมายนั้นอย่างเคร่งครัดดุจกัน[184]

จากเหตุผลในการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ว่า[185] “เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์

---

183 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 103

184 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 105

185 เป็นเหตุผลที่เขียนไว้ในหมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้" นั้น ผู้เขียนเห็นว่า ก็ยังไม่อาจแปลได้ว่า กฎหมายดังกล่าวจะมีเจตนารมณ์ในการคุ้มครองถึงการขโมยข้อมูลที่เกิดจากชุดคำสั่งไม่พึงประสงค์ด้วย

5.2.3 กรณีเป็นที่สงสัย

ในกรณีที่บทบัญญัติกฎหมายอาญามี "กรณีเป็นที่สงสัย" กล่าวคือ อาจตีความได้เป็นหลายนัย ศาลจะตีความตามนัยที่เป็นประโยชน์หรือเป็นผลดีแก่จำเลยได้หรือไม่เพียงใด ซึ่งในประเด็นดังกล่าวมีผู้ให้ความเห็นไว้เป็น 2 ความเห็นด้วยกัน กล่าวคือ ความเห็นแรก ศาสตราจารย์พระยาอรรถการียนิพนธ์ กล่าวไว้ว่า "การตีความตัวบทกฎหมายต่างกับการวินิจฉัยข้อเท็จจริงในส่วนที่เกี่ยวกับข้อเท็จจริง เราพบบ่อยๆ ว่าศาลยกประโยชน์แก่จำเลย เพราะกรณีเป็นที่สงสัย แต่การตีความตามตัวบท ศาลจะลงความเห็นว่าสงสัยไม่แน่นอนไม่ได้ ต้องค้นหาหลักฐานและตีความไปให้เสร็จ นอกจากนี้คำใดในกฎหมายที่สงสัย ศาลจะแปลไปในทางที่เป็นประโยชน์แก่จำเลยโดยขยายความไปไม่ได้ เพราะศาลไม่มีหน้าที่ช่วยจำเลย มีแต่ลงโทษคนผิด และไม่ลงโทษผู้ไม่ผิด..." ส่วนความเห็นที่สอง ศาสตราจารย์หยุด แสงอุทัย กล่าวไว้ว่า "นอกจากนี้ยังมีหลักการตีความกฎหมายข้อหนึ่งว่า ถ้ากรณีเป็นที่สงสัย ศาลจะต้องตีความให้เป็นประโยชน์แก่ผู้ต้องหา (in dubio pro reo) ฉะนั้น ถ้าจะมีการตีความได้สองทางและทางหนึ่งเป็นประโยชน์แก่ผู้ต้องหามากกว่า ศาลพึงจะเลือกตีความในทางที่เป็นประโยชน์แก่ผู้ต้องหา แต่ทั้งนี้หมายความถึงเมื่อมีข้อสงสัยเกิดขึ้น ซึ่งศาลจะต้องตีความเช่นนั้นเท่านั้นศาลไม่มีหน้าที่ที่จะพิจารณาหาลู่ทางช่วยเหลือผู้ต้องหาในกรณีที่ไม่มีข้อสงสัยอันจะทำให้ศาลต้องตีความ และแม้ศาลจะมีความเห็นว่าจำเลยไม่ควรรับโทษ แต่เมื่อปรากฏว่าตามกฎหมายจำเลยได้กระทำความผิดและต้องรับโทษแล้ว ศาลต้องลงโทษจำเลย" นอกจากนี้ยังมีความเห็นของ ศาสตราจารย์ธานินทร์ ไกรวิเชียร ซึ่งมีความเห็นเป็นแนวเดียวกับความเห็นของศาสตราจารย์หยุด แสงอุทัย โดยกล่าวไว้ว่า "...ในกรณีที่มีข้อสงสัยในเจตนารมณ์ของกฎหมายและอาจตีความบทบัญญัติของกฎหมายได้เป็นหลายนัย ศาลย่อมตีความในแง่ที่เป็นประโยชน์แก่จำเลยมากที่สุดได้เสมอ ไม่มีเหตุผลอันใดที่จะจำกัดการให้ประโยชน์แก่จำเลย

ในคดีอาญาแต่เฉพาะปัญหาข้อเท็จจริง แม้แต่ในปัญหาข้อกฎหมายโดยเฉพาะในการตีความกฎหมาย ศาลย่อมให้ประโยชน์แห่งความสงสัยแก่จำเลยได้ดุจกัน"[186]

สำหรับผู้เขียนแล้ว เห็นด้วยอย่างยิ่งกับแนวความเห็นที่สองทั้งของศาสตราจารย์หยุด แสงอุทัย และของศาสตราจารย์ธานินทร์ ไกรวิเชียร

5.2.4 การเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง[187]

สำหรับการบังคับใช้กฎหมายอาญานั้น การตีความบทบัญญัติกฎหมาย จะนำหลักการเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง (Analogy) มาใช้บังคับให้เป็นผลร้ายมิได้ ซึ่งนักนิติศาสตร์ทั้งหลายมีความเห็นเป็นแนวเดียวกัน กล่าวคือ ศาสตราจารย์ เอกูต์ ได้ให้หลักไว้ว่า "บทบัญญัติแห่งกฎหมายอาญาซึ่งกำหนดความผิดหรือบัญญัติโทษไว้จะต้องใช้บังคับตามตัวอักษร จะลงโทษบุคคลเพราะได้กระทำการอันคล้ายคลึงกับที่ได้มีกฎหมายบัญญัติไว้นั้นไม่ได้"

ศาสตราจารย์ พระยาอรรถการียพันธ์ กล่าวไว้ว่า "การแปลกฎหมายอาญามีหลักต่างกว่ากฎหมายแพ่ง เช่น เทียบกับกฎหมายใกล้เคียงไม่ได้ อาทิตัวบทกล่าวว่า ผู้ใดกระทำโดยเจตนาให้ผู้หนึ่งผู้ใดถึงแก่ความตาย ท่านว่ามันฆ่าคนโดยเจตนา แต่ถ้าฆ่าตนเองจะนำบทนี้มาลงโทษไม่ได้ เพราะไม่มีกฎหมายบัญญัติโดยตรงว่าผิด ทั้งนี้อย่าลืมว่าเป็นคนละเรื่องกับการตีความของศาล ไม่มีอะไรห้ามมิให้ศาลตีความ..."

ศาสตราจารย์หยุด แสงอุทัย กล่าวไว้ว่า "ศาลอาจเอาบทที่ใกล้เคียงอย่างยิ่งมาใช้เพื่อประโยชน์แก่ผู้ต้องหาได้ แต่จะนำหลักนี้มาใช้เพื่อให้เป็นผลร้ายแก่ผู้ต้องหาไม่ได้ เช่น การหลอกลวงโดยแสดงข้อความเป็นเท็จ จนได้ไปซึ่งบริการจากผู้ถูกหลอกลวง เช่น ขุดบ่อน้ำให้ไม่เป็นความผิดอาญา ศาลจะพิจารณาว่าการได้ไปซึ่งบริการก็เหมือนกันทรัพย์สิน ฉะนั้นจึงลงโทษผู้กระทำฐานฉ้อโกงตามมาตรา 341 โดยอาศัยหลักเทียบเคียงบทที่ใกล้เคียงอย่างยิ่งไม่ได้ เพราะเป็นการนำบทเทียบเคียงมาใช้เป็นผลร้ายแก่ผู้ต้องหา"

จากความเห็นดังกล่าวพอสรุปได้ว่า การเทียบเคียงบทกฎหมายที่ใกล้เคียงอย่างยิ่งนั้นอาจนำมาใช้เพื่อเป็นคุณหรือเป็นประโยชน์แก่ผู้กระทำได้ แต่จะนำมาใช้เพื่อเป็นโทษหรือเป็นผลร้ายมิได้ ดังนั้น การเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลโดยมิชอบตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงมิอาจนำไปเปรียบเทียบกับการเข้าถึงทางกายภาพได้

---

186 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 106-107

187 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 108

5.2.5 การตีความโดยขยายความ[188]

การตีความโดย “ขยายความ” กับ “เทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง” นั้น เป็นการยากที่จะแบ่งแยกออกจากกันได้โดยเด็ดขาด ด้วยเหตุดังกล่าวนักนิติศาสตร์ทั้งหลายจึงมีความเห็นในเรื่องการตีความโดยขยายว่าจะกระทำได้หรือไม่เพียงใดนั้น แตกต่างกันไป ดังเช่น

ศาสตราจารย์ พระยาอรรถการียนิพนธ์ กล่าวไว้ว่า “...ทางอาญาการตีความต้องใช้หลักเคร่งครัดไม่ใช่ extensive ต้องตีความโดยเด็ดขาดไม่ใช่ขยายความ โดยหลักนี้ศาลมีอำนาจจะค้นหาเจตนาของผู้ร่างว่า ผู้ร่างมีความมุ่งหมายอย่างไร แต่ศาลจะตีความให้ฝ่าฝืนลายลักษณ์อักษรที่เขียนไว้ไม่ได้ ต้องตีความภายในลายลักษณ์อักษร...”

ศาสตราจารย์หยุด แสงอุทัย กล่าวไว้ว่า “ไม่หมายความว่าศาลจะต้องดำเนินตามตัวอักษรเป็นแถวตรง การแปลโดยเคร่งครัดอาจทำให้ต้องตีความโดยขยายความในบางกรณีได้ หลักการตีความโดยเคร่งครัดเป็นแต่การห้ามมิให้ศาลขยายความตามใจชอบเท่านั้น แต่ถ้าการตีความโดยขยายความเป็นแต่ตีความตรงตามความมุ่งหมายแห่งกฎหมายตามที่ปรากฏจากตัวกฎหมายเองแล้ว ศาลยุติธรรมก็ชอบที่จะทำได้

ศาสตราจารย์จิตติ ติงศภัทิย์ ได้ให้ความเห็นว่า “หลักที่ว่าต้องตีความกฎหมายอาญาโดยเคร่งครัด จะขยายความไม่ได้นั้น หมายความเฉพาะกรณีที่หากขยายความในตัวบทออกไปจะเป็นผลร้ายแก่จำเลย หรือผู้ต้องหาเท่านั้น ไม่หมายความถึงการตีความไปในทางที่เป็นคุณแก่เขาเหล่านั้น ซึ่งอาจตีความโดยขยายความในเมื่อเป็นความประสงค์ของตัวบทกฎหมายนั้นๆ ได้”

ในประเด็นเดียวกันนี้ ดร.เกียรติขจร วัจนะสวัสดิ์ ได้ให้ความเห็นไว้ว่า “ในกฎหมายอาญานั้นห้ามเฉพาะการเทียบเคียง (Analogy) เพื่อเป็นโทษแต่ไม่ห้ามการตีความโดยขยายความ (extensive interpretation) แม้จะเป็นการขยายความเพื่อเป็นโทษก็ตาม”

5.3 ความสัมพันธ์ระหว่างการกระทำและผล

ความผิดที่ต้องมีผลแยกออกจากการกระทำ หรือที่เรียกกันว่า ความผิดที่ต้องมีผลปรากฏ เช่น ความผิดฐานฆ่าคนตาย ตามประมวลกฎหมายอาญา มาตรา 288 นั้น หากมีผลคือความตายของผู้ถูกกระทำเกิดขึ้น ผู้กระทำก็จะต้องรับผิดฐานฆ่าคนตายก็ต่อเมื่อความตายนั้นสัมพันธ์กับ

---

188 มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขาวิชานิติศาสตร์ (2544), อ้างแล้วในเชิงอรรถที่ 180 หน้า 110

