ปัญหาการบังคับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 : ศึกษากรณีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์

สถาพร สอนเสนา

บทนำ

ด้วยปัจจุบันพบว่ามีการจัดทำและเผยแพร่โปรแกรมคอมพิวเตอร์ (Computer Program) หรือชุดคำสั่งไม่พึงประสงค์ (Malicious Software) ผ่านทางเครือข่ายคอมพิวเตอร์ (Computer Network) โดยเฉพาะอย่างยิ่งเครือข่ายอินเทอร์เน็ต (Internet) กันอย่างแพร่หลาย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Worm) ม้าโทรจัน (Trojan Horses) สปายแวร์ (Spyware) เป็นต้น อันเป็นเหตุให้มีการใช้โปรแกรมหรือชุดคำสั่งดังกล่าวเพื่อมุ่งก่อให้เกิดความเสียหายทั้งต่อการรักษาความลับ (confidentiality) ความครบถ้วน (integrity) และเสถียรภาพในการใช้งาน (availability) ของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ตลอดจนความเป็นอยู่ส่วนตัวในการติดต่อสื่อสาร (the right of privacy of data communication) ของประชาชนเป็นอย่างมาก ทั้งนี้ แม้ว่าพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะได้บัญญัติให้มีมาตรการในการดำเนินการเกี่ยวกับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ไว้ในมาตรา 21 แล้วก็ตาม แต่บทบัญญัติในมาตราดังกล่าวยังมีข้อบกพร่องและความไม่ชัดเจนในทางปฏิบัติที่จะสามารถเอื้ออำนวยและใช้เป็นเครื่องมือในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ให้มีประสิทธิภาพและประสิทธิผลได้อย่างเต็มที่อยู่หลายประการ

ดังนั้น จึงมีความจำเป็นที่จะต้องศึกษาค้นคว้าเกี่ยวกับโปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์เพื่อให้ทราบถึงคุณสมบัติและภัยที่ตามมากับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์และเพื่อค้นหาวิธีการรับมือกับปัญหาดังกล่าว โดยการศึกษาและวิเคราะห์ถึงรูปแบบของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่เกิดจากการใช้โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือหรือปัจจัยหลักในการกระทำความผิดและทำให้เกิดปัญหาทางกฎหมายขึ้น เพื่อค้นหามาตรการและแนวทางในการป้องกันและปราบปรามการกระทำความผิดดังกล่าวให้มีประสิทธิภาพและได้ผลในทางปฏิบัติมากยิ่งขึ้น

วัตถุประสงค์

1. เพื่อให้ทราบถึงความหมายและรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดจากชุดคำสั่งไม่พึงประสงค์
2. เพื่อให้ทราบถึงความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ และสามารถจัดประเภทของชุดคำสั่งไม่พึงประสงค์ได้
3. เพื่อให้ทราบถึงมาตรการทางกฎหมายที่ใช้อยู่ในปัจจุบันในการจัดการกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์
4. เพื่อให้ทราบถึงความหมายและสภาพความเป็นทรัพย์ของข้อมูลคอมพิวเตอร์ในความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา
5. เพื่อให้ทราบถึงความหมาย คุณสมบัติและลักษณะของชุดคำสั่งไม่พึงประสงค์ตลอดจนความหมายของการเข้าถึงและการบริหารจัดการในเชิงกฎหมายกับการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ในกฎหมายระหว่างประเทศและกฎหมายต่างประเทศ
6. เพื่อให้มีระบบการบริหารจัดการชุดคำสั่งไม่พึงประสงค์โดยการแยกแยะและจัดระเบียบชุดคำสั่งไม่พึงประสงค์อย่างชัดเจนและสามารถนำชุดคำสั่งไม่พึงประสงค์แต่เป็นชุดคำสั่งที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งอื่นไปใช้ให้เกิดประโยชน์โดยให้มีบทบัญญัติของกฎหมายรองรับ

ความเบื้องต้นเกี่ยวกับชุดคำสั่งไม่พึงประสงค์

จากสภาพโดยธรรมชาติของอาชญากรรมคอมพิวเตอร์ที่ผู้กระทำความผิดจะอยู่ที่ใดในโลกก็ได้ ดังนั้น ระบบคอมพิวเตอร์และเครือข่ายจึงอาจถูกคุกคามหรือถูกโจมตีจากนักเจาะระบบ (Hacker) หรือผู้ใช้งานทั่วไปที่มีความคึกคะนองหรืออยากรู้อยากทดลองซึ่งอาจจะเป็นคนภายในองค์กรเองหรือนักเรียนนักศึกษา ทั้งนี้ โดยการใช้โปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ที่จัดทำขึ้นเป็นการเฉพาะเพื่อเป็นเครื่องมือในการเข้าถึงหรือการโจมตีทรัพยากรด้านคอมพิวเตอร์โดยผ่านทางระบบเครือข่ายสื่อสารในหลาย ๆ ด้านและหลาย ๆ ทางด้วยกัน ไม่ว่าจะเป็นการโจมตีผ่านทางระบบเครือข่ายคอมพิวเตอร์โดยทั่ว ๆ ไป หรือผ่านทางระบบเครือข่ายคอมพิวเตอร์ระดับโลกอย่างเครือข่ายอินเทอร์เน็ต

1. ความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองนักคอมพิวเตอร์

โดยธรรมชาติของโปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ย่อมต้องมีพัฒนาการของตัวเองไปเรื่อย ๆ ตามยุคสมัยและตามความต้องการของเหล่าอาชญากรหรือผู้ใช้งาน

ที่ไม่มีขีดจำกัด ซึ่งแนวโน้มของอาชญากรรมคอมพิวเตอร์ทั้งในปัจจุบันและอนาคตจะมีความซับซ้อนและเพิ่มความรุนแรงและส่งผลกระทบมากขึ้น จากการรวบรวมข้อมูลของโปรแกรมคอมพิวเตอร์หรือชุดคำสั่งไม่พึงประสงค์ตั้งแต่อดีตจนถึงปัจจุบันพบว่า มีชุดคำสั่งไม่พึงประสงค์อยู่หลาย ๆ ประเภทและมีคุณลักษณะหรือวัตถุประสงค์ในการใช้งานและมีชื่อเรียกแตกต่างกันออกไป เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนคอมพิวเตอร์ (Worm) ม้าโทรจัน (Trojan Horses) สปายแวร์ (Spyware) เป็นต้น ซึ่งต่อไปนี้ผู้เขียนจะขอเรียกชื่อโดยรวมว่า "ชุดคำสั่งไม่พึงประสงค์ (Malicious Software)" หรือเรียกโดยย่อว่า "มัลแวร์ (Malware)" โดยจะขอแยกและกล่าวถึงมัลแวร์ตามความหมายและคุณสมบัติ ดังนี้

1.1 ชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

มีผู้รู้ตลอดจนนักวิชาการและแหล่งความรู้จากหลายแหล่งพยายามให้ความหมายและเรียกชื่อชุดคำสั่งไม่พึงประสงค์ไว้แตกต่างกันออกไป ซึ่งก็สุดแท้แต่ว่าผู้รู้หรือนักวิชาการแต่ละท่านหรือแหล่งความรู้แต่ละแหล่งเหล่านั้นจะเรียกชุดคำสั่งไม่พึงประสงค์ว่าอย่างไร แต่หากได้มีการพิจารณาถึงความหมายโดยรวมของชื่อที่ถูกเรียกเหล่านั้นแล้วก็คงหมายถึงชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายนั่นเอง ซึ่งในที่นี้จะขอนำตัวอย่างของการเรียกชื่อชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายตามที่ปรากฏและพบเห็นได้โดยทั่วไปมาให้ทราบ เช่น มัลแวร์ (Malware), แทรคแวร์ (Trackware), ไฮแจ็คแวร์ (Hijackware), ธีฟแวร์ (Thiefware), สนู๊ปแวร์ (Snoopware) หรือสคัมแวร์ (Scum ware) เป็นต้น

1.2 ชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหาย

ชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายในชีวิตจริงที่มักประสบและรู้จักกันดีก็ได้แก่ บรรดาโปรแกรมกำจัดหรือแอนตี้ไวรัส โปรแกรมฆ่าหนอน หรือโปรแกรมกำจัดม้าโทรจันต่าง ๆ เป็นต้น โดยมีผู้ผลิตโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันหรือแก้ไขความเสียหายเหล่านั้นให้เลือกมายมายมีทั้งที่ต้องเสียเงินซื้อมาและแบบที่ให้ใช้กันฟรี ๆ แต่ส่วนใหญ่แล้วจะต้องเสียเงินหรือซื้อมาโดยมี License สำหรับการใช้งานด้วย ทั้งนี้เพื่อเป็นการปกป้องระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ โดยผู้ใช้สามารถใช้หรือติดตั้งชุดคำสั่งไม่พึงประสงค์ในทางการป้องกันหรือแก้ไขความเสียหายภายใต้เทคโนโลยีต่าง ๆ ที่มีอยู่ในปัจจุบัน