การกระทำของผู้ถูกกระทำตามหลักในเรื่องความสัมพันธ์ระหว่างการกระทำและผล หากความตายนั้นไม่สัมพันธ์กับการกระทำของผู้กระทำ ตามหลักในเรื่องความสัมพันธ์ระหว่างการกระทำแล้ว ผู้กระทำก็ไม่ต้องรับผิดในความตายนั้น แต่อาจต้องรับผิดในการกระทำของตนก่อนเกิดผลนั้น เช่น รับผิดฐานพยายามฆ่า เป็นต้น

ทั้งนี้ ผู้กระทำจะต้องรับผิดในผลนั้น หากผลนั้นเป็น “ผลโดยตรง” หากไม่ใช่ “ผลโดยตรง” ก็ไม่ต้องรับผิดในผลนั้น ผลโดยตรง คือ ผลตาม “ทฤษฎีเงื่อนไข” ซึ่งมีหลักว่า “ถ้าไม่มีการกระทำผลไม่เกิด ถือว่า ผลเกิดจากการกระทำนั้น แม้ผลนั้นจะเกิดขึ้นได้ ต้องมีเหตุอื่นๆ ร่วมด้วยก็ตาม”

ถ้า “ผลโดยตรง” เกิดจาก “เหตุแทรกแซง” ผู้กระทำจะต้องรับผิดในผลนั้นก็ต่อเมื่อผลนั้นเกิดจาก “เหตุแทรกแซง” ที่คาดหมายได้ ในการวินิจฉัยว่าคาดหมายได้หรือไม่ ต้องใช้มาตรฐานของวิญญูชน “เหตุแทรกแซง” ที่ “คาดหมายได้” คือ เหตุตาม “ทฤษฎีเหตุที่เหมาะสม” นั่นเอง

ในกรณีที่ผลของการกระทำ ทำให้ผู้กระทำต้องรับโทษหนักขึ้น ผู้กระทำจะต้องรับผิดในผลนั้นก็ต่อเมื่อ เป็นทั้ง “ผลโดยตรง” และ “ผลธรรมดา”

“ผลธรรมดา” คือ ผลตาม “ทฤษฎีที่เหมาะสม” กล่าวคือ เป็นผลที่ผู้กระทำสามารถ “คาดเห็น” ความเป็นไปได้ของผลนั้น การวินิจฉัยความสามารถในการคาดเห็นใช้หลักมาตรฐานของวิญญูชน

แนวคิดและทฤษฎี เกี่ยวกับความสัมพันธ์ระหว่างการกระทำและผลข้างต้นนั้น ผู้เขียนเห็นว่า หากนำมาปรับใช้กับการกระทำความผิดฐานการเข้าถึงโดยมิชอบที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว จะเกิดปัญหาในการตีความในความรับผิดเป็นอย่างมาก กล่าวคือ หากพิจารณาตามความเสียหายหรือผลกระทบที่เกิดจากม้าโทรจันหรือสปายแวร์นั้น ความเสียหายที่เกิดขึ้นมิได้เป็นไปตามความหมายของชุดคำสั่งไม่พึงประสงค์ตามนัยแห่งมาตรา 21 วรรคสอง ที่จะต้องเป็นความเสียหายที่เห็นและปรากฏออกมาได้โดยชัดแจ้งในเชิงกายภาพ เช่น การที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เป็นต้น แต่ความเสียหายที่เกิดจากม้าโทรจันหรือสปายแวร์โดยการทำสำเนาหรือขโมยหรือดักข้อมูลแล้วส่งออกไปยังภายนอกนั้น ความเสียหายดังกล่าวจะไม่ได้ปรากฏขึ้นโดยชัดแจ้งหรืออาจเรียกได้ว่าเป็นความเสียหายโดยอ้อม เช่น ความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับ ไม่ว่าจะเป็นความลับต่อส่วนตัว หรือความลับในทางการค้า เป็นต้น ซึ่งในบางกรณีเจ้าของข้อมูลแทบจะไม่รู้ตัวด้วยซ้ำว่าถูกขโมยข้อมูล

ออกไป แม้ว่าในทางวิชาการและในเชิงของเทคนิคเฉพาะแล้ว จะสามารถหาพยานหลักฐานจากข้อมูลจราจรทางคอมพิวเตอร์เพื่อการค้นหาตัวผู้กระทำความผิดได้ก็ตาม แต่เมื่อได้ตัวผู้กระทำผิดมาแล้ว จะสามารถพิสูจน์ความเสียหายและผลกระทบที่เกิดจากม้าโทรจันหรือสปายแวร์นั้นได้อย่างไรว่า ความเสียหายที่เกิดขึ้นเป็นความเสียหายที่มีความสัมพันธ์กับการกระทำนั้น ที่จะถือเป็น “ผลโดยตรง” จากการกระทำนั้น นอกจากนี้ ยังมีกรณี “เหตุแทรกแซง” ที่จะต้องนำมาพิจารณาประกอบด้วย “เหตุแทรกแซง” ที่อาจเกิดขึ้นได้ในกรณีการเข้าถึงโดยมิชอบที่เกิดจากม้าโทรจันและสปายแวร์ก็เช่น ในระหว่างที่มีการส่งข้อมูลออกจากเครื่องที่ตกเป็นเหยื่อออกไปนั้นได้ถูกแฮกเกอร์หรือผู้บุกรุกอีกรายหนึ่งแอบดักข้อมูลนั้นไว้แล้วนำไปสร้างความเสียหายต่อไป หรือกรณีที่เจ้าของเครื่องที่ตกเป็นเหยื่อทราบว่ามีม้าโทรจันหรือสปายแวร์ติดตั้งหรือฝังตัวอยู่ในเครื่องแล้วทำการกำจัด (Clean) ออกไปจากระบบแต่ระหว่างการกำจัดได้เกิดความเสียหายกับข้อมูลที่อยู่ภายในเครื่อง (ซึ่งถ้าหากไม่เกิดจากการถูกเข้าถึงจากม้าโทรจันหรือสปายแวร์จนต้องทำการกำจัดดังกล่าวแล้วข้อมูลก็คงไม่เกิดความเสียหายขึ้น)[189] กรณีจึงมีปัญหาว่า เหตุแทรกแซงทั้งสองกรณีดังกล่าวจะถือเป็น “เหตุแทรกแซง” ที่คาดหมายได้ที่จะทำให้ผู้กระทำผิดต้องรับผิดตามทฤษฎีความสัมพันธ์ระหว่างการกระทำและผลหรือไม่

ที่กล่าวมาข้างต้นนั้น คือปัญหาที่อาจเกิดขึ้นเนื่องจากการใช้และการตีความกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่ผู้เขียนเห็นว่า บทบัญญัติและคำนิยามทางเทคนิคยังไม่มีความชัดเจนพอที่จะสามารถปรับใช้และแก้ไขปัญหาที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ได้ ทั้งนี้ ผู้เขียนจะได้นำเสนอในส่วนของบทสรุปและข้อเสนอแนะเพื่อหาทางการแก้ไขปัญหาเหล่านั้น ต่อไป

6. ปัญหาปลีกย่อยอื่น ๆ

ปัญหาทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ นอกจากปัญหาต่าง ๆ ตามที่ได้กล่าวไปแล้วข้างต้น ไม่ว่าจะเป็นปัญหาในการบัญญัติกฎหมาย หรือปัญหาในการใช้และการตีความกฎหมายแล้ว ยังมีปัญหาปลีกย่อยและเกร็ดเล็กเกร็ดน้อยจากมุมมองของนักวิชาการที่อยู่ในวงการ

---

189 การทำงานของบรรดาโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆ นั้น ในบางกรณีจะมีผลทำให้ข้อมูลที่มีอยู่ได้รับความเสียหายตามไปด้วย

คอมพิวเตอร์ได้ให้ความเห็นหรือมุมมองเกี่ยวกับมาตรา 21 ไว้อีกว่า[190] อาจถูกใช้เป็นเครื่องมือให้กับพนักงานเจ้าหน้าที่ไปในทางมิชอบได้ กล่าวคือ มาตรานี้จะสามารถใช้และปฏิบัติได้จริงหรือไม่ ทั้งนี้ เนื่องจากโดยปกติแล้วหากยังไม่มีการใช้งานโปรแกรมนั้นๆ หรือเกิดการกระทำความผิดใดๆ โดยโปรแกรมนั้นๆ ขึ้นก่อน การที่พนักงานเจ้าหน้าที่สักคนจะล่วงรู้ หรือพบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย หรือไม่นั้น จะต้องเป็นกรณีที่พนักงานเจ้าหน้าที่เรียกเจ้าของโปรแกรมมาเปิดซอร์สโค้ดให้ดูเพราะในทางปฏิบัติ โอกาสที่พนักงานเจ้าหน้าที่จะตรวจพบชุดคำสั่งคอมพิวเตอร์ไม่พึงประสงค์ที่แอบแฝงหรือปะปนอยู่กับข้อมูลคอมพิวเตอร์อื่นเป็นไปได้ยากมากหรือแทบจะเป็นไปไม่ได้เลย หรือไม่ก็ต้องมีการตรวจสอบหรือสแกนโดยพนักงานเจ้าหน้าที่เองเสียก่อน ซึ่งถ้าเป็นเช่นนั้นก็แสดงว่าพนักงานเจ้าหน้าที่จะต้องมีอำนาจบางอย่างที่จะเข้าไปสแกนเพื่อตรวจสอบซอร์สโค้ดของโปรแกรมต่างๆ ที่อยู่ในความครอบครองของเจ้าของหรือผู้ประกอบการก่อนที่มีการใช้งานจริง หรือก่อนที่จะมีการนำไปใช้เพื่อกระทำความผิดโดยชุดคำสั่งนั้นๆ ด้วย ซึ่งบทบัญญัติของกฎหมายในปัจจุบันมิได้ให้อำนาจเช่นนั้นกับพนักงานเจ้าหน้าที่ หรือหากเป็นเช่นนั้นจริงก็จะส่งผลกระทบและเกิดความปั่นป่วนต่ออุตสาหกรรมที่ผลิตชุดคำสั่งในทางป้องกันหรือแก้ไขความเสียหายซึ่งได้แก่ อุตสาหกรรมซอฟท์แวร์เพื่อการป้องกันหรือแก้ไขไวรัสหรือแก้ไขปัญหาจากมัลแวร์ในรูปแบบต่างๆ ได้ ซึ่งก็คงไม่ใช่เจตนารมณ์ของกฎหมายอย่างแน่นอน

นอกจากนี้ ความหมายของ “ชุดคำสั่งไม่พึงประสงค์” ในวรรคสองของมาตรา 21 ที่ว่า “ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้” นั้น ในกรณีที่เป็นบั๊ก (Bug หมายถึง จุดบกพร่อง)[191] ของโปรแกรมหรือชุดคำสั่งต่างๆ จะจัดให้อยู่ในความหมายดังกล่าวหรือไม่ เนื่องจากบั๊กสามารถเกิดขึ้นได้กับทุกๆ โปรแกรมแม้จะไม่ใช่โปรแกรมไม่พึงประสงค์ก็ตาม ซึ่งก็เท่ากับว่าหากพนักงานเจ้าหน้าที่สักคนลุกขึ้นมาบอกว่าโปรแกรมหรือชุดคำสั่งใดเป็นบั๊กก็ต้องถือเป็นชุดคำสั่งไม่พึงประสงค์ด้วย ซึ่งเข้าข่ายที่จะสั่งให้ เลิกขาย เลิกจำหน่าย เลิกใช้ได้” หากเป็นเช่นนั้น สังคมก็คงเกิดความปั่นป่วนน่าดู

ดังนั้น จากปมปัญหาทางกฎหมายที่สำคัญในหลาย ๆ ประเด็น ตามที่ได้กล่าวถึงและวิเคราะห์ไปแล้วข้างต้น ล้วนแต่เป็นปัญหาที่เกี่ยวข้องกับชุดคำสั่งไม่พึงประสงค์ทั้งสิ้น สาเหตุที่ทำให้เกิดปัญหาเช่นนั้น ก็อาจเป็นเพราะความที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับ

---

190 ความเห็นจากเจ้าของบทความ “กฎหมาย ที่ร่างกันแบบไม่เร่ง แต่ผ่านกันแบบรีบๆ (ตอน 3)” จากบล็อก (Blog) กฎหมาย ในเว็บไซต์ http://www.BioLawCom.De Retrieved December, 24, 2010

191 ราชบัณฑิตยสถาน, อ้างแล้วในเชิงอรรถที่ 15 หน้า 16

คอมพิวเตอร์เป็นกฎหมายพิเศษเฉพาะและต้องมีรายละเอียดด้านเทคนิคอื่นๆ ประกอบอีกมากมาย จึงทำให้ผู้ที่เกี่ยวข้องในการบัญญัติกฎหมายดังกล่าว คาดการณ์ไม่ถึงว่าจะเกิดปัญหาเช่นนั้นได้ หรืออาจเป็นเพราะการขาดความเข้าใจในเชิงการคิดและวิเคราะห์ รวมทั้งมิได้มีการศึกษาข้อเท็จจริงเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ให้ละเอียดลึกซึ้งอย่างแท้จริงจนเพียงพอเสียก่อนที่จะบัญญัติมาตรการทางกฎหมายต่างๆ อันเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ออกมา ซึ่งผู้เขียนจะได้นำเสนอในส่วนของบทสรุปและข้อเสนอแนะเพื่อหาทางการแก้ไขปัญหา ต่อไป

บทที่ 6
บทสรุปและข้อเสนอแนะ

1. บทสรุป

จากการศึกษาเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์และมาตรการทางกฎหมายในต่างประเทศและแนวทางขององค์การระหว่างประเทศโดยการวิเคราะห์และเปรียบเทียบกับมาตรการทางกฎหมายในประเทศไทย ทั้งในส่วนของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ประมวลกฎหมายอาญา และมาตรการในการคุ้มครองข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในรูปแบบข้อมูลคอมพิวเตอร์ของประเทศไทยแล้วพบว่า แนวทางขององค์การระหว่างประเทศ (อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของคณะมนตรีแห่งยุโรป (Council of Europe)) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์มีการเสนอแนะให้แต่ละประเทศตรากฎหมายภายในให้มีความสอดคล้องกันในฐานความผิดที่สำคัญ ซึ่งกฎหมายของต่างประเทศส่วนใหญ่แล้วเป็นไปในแนวทางเดียวกัน คือ มีการกำหนดฐานความผิดการรบกวนข้อมูลหรือโปรแกรมคอมพิวเตอร์เพื่อให้ได้มาซึ่งประโยชน์ในทางทรัพย์สิน การปลอมแปลงทางคอมพิวเตอร์ การขัดขวางการทำงานของคอมพิวเตอร์และระบบโทรคมนาคม การเข้าถึงหรือลักลอบดักการข้อมูลที่สื่อสารในระบบคอมพิวเตอร์หรือระบบโทรคมนาคมโดยมิชอบ เป็นต้น ทั้งนี้ประเทศไทยก็ได้นำหลักการดังกล่าวมาบัญญัติไว้ในกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แทบทั้งหมดแล้ว ทั้งในส่วนของกฎหมายสารบัญญัติและกฎหมายวิธีสบัญญัติ กล่าวคือ หมวด 1 (ความผิดเกี่ยวกับคอมพิวเตอร์) ถือเป็นกฎหมายในส่วนสารบัญญัติ ส่วน หมวด 2 (พนักงานเจ้าหน้าที่) ถือเป็นกฎหมายในส่วนวิธีสบัญญัติเพื่อใช้สำหรับการดำเนินกระบวนพิจารณาทางอาญาเฉพาะคดีความผิดเกี่ยวกับคอมพิวเตอร์

สำหรับประเภทของชุดคำสั่งไม่พึงประสงค์นั้น สามารถแยกได้เป็น 2 ประเภทใหญ่ ๆ ตามความหมายและคุณสมบัติ คือ (1) ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายที่สามารถรวบรวมและจัดเป็นหมวดหมู่ได้ 17 ประเภท ได้แก่ ไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ ม้าโทรจัน สปายแวร์ แอดแวร์ โปรแกรมทดสอบช่องโหว่ โปรแกรมเจาะระบบ โปรแกรมดาวน์โหลดไวรัส โปรแกรมปล่อยไวรัส โปรแกรมฉีดไวรัส

โปรแกรมชุดสร้างไวรัส โปรแกรมสำหรับส่งสแปม โปรแกรมระเบิด โปรแกรมโทรศัพท์อัตโนมัติ โปรแกรมล้อกันเล่น ฟลัดเดอร์ รูทคิท ซึ่งแต่ละประเภทก็สามารถแยกออกเป็นชนิดได้อีก และ (2) ชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายซึ่งได้แก่ บรรดาโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่างๆ เป็นต้น

อย่างไรก็ตาม เมื่อได้ศึกษาและวิเคราะห์ถึงคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายแล้วพบว่า มีชุดคำสั่งไม่พึงประสงค์อยู่สองประเภทที่ทำให้เกิดปัญหาในทางกฎหมาย คือ ม้าโทรจันและสปายแวร์ กล่าวคือ ม้าโทรจันและสปายแวร์จะมีคุณสมบัติพิเศษกว่าชุดคำสั่งไม่พึงประสงค์ประเภทอื่น ๆ ตรงที่ หากมีการเผยแพร่หรือจำหน่ายหรือใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ในการกระทำความผิดแล้ว ก็จะทำให้พนักงานเจ้าหน้าที่มิอาจอาศัยอำนาจตามมาตรา 21 วรรคหนึ่ง ในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ที่มีม้าโทรจันและสปายแวร์ติดตั้งหรือฝังอยู่ได้ หรือจะขอให้ศาลมีคำสั่งเพื่อกำหนดเงื่อนไขในการใช้มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวนั้นก็ไม่ได้อีกเช่นกัน สาเหตุที่เป็นเช่นนั้นก็เพราะความหมายของชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคสอง ที่บัญญัติว่า“ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา” นั้น ยังมิอาจแปลความได้ว่าม้าโทรจันและสปายแวร์จัดเป็นชุดคำสั่งไม่พึงประสงค์ตามความหมายดังกล่าว เนื่องจาก คุณสมบัติของม้าโทรจันและสปายแวร์มิได้มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด

จากการศึกษาและวิเคราะห์ในประเด็นปัญหาทางกฎหมายและปัญหาในทางปฏิบัติเพื่อการบังคับใช้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์แล้ว พบประเด็นปัญหาที่ควรหาแนวทางการแก้ไขให้เหมาะสมอยู่ด้วยกัน 5 ประเด็น คือ

1. ปัญหาในการบังคับใช้กฎหมาย ได้แก่

1.1 ความไม่ชัดเจนและไม่สอดคล้องกับทางปฏิบัติของส่วนกฎหมายวิธีสบัญญัติตาม มาตรา 21 โดยแยกเป็น (1) ปัญหาในการบังคับใช้กฎหมายในมาตรา 21 วรรคหนึ่ง ซึ่งมีอยู่สองประการ คือ ปัญหาในทางปฏิบัติที่พนักงานเจ้าหน้าที่ไม่อาจตรวจสอบได้ว่าข้อมูลคอมพิวเตอร์ใดมี

ชุดคำสั่งไม่พึงประสงค์แอบแฝงหรือปะปนรวมอยู่ด้วยได้ และในความเป็นจริงชุดคำสั่งไม่พึงประสงค์นอกจากจะถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์แล้ว ยังถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลอื่นอีกมากมาย เช่น แฟลชไดรว์, แผ่นซีดี, แผ่น DVD, External Hard Disk เป็นต้น แต่กฎหมายมิได้มีฐานอำนาจรองรับเพื่อให้พนักงานเจ้าหน้าที่เข้าไปตรวจเพื่อหาชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลเหล่านั้นได้ และ (2) หากมีการเผยแพร่หรือจำหน่ายหรือใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือ สปายแวร์ในการกระทำความผิดแล้ว ก็จะทำให้พนักงานเจ้าหน้าที่มิอาจอาศัยอำนาจตามมาตรา 21 วรรคหนึ่ง ในการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่าย หรือเผยแพร่ข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลายหรือแก้ไขข้อมูลคอมพิวเตอร์ที่มีม้าโทรจันและสปายแวร์ติดตั้งหรือฝังอยู่ได้ หรือจะขอให้ศาลมีคำสั่งเพื่อกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวนั้นก็ไม่ได้อีกเช่นกัน

1.2 การมิได้แยกแยะประเภทของชุดคำสั่งไม่พึงประสงค์ มีผลทำให้ปัจจุบันยังไม่มีชุดคำสั่งไม่พึงประสงค์ใดที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันและแก้ไขชุดคำสั่งอื่นเลย ทั้งที่ในความเป็นจริงแล้วยังมีชุดคำสั่งอีกหลายประเภทที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์อื่นที่ถูกพบเห็นและนำมาใช้ในชีวิตประจำวันของประชาชนทั่วไป เช่น โปรแกรมต่อต้านและตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ หรือม้าโทรจัน โปรแกรมต่อต้านการส่งสแปมเมล์ เป็นต้น จึงทำให้พนักงานเจ้าหน้าที่และประชาชนเกิดความสับสนและความไม่แน่ใจในทางปฏิบัติและมิได้เป็นไปตามเจตนารมณ์ของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2. ปัญหาในการบัญญัติกฎหมาย ได้แก่

2.1 ปัญหาการกำหนดนิยามและความหมายทางเทคนิคที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มิได้กำหนดนิยามความหมายของคำว่า “เข้าถึง (access)” ไว้โดยตรงทำให้มิอาจบังคับและตีความไปถึงการกระทำผิดโดยใช้ม้าโทรจันและสปายแวร์ได้ และเมื่อนำกฎหมายของไทยไปเปรียบเทียบกับกฎหมายของต่างประเทศจะพบว่ามีความแตกต่างกันอย่างมีนัยสำคัญ กล่าวคือ ตามกฎหมายของไทยหากสามารถเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ผู้กระทำประสงค์จะเข้าถึง และเมื่อสามารถเข้าถึงได้แล้ว ก็ย่อมจะถือว่าการกระทำการเข้าถึงดังกล่าวได้สำเร็จลงแล้ว และภายหลังจากนั้นหากมีการทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ หรือทำการรบกวนต่างๆ จนทำให้ระบบคอมพิวเตอร์หยุดทำงานนั้นก็ยังอยู่ในความหมายของการเข้าถึงตามกฎหมายของไทย แต่หากมีกรณีการได้ใช้ประโยชน์อื่นใดภายหลังจากการเข้าถึงที่ไม่เข้ากรณีดังกล่าว เช่น (1) มีการทำซ้ำหรือ

โอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ (2) การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการเพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์หรือได้รับข้อมูลคอมพิวเตอร์จากระบบคอมพิวเตอร์ดังกล่าว หรือ (3) การสั่งการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลหรือหน่วยบันทึกผลของระบบคอมพิวเตอร์อื่นได้ ตลอดจนการกระทำการอื่นใดเพื่อแสวงหาประโยชน์จากระบบคอมพิวเตอร์ที่ถูกเข้าถึงโดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้นั้นกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยคงมิอาจบังคับและตีความไปถึงได้ เพราะหลักการตีความกฎหมายอาญาต้องตีความโดยเคร่งครัดและเป็นไปตามหลักสากลที่ว่า “ไม่มีกฎหมาย ไม่มีความผิด”