อย่างไรก็ตาม มัลแวร์รุ่นใหม่ ๆ ต่างมีพิษสงรอบด้านและมีความฉลาดเปรียบได้กับเป็นแฮกเกอร์ไปในตัวซึ่งจะมีความสามารถในการเจาะระบบโดยอาศัยช่องโหว่ต่าง ๆ ในระบบที่ยังไม่ได้รับการติดตั้งชุดแก้ไขข้อบกพร่อง (Patch) ดังนั้น แนวความคิดใหม่ในการทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์มีความปลอดภัยจากมัลแวร์ต่าง ๆ นั้น โปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันความเสียหายนอกจากจะเป็นโปรแกรมป้องกันมัลแวร์ซึ่งถือเป็นโปรแกรมขั้นพื้นฐานที่จำต้องมีไว้ในเครื่องคอมพิวเตอร์แล้ว ควรมีช่องทางให้ปรับปรุงรูปแบบมัลแวร์ของโปรแกรมนั้น (Malware Signature) ให้ทันสมัยกับมัลแวร์รุ่นใหม่ ๆ อยู่เสมอ ทั้งนี้ หากสามารถควบคุมหรือบริหารจากส่วนกลางได้ก็จะได้ผลในการป้องกันมัลแวร์ได้ดีมากขึ้น กล่าวคือ เมื่อมีการ

ออนไลน์เครื่องคอมพิวเตอร์ไคลเอนท์ก็จะติดต่อไปยังเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลางของเจ้าของผลิตภัณฑ์หรือโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ในทางป้องกันความเสียหายนั้นแล้วปล่อยให้เป็นหน้าที่ของส่วนกลางที่จะควบคุมและบริหารจัดการเรื่องมัลแวร์ให้ นอกจากนี้ยังจะต้องเป็นโปรแกรมที่มีคุณสมบัติในการตรวจจับมัลแวร์ได้ดีอีกด้วย

2. ความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองนักกฎหมาย

สำหรับความหมายและคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในมุมมองของนักกฎหมายนั้นก็อยู่ภายใต้หลักการและข้อเท็จจริงตามลักษณะของภัยคุมคามต่าง ๆ ที่เกิดจากชุดคำสั่งไม่พึงประสงค์ตามที่นักคอมพิวเตอร์ได้รวบรวมและวิเคราะห์ไว้ ซึ่งลักษณะของการกระทำความผิดทางคอมพิวเตอร์มักเป็นการคุกคามหรือลักลอบเข้าไปในระบบหรือเจาะระบบโดยไม่ได้รับอนุญาตหรือโดยไม่มีอำนาจให้กระทำการดังกล่าวอันเทียบเคียงได้กับลักษณะการบุกรุกในทางกายภาพ หรือในบางกรณีอาจเป็นการเข้าไปโดยความยินยอมของเจ้าของคอมพิวเตอร์นั้น หรือบางกรณีอาจใช้เทคนิคหลอกล่อเพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป ซึ่งวิธีการเข้าไปเหล่านั้นมักมีการพัฒนาโปรแกรมคอมพิวเตอร์ในรูปแบบต่าง ๆ โดยกำหนดคำสั่งให้กระทำการใด ๆ อันก่อให้เกิดความเสียหายหรือภยันตรายขึ้นได้ด้วย เช่น ไวรัสคอมพิวเตอร์ซึ่งสร้างขึ้นเพื่อทำลายระบบและมักมีการแพร่กระจายตัวได้ง่ายและรวดเร็ว หรือมัลแวร์ในรูปแบบอื่น ๆ เป็นต้น ทั้งนี้ นักกฎหมายได้นำข้อเท็จจริงที่รวบรวมจากภัยคุกคามหรือการลักลอบเข้าไปในระบบหรือการเจาะระบบโดยไม่ได้รับอนุญาตมาวิเคราะห์หาสาเหตุจนได้ข้อยุติแล้วจึงนำมาบัญญัติเป็นภาษากฎหมายเพื่อรองรับกับภัยคุกคามต่าง ๆ เหล่านั้นนั่นเอง

3. ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

ผลจากการรวบรวม ศึกษาและพิเคราะห์เกี่ยวกับคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายพบว่า ชุดคำสั่งประเภทนี้สามารถแยกได้เป็น 17 ประเภทด้วยกัน แต่ที่ถือว่าเป็นชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ตามความหมายในมาตรา 21 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มี 15 ประเภท ได้แก่ ไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ แอดแวร์ โปรแกรมทดสอบช่องโหว่ โปรแกรมเจาะระบบ โปรแกรมดาวน์โหลดไวรัส โปรแกรมปล่อยไวรัส โปรแกรมฉีดไวรัส โปรแกรมชุดสร้างไวรัส โปรแกรมสำหรับส่งสแปม โปรแกรมระเบิด โปรแกรมโทรศัพท์อัตโนมัติ โปรแกรมล้อกันเล่น ฟลัดเดอร์ รูทคิท

สำหรับม้าโทรจันและสปายแวร์นั้น ผู้เขียนเห็นว่าไม่มีคุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูก

แก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ตามความหมายในมาตรา 21 แห่งพระราชบัญญัตินี้แต่อย่างใด สาเหตุที่เป็นเช่นนั้นก็เพราะเมื่อม้าโทรจันและสปายแวร์ถูกนำไปติดตั้งหรือฝังไว้ในระบบคอมพิวเตอร์ที่ตกเป็นเหยื่อแล้วจะมิได้ก่อให้เกิดความเสียหายใด ๆ ต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น ทั้งนี้ สามารถพิจารณาได้จากการที่ระบบคอมพิวเตอร์นั้นยังสามารถทำงานได้โดยสมบูรณ์อยู่นั่นเอง ดังตารางสรุปคุณสมบัติของชุดคำสั่งไม่พึงประสงค์ ต่อไปนี้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	**คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้**
1. ไวรัสคอมพิวเตอร์ (Computer Virus) เช่น ไวรัสตั้งต้น (Germs), Boot viruses, Program viruses, Multipartite viruses, Stealth viruses, Polymorphic viruses, Macro viruses, Active X เป็นต้น	ไวรัสสามารถสร้างความรำคาญเล็ก ๆ น้อย ๆ ไปจนถึงการทำลายหรือล้างข้อมูลในฮาร์ดดิสก์ แต่ไวรัสบางชนิดไม่ได้ออกแบบมาเพื่อที่จะทำลายล้างแต่ออกแบบมาอย่างง่าย ๆ และแพร่กระจายไปเรื่อย ๆ เพื่อก่อกวนหรืออาจสร้างปัญหาให้ถึงขั้นที่ระบบคอมพิวเตอร์ล่มหรือปฏิเสธการทำงานได้ ดังนั้น นอกจากไวรัสจะมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมแล้ว ไวรัสยังมีผลทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้อีกด้วย
2. ม้าโทรจัน (Trojan Horses) เช่น โปรแกรมดักข้อมูลผ่านปุ่มคีบอร์ด (Keylogger/Keystroker Generators), โปรแกรมจับรหัสผ่าน (Password Retrievers) เป็นต้น	ม้าโทรจันไม่ได้ถูกออกแบบมาเพื่อทำลายระบบหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ แต่ถูกออกแบบมาให้สอดคล้องและแฝงตัวเองเข้าไปในระบบคอมพิวเตอร์และจะทำงานโดยการดักจับเอารหัสผ่านต่าง ๆ หรือข้อมูลจากปุ่มของคีย์บอร์ดที่ถูกกดในเครื่องคอมพิวเตอร์ที่ถูกม้าโทรจันฝังตัวไว้ แล้วส่งข้อมูลนั้นออกไป เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ดังนั้น ด้วยคุณสมบัติดังกล่าวของม้าโทรจัน จึงมิได้มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
3. สปายแวร์ (Spyware)	สปายแวร์เป็นโปรแกรมที่มีจุดมุ่งหมายเพื่อเก็บรวบรวมข้อมูลส่วนบุคคลที่สำคัญต่าง ๆ ภายในเครื่องคอมพิวเตอร์ที่ถูกโปรแกรมประเภทนี้ติดตั้งอยู่ และเทคนิคที่ใช้นั้นได้แก่ การดักข้อมูลที่ถูกกดปุ่มคีย์บอร์ด การบันทึกเว็บไซต์ที่เคยเข้าเยี่ยมชมมา หรือไฟล์เอกสารต่าง ๆ ที่อยู่ภายในเครื่องโดยไม่ทำอันตรายใด ๆ ต่อเครื่อง 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 หรือการ์ตูนน่ารักต่าง ๆ เพื่อหลอกล่อให้เหยื่อเผลอคลิกเข้าไปยังเว็บไซต์ขายสินค้าในขณะที่มีการเรียกใช้งาน เช่น เว็บไซต์ขายภาพหรือวีดีโอโป๊ เว็บไซต์ของธุรกิจขายตรง เป็นต้น นอกจากนี้ แอดแวร์มักจะถูกแนบมากับอีเมล์ขยะหรือโปรแกรมประเภทพักหน้าจอ โดยแอดแวร์สามารถทำงานได้โดยอัตโนมัติเมื่อเหยื่อเริ่มใช้งานหรือเข้าสู่อินเทอร์เน็ต ดังนั้น แอดแวร์จึงมีผลทำให้ระบบคอมพิวเตอร์เพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม 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 เมื่อถูกติดตั้งและถูกเอ็กซิคิวต์แล้วจะดาวน์โหลดโปรแกรมอื่น ๆ ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์และระบบเครือข่ายจากเว็บไซต์หรือแหล่งอื่น ๆ แล้วทำการรันโปรแกรมนั้นโดยอัตโนมัติ จึงเป็นการทำให้ระบบคอมพิวเตอร์ถูกเพิ่มเติมโดยโปรแกรมที่ดาวน์โหลดมา
9. โปรแกรมปล่อยไวรัส (Virus Droppers)	เป็นโปรแกรมที่ใช้ในการปล่อยไวรัสจากโปรแกรมไวรัสเอง จึงเป็นการทำให้ระบบคอมพิวเตอร์ถูกเพิ่มเติมโดยไวรัสที่ปล่อยออกมา
10. โปรแกรมฉีดไวรัส (Virus Injectors)	โปรแกรมฉีดไวรัสทำงานคล้ายกับโปรแกรมปล่อยไวรัส แตกต่างกันที่โปรแกรมประเภทนี้จะทำการติดตั้งและโหลดส่วนของไวรัสไปไว้ในหน่วยความจำได้ เหมือนกับการฉีดไวรัสเข้าไปสู่หน่วยความจำ นอกจากนี้อาจจะฉีดไวรัสเข้าไปกับข้อมูลที่เคลื่อนที่อยู่ในระบบเครือข่ายคอมพิวเตอร์ได้ จึงเป็นการทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลง

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
11. โปรแกรมชุดสร้างไวรัส (Kits-Virus Generators)	แม้โปรแกรมชุดสร้างไวรัสจะถูกใช้เพื่อสร้างไวรัสตัวใหม่ ๆ โดยอัตโนมัติ แต่หากมีการสร้างไวรัสนั้นในระบบคอมพิวเตอร์ก็จะมีผลทำให้ระบบคอมพิวเตอร์นั้นถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลงตามไปด้วย
12. โปรแกรมสำหรับส่งสแปม (Spammer Programs)	โปรแกรมสำหรับส่งสแปมมักจะถูกใช้เพื่อส่งข้อความในลักษณะของการชักจูงหรือโฆษณาไปยังกลุ่มผู้รับต่าง ๆ ผ่านทางอีเมล์ โปรแกรมสนทนา รวมทั้งอีเมล์และ SMS ในโทรศัพท์มือถือ จึงมีผลทำให้ระบบคอมพิวเตอร์นั้น ถูกเพิ่มเติมข้อความนั้นลงไปด้วย
13. โปรแกรมระเบิด (Bombs Programs)	โปรแกรมระเบิดเป็นโปรแกรมที่กำหนดเงื่อนไขให้ทำงานเมื่อมีเหตุการณ์หรือเงื่อนไขใด ๆ เกิดขึ้น ลักษณะที่พบ เช่น โปรแกรมจะถูกลบเองเมื่อถูกรันไปแล้ว 2-3 ครั้ง จึงอาจส่งผลทำให้ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีอยู่เสียหาย หรือถูกทำลายตามไปด้วย
14. โปรแกรมโทรศัพท์อัตโนมัติ (Dialers Programs)	หากมีการติดตั้งโปรแกรมประเภทนี้ในเครื่องคอมพิวเตอร์ จะมีการต่อโทรศัพท์อัตโนมัติ ซึ่งจุดมุ่งหมายก็เพื่อที่จะให้เหยื่อนั้นต้องจ่ายค่าโทรศัพท์ในอัตราที่แพงที่สุดหรือทำให้เสียค่าโทรศัพท์ระหว่างประเทศ จึงเป็นการทำให้ระบบคอมพิวเตอร์ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
15. โปรแกรมล้อกันเล่น (Joke Programs)	เป็นโปรแกรมที่ไม่ได้ตั้งใจทำอันตรายต่อเครื่องหรือระบบโดยตรง หากเพียงแค่ต้องการก่อกวนหรือสร้างความรำคาญให้แก่ผู้ใช้งานโดยการเข้าไปเปลี่ยนพฤติกรรมปกติของเครื่องคอมพิวเตอร์ เช่น หากโปรแกรมนี้เป็นสกรีนเซฟเวอร์ก็อาจจะทำการล็อกหน้าจอได้เองทั้ง ๆ ที่ผู้ใช้งานเองไม่ได้ปรับแต่งค่าให้ล็อก อย่างไรก็ตามโปรแกรมนี้อาจทำอันตรายได้ในบางกรณี เช่น เมื่อทำการล็อกหน้าจอแต่ไม่ปลดล็อกให้ ดังนั้น อาจจะต้องปิดเครื่องคอมพิวเตอร์โดยที่ไม่ได้บันทึกงานไว้ก่อน ทำให้เกิดความเสียหายต่อผู้ใช้งานได้ เป็นต้น กรณีดังกล่าวจึงเป็นการทำให้ระบบคอมพิวเตอร์ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ประเภทของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย	คุณสมบัติในการทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
16. ฟลัดเดอร์ (Flooders)	แฮกเกอร์จะใช้โปรแกรมประเภทนี้ในการโจมตีระบบเครือข่ายเป้าหมายด้วยการส่งข้อมูลในปริมาณมหาศาล เพื่อทำให้เกิดความคับคั่งในระบบเครือข่าย ส่งผลให้เครือข่ายเป้าหมายไม่สามารถให้บริการต่อไปได้ เรียกการโจมตีประเภทนี้ว่า Denial of Service (DoS) ถ้าหากว่ามีเครื่องคอมพิวเตอร์ที่ถูกควบคุมและจะถูกใช้โจมตีแบบ DoS พร้อมกันหลาย ๆ เครื่องไปยังเป้าหมายเดียวกัน จะเรียกการโจมตีแบบนี้ว่า Distributed Denial of Service (DDoS) ดังนั้น ฟลัดเดอร์จึงมีผลทำให้ระบบคอมพิวเตอร์ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
17. รูทคิท (Rootkit)	หลังจากแฮกเกอร์สามารถเจาะระบบเข้าไปจนได้สิทธิการควบคุมระบบแล้ว จากนั้นก็จะติดตั้งโปรแกรมรูทคิทโดยการดัดแปลงโปรแกรมที่ถูกติดตั้งไว้อยู่แล้ว เพื่อหลอกให้ผู้ดูแลระบบไม่ให้สังเกตเห็นไฟล์ผิดปกติที่ถูกสร้างโดยแฮกเกอร์ จึงมีผลทำให้ระบบคอมพิวเตอร์นั้นถูกเพิ่มเติมหรือถูกแก้ไขเปลี่ยนแปลงตามไปด้วย

4. วงจรชีวิตของชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหาย

จากการศึกษาพบว่าชุดคำสั่งไม่พึงประสงค์จะมีวงจรชีวิตเหมือนเฉกเช่นสิ่งมีชีวิตที่เกิดขึ้นเองตามธรรมชาติโดยทั่วไป แต่มีความแตกต่างและข้อจำกัดในเกณฑ์บางประการ โดยชุดคำสั่งไม่พึงประสงค์ในทางทำให้เกิดความเสียหายมีจรชีวิต คือ การกำเนิด การแพร่เชื้อ การโจมตีระบบ และการถูกกำจัดซึ่งมักจะใช้ 2 วิธี คือ การจำกัดด้วยมือ (เช่น การเข้าไปแก้ไขค่าในรีจิสทรีย์ (Registry) ให้กลับคืนเหมือนเดิมและลบไฟล์ของชุดคำสั่งไม่พึงประสงค์โดยตรง เป็นต้น) และการใช้โปรแกรมต่อต้านและตรวจสอบ