2.2 ปัญหาการกำหนดฐานความผิดที่แม้พระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะได้กำหนดฐานความผิดและบทลงโทษสำหรับผู้ที่จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 ถึงมาตรา 11 และมีมาตรการในการดำเนินการเกี่ยวกับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ไว้ในมาตรา 21 แล้วก็ตาม แต่บทบัญญัติในมาตราดังกล่าวยังไม่ครอบคลุมถึงลักษณะของการกระทำความผิดที่เกิดจากการใช้ม้าโทรจันและสปายแวร์นำไปฝังหรือติดตั้งไว้ในระบบคอมพิวเตอร์แล้วจะมีการแอบส่งข้อมูลคอมพิวเตอร์ หรือแอบดักข้อมูลต่างๆ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลสำคัญที่เป็นเอกลักษณ์บุคคลส่งออกไปยังคนร้ายหรือผู้บุกรุก หากการกระทำความผิดดังกล่าวเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เป็นการเข้าไปทำลาย แก้ไข เปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือเป็นการเข้าไปรบกวนต่อระบบคอมพิวเตอร์โดยการฝ่าฝืนมาตรการป้องกันที่จัดทำไว้เป็นการเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ก็จะถือเป็นความผิดตามมาตรา 5 ถึง มาตรา 11 ได้ แต่หากการเข้าถึงดังกล่าวนั้นเป็นการเข้าถึงโดยชอบไม่ว่าจะเป็นเพราะความยินยอมของเจ้าของคอมพิวเตอร์นั้น หรือในบางกรณีแฮกเกอร์หรือคนร้ายอาจใช้เทคนิคการหลอกล่อเพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป แล้วต่อมามีการแอบส่งข้อมูลคอมพิวเตอร์ออกไปยังคนร้าย ก็จะทำให้การเข้าถึงในกรณีนี้ไม่เข้าข่ายเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และไม่เป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา และไม่เป็นความผิดตามพระราชบัญญัติอื่นที่มีโทษทางอาญาเลย ทั้งนี้ประเด็นการขโมยหรือแอบส่งหรือแอบดักข้อมูลด้วยม้าโทรจันหรือสปายแวร์ยังถือเป็นการกระทำละเมิดต่อข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์อีกด้วย ซึ่งปัจจุบันก็ยังไม่มีกฎหมายใดที่จะสามารถปรับใช้เพื่อการป้องกันหรือปราบปรามการกระทำความผิดดังกล่าวได้

2.3 ปัญหาความหมายคำว่า “โดยมิชอบ” ซึ่งผู้เขียนเห็นว่าองค์ประกอบของความผิด “เข้าถึงโดยมิชอบ” เป็นการรวมคำสองคำเข้าด้วยกัน คือ คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” แต่มิได้หมายความว่าเมื่อนำไปปรับใช้กับฐานความผิดการเข้าถึงโดยมิชอบแล้วจะต้องตีความรวมเป็นคำเดียวกัน แต่ในทางตรงกันข้ามผู้เขียนเห็นว่า คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” จะต้องตีความแยกออกจากกันซึ่งจะทำให้ง่ายแก่การทำความเข้าใจความหมายของทั้งสองคำดังกล่าว หรือหากจะนำแนวคำพิพากษาศาลฎีกามาเป็นเกณฑ์ในการกำหนดหลักเกณฑ์ในการตีความ คำว่า “โดยมิชอบ” และปล่อยให้เป็นหน้าที่ของศาลที่จะตีความให้เหมาะสมกับพฤติกรรมของผู้กระทำผิดในแต่ละคดีนั้นคงไม่เหมาะสม เพราะแนวคำพิพากษาของศาลฎีกาในปัจจุบันมิใช่เป็นคดีความผิดที่เกี่ยวกับคอมพิวเตอร์ แต่เป็นคดีแพ่งและคดีอาญาทั่วไป ซึ่งที่มาของการบัญญัติกฎหมายมีความแตกต่างจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และตัวผู้พิพากษาที่ตัดสินคดีนั้นก็อาจมิได้เป็นผู้ที่มีความรู้หรือมีความเชี่ยวชาญด้านคอมพิวเตอร์อย่างเพียงพอที่จะสามารถใช้เป็นบรรทัดฐานในการตัดสินคดีความผิดเกี่ยวกับคอมพิวเตอร์ได้

3. ปัญหาการใช้และการตีความกฎหมาย ได้แก่

3.1 กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง ที่ประกอบด้วย 3 ส่วนที่สำคัญคือ (1) บทบัญญัติกฎหมายอาญาต้องเป็นลายลักษณ์อักษรซึ่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มิได้บัญญัติหรือกำหนดความหมายของคำว่า “เข้าถึง” ไว้ ทำให้กรณีของการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลโดยเฉพาะอย่างยิ่งการเข้าถึงโดยใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์เป็นช่องว่างของกฎหมาย ทำให้ผู้กระทำผิดไม่ต้องรับผิดทั้งๆที่จริงแล้วผู้กระทำผิดสมควรจะต้องได้รับโทษนั้นแต่บทบัญญัติของกฎหมายตีความไปไม่ถึง ทำให้ต้องปล่อยตัวผู้ต้องหาหรือจำเลยไปในที่สุด (2) กฎหมายอาญาต้องมีบทบัญญัติความผิดและโทษไว้ในขณะกระทำ (3) บทบัญญัติกฎหมายอาญาต้องชัดเจนปราศจากการคลุมเครือ ซึ่งคำว่า “เข้าถึง” จัดได้ว่าเป็นศัพท์เฉพาะที่มิใช่ภาษาสามัญธรรมดา จึงจำเป็นต้องกำหนดเป็นคำนิยามไว้ เพื่อจะได้เป็นบรรทัดฐานในการบังคับใช้และการตีความกฎหมายของเจ้าพนักงานในการยุติธรรมโดยเฉพาะพนักงานเจ้าหน้าที่

3.2 กฎหมายอาญาต้องตีความโดยเคร่งครัด ที่ประกอบด้วย 4 ส่วนสำคัญ ได้แก่ (1) การตีความตามตัวอักษรโดยความผิดฐานการเข้าถึงโดยมิชอบจะถือว่าเป็นความผิดสำเร็จก็เมื่อผ่านการเข้าถึงโดยฝ่าฝืนมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน แต่ต่อจากนั้นหากการติดต่อสื่อสารระหว่างคอมพิวเตอร์ที่ใช้ในการเข้าถึงกับเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อถูกตัดขาดจากกันแล้ว การเข้าถึงในคราวนั้นจึงสิ้นสุดลง หากต่อมาม้าโทรจันหรือ

สปายแวร์ได้ทำการสำเนาหรือขโมยหรือดักข้อมูลแล้วส่งออกไปยังภายนอก หากจะแปลความว่ามีการติดต่อสื่อสารในขณะที่เครื่องที่ตกเป็นเหยื่อส่งข้อมูลออกไปนั้นเป็นการสื่อสารที่เกิดขึ้นใหม่ก็มิได้หมายความว่าเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายถูกเข้าถึงอีกครั้ง แต่ในทางตรงกันข้ามเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายเข้าถึงเครื่องที่ใช้ในการโจมตีในครั้งก่อน กรณีจึงเป็นเรื่องยากที่จะตีความได้ว่าเครื่องที่ตกเป็นเหยื่อเป็นฝ่ายถูกเข้าถึง เพราะไม่มีถ้อยคำใดในกฎหมายฉบับนี้ที่บัญญัติไว้ให้ตีความได้เช่นนั้น (2) การตีความตามเจตนารมณ์ ที่เมื่อพิจารณาจากเหตุผลในการตราพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้ว ก็ยังไม่อาจแปลได้ว่า กฎหมายดังกล่าวจะมีเจตนารมณ์ในการคุ้มครองถึงการขโมยข้อมูลที่เกิดจากชุดคำสั่งไม่พึงประสงค์ด้วย (3) กรณีเป็นที่สงสัยที่อาจตีความได้เป็นหลายนัย ศาลอาจจะตีความได้เป็น 2 แนวความเห็น คือแนวความเห็นที่หนึ่งศาลจะแปลไปในทางที่เป็นประโยชน์แก่จำเลยโดยขยายความไปไม่ได้ เพราะศาลไม่มีหน้าที่ช่วยจำเลย มีแต่ลงโทษคนผิด และไม่ลงโทษผู้ไม่ผิด และแนวความเห็นที่สอง ศาลจะต้องตีความให้เป็นประโยชน์แก่ผู้ต้องหา (in dubio pro reo) มากกว่าและไม่มีเหตุผลอันใดที่จะจำกัดการให้ประโยชน์แก่จำเลยในคดีอาญาแต่เฉพาะปัญหาข้อเท็จจริง แม้แต่ในปัญหาข้อกฎหมายโดยเฉพาะในการตีความกฎหมาย ศาลย่อมให้ประโยชน์แห่งความสงสัยแก่จำเลยได้ดุจกัน (4) การเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง (Analogy) อาจนำมาใช้เพื่อเป็นคุณหรือเป็นประโยชน์แก่ผู้กระทำได้ แต่จะนำมาใช้เพื่อเป็นโทษหรือเป็นผลร้ายมิได้ ซึ่งนักนิติศาสตร์ทั้งหลายมีความเห็นเป็นแนวเดียวกัน คือ ศาสตราจารย์ เอกูต์ ศาสตราจารย์ พระยาอรรถการียพันธ์ และศาสตราจารย์หยุด แสงอุทัย (5) การตีความโดยขยายความ จะนำมาใช้ในทางที่เป็นโทษแก่จำเลยหรือผู้ต้องหาไม่ได้

4. ปัญหาความรับผิดในทางอาญา ซึ่งแยกออกได้เป็น

4.1 ปัญหาในเรื่ององค์ประกอบภายนอกของความรับผิดทางอาญาว่า การเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลที่เกิดจากม้าโทรจันและสปายแวร์จะถือเป็น “การกระทำ” ตามประมวลกฎหมายอาญา หรือไม่ เนื่องจากบทบัญญัติตามมาตรา 59 แห่งประมวลกฎหมายอาญาในตอนต้นที่ว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำ...” แสดงว่าการกระทำเป็นเงื่อนไขประการแรกของความรับผิดในทางอาญา ทั้งนี้ องค์ประกอบภายนอกของความรับผิดทางอาญาในอาชญากรรมพื้นฐาน (Conventional Crimes) นั้น จะพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึก กล่าวคือ การเคลื่อนไหวร่างกายนั้นต้องอยู่ภายใต้บังคับของจิตใจ แต่สำหรับอาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ที่ใช้ชุดคำสั่งไม่ถึงประสงค์เป็นเครื่องมือในกระทำผิดโดยการเข้าถึงนั้น การพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึกเพียงอย่างเดียวนั้นไม่เพียงพอที่จะถือว่า

บุคคลนั้นมี “การกระทำ” หรือไม่ แต่จะต้องพิจารณาจากลักษณะหรือผลที่ปรากฏออกมา ซึ่งได้แก่ การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ประกอบด้วยเสมอ

ทั้งนี้ ผลจากการศึกษาและวิเคราะห์ถึงคุณสมบัติของม้าโทรจันและสปายแวร์ พบว่า ม้าโทรจันและสปายแวร์นั้น ไม่มีคุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แต่อย่างใด สาเหตุที่เป็นเช่นนั้นก็เพราะเมื่อม้าโทรจันและสปายแวร์ถูกนำไปติดตั้งหรือฝังไว้ในระบบคอมพิวเตอร์ที่ตกเป็นเหยื่อแล้วจะมิได้ก่อให้เกิดความเสียหายใดๆ ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น โดยสามารถพิจารณาได้จากการที่ระบบคอมพิวเตอร์นั้นยังสามารถทำงานได้โดยสมบูรณ์อยู่นั่นเอง กรณีดังกล่าวจึงก่อให้เกิดปัญหาการตีความในองค์ประกอบภายนอกของความรับผิดทางอาญาที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์เป็นอย่างมาก

4.2 ปัญหาในเรื่องของความสัมพันธ์ระหว่างการกระทำและผล ที่หากนำมาปรับใช้กับการกระทำความผิดฐานการเข้าถึงโดยมิชอบที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว จะเกิดปัญหาในการตีความในความรับผิดเป็นอย่างมาก เพราะความเสียหายหรือผลกระทบที่เกิดจากม้าโทรจันหรือสปายแวร์นั้น มิได้เป็นความเสียหายที่เห็นและปรากฏออกมาได้โดยชัดแจ้งในเชิงกายภาพ อาจเรียกได้ว่าเป็นความเสียหายโดยอ้อม เช่น ความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับ ไม่ว่าจะเป็นความลับต่อส่วนตัว หรือความลับในทางการค้า เป็นต้น นอกจากนี้ ยังมีกรณี “เหตุแทรกแซง” ที่จะต้องนำมาพิจารณาประกอบด้วย ซึ่งจะต้องเป็น “เหตุแทรกแซง” ที่คาดหมายได้จึงจะทำให้ผู้กระทำผิดต้องรับผิดตามทฤษฎีความสัมพันธ์ระหว่างการกระทำและผลได้

5. ปัญหาปลีกย่อยอื่น ๆ ได้แก่ (1) มาตรา 21 อาจถูกใช้เป็นเครื่องมือให้กับพนักงานเจ้าหน้าที่ไปในทางมิชอบได้ (2) ความหมาย “ชุดคำสั่งไม่พึงประสงค์” ที่ว่า “ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้” นั้น ในกรณีที่เป็นบั๊ก (Bug) ของโปรแกรมหรือชุดคำสั่งต่างๆ จะจัดให้อยู่ในความหมายดังกล่าวหรือไม่

นอกจากปัญหาเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ทั้ง 5 ประเด็นข้างต้นแล้ว ยังมีประเด็นปัญหาการขโมยเอกลักษณ์บุคคล (Identity Theft) ที่ผู้เขียนเห็นว่า เป็นประเด็นที่มีความสำคัญและมีความเกี่ยวพันโดยตรงกับชุดคำสั่งไม่พึงประสงค์ กล่าวคือ เป้าประสงค์หรือวัตถุแห่งการกระทำที่ผู้กระทำผิดต้องการเนื่องจากการใช้ชุดคำสั่งไม่พึงประสงค์นอกจากความเสียหายหรือผลกระทบต่อ

ระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ที่ปรากฏออกมาในรูปแบบต่างๆ ได้หลายๆ รูปแบบ เช่น ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ แล้ว ความเสียหายจากการถูกขโมยเอกลักษณ์บุคคลก็เป็นสิ่งที่ผู้กระทำผิดต้องการ เพื่อนำไปประกอบอาชญากรรมอื่นๆ ต่อไป ซึ่งประมวลกฎหมายอาญา และกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยมิอาจบังคับให้ครอบคลุมไปถึงฐานความผิดที่เกิดจากการใช้ชุดคำสั่งไม่พึงประสงค์ในการขโมยข้อมูลส่วนบุคคลที่เก็บอยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ได้ เนื่องจากกฎหมายไทยมีช่องว่างในประเด็นของการกำหนดนิยามความหมายของคำว่า “เข้าถึง (access)” และประเด็นการกำหนดองค์ประกอบของความผิดฐานเข้าถึงโดยมิชอบ (Illegal access) ที่ยังไม่ครอบคลุมถึงลักษณะและพฤติการณ์ของการกระทำความผิดที่เกิดจากการนำชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์ที่อาจถูกนำไปฝังหรือติดตั้งไว้ในระบบคอมพิวเตอร์แล้วทำการขโมยข้อมูลสำคัญหรือข้อมูลเอกลักษณ์บุคคลออกไปโดยมิอาจปรับเป็นความผิดในฐานใดตามกฎหมายที่มีโทษทางอาญาได้เลย

เกี่ยวกับประเด็นการกำหนดฐานความผิดการเข้าถึงโดยมิชอบขโมยข้อมูลเอกลักษณ์บุคคลด้วยมัลแวร์ตามกรณีข้างต้นนี้ ได้มีนักกฎหมายนำไปเปรียบเทียบกับการบุกรุกทางกายภาพว่าเมื่อการเข้าถึงนั้นชอบด้วยกฎหมายหรือมีอำนาจก็จะทำให้การกระทำต่อมาภายหลังจากการเข้าถึงแล้วนั้นย่อมไม่เป็นความผิดฐานเข้าถึงอีกเนื่องจากการเข้าถึงในตอนแรกชอบแล้ว ผู้เข้าถึงจึงมีสิทธิที่จะกระทำได้ ความยินยอมย่อมทำให้การเข้าถึงนั้นชอบเช่นเดียวกับการเข้าไปโดยชอบแล้วทะเลาะกันภายหลังก็ไม่เป็นบุกรุก อย่างไรก็ตาม เนื่องจากคำว่า “เข้าถึง” นั้น มีความหมายที่แตกต่างจากคำว่า “บุกรุก” จึงอาจมองได้ในอีกแง่มุมหนึ่งว่าการเข้าถึงคอมพิวเตอร์นั้นหากการเข้าถึงยังคงมีอยู่ตลอดไปตราบใดที่ยังมีการสื่อสารกับคอมพิวเตอร์อยู่ ไม่ว่าจะได้รับอนุญาตโดยชอบหรือมีอำนาจตามกฎหมายแล้วก็ตาม ก็อาจเป็นการเข้าถึงโดยมิชอบได้ทันทีที่ผู้เข้าถึงนั้นกระทำสิ่งที่ไม่ถูกต้องหรือไม่เหมาะสมขึ้น เช่น การขโมยข้อมูลในคอมพิวเตอร์ที่ตนได้รับอนุญาตให้เข้าถึงได้เนื่องจากผู้อนุญาตให้เข้าถึงนั้นไม่มีเจตนาให้ผู้ที่ได้รับอนุญาตกระทำสิ่งที่ตนไม่ต้องการ เช่น ขโมยข้อมูล เป็นต้น ซึ่งหากพิจารณาในแง่นี้แล้ว การเข้าถึงจะคงอยู่ตลอดและเมื่อทำสิ่งที่ไม่ชอบขึ้นก็จะเป็นการเข้าถึงที่ไม่ชอบและเป็นความผิดทันที[192] ซึ่งผู้เขียนไม่เห็นด้วยกับแนวคิดดังกล่าว เนื่องจากไม่มีเหตุผลรองรับอย่างเพียงพอ และไม่เป็นไปตามหลักของการบังคับใช้

---

192 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 163

กฎหมายในหลายๆ ประเด็นได้แก่ กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง และกฎหมายอาญาต้องตีความโดยเคร่งครัด ตามที่ได้กล่าวไปแล้วในข้อ 3 ข้างต้น

อย่างไรก็ตาม ในส่วนของรูปแบบการขโมยเอกลักษณ์บุคคล (Identity theft) นั้น ในต่างประเทศได้มีการตรากฎหมายขึ้นมาควบคุมปัญหานี้เป็นการเฉพาะ ทั้งนี้สามารถสรุปรูปแบบของภัยดังกล่าวได้เป็น 4 ประเภทด้วยกัน คือ

1. การขโมยความเป็นเอกลักษณ์บุคคลทางการเงิน (Financial Identity Theft) ได้แก่ การใช้ชื่อของผู้อื่นและ SSN เพื่อให้ได้มาซึ่งสินค้าและการบริการ

2. การขโมยความเป็นเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรม (Criminal Identity Theft) โดยทำทีว่าเป็นบุคคลอื่นเมื่อถูกสงสัยว่าได้ก่ออาชญากรรม

3. โคลนนิ่งความเป็นเอกลักษณ์บุคคลของบุคคลอื่น (Identity Cloning) โดยการใช้ข้อมูลของผู้อื่น เพื่อให้เข้าใจว่าผู้ถูกปลอมแปลงความเป็นเอกลักษณ์บุคคลเป็นผู้กระทำการด้วยตนเอง

4. การขโมยความเป็นเอกลักษณ์บุคคลในทางการค้าและธุรกิจ (Business/ Commercial Identity Theft) โดยการใช้ชื่อผู้อื่นเพื่อให้ได้มาซึ่งเครดิตต่างๆ

สำหรับประเทศไทยนั้น พัฒนาการของปัญหาด้านการขโมยเอกลักษณ์บุคคลยังไม่พัฒนาไปไกลเหมือนในต่างประเทศเพียงแต่พบว่า มีการปลอมและแปลงเอกสารซึ่งเป็นการปลอมและแปลงทางกายภาพเพื่อใช้ในการหลอกลวง ฉ้อโกง ต่างๆ และการขโมยเอกลักษณ์บุคคลในทางการเงิน เช่น อีแบงค์กิ้ง (e-Banking), อีเปย์ (e-Pay) หรือระบบการให้บริการของธนาคารผ่านทางอินเทอร์เน็ต เป็นต้น ส่วนการขโมยเอกลักษณ์บุคคลในทางการค้าและธุรกิจโดยการใช้ชื่อผู้อื่นเพื่อให้ได้มาซึ่งเครดิตต่างๆ นั้นยังไม่ปรากฏข้อมูลในส่วนนี้ จะมีก็เพียงคดีเกี่ยวกับการปลอมและแปลงบัตรเครดิตที่มีให้เห็นและเป็นข่าวทางสื่อต่างๆ อยู่เป็นระยะซึ่งก็ถือเป็นความผิดตามประมวลกฎหมายอาญามิใช่ความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์แต่อย่างใด ส่วนการใช้ชุดคำสั่งไม่พึงประสงค์ก็มักจะใช้เพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์ที่แสดงถึงตัวตนหรือเอกลักษณ์ของบุคคลและถือเป็นข้อมูลส่วนบุคคลรวมอยู่ด้วย โดยมูลเหตุจูงใจก็เพื่อสำหรับการนำไปใช้ในการก่ออาชญากรรมด้านการเงิน หรืออาชญากรรมด้านอื่นๆ หรือเพื่อการก่อความเดือดร้อนรำคาญหรือความเสียหายต่อเจ้าของข้อมูลต่อไป ซึ่งอาจไม่ถึงขั้นที่จะถือว่าเป็นการขโมยเอกลักษณ์บุคคลตามแบบอย่างของต่างประเทศ ดังนั้น ประเด็นการนำหลักการของกฎหมายเกี่ยวกับการขโมยเอกลักษณ์บุคคลของต่างประเทศมาใช้หรือมาบัญญัติในกฎหมายของประเทศไทยในปัจจุบัน จึงอาจยังไม่มีความจำเป็นในขณะนี้ เพียงแต่หากได้กำหนดให้มีมาตรการทางกฎหมายที่ดีพอเพื่อระงับยับยั้งหรือป้องปรามการใช้ชุดคำสั่งไม่พึงประสงค์ในการก่ออาชญากรรม

ตามที่ได้กล่าวไปแล้ว ก็น่าจะเพียงพอในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ดังกล่าวได้