5. เทคนิคและวิธีการตรวจจับชุดคำสั่งไม่พึงประสงค์

เทคนิคและวิธีการที่ใช้ในการตรวจจับ เพื่อกำจัดชุดคำสั่งไม่พึงประสงค์โดยทั่วไปแล้วสามารถแบ่งได้เป็น 4 วิธีการ คือ การตรวจหา (Scanning) การตรวจสอบความคงอยู่หรือความครบถ้วนสมบูรณ์ (Integrity Checking) การตรวจจับชุดคำสั่งไม่พึงประสงค์ด้วยการวิเคราะห์พฤติกรรม (Heuristic) และการตรวจจับชุดคำสั่งไม่พึงประสงค์โดยการดักจับ (Interception)

6. รูปแบบของการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์ สามารถแยกได้เป็น

6.1 การกระทำความผิดโดยการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เช่น การขโมยเอกลักษณ์บุคคล (Identity Theft) การโจมตีเครื่องคอมพิวเตอร์แม่ข่ายผ่านช่องโหว่ (Software flaws) การปล่อยมัลแวร์ผ่านโปรแกรมประเภท Peer-to-Peer (P2P) และโปรแกรมประเภท Instant Messaging (IM) การโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) เป็นต้น

6.2 การกระทำความผิดโดยการดักข้อมูล แยกได้เป็นการดักข้อมูลในเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ และการดักข้อมูลผ่านปุ่มคีย์บอร์ดด้วยมัลแวร์

มาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศ

หลายประเทศได้บัญญัติกฎหมายเพื่อใช้บังคับกับการกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ เนื่องจากกฎหมายที่มีอยู่เดิมไม่สามารถใช้บังคับกับการก่ออาชญากรรมทางคอมพิวเตอร์หรือการใช้คอมพิวเตอร์ในทางมิชอบได้ โดยบางประเทศได้บัญญัติเป็นกฎหมายพิเศษ หรือในบางประเทศอาจต้องปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่ให้ทันต่อการกระทำความผิดดังกล่าว หรือในบางประเทศอาจใช้ทั้งสองวิธีคือทั้งการปรับแก้กฎหมายอาญาที่ใช้บังคับอยู่และบัญญัติเป็นกฎหมายพิเศษเพื่อการกำหนดฐานความผิดและบทกำหนดโทษขึ้นมาเป็นการเฉพาะเป็นเรื่อง ๆ ไปภายใต้ความเหมาะสมของแต่ละประเทศ ทั้งนี้ก็เพื่อให้กฎหมายที่มีอยู่สามารถบังคับใช้และทันต่อการกระทำความผิดดังกล่าวได้ โดยกฎหมายของต่างประเทศตามที่ปรากฏใน A Global Survey of Cybercrime Legislation[1] 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) การใช้อุปกรณ์ในทางมิชอบ (Misuse of devices)

---

[1] *อ่านรายละเอียดและสืบค้นข้อมูลเพิ่มเติมได้ที่ http://www.cybercrimelaw.net*

(6) การปลอมแปลงทางคอมพิวเตอร์ (Computer related-forgery) และ

(7) การฉ้อโกงทางคอมพิวเตอร์ (Computer-related fraud)[2]

อย่างไรก็ตาม หากจะพิจารณาเฉพาะฐานความผิดที่อาจใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือในการกระทำความผิดตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์แล้ว 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 ก็คงจะถูกส่งและนำไปฝังไว้ในระบบคอมพิวเตอร์ของผู้อื่นไม่ได้ โดยจะได้พิจารณามาตรการในการกำหนดนิยามและความหมายของคำว่า “เข้าถึง (access)” ในกฎหมายต่างประเทศพร้อมกับยกตัวอย่างกฎหมายของต่างประเทศที่มีการกำหนดคำนิยามดังกล่าวไว้ ต่อจากนั้นจะเป็นการพิจารณาและกล่าวถึงในรายละเอียดและองค์ประกอบของการเข้าถึงโดยมิชอบ (Illegal access) ตาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พร้อมกับยกตัวอย่างมาตรการทางกฎหมายในการป้องกันการเข้าถึงโดยมิชอบของต่างประเทศด้วย

1. **มาตรการกำหนดนิยามและความหมายของการเข้าถึง (access) ให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดที่เกิดจากชุดคำสั่งไม่พึงประสงค์**

นอกจากมาตรการป้องกันการเข้าถึงโดย

---

[2] *นอกเหนือจากฐานความผิดที่สำคัญทั้ง 7 ฐานแล้ว ยังมีบทบัญญัติในฐานความผิดที่เกี่ยวกับเนื้อหาสาระ ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง การพยายามและการสนับสนุนการกระทำความผิดที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป ได้แนะนำไว้ให้แต่ละประเทศนำไปบัญญัติเพิ่มเติม โดยในส่วนของบทบัญญัติความผิดที่เกี่ยวกับเนื้อหาสาระ ความผิดเกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิที่เกี่ยวข้อง การพยายามและการสนับสนุนการกระทำความผิดได้ถูกบัญญัติไว้ในประมวลกฎหมายอาญาและกฎหมายทรัพย์สินทางปัญญาของประเทศไทยแล้ว ดังนั้นการปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยในส่วนที่พระราชบัญญัตินี้มิได้บัญญัติไว้เป็นการเฉพาะก็ต้องปรับใช้ร่วมกับประมวลกฎหมายอาญาด้วย โดยเฉพาะอย่างยิ่งในส่วนของเจตนา ตัวการ การพยายามและการสนับสนุนการกระทำความผิด เป็นต้น*

มิชอบ (Illegal access) แล้ว ในกฎหมายต่างประเทศยังมีการบัญญัติความหมายของคำว่า "เข้าถึง (access)" ไว้เพื่อให้การปรับใช้กฎหมายเป็นไปอย่างชัดเจนอีกด้วย ซึ่งถือว่าเป็นความแตกต่างที่เป็นนัยสำคัญเกี่ยวกับเทคนิคการบัญญัติกฎหมายในส่วนที่เกี่ยวกับความหมายของชุดคำสั่งไม่พึงประสงค์ โดยกฎหมายไทยพยายามจะบัญญัติความหมายของชุดคำสั่งไม่พึงประสงค์ให้มีความทันสมัยและสามารถรองรับกับอนาคตของเทคโนโลยีที่เปลี่ยนแปลงไปได้ตามยุคสมัย กล่าวคือ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยจะใช้วิธีการให้ความหมายแก่บรรดาไวรัสคอมพิวเตอร์ ม้าโทรจัน หนอนคอมพิวเตอร์ สปายแวร์ หรือมัลแวร์ชนิดต่าง ๆ เหล่านั้น โดยเรียกรวมเป็นชื่อเดียวกันว่า "ชุดคำสั่งไม่พึงประสงค์ (malicious software หรือ undesirable sets of instructions)"[3] แล้วใช้เทคนิคการอธิบายเพื่อขยายความหมายชุดคำสั่งไม่พึงประสงค์เหล่านั้นในวรรคสอง ของมาตรา 21 แห่งพระราชบัญญัติฯ โดยเปิดโอกาสให้มีการเพิ่มเติมเพื่อการขยายขอบเขตและความหมายของชุดคำสั่งไม่พึงประสงค์ที่จะเกิดขึ้นในอนาคตโดยการตราเป็นกฎกระทรวง ซึ่งเป็นกฎหมายในลำดับรองได้อีกด้วย ส่วนในฝั่งของต่างประเทศนั้น จะไม่ใช้เทคนิคการบัญญัติความหมายของชุดคำสั่งไม่พึงประสงค์รวมไว้เป็นชื่อเดียวกันเหมือนดังประเทศไทย แต่จะใช้วิธีการบัญญัติกฎหมายเป็นสองวิธีดังนี้