ดังนั้น จากผลการศึกษาและการวิเคราะห์ปัญหาในการบังคับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รวมทั้งการศึกษาถึงมาตรการทางกฎหมายของต่างประเทศหรือขององค์การระหว่างประเทศที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์แล้วพบว่า หลักการที่สำคัญต่างๆ ในกฎหมายต่างประเทศหรือขององค์การระหว่างประเทศได้ถูกนำมาบัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยเกือบทั้งหมดแล้ว เพียงแต่ยังมีข้อบกพร่องในการบัญญัติกฎหมายในส่วนที่เกี่ยวกับความหมายของคำว่า “เข้าถึง (access)” และมาตรการป้องกันการเข้าถึงโดยไม่มีอำนาจ (Illegal access) ที่ยังไม่ชัดเจนเพียงพอ ที่สมควรได้รับการแก้ไขโดยเร็วต่อไป

2. ข้อเสนอแนะ

ก่อนที่ผู้เขียนจะมีข้อเสนอใดๆ นั้น จำต้องขออนุญาตชี้แจงเสียก่อนว่า แม้จะมีผู้วิจัยเกี่ยวกับความรับผิดทางอาญาของการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์[193] รวมทั้งได้มีการศึกษาวิเคราะห์เกี่ยวกับการเข้าถึงโดยมิชอบไว้แล้ว[194] แต่งานวิจัยทั้งสองเรื่องดังกล่าวยังมีข้อบกพร่องและมิอาจแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ ผู้เขียนจึงขอเสนอแนวทางการแก้ไขที่ดีกว่า และจะขอชี้ให้เห็นถึงข้อบกพร่องของงานวิจัยทั้งสองเรื่องดังกล่าวที่มีความเห็นและข้อเสนอแนะเป็นไปในทำนองเดียวกันว่า “เพื่อการบังคับใช้กฎหมาย ศาลจึงต้องมีการตีความคำว่า “เข้าถึง” อย่างกว้างเพื่อให้เหมาะสมกับพฤติกรรมการใช้คอมพิวเตอร์ที่หลากหลาย ทำให้สามารถนำตัวผู้กระทำความผิดมาลงโทษได้ เนื่องจากหากตีความอย่างแคบแล้วก็จะทำให้เกิดปัญหาว่ามีการเข้าถึงแล้วหรือยัง และอาจทำให้ไม่สามารถนำตัวผู้กระทำผิดมาลงโทษได้ และการวินิจฉัยเขตของการเข้าถึงที่จะต้องรับผิดทางอาญาเพียงใดควรที่จะปล่อยให้เป็นหน้าที่ของศาลที่จะพิจารณาว่าการเข้าถึงที่จะเป็นความผิดนั้นควรมีลักษณะอย่างไร โดยไม่จำกัดว่าต้องไม่ชอบด้วยกฎหมายหรือโดยปราศจากอำนาจเท่านั้น เนื่องจากมีลักษณะการกระทำอื่นที่เป็นการกระทำที่ไม่ถูกต้องหากแต่ไม่ผิดกฎหมายหรือทำโดยมีอำนาจ ซึ่งหากตีความอย่างแคบแล้วจะทำให้ผู้กระทำความผิดไม่ต้องรับโทษทางกฎหมาย”

ทั้งนี้ ผู้เขียนไม่เห็นด้วยกับข้อเสนอแนะดังกล่าวและเห็นว่าข้อเสนอแนะนั้นยิ่งจะทำให้เกิดปัญหาในการบังคับใช้และการตีความกฎหมายเพิ่มมากยิ่งขึ้น เนื่องจากศาสตร์ทางด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศและการสื่อสารกว้างขวางมากเกินกว่าที่จะปล่อยให้บุคคลที่อาจมิได้มีความรู้หรือมีความเชี่ยวชาญด้านดังกล่าวเป็นผู้แปลหรือตีความคำว่า “เข้าถึง” ซึ่งเป็นศัพท์และเทคนิคเฉพาะด้าน ในทางตรงกันข้ามหากมีกรอบของคำว่า “เข้าถึง” ไว้เพื่อให้เจ้าพนักงานในการยุติธรรมที่เกี่ยวข้องได้ใช้เป็นบรรทัดฐานในการตีความเหมือนดังเช่นนานาอารยประเทศก็จะเป็นประโยชน์ต่อกระบวนการยุติธรรมมากกว่า และสิ่งที่สำคัญก็คือหากปล่อยให้มีการตีความคำว่า “เข้าถึง” โดยไม่มีกรอบแนวคิดเช่นนั้น ก็จะเป็นการขัดกับหลักการบังคับใช้กฎหมายอาญาที่จะต้องมีบทบัญญัติโดยชัดแจ้งและต้องตีความโดยเคร่งครัดและไม่อาจขยายความเพื่อให้เป็นโทษแก่จำเลยได้ แต่ตรงกันข้ามจะต้องตีความให้เป็นคุณกับจำเลย ซึ่งหากปล่อยให้เป็นไปตามข้อเสนอของ

---

193 พิญดา เลิศกิตติกุล, อ้างแล้วในเชิงอรรถที่ 131 หน้า 191

194 ชาตรี ส่งสัมพันธ์, อ้างแล้วในเชิงอรรถที่ 77 หน้า 118

วิทยานิพนธ์ทั้งสองฉบับเสนอแนะไว้แล้ว ก็ยิ่งจะทำให้ผู้กระทำผิดลอยนวลและมิอาจนำมารับโทษตามกฎหมายได้

ดังนั้น เพื่อให้การแก้ไขปัญหาทั้ง 5 ประเด็นดังกล่าวข้างต้น รวมทั้งปัญหาจากการขโมยเอกลักษณ์บุคคลเป็นไปอย่างมีรูปธรรมและเป็นไปตามหลักสากล ดังที่นานาประเทศได้ดำเนินการไปแล้ว ผู้เขียนจึงขอเสนอแนะวิธีการแก้ไขปัญหาเหล่านั้น ดังนี้

1. การแก้ไขปัญหาความไม่ชัดเจนและไม่สอดคล้องกับทางปฏิบัติของส่วนกฎหมายวิธีสบัญญัติตามมาตรา 21 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ตามที่ได้กล่าวไว้ในเชิงการวิเคราะห์ในบทที่ 5 ข้อ 2.1 ปัญหาประการแรกที่ว่า “ในทางปฏิบัติพบว่าโอกาสที่พนักงานเจ้าหน้าที่จะตรวจพบชุดคำสั่งไม่พึงประสงค์ที่แอบแฝงหรือปะปนอยู่กับข้อมูลคอมพิวเตอร์อื่นเป็นไปได้ยากมาก เพราะหากพนักงานเจ้าหน้าที่เข้าไปตรวจโดยไม่ได้รับอนุญาตหรือยังมิได้เกิดอำนาจในการสืบสวนสอบสวนคดีก่อนแล้ว ก็จะกลายเป็นว่าพนักงานเจ้าหน้าที่จะเป็นผู้กระทำผิดกฎหมายเสียเอง (โดยการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบ) ซึ่งอาจทำให้เกิดภาพในทางลบในสายตาประชาชนเกี่ยวกับการใช้อำนาจซึ่งไม่มีกฎหมายบัญญัติให้กระทำเช่นนั้นได้ หรือหากพนักงานเจ้าหน้าที่แจ้งเจ้าของข้อมูลคอมพิวเตอร์ก่อนเข้าไปตรวจ เจ้าของข้อมูลคอมพิวเตอร์ก็คงจะโยกย้าย ทำลาย หรือสับเปลี่ยนที่อยู่ของข้อมูลคอมพิวเตอร์หรือหาหนทางหลีกเลี่ยงการตรวจก่อนที่พนักงานเจ้าหน้าที่จะเข้าไปตรวจ นอกจากนี้ในความเป็นจริงยังพบอีกว่า ชุดคำสั่งไม่พึงประสงค์นอกจากจะถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์แล้ว ยังถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลอื่นอีกมากมาย เช่น แฟลชไดรว์ (Flash Drive), แผ่นซีดี (Compact Disc : CD), แผ่นดิจิทัลอเนกประสงค์ (Digital Versatile Disc : DVD), External Hard Disk เป็นต้น แต่กฎหมายมิได้มีฐานอำนาจรองรับเพื่อให้พนักงานเจ้าหน้าที่เข้าไปตรวจเพื่อหาชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลเหล่านั้นได้ การบัญญัติกฎหมายที่สวนทางกับวิธีปฏิบัติจริงเช่นนี้ย่อมเป็นการไร้ผล จึงทำให้เกิดความสับสนแก่พนักงานเจ้าหน้าที่ผู้ซึ่งต้องบังคับใช้กฎหมายเป็นอย่างมาก” นั้น

ผู้เขียนเห็นว่า ในเมื่อมาตรา 21 อยู่ในหมวดพนักงานเจ้าหน้าที่ซึ่งถือเป็นส่วนของกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายวิธีสบัญญัติแล้ว ถ้อยคำในวรรคหนึ่ง ที่ว่า “ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้” นั้น เหตุใดจึงบัญญัติให้พนักงานเจ้าหน้าที่มีอำนาจในการตรวจสอบหาชุดคำสั่ง

ไม่พึงประสงค์ที่แอบแฝงหรือปะปนอยู่กับข้อมูลคอมพิวเตอร์อื่นได้ ทั้งๆ ที่ในทางปฏิบัติก็ย่อมรู้ดีอยู่แล้วว่าแทบไม่มีทางเป็นไปได้เลย

ผู้เขียนจึงขอเสนอว่า หากย้อนกลับไปพิจารณาความหมายของข้อมูลคอมพิวเตอร์ในมาตรา 3 ที่ว่า “ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย” นั้น ย่อมแปลความได้ว่าข้อมูลคอมพิวเตอร์ที่จะตรวจสอบได้นอกจากจะอยู่ในระบบคอมพิวเตอร์แล้ว ยังหมายความรวมถึงข้อมูลคอมพิวเตอร์ที่อยู่ในสื่อบันทึกข้อมูลอื่นด้วย เพราะคำว่า “ข้อมูลอิเล็กทรอนิกส์” ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์นั้น มิได้จำกัดเฉพาะแต่ข้อมูลอิเล็กทรอนิกส์ที่ใช้ในการติดต่อสื่อสารเท่านั้น แต่ยังครอบคลุมถึงข้อมูลหรือบันทึกที่ได้สร้างขึ้นโดยคอมพิวเตอร์ด้วย[195]

ดังนั้น ข้อมูลคอมพิวเตอร์ที่จะให้พนักงานเจ้าหน้าที่ดำเนินการตรวจสอบตามมาตรา 21 วรรคหนึ่ง นี้ จึงหมายความรวมถึงข้อมูลคอมพิวเตอร์ที่ถูกจัดเก็บอยู่ในสื่อบันทึกข้อมูลอื่นที่มิได้อยู่ในระบบคอมพิวเตอร์ด้วย และเพื่อให้มีฐานอำนาจมารองรับและเป็นการสอดรับกับทางปฏิบัติที่เกิดขึ้นจริง ดังนั้น มาตรการที่จะให้พนักงานเจ้าหน้าที่ทำการตรวจสอบชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคหนึ่ง จึงต้องเป็นกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามกฎหมายนี้และเป็นไปเพื่อประโยชน์ในการสืบสวนและสอบสวนตามที่บัญญัติไว้ในมาตรา 18 ก่อน กล่าวคือ ผู้เขียนจะขอเชื่อมโยงไปที่พฤติการณ์ของผู้ที่จะกระทำการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ตามมาตรา 13 ซึ่งย่อมจะมีการจัดเก็บชุดคำสั่งไม่พึงประสงค์ไว้ในสื่อบันทึกข้อมูลอื่นเพื่อความสะดวกในการจำหน่ายหรือเผยแพร่เสมอ ดังนั้น หากพนักงานเจ้าหน้าที่ไปตรวจพบชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลอื่นและมีเหตุอันควรเชื่อได้ว่ามีการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์นั้นซึ่งถือเป็นความผิดตามมาตรา 13 แล้ว พนักงานเจ้าหน้าที่ก็จะสามารถอาศัยอำนาจตามมาตรา 18 เพื่อการยื่นคำร้องต่อศาลตามมาตรา 21 วรรคหนึ่ง ได้ต่อไป

นอกจากนี้ การบัญญัติให้มาตรา 21 วรรคหนึ่ง ให้เชื่อมโยงไปยังมาตรา 18 ก็ยังมีผลดีอีกประการหนึ่งก็คือ หากเป็นกรณีที่พนักงานเจ้าหน้าที่ได้ใช้อำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด หรือได้ยึดระบบคอมพิวเตอร์ไว้เพื่อการตรวจสอบ พนักงานเจ้าหน้าที่ก็จะสามารถตรวจสอบได้ว่ามีชุดคำสั่งไม่พึงประสงค์ปะปนอยู่ในระบบคอมพิวเตอร์ด้วยหรือไม่ ซึ่งการ

---

195 ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ “คำอธิบายพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544”, เอกสารอิเล็กทรอนิกส์ หน้า 50

กำหนดเช่นนั้น ย่อมจะทำให้เกิดความรอบคอบมากขึ้นและเป็นการป้องกันมิให้พนักงานเจ้าหน้าที่ใช้อำนาจในมาตรา 21 ไปในทางมิชอบได้ เนื่องจากพนักงานเจ้าหน้าที่จะต้องได้รับอนุญาตจากศาลตามมาตรา 19[196] ก่อนที่จะดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8)[197] เสมอ ทั้งนี้ ผู้เขียนขอเสนอให้แก้ไขเพิ่มเติมมาตรา 21 วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็น ดังนี้

---

196 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 19 ความว่า

"มาตรา 19 การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (4) (5) (6) (7) และ (8) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว...

197 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 18 ความว่า

"มาตรา 18 ภายใต้บังคับมาตรา 19 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใดดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

...

(4) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(5) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(6) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(7) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(8) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

“มาตรา 21 ในกรณีที่พนักงานเจ้าหน้าที่ซึ่งดำเนินการตามมาตรา 18 พบว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้...”

2. การกำหนดนิยามคำว่า “เข้าถึง (access)” เพิ่มเติมเข้าไปในมาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่ออุดช่องว่างของกฎหมายในกรณีที่มีการกระทำความผิดฐานเข้าถึงโดยไม่มีอำนาจจากชุดคำสั่งไม่พึงประสงค์ในทุกรูปแบบ โดยจะเป็นการแก้ไขปัญหาแบบครบวงจร ทั้งในส่วนของกฎหมายสารบัญญัติ (โดยเฉพาะความผิดตามมาตรา 5 และมาตรา 7) และส่วนของกฎหมายวิธีสบัญญัติ กล่าวคือ เพื่อให้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยสามารถบังคับใช้ได้กับการโจมตี หรือภัยคุมคามที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ในทุกรูปแบบซึ่งรวมทั้งม้าโทรจันและสปายแวร์ด้วย โดยมีหลักการการบัญญัตินิยามคำว่า “เข้าถึง” ดังนี้

“เข้าถึง” หมายความว่า การกระทำอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(1) การทำให้สามารถเข้าสู่ระบบคอมพิวเตอร์ การสั่งการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผล หน่วยบันทึกผลของระบบคอมพิวเตอร์ได้ หรือ

(2) การแสดงผลข้อมูลคอมพิวเตอร์โดยระบบคอมพิวเตอร์ หรือข้อมูลอื่นใดจากระบบคอมพิวเตอร์ หรือ

(3) การทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ

(4) การกระทำอื่นใดเพื่อแสงหาประโยชน์จากข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์

3. การออกกฎกระทรวงเพื่อเพิ่มเติมความหมายของ “ชุดคำสั่งไม่พึงประสงค์” ตามที่กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ให้อำนาจไว้ภายใต้หลักการที่สำคัญว่า “ชุดคำสั่งไม่พึงประสงค์นอกจากจะหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แล้ว ยังให้หมายความรวมถึงชุดคำสั่งที่มีผลทำให้มีการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบด้วย” ก็จะทำให้ความหมายของชุดคำสั่งไม่พึงประสงค์มีความหมายครอบคลุมถึงลักษณะของการกระทำความผิดในประเด็น

ปัญหาดังกล่าวข้างต้นได้ทุกๆ ประเด็น ซึ่งจะส่งผลในการป้องกันและปราบปรามการกระทำความผิดดังกล่าวให้มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

4. การดำเนินการเพื่อแยกแยะชุดคำสั่งไม่พึงประสงค์ที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนด ออกจากชุดคำสั่งไม่พึงประสงค์ที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าว โดยการจัดทำเป็นประกาศของรัฐมนตรีว่าการกระทรวงเทคโนโลยีและการสื่อสาร และประกาศในราชกิจจานุเบกษาเพื่อให้ประชาชนรับรู้เป็นการทั่วกัน ก็จะสามารถเป็นเครื่องมือของพนักงานเจ้าหน้าที่ในการแก้ไขปัญหาในประเด็นดังกล่าวข้างต้นได้เป็นอย่างดีอีกทางหนึ่งด้วย

สำหรับวิธีการที่จะออกประกาศนั้นก็มีปัญหาที่ควรนำมาพิจารณาประกอบด้วยว่าจะทราบได้อย่างไรว่ามีชุดคำสั่งไม่พึงประสงค์ใดออกมาบ้าง ประเด็นนี้ผู้เขียนเห็นว่า ควรมีการสร้างพันธมิตรขึ้นระหว่างภาครัฐและภาคเอกชนที่เป็นผู้ประกอบการในอุตสาหกรรมซอฟท์แวร์ประเภทแอนตี้ไวรัสหรือกำจัดมัลแวร์ชนิดต่างๆ ซึ่งส่วนใหญ่แล้วผู้ประกอบการเหล่านี้จะมีผู้รับผิดชอบโดยตรงเพื่อคอยสอดส่องและติดตามเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ที่เกิดขึ้นใหม่ในแต่ละวัน รวมทั้งอาจมีทีมงานสำหรับการวิจัยเกี่ยวกับชุดคำสั่งไม่พึงประสงค์โดยตรงอยู่แล้วด้วย ซึ่งหากสามารถร่วมกันทำงานในรูปแบบของการบูรณาการทั้งภาครัฐและเอกชนเหล่านั้นอย่างเป็นรูปธรรม โดยมีการแต่งตั้งคณะทำงานและกำหนดภารกิจและการติดตามผลไว้อย่างชัดเจน ก็จะทำให้สามารถสร้างระบบหรือกลไกในการแยกแยะชุดคำสั่งไม่พึงประสงค์ได้อย่างสมบูรณ์และมีประสิทธิภาพและนำไปสู่การออกประกาศรับรองชุดคำสั่งไม่พึงประสงค์ที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวได้สมตามเจตนารมณ์ของกฎหมาย ทั้งนี้สำหรับวิธีการหรือเทคนิคในการออกประกาศรับรองอาจจะรับรองเป็นตระกูลและรุ่นหรือเวอร์ชั่นของซอฟท์แวร์ก็ได้ เช่น ตระกูลของเทรนด์ไมโคร (Trend micro) ตระกูลของนอร์ตั้น (Norton) หรือตระกูลของแม็คเอฟี (McAfee) หรือตระกูลของไซแมนเทค (Symantec) ที่ปัจจุบันถือว่าเป็นผู้ประกอบการอุตสาหกรรมซอฟท์แวร์ประเภทแอนตี้ไวรัสหรือกำจัดมัลแวร์ รายใหญ่ เป็นต้น

5. สำหรับประเด็นของบั๊กที่ว่า จะถือเป็นชุดคำสั่งไม่พึงประสงค์หรือไม่นั้น ผู้เขียนเห็นว่า ต้องนำหลักการของความรับผิดทางอาญาซึ่งเป็นองค์ประกอบภายใน (เจตนา) ในการกระทำความผิดมาประกอบการวินิจฉัยดังกล่าวด้วย กล่าวคือ การเกิดบั๊กในโปรแกรมต่างๆ นั้นโดยปกติมักจะเกิดจากความพลั้งเผลอหรือความไม่รอบคอบของโปรแกรมเมอร์หรือผู้เขียนโปรแกรม ซึ่งมิได้มีเจตนาในการทำให้เกิดบั๊กในโปรแกรมที่ตนได้พัฒนาขึ้น ดังนั้น โปรแกรมที่เกิดบั๊กขึ้นโดยปกติจึงมิอาจถือได้ว่าเป็นชุดคำสั่งไม่พึงประสงค์ เว้นแต่จะพิสูจน์ได้ว่าผู้พัฒนาโปรแกรมมีเจตนาให้เกิดบั๊กขึ้น ก็อาจถือได้ว่าโปรแกรมที่เกิดจากเจตนาให้เกิดบั๊กขึ้นนั้นเป็นชุดคำสั่งไม่พึงประสงค์

บรรณานุกรม

บรรณานุกรม

กองบรรณาธิการในวารสาร (2548) "บทความทั่วไป" *สาร NECTEC* , (มกราคม– กุมภาพันธ์) : 34

คณะกรรมการยกร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์ (2544) *เอกสารสรุปการประชุมคณะอนุกรรมการเฉพาะกิจยกร่างกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ครั้งที่ 6 (1/2544)* เมื่อวันพฤหัสบดี ที่ 8 มีนาคม 2544 เวลา 14.00-17.00 น. ณ ห้องประชุม ชั้น 4 อาคารกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม

ครรชิต มาลัยวงศ์ (2538) *พจนานุกรมคอมพิวเตอร์สำหรับเยาวชน* กรุงเทพมหานคร กองบริการสื่อสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อม

คำพิพากษาศาลฎีกาที่ 5161/2547.

คำให้สัมภาษณ์ของนายสิทธิชัย โภไคยอุดม ภายหลังการอภิปรายของ สนช. เมื่อวันที่ 16 พฤศจิกายน 2549 *สมาคมผู้ดูแลเว็บไทย http://www.webmaster.or.th/news/*

ชาตรี ส่งสัมพันธ์ (2552) “อาชญากรรมคอมพิวเตอร์ : ศึกษาวิเคราะห์การเข้าถึงโดยมิชอบ” นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

ไซแมนเทค (Symantec) รายงานสถานการณ์ภัยคุมคามบนอินเทอร์เน็ตของไซแมนเทค เมษายน 2010 หน้า 11 เอกสารข้อมูลสำหรับภูมิภาคเอเชียแปซิฟิกและญี่ปุ่น

ญาณพล ยั่งยืน (2552) เอกสารประกอบการสัมมนา ณ มหาวิทยาลัยรังสิต กรุงเทพฯ เรื่อง “จับฉันให้ได้ ถ้านายแน่จริง : แนวทางสืบค้น แกะรอยอาชญากรรมทางคอมพิวเตอร์” คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต หน้า 2-3 วันอังคารที่ 22 กันยายน พ.ศ. 2552

ดวงกมล ทรัพย์พิทยากร (4 ตุลาคม 2544) “สปายแวร์ ปรสิตแวร์ แอดแวร์ เครือข่ายแฝงและวิธีการป้องกัน” *(ออนไลน์)* ค้นคืนเมื่อวันที่ 11 มีนาคม 2553

ทวีศักดิ์ กออนันตกูล (2542) "อาชญากรรมในยุคโลกาภิวัฒน์" *บทบัณฑิตย์* , เล่มที่ 55 (มีนาคม)

ธรรมศักดิ์ วิชชารยะ (2542) “อาชญากรรมร่วมสมัย แนวคิดในการป้องกันและควบคุมปัญหาอาชญากรรมทางคอมพิวเตอร์” ใน *เอกสารประกอบการสัมมนา เรื่อง แฮคเกอร์: มหันตภัยยุคไอที*

ธวัชชัย ชมศิริ (2553) *Computer & Network Security ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์* กรุงเทพมหานคร โปรวิชั่น

น้ำทิพย์ บุญเกิด (2548) “ความรับผิดทางอาญากรณีละเมิดข้อมูลส่วนบุคคล : ศึกษาเฉพาะกรณีข้อมูลส่วนบุคคลที่จัดเก็บในระบบคอมพิวเตอร์ (Criminal Liability for the Transgression of Personal Data : Particularly Study about Personal Data which be Kept in the Computer System.)” นิติศาสตร์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

นิพนธ์ นาชิน,ประธาน พงศ์ทิพย์ฤกษ์, อนันต์ โซนี่ Edited by ปริญญา หอมอเนก. (2553) “เรียนรู้และทำความเข้าใจภัยจากการใช้งานโปรแกรมประเภท Social Networking Understand How Hacker attack Social Networking by using Social Engineering” เอกสารประกอบการสัมมนา Social Networking Secutiry Conference 2010 : SNS CON 2010 *จัดโดย เขตอุตสาหกรรมซอฟร์แวร์ ศูนย์บริหารจัดการเทคโนโลยี ภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยความร่วมมือกับสมาคมความมั่นคงปลอดภัยสารสนเทศ Thailand Information Security Association–TISA) และ บริษัท เอซิสโปรเฟสชั่นนัล เซ็นเตอร์ (ACIS Professional Center)* จำกัด วันที่ 21 กรกฎาคม 2553 ณ ห้องแกรนด์บอลลูม ชั้น 3 โรงแรม อโนมา กรุงเทพฯ

บันทึกสำนักงานคณะกรรมการกฤษฎีกาประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เรื่องเสร็จที่ 257/2548.