วิธีที่หนึ่ง โดยการเรียกชื่อและกำหนดนิยามความหมายของชุดคำสั่งไม่พึงประสงค์ตามแต่ละประเภทของชุดคำสั่งไม่พึงประสงค์ที่นักคอมพิวเตอร์และที่สากลนิยมเรียกกัน ซึ่งทำให้สามารถสื่อความหมายและเข้าใจได้โดยตรงตามแต่ละประเภทของชุดคำสั่งไม่พึงประสงค์ ตัวอย่างของการเรียกหรือนิยามชุดคำสั่งไม่พึงประสงค์ที่ปรากฏในกฎหมายต่างประเทศ เช่น ประมวลกฎหมายอาญาแห่งมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา (Computer Crimes-Texas Penal Code) ใน Title 7 Chapter 33 ได้ให้นิยามความหมายของไวรัสคอมพิวเตอร์ว่า[4] หมายถึง "โปรแกรมคอมพิวเตอร์ที่ไม่พึงประสงค์หรือชุดคำสั่งอื่นใดหรือโปรแกรมที่ถูกสร้างขึ้นเฉพาะซึ่งเมื่อบันทึกลงในหน่วยความจำของเครื่องคอมพิวเตอร์หรือระบบปฏิบัติการหรือโปรแกรมอื่นแล้ว สามารถสร้างหรือทำสำเนาตนเองหรือติดตั้งตนเองไปกับโปรแกรมอื่นหรือไฟล์อื่น" แล้วจึงกำหนดความผิดฐานเข้าถึงโดยมิชอบด้วยไวรัสคอมพิวเตอร์ตามนิยามดังกล่าว เป็นต้น

วิธีที่สอง โดยการพิจารณาจากพฤติการณ์และองค์ประกอบของความผิดฐานการเข้าถึงโดยมิชอบเป็นสำคัญ ทั้งนี้ มีทั้งการกำหนดนิยามของการเข้าถึงไว้ และมิได้กำหนดนิยามของการเข้าถึงไว้แต่จะกำหนดเป็นพฤติการณ์

---

[3] *พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฉบับภาษาอังกฤษเรียกชุดคำสั่งไม่พึงประสงค์ว่า "undesirable sets of instructions" ซึ่ง หมายถึง ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ทั้งนี้ ความหมายดังกล่าวก็ตรงกับความหมายในมุมมองของนักคอมพิวเตอร์และหลักสากลที่เรียกชุดคำสั่งไม่พึงประสงค์ว่า "malicious code หรือ malicious program หรือ malicious software" ที่หมายถึงบรรดาไวรัสคอมพิวเตอร์ ม้าโทรจัน หนอนคอมพิวเตอร์ สปายแวร์ หรือมัลแวร์ชนิดต่าง ๆ นั่นเอง*

[4] *"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.*

และองค์ประกอบในฐานความผิดนั้น ๆ ไว้ โดยไม่คำนึงว่าจะใช้ชุดคำสั่งไม่พึงประสงค์ประเภทใดในการเข้าถึงซึ่งหากเข้าข่ายตามพฤติการณ์และองค์ประกอบของฐานความผิดที่กำหนดไว้แล้ว ก็จะถือว่าเป็นการกระทำความผิดฐานเข้าถึงโดยมิชอบ ซึ่งกฎหมายในต่างประเทศส่วนใหญ่มักจะใช้วิธีที่สองนี้เป็นองค์ประกอบในการบัญญัติฐานความผิดการเข้าถึงโดยมิชอบ

ตัวอย่างกฎหมายของต่างประเทศที่มีการกำหนดนิยามและความหมายของคำว่า "เข้าถึง (access)" ไว้ เช่น ประเทศออสเตรเลียกำหนดไว้ใน Cybercrime Act 2001 ประเทศนิวซีแลนด์กำหนดไว้ใน Crimes Amendment Act 2003 No 39 Part 1 s 15, of July 7th ประเทศอินเดียกำหนดไว้ใน The Information Technology Act 2000 เป็นต้น ส่วนสหรัฐอเมริกานั้นมิได้กำหนดนิยามการเข้าถึงไว้โดยตรง 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)" อย่างไรก็ตามในกฎหมายระดับมลรัฐของสหรัฐอเมริกาก็ได้มีการกำหนดนิยามการเข้าถึงไว้ เช่น รัฐแคลิฟอร์เนีย รัฐแมริแลนด์ รัฐนิวเม็กซิโก เป็นต้น

2. มาตรป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ตามอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของคณะมนตรีแห่งยุโรป

การกระทำความผิดฐานเข้าถึงโดยมิชอบตามอนุสัญญานี้อาจเกิดขึ้นได้หลายวิธีด้วยกัน เช่น การเจาะระบบ (Hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) เป็นต้น คำว่า "เข้าถึง (access)" ตามอนุสัญญานี้หมายความว่า การเข้าถึงทั้งในระดับกายภาพด้วย เช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์ และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายรวมถึงการเข้าระบบคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์ที่ตนต้องการได้ นอกจากนี้ ยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้น จึงอาจหมายถึง การเข้าถึงฮาร์ดแวร์ หรือส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ ข้อมูลที่ถูกบันทึกเก็บไว้ในระบบเพื่อใช้ในการส่งหรือโอนถึงอีกบุคคลหนึ่ง เช่น ข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น

อนึ่ง "เข้าถึง" ยังหมายถึงการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต อันเป็นการเชื่อมโยงระหว่างเครือข่ายหลาย ๆ เครือข่ายเข้าด้วยกันทั่วโลก และยังหมายถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบเครือข่ายท้องถิ่น (Local Area Network : LAN) ระบบอินทราเน็ต (Intranet) ภายในองค์กรเดียวกันโดยไม่ต้องพิจารณาถึงระยะทาง และรูปแบบของการติดต่อสื่อสารว่าใช้วิธีการทางสายหรือไร้สาย นอกจากนี้ ประเทศภาคีอาจกำหนดเงื่อนไขเพิ่มเติมว่า ผู้กระทำความผิดฐานนี้จะต้องละเมิดระบบการรักษาความปลอดภัย (infringing security measures) หรือมีเจตนาเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์หรือเจตนาทุจริตอื่น หรือดำเนินการอื่นใดต่อ

ระบบคอมพิวเตอร์ซึ่งได้เชื่อมต่อเข้ากับระบบคอมพิวเตอร์อื่นด้วยก็ได้

3. มาตรการป้องกันการเข้าถึงโดยมิชอบ (Illegal access) ในกฎหมายต่างประเทศ

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

3.1 กฎหมายที่ให้การคุ้มครองระบบคอมพิวเตอร์ ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองระบบคอมพิวเตอร์ เช่น ประเทศฝรั่งเศสได้บัญญัติไว้ใน Penal Code (Chapter III – Attacks on systems for automated data processing) ประเทศอิตาลีได้บัญญัติไว้ใน Penal Code (Article 615 ter : Unauthorized access into a computer or telecommunication systems) ประเทศเนเธอร์แลนด์ได้บัญญัติไว้ใน Criminal Code (Article 138a:) ประเทศโปรตุเกสได้บัญญัติไว้ใน Criminal Information Law of August 17, 1991: (Chapter 1 Article 7:) ประเทศสวิตเซอร์แลนด์ได้บัญญัติไว้ใน Penal Code (Article 143 bis: Unauthorized access to data processing system) เป็นต้น

3.2 กฎหมายต่างประเทศที่ให้การคุ้มครองข้อมูลคอมพิวเตอร์ ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองข้อมูลคอมพิวเตอร์ เช่น ประเทศเยอรมันได้บัญญัติไว้ใน Criminal Law (Section 202a) ประเทศอังกฤษได้บัญญัติไว้ใน Computer Misuse Act 1990 (section 1) เป็นต้น

3.3 กฎหมายต่างประเทศที่ให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ ตัวอย่างกฎหมายต่างประเทศที่ให้การคุ้มครองทั้งระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ เช่น ประเทศฟิลิปปินส์ได้บัญญัติไว้ใน Electronic Commerce Act 2000 (section 33) ประเทศอินเดียได้บัญญัติไว้ใน The Information Technology Act 2000 (section 66) ประเทศสหรัฐอเมริกาได้บัญญัติไว้ใน 18 U.S.C. 1030. Fraud and Related Activity in Connection with Computers เป็นต้น

วิเคราะห์และสรุปปัญหาเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. วิเคราะห์ความสัมพันธ์ระหว่างชุดคำสั่งไม่พึงประสงค์กับการเข้าถึง

เหตุที่ต้องกล่าวและวิเคราะห์ถึงความสัมพันธ์ระหว่างชุดคำสั่งไม่พึงประสงค์กับการเข้าถึงนั้น ก็เนื่องมาจากการกระทำความผิดโดยใช้ชุดคำสั่งไม่พึงประสงค์เป็นเครื่องมือนั้นถือได้ว่าเป็นการกระทำความผิดต่อคอมพิวเตอร์โดยแท้ที่จะต้องผ่านกระบวนการเข้าถึง (การเข้าถึงในที่นี้หมายความถึงเฉพาะการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลเท่านั้น) ก่อนเสมอจึงจะสามารถนำไปสู่การกระทำที่จะก่อให้เกิดความเสียหายและส่งผลกระทบอื่น ๆ ตามมาตามที่ได้กล่าวไปแล้ว ทั้งนี้ หากปราศจากการเข้าถึงเสียแล้ว ความเสียหายและผลกระทบต่าง ๆ ก็คงมิอาจเกิดขึ้นได้ จึงอาจกล่าวได้ว่าการเข้าถึงเป็นบ่อเกิดหรือเป็นต้นธารแห่งการกระทำความผิดต่อคอมพิวเตอร์โดยแท้