ประมวลกฎหมายแพ่งและพาณิชย์.

ประมวลกฎหมายอาญา.

บล็อก (Blog) กฎหมาย ในเว็บไซต์ http://www.BioLawCom.De “กฎหมาย ที่ร่างกันแบบไม่เร่งแต่ผ่านกันแบบรีบๆ (ตอน 1)” *(ออนไลน์)* ค้นคืนเมื่อวันที่ 24 ธันวาคม 2553

ปริญญา หอมอเนก (2552) “The Latest Update Computer Crime Law Implementation Status in Thailand สรุปความเคลื่อนไหวเกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หลังมีผลบังคับใช้” (*ออนไลน์*) จาก http://www.acisonline.net/article/?p=9 เผยแพร่เมื่อ 27 มีนาคม 2552 ค้นคืนเมื่อวันที่ 30 กันยายน 2553

_____ . (2545) “เจาะลึก Malicious Mobile Code (MMC) ตอนที่ 1” *(ออนไลน์)* (31 พฤษภาคม 2545) ค้นคืนเมื่อวันที่ 15 มิถุนายน 2553

_____ . (2547) “เมื่อโปรแกรมป้องกันไวรัสไม่ใช่คำตอบสุดท้ายในการปราบไวรัส” บทความออนไลน์ซึ่งนำมาจาก *eWeek Thailand* , (เดือนกรกฎาคม 2547) ค้นคืนเมื่อวันที่ 20 สิงหาคม 2553

_____ . (2549) “ยุทธศาสตร์การเตรียมพร้อมป้องกันภัยจากมัลแวร์อย่างได้ผลในทางปฏิบัติ Understanding MalWare Point-of-Entry and How to protect by implementing practical Anti-Malware strategy” *eWeek Thailand* , ปักษ์แรก (ธันวาคม) ค้นคืนเมื่อวันที่ 30 มิถุนายน 2553

พรทิพย์ ตัณฑวนันท์ (2548) “อาชญากรรมเกี่ยวกับข้อมูลอิเล็กทรอนิกส์ (Crime Related to Data Message)” นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

พรเพชร วิชิตชลชัย (2550) *คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550* เอกสารอิเล็กทรอนิกส์ (วันที่ค้นข้อมูล 21 กรกฎาคม 2553)

พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544.

พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544.

พิญดา เลิศกิตติกุล (2550) “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีความรับผิดทางอาญาเกี่ยวกับการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์” นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

มาโนช ตันตระเธียร (2542) “อาชญากรรมคอมพิวเตอร์ : กระบวนการยุติธรรมไทยพร้อมหรือยัง ?” ใน *เอกสารประกอบการสัมมนาทางวิชาการเรื่อง “กฎหมายพาณิชย์อิเล็กทรอนิกส์ (E-Commerce Laws) : นวัตกรรมทางกฎหมายที่จำเป็นและเร่งด่วนแห่งสังคมไทย* วันที่ 6-7 พฤษภาคม 2542 ณ หอประชุมมหิศร อาคารไทยพาณิชย์ ปาร์ค พลาซ่า กรุงเทพมหานคร กองทุนศาสตราจารย์สัญญา ธรรมศักดิ์, คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, สภาทนายความ, ชมรมนักข่าวสายเทคโนโลยีสารสนเทศ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2550.

ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .....

ราชบัณฑิตยสถาน (2542) *ศัพท์เทคโนโลยีสารสนเทศฉบับราชบัณฑิตยสถาน* กรุงเทพมหานคร อรุณการพิมพ์

ศิริวรรณ อภิสิริเดช และ มนัชยา ชมธวัช (2546) "20 ช่องโหว่สำคัญที่เป็นอันตรายร้ายแรงต่อความปลอดภัยของอินเทอร์เน็ต" *(ออนไลน์)* ค้นคืนเมื่อวันที่ 20 มิถุนายน 2553

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) (2546) “จะไล่ล่าอาชญากรอย่างไรเมื่อไม่มีประจักษ์พยานและกฎหมายวิธีพิจารณาความที่จำเป็นในคดีอาชญากรรมทางคอมพิวเตอร์” ใน *เอกสารคำอธิบายร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ....* เพื่อเป็นข้อมูลประกอบการนำเสนอ วันที่ 16 ธันวาคม 2546 เวลา 13.30 – 16.00 น. ณ ห้องพิมานเมฆ แกรนด์บอลรูม ชั้น 3 โรงแรม เดอะแกรนด์ กรุงเทพฯ

_____ . (2546) *แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์* กรุงเทพมหานคร

สราวุธ เบญจกุล (2550) ““E-crime” อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่” บทความ*ออนไลน์พิเศษในเว็บไซต์ผู้จัดการออนไลน์ http://www.manager.co.th/Daily/ViewNews.aspx?NewsID= 9500000078831* เผยแพร่เมื่อ 6 กรกฎาคม 2550 (วันที่ค้นข้อมูล 13 สิงหาคม 2554)

สาขาวิชานิติศาสตร์ มหาวิทยาลัยสุโขทัยธรรมาธิราช (2544) *กฎหมายอาญา 1 : ภาคบทบัญญัติทั่วไป* พิมพ์ครั้งที่ 13 นนทบุรี สำนักพิมพ์ มหาวิทยาลัยสุโขทัยธรรมาธิราช

สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา (2536) *กฎหมายอาญาภาค 1* กรุงเทพมหานคร สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตสภา

18 U.S.C. 1030. Fraud and Related Activity in Connection with Computers.

Computer Crimes - California Penal Code.

Computer Crimes - Texas Penal Code.

Computer Misuse Act 1990.

Convention on Cybercrime.

Convention on Cybercrime (ETS No. 185) Explanatory Report.

Crimes Amendment Act 2003 No 39 Part 1 s 15, of July 7th.

Criminal Code.

Criminal Information Law of August 17, 1991.

Criminal Law.

Cyber Crime Law-Code of Maryland.

Cybercrime Act 2001.

Electronic Commerce Act 2000.

GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS 26 November 1992

International review of criminal policy - United Nations Manual on the prevention and control of computer-related crime.

Penal Code ประเทศฝรั่งเศส.

Penal Code ประเทศฟินแลนด์.

Penal Code ประเทศสวิตเซอร์แลนด์.

Penal Code ประเทศอิตาลี.

RECOMMENDATION No. R (89) 9 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON COMPUTER-RELATED CRIME (Adopted by the Committee of Ministers on 13 September 1989).

Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology adopted by the Committee of Ministers on 11 September 1995.

The Information Technology Act 2000.

ภาคผนวก

หน้า ๔
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. ๒๕๕๐

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑๐ มิถุนายน พ.ศ. ๒๕๕๐

เป็นปีที่ ๖๒ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกกฎกระทรวงเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑
ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

มาตรา ๑๕ ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์โดยสุจริต ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ

จะต้องรับโทษภายในราชอาณาจักร

หมวด ๒
พนักงานเจ้าหน้าที่

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดตามพระราชบัญญัตินี้มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๕ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิดตามพระราชบัญญัตินี้ เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วยในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๔ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๔ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๔ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้วพนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง

มาตรา ๒๐ ในกรณีที่การกระทำความผิดตามพระราชบัญญัตินี้เป็นการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาคสอง ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นได้

ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ตามวรรคหนึ่ง ให้พนักงานเจ้าหน้าที่ทำการระงับการทำให้แพร่หลายนั้นเอง หรือสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์นั้นก็ได้

มาตรา ๒๑ ในกรณีที่พนักงานเจ้าหน้าที่พบว่า ข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย พนักงานเจ้าหน้าที่อาจยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอให้มีคำสั่งห้ามจำหน่ายหรือเผยแพร่ หรือสั่งให้เจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นระงับการใช้ ทำลาย หรือแก้ไขข้อมูลคอมพิวเตอร์นั้นได้ หรือจะกำหนดเงื่อนไขในการใช้ มีไว้ในครอบครอง หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ดังกล่าวก็ได้

ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง ทั้งนี้ เว้นแต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้ หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่ผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลของผู้ใช้บริการ ที่พนักงานเจ้าหน้าที่ได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

มาตรา ๒๗ ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๑๘ หรือมาตรา ๒๐ หรือไม่ปฏิบัติตามคำสั่งของศาลตามมาตรา ๒๑ ต้องระวางโทษปรับไม่เกินสองแสนบาท และปรับเป็นรายวันอีกไม่เกินวันละห้าพันบาทจนกว่าจะปฏิบัติให้ถูกต้อง

มาตรา ๒๘ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากผู้มีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และมีคุณสมบัติตามที่รัฐมนตรีกำหนด

มาตรา ๒๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญามีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

หน้า ๑๒
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง

มาตรา ๓๐ ในการปฏิบัติหน้าที่ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวของพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หน้า ๑๓
เล่ม ๑๒๔ ตอนที่ ๒๗ ก ราชกิจจานุเบกษา ๑๘ มิถุนายน ๒๕๕๐

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ เนื่องจากในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว จึงจำเป็นต้องตราพระราชบัญญัตินี้

ประวัติผู้วิจัย

ชื่อ	นายสถาพร สอนเสนา
วัน เดือน ปีเกิด	11 มิถุนายน พ.ศ. 2514
สถานที่เกิด	จังหวัดมหาสารคาม
ประวัติการศึกษา	- บริหารธุรกิจบัณฑิต สาขาวิชาคอมพิวเตอร์ธุรกิจ (บธ.บ.) มหาวิทยาลัยสยาม พ.ศ. 2537 - นิติศาสตรบัณฑิต (นบ.) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2545 - ศึกษาในหลักสูตรนิติศาสตรมหาบัณฑิต วิชาเอกกฎหมายธุรกิจ (นม.) มหาวิทยาลัยสุโขทัยธรรมาธิราช พ.ศ. 2552 - เนติบัณฑิตไทย (นบท.) พ.ศ. 2553
สถานที่ทำงาน	สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติฯ ชั้น 8 อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพมหานคร
ตำแหน่ง	นิติกรชำนาญการ (นักกฎหมายไอที)