หากพิจารณามาตรการทางกฎหมายที่

เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศจะมิได้มีแต่เฉพาะมาตรการป้องกันหรือแก้ไขปัญหาที่เกิดจากการที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม หรือขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้เท่านั้น แต่มาตรการทางกฎหมายที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์ในต่างประเทศนั้นสามารถครอบคลุมถึงความเสียหายหรือผลกระทบ และพฤติการณ์จากชุดคำสั่งไม่พึงประสงค์ได้อย่างครบถ้วนในทุกรูปแบบซึ่งรวมถึงความเสียหายและผลกระทบต่อความเป็นอยู่ส่วนตัวในการติดต่อสื่อสารของประชาชน และความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับด้วย จนทำให้การกระทำความผิดโดยการใช้ชุดคำสั่งไม่พึงประสงค์ทุกๆ ประเภทไม่ว่าจะเป็นไวรัสคอมพิวเตอร์ ม้าโทรจัน สปายแวร์ และแอดแวร์ ในบางประเทศนั้น สามารถปรับเข้ากับฐานความผิดในกฎหมายที่มีอยู่ได้แทบทุกกรณีที่เกิดขึ้น โดยไม่เกิดความคลุมเครือในการบังคับใช้กฎหมาย สาเหตุที่เป็นเช่นนั้นก็เพราะในกฎหมายของต่างประเทศได้มีการกำหนดนิยามและความหมายของการ “เข้าถึง (access)” ไว้โดยชัดแจ้ง เพื่อให้ครอบคลุมถึงพฤติการณ์แห่งการกระทำความผิดได้ในทุกๆ รูปแบบและใช้เป็นบรรทัดฐานสำหรับผู้ที่ต้องปรับใช้กฎหมายได้เป็นอย่างดีนั่นเอง

2. วิเคราะห์องค์ประกอบภายนอกของความรับผิดทางอาญาที่เกิดจากชุดคำสั่งไม่พึงประสงค์

องค์ประกอบภายนอกของความรับผิดทางอาญาแทบทุกฐานแยกออกได้เป็น ผู้กระทำ การกระทำ และวัตถุแห่งการกระทำ เช่น ความผิดฐานฆ่าคนตายโดยเจตนาตามประมวลกฎหมายอาญามาตรา 288 ได้แก่ ผู้ใด (ผู้กระทำ) ฆ่า (การกระทำ) ผู้อื่น (วัตถุแห่งการกระทำ) เป็นต้น ทั้งนี้ในการวินิจฉัยความรับผิดทางอาญาของบุคคลนั้น มีหลักเกณฑ์ในการวินิจฉัยที่สำคัญที่สุดประการแรกคือ ต้องพิจารณาเสียก่อนว่าบุคคลนั้นมี “การกระทำ” หรือไม่ เพราะประมวลกฎหมายอาญามาตรา 59 บัญญัติว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำโดยเจตนา เว้นแต่จะได้กระทำโดยประมาทในกรณีที่กฎหมายบัญญัติให้ต้องรับผิดเมื่อได้กระทำโดยประมาท หรือเว้นแต่ในกรณีที่กฎหมายบัญญัติไว้โดยชัดแจ้งให้ต้องรับผิดแม้ได้กระทำโดยไม่มีเจตนา” จากบทบัญญัติดังกล่าวในตอนต้นที่ว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำ...” แสดงว่าการกระทำเป็นเงื่อนไขประการแรกของความรับผิดในทางอาญา

ทั้งนี้ สำหรับองค์ประกอบภายนอกของความรับผิดทางอาญาในอาชญากรรมพื้นฐาน (Conventional Crimes) นั้น จะพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึก กล่าวคือ การเคลื่อนไหวร่างกายนั้นต้องอยู่ภายใต้บังคับของจิตใจ แต่สำหรับอาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ที่ใช้ชุดคำสั่งไม่ถึงประสงค์เป็นเครื่องมือในกระทำผิดโดยการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลนั้น การพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึกเพียงอย่างเดียวคงไม่เพียงพอที่จะถือว่าบุคคลนั้นมี “การกระทำ” หรือไม่ ทั้งนี้จะต้องพิจารณาจากลักษณะหรือผลที่ปรากฏออกมา ซึ่งได้แก่ การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุด

คำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ประกอบด้วยเสมอ ส่วนวัตถุแห่งการกระทำสำหรับความผิดนี้ก็คือ ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นนั่นเอง ทั้งนี้ จะต้องพิจารณาถึงองค์ประกอบภายในซึ่งเป็นส่วนของเจตนาตามมาตรา 59 ประกอบด้วย

2.1 การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม

อย่างไรจึงจะเรียกว่าเป็น "การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม" ลักษณะดังกล่าวนี้เป็นการใช้ถ้อยคำซึ่งเป็นองค์ประกอบความผิดฐานทำให้เสียทรัพย์ตามประมวลกฎหมายอาญา มาตรา 358 คือคำว่า "ทำให้เสียหาย" และ "ทำลาย" แต่ในส่วนที่เกี่ยวกับการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมนั้น ไม่ได้ยกองค์ประกอบของความผิดฐานปลอมเอกสารมา อาจเป็นเพราะชุดคำสั่งไม่พึงประสงค์จะอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์หรือดิจิทัลจึงนำลักษณะของการแก้ไขเปลี่ยนแปลงหรือเพิ่มเติมในข้อมูลอิเล็กทรอนิกส์ไปเปรียบเทียบกับความผิดฐานปลอมเอกสารไม่ได้ ทั้งนี้คำว่า "การแก้ไข เปลี่ยนแปลง เพิ่มเติม" จัดได้ว่าเป็นคำสามัญที่มีความชัดเจนเพียงพอและพึงเข้าใจได้

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

2.2 การทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้

การทำให้ระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานตามปกติได้นั้น สามารถพบได้ในสองลักษณะ คือ การที่ระบบคอมพิวเตอร์เกิดความขัดข้อง หรือการที่ระบบคอมพิวเตอร์ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ สำหรับประเด็นที่ว่าอย่างไรจึงจะเรียกว่าเป็นการ "ขัดข้องหรือการปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้" นั้น ย่อมพิจารณาได้จากการที่ระบบคอมพิวเตอร์นั้นไม่สามารถทำงานได้โดยสมบูรณ์ ดังนั้น ถึงแม้ว่าระบบคอมพิวเตอร์จะทำงานได้ แต่เป็นการทำงานที่ไม่สมบูรณ์หรือผิดปกติไป (malfunctioning) ก็ย่อมอยู่ในความหมายของถ้อยคำดังกล่าวแล้ว

3. สรุปปัญหาทางกฎหมายเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

3.1 ปัญหาในการบังคับใช้กฎหมาย ได้แก่

3.1.1 ความไม่ชัดเจนและไม่สอดคล้องกับทางปฏิบัติของส่วนกฎหมายวิธีสบัญญัติตามมาตรา 21 โดยแยกเป็น (1) ปัญหาในการ

บังคับใช้กฎหมายในมาตรา 21 วรรคหนึ่ง ซึ่งมีอยู่สองประการ คือ ปัญหาในทางปฏิบัติที่พนักงานเจ้าหน้าที่ไม่อาจตรวจสอบได้ว่าข้อมูลคอมพิวเตอร์ใดมีชุดคำสั่งไม่พึงประสงค์แอบแฝงหรือปะปนรวมอยู่ด้วยได้ 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

3.1.2 การมิได้แยกแยะประเภทของชุดคำสั่งไม่พึงประสงค์ มีผลทำให้ปัจจุบันยังไม่มีชุดคำสั่งไม่พึงประสงค์ใดที่กฎหมายรับรองว่าเป็นชุดคำสั่งที่มุ่งหมายในการป้องกันและแก้ไขชุดคำสั่งอื่นเลย ทั้งที่ในความเป็นจริงแล้วยังมีชุดคำสั่งอีกหลายประเภทที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์อื่นที่ถูกพบเห็นและนำมาใช้ในชีวิตประจำวันของประชาชนทั่วไป เช่น โปรแกรมต่อต้านและตรวจสอบไวรัสคอมพิวเตอร์ สปายแวร์ หรือม้าโทรจัน โปรแกรมต่อต้านการส่งสแปมเมล์ เป็นต้น จึงทำให้พนักงานเจ้าหน้าที่และประชาชนเกิดความสับสนและความไม่แน่ใจในทางปฏิบัติและมิได้เป็นไปตามเจตนารมณ์ของพระราชบัญญัตินี้

3.2 ปัญหาในการบัญญัติกฎหมาย ได้แก่

3.2.1 ปัญหาการกำหนดนิยามและความหมายทางเทคนิค ที่พระราชบัญญัตินี้มิได้กำหนดนิยามความหมายของคำว่า “เข้าถึง (access)” ไว้โดยตรงทำให้มิอาจบังคับและตีความไปถึงการกระทำผิดโดยใช้ม้าโทรจันและสปายแวร์ได้ และเมื่อนำกฎหมายของไทยไปเปรียบเทียบกับกฎหมายของต่างประเทศจะพบว่ามีความแตกต่างกันอย่างมีนัยสำคัญ กล่าวคือ ตามกฎหมายของไทยหากสามารถเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ผู้กระทำประสงค์จะเข้าถึง และเมื่อสามารถเข้าถึงได้แล้ว ก็ย่อมจะถือว่าการกระทำการเข้าถึงดังกล่าวได้สำเร็จลงแล้ว และภายหลังจากนั้นหากมีการทำลาย แก้ไขเปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ หรือทำการรบกวนต่าง ๆ จนทำให้ระบบคอมพิวเตอร์หยุดทำงานนั้นก็ยังอยู่ในความหมายของการเข้าถึงตามกฎหมายของไทย แต่หากมีกรณีการได้ใช้ประโยชน์อื่นใดภายหลังจากการเข้าถึงที่ไม่เข้ากรณีดังกล่าว เช่น (1) มีการทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความความจำอื่นในระบบคอมพิวเตอร์นั้นเองหรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ (2) การสั่งการให้ระบบคอมพิวเตอร์ปฏิบัติการเพื่อให้สามารถบันทึกข้อมูลคอมพิวเตอร์หรือได้รับข้อมูลคอมพิวเตอร์จาก

ระบบคอมพิวเตอร์ดังกล่าว หรือ (3) การสั่งการให้คอมพิวเตอร์ปฏิบัติการหรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผลหรือหน่วยบันทึกผลของระบบคอมพิวเตอร์อื่นได้ ตลอดจนการกระทำการอื่นใดเพื่อแสวงหาประโยชน์จากระบบคอมพิวเตอร์ที่ถูกเข้าถึงโดยที่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นมิได้เกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้นั้นกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยคงมิอาจบังคับและตีความไปถึงได้ เพราะหลักการตีความกฎหมายอาญาต้องตีความโดยเคร่งครัดและเป็นไปตามหลักสากลที่ว่า “ไม่มีกฎหมาย ไม่มีความผิด”

3.2.2 ปัญหาการกำหนดฐานความผิด ที่แม้พระราชบัญญัตินี้จะได้กำหนดฐานความผิดและบทลงโทษสำหรับผู้ที่จำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 ถึงมาตรา 11 และมีมาตรการในการดำเนินการเกี่ยวกับโปรแกรมหรือชุดคำสั่งไม่พึงประสงค์ไว้ในมาตรา 21 แล้วก็ตาม แต่บทบัญญัติในมาตราดังกล่าวยังไม่ครอบคลุมถึงลักษณะของการกระทำความผิดที่เกิดจากการใช้ม้าโทรจันและสปายแวร์นำไปฝังหรือติดตั้งไว้ในระบบคอมพิวเตอร์แล้วจะมีการแอบส่งข้อมูลคอมพิวเตอร์ หรือแอบดักข้อมูลต่าง ๆ ไม่ว่าจะเป็นข้อมูลส่วนบุคคลหรือข้อมูลสำคัญที่เป็นเอกลักษณ์บุคคลส่งออกไปยังคนร้ายหรือผู้บุกรุก หากการกระทำความผิดดังกล่าวเป็นการเข้าถึงระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่เป็นการเข้าไปทำลาย แก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ หรือเป็นการเข้าไปรบกวนต่อระบบคอมพิวเตอร์โดยการฝ่าฝืนมาตรการป้องกันที่จัดทำไว้เป็นการเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ก็จะถือเป็นความผิดตามมาตรา 5 ถึง มาตรา 11 ได้ แต่หากการเข้าถึงดังกล่าวนั้นเป็นการเข้าถึงโดยชอบไม่ว่าจะเป็นเพราะความยินยอมของเจ้าของคอมพิวเตอร์นั้น หรือในบางกรณีแฮกเกอร์หรือคนร้ายอาจใช้เทคนิคการหลอกล่อเพื่อให้เจ้าของคอมพิวเตอร์ให้ความยินยอมในการเข้าไป แล้วต่อมามีการแอบส่งข้อมูลคอมพิวเตอร์ออกไปยังคนร้าย ก็จะทำให้การเข้าถึงในกรณีนี้ไม่เข้าข่ายเป็นความผิดตามพระราชบัญญัตินี้ และไม่เป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา และไม่เป็นความผิดตามพระราชบัญญัติอื่นที่มีโทษทางอาญาเลย ทั้งนี้ประเด็นการขโมยหรือแอบส่งหรือแอบดักข้อมูลด้วยม้าโทรจันหรือสปายแวร์ยังถือเป็นการกระทำละเมิดต่อข้อมูลส่วนบุคคลที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์อีกด้วย ซึ่งปัจจุบันก็ยังไม่มีกฎหมายใดที่จะสามารถปรับใช้เพื่อการป้องกันหรือปราบปรามการกระทำความผิดดังกล่าวได้

3.2.3 ปัญหาความหมายคำว่า “โดยมิชอบ” ซึ่งผู้เขียนเห็นว่าองค์ประกอบของความผิด “เข้าถึงโดยมิชอบ” เป็นการรวมคำสองคำเข้าด้วยกัน คือ คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” แต่มิได้หมายความว่าเมื่อนำไปปรับใช้กับฐานความผิดการเข้าถึงโดยมิชอบแล้วจะต้องตีความรวมเป็นคำเดียวกัน แต่ในทางตรงกันข้ามผู้เขียนเห็นว่า คำว่า “เข้าถึง” กับคำว่า “โดยมิชอบ” จะต้องตีความแยกออกจากกันซึ่งจะทำให้ง่ายแก่การทำความเข้าใจความหมายของทั้งสองคำดังกล่าว หรือหาก

จะนำแนวคำพิพากษาศาลฎีกามาเป็นเกณฑ์ในการกำหนดหลักเกณฑ์ในการตีความ คำว่า "โดยมิชอบ" และปล่อยให้เป็นหน้าที่ของศาลที่จะตีความให้เหมาะสมกับพฤติกรรมของผู้กระทำผิดในแต่ละคดีนั้นคงไม่เหมาะสม เพราะแนวคำพิพากษาของศาลฎีกาในปัจจุบันมิใช่เป็นคดีความผิดที่เกี่ยวกับคอมพิวเตอร์แต่เป็นคดีแพ่งและคดีอาญาทั่วไป ซึ่งที่มาของการบัญญัติกฎหมายมีความแตกต่างจากพระราชบัญญัตินี้ และตัวผู้พิพากษาที่ตัดสินคดีนั้นก็อาจมิได้เป็นผู้ที่มีความรู้หรือมีความเชี่ยวชาญด้านคอมพิวเตอร์อย่างเพียงพอที่จะสามารถใช้เป็นบรรทัดฐานในการตัดสินคดีความผิดเกี่ยวกับคอมพิวเตอร์ได้

3.3 ปัญหาการใช้และการตีความกฎหมาย ได้แก่

3.3.1 กฎหมายอาญาต้องมีบทบัญญัติโดยชัดแจ้ง ประกอบด้วย 3 ส่วนที่สำคัญคือ (1) บทบัญญัติกฎหมายอาญาต้องเป็นลายลักษณ์อักษรซึ่งกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มิได้บัญญัติหรือกำหนดความหมายของคำว่า "เข้าถึง" ไว้ ทำให้กรณีของการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลโดยเฉพาะอย่างยิ่งการเข้าถึงโดยใช้ชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์เป็นช่องว่างของกฎหมาย ทำให้ผู้กระทำผิดไม่ต้องรับผิดทั้ง ๆ ที่จริงแล้วผู้กระทำผิดสมควรจะต้องได้รับโทษนั้นแต่บทบัญญัติของกฎหมายตีความไปไม่ถึง ทำให้ต้องปล่อยตัวผู้ต้องหาหรือจำเลยไปในที่สุด (2) กฎหมายอาญาต้องมีบทบัญญัติความผิดและโทษไว้ในขณะกระทำ (3) บทบัญญัติกฎหมายอาญาต้องชัดเจนปราศจากการคลุมเครือ ซึ่งคำว่า "เข้าถึง" จัดได้ว่าเป็นศัพท์เฉพาะที่มิใช่ภาษาสามัญธรรมดาจึงจำเป็นต้องกำหนดเป็นคำนิยามไว้ เพื่อจะได้เป็นบรรทัดฐานในการบังคับใช้และการตีความกฎหมายของเจ้าพนักงานในการยุติธรรมโดยเฉพาะพนักงานเจ้าหน้าที่

3.3.2 กฎหมายอาญาต้องตีความโดยเคร่งครัด ประกอบด้วย 4 ส่วนสำคัญ ได้แก่ (1) การตีความตามตัวอักษรโดยความผิดฐานการเข้าถึงโดยมิชอบจะถือว่าเป็นความผิดสำเร็จก็เมื่อผ่านการเข้าถึงโดยฝ่าฝืนมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน แต่ต่อจากนั้นหากการติดต่อสื่อสารระหว่างคอมพิวเตอร์ที่ใช้ในการเข้าถึงกับเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อถูกตัดขาดจากกันแล้ว การเข้าถึงในคราวนั้นจึงสิ้นสุดลง หากต่อมาม้าโทรจันหรือสปายแวร์ได้ทำการสำเนาหรือขโมยหรือดักข้อมูล แล้วส่งออกไปยังภายนอก หากจะแปลความว่ามีการติดต่อสื่อสารในขณะที่เครื่องที่ตกเป็นเหยื่อส่งข้อมูลออกไปนั้นเป็นการสื่อสารที่เกิดขึ้นใหม่ก็มิได้หมายความว่าเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายถูกเข้าถึงอีกครั้ง แต่ในทางตรงกันข้ามเครื่องที่ตกเป็นเหยื่อจะเป็นฝ่ายเข้าถึงเครื่องที่ใช้ในการโจมตีในครั้งก่อน กรณีจึงเป็นเรื่องยากที่จะตีความได้ว่าเครื่องที่ตกเป็นเหยื่อเป็นฝ่ายถูกเข้าถึงเพราะไม่มีถ้อยคำใดในกฎหมายฉบับนี้ที่บัญญัติไว้ให้ตีความได้เช่นนั้น (2) การตีความตามเจตนารมณ์ ที่เมื่อพิจารณาจากเหตุผลในการตราพระราชบัญญัตินี้แล้ว ก็ยังไม่อาจแปลได้ว่า กฎหมายดังกล่าวจะมีเจตนารมณ์ในการคุ้มครองถึงการขโมยข้อมูลที่เกิดจากชุดคำสั่งไม่พึงประสงค์ด้วย (3) กรณีเป็นที่สงสัยที่อาจตีความได้เป็นหลายนัย ศาลอาจจะตีความได้เป็น 2 แนวความเห็น คือแนวความเห็นที่หนึ่งศาลจะแปลไปในทางที่เป็นประโยชน์แก่จำเลย

โดยขยายความไปไม่ได้ เพราะศาลไม่มีหน้าที่ช่วยจำเลย มีแต่ลงโทษคนผิด และไม่ลงโทษผู้ไม่ผิด และแนวความเห็นที่สอง ศาลจะต้องตีความให้เป็นประโยชน์แก่ผู้ต้องหา (in dubio pro reo) มากกว่าและไม่มีเหตุผลอันใดที่จะจำกัดการให้ประโยชน์แก่จำเลยในคดีอาญาแต่เฉพาะปัญหาข้อเท็จจริง แม้แต่ในปัญหาข้อกฎหมายโดยเฉพาะในการตีความกฎหมาย ศาลย่อมให้ประโยชน์แห่งความสงสัยแก่จำเลยได้ดุจกัน (4) การเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง (Analogy) อาจนำมาใช้เพื่อเป็นคุณหรือเป็นประโยชน์แก่ผู้กระทำได้ แต่จะนำมาใช้เพื่อเป็นโทษหรือเป็นผลร้ายมิได้ ซึ่งนักนิติศาสตร์ทั้งหลายมีความเห็นเป็นแนวเดียวกัน คือ ศาสตราจารย์เอกูต์ ศาสตราจารย์พระยาอรรถการียพันธ์ และศาสตราจารย์หยุด แสงอุทัย (5) การตีความโดยขยายความ จะนำมาใช้ในทางที่เป็นโทษแก่จำเลยหรือผู้ต้องหาไม่ได้

3.4 ปัญหาความรับผิดในทางอาญา ซึ่งแยกออกได้เป็น

3.4.1 ปัญหาในเรื่ององค์ประกอบภายนอกของความรับผิดทางอาญา โดยมีประเด็นปัญหาว่าการเข้าถึงทางอิเล็กทรอนิกส์หรือทางดิจิทัลที่เกิดจากม้าโทรจันและสปายแวร์จะถือเป็น “การกระทำ” ตามประมวลกฎหมายอาญา หรือไม่ เนื่องจากบทบัญญัติตามมาตรา 59 แห่งประมวลกฎหมายอาญาในตอนต้นที่ว่า “บุคคลจะต้องรับผิดในทางอาญาก็ต่อเมื่อได้กระทำ...” แสดงว่าการกระทำเป็นเงื่อนไขประการแรกของความรับผิดในทางอาญา ทั้งนี้องค์ประกอบภายนอกของความรับผิดทางอาญาในอาชญากรรมพื้นฐาน (Conventional Crimes) นั้น จะพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึก กล่าวคือ การเคลื่อนไหวร่างกายนั้นต้องอยู่ภายใต้บังคับของจิตใจ แต่สำหรับอาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ที่ใช้ชุดคำสั่งไม่ถึงประสงค์เป็นเครื่องมือในกระทำผิดโดยการเข้าถึงนั้น การพิจารณาการกระทำจากการเคลื่อนไหวร่างกายหรือไม่เคลื่อนไหวร่างกายโดยรู้สำนึกเพียงอย่างเดียวนั้นไม่เพียงพอที่จะถือว่าบุคคลนั้นมี “การกระทำ” หรือไม่ แต่จะต้องพิจารณาจากลักษณะหรือผลที่ปรากฏออกมา ซึ่งได้แก่ การทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ ประกอบด้วยเสมอกรณีดังกล่าว จึงก่อให้เกิดปัญหาการตีความในองค์ประกอบภายนอกของความรับผิดทางอาญาที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันและสปายแวร์เป็นอย่างมาก

3.4.2 ปัญหาในเรื่องของความสัมพันธ์ระหว่างการกระทำและผล ที่หากนำมาปรับใช้กับการกระทำความผิดฐานการเข้าถึงโดยมิชอบที่เกิดจากชุดคำสั่งไม่พึงประสงค์ประเภทม้าโทรจันหรือสปายแวร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้วจะเกิดปัญหาในการตีความในความรับผิดเป็นอย่างมาก เพราะความเสียหายหรือผลกระทบที่เกิดจากม้าโทรจันหรือสปายแวร์นั้น มิได้เป็นความเสียหายที่เห็น และปรากฏออกมาได้โดยชัดแจ้งในเชิงกายภาพ อาจเรียกได้ว่าเป็นความเสียหายโดยอ้อม เช่น ความเสียหายอันเนื่องมาจากการถูกเปิดเผยข้อมูลที่เป็นความลับไม่ว่าจะเป็นความลับต่อส่วนตัว หรือความลับในทางการค้า เป็นต้น นอกจากนี้ ยังมีกรณี

"เหตุแทรกแซง" ที่จะต้องนำมาพิจารณาประกอบด้วย ซึ่งจะต้องเป็น "เหตุแทรกแซง" ที่คาดหมายได้จึงจะทำให้ผู้กระทำผิดต้องรับผิดตามทฤษฎีความสัมพันธ์ระหว่างการกระทำและผลได้ ตัวอย่างของเหตุแทรกแซง เช่น ในระหว่างที่มีการส่งข้อมูลออกจากเครื่องที่ตกเป็นเหยื่อออกไปนั้นได้ถูกแฮกเกอร์หรือผู้บุกรุกอีกรายหนึ่งแอบดักข้อมูลนั้นไว้แล้วนำไปสร้างความเสียหายต่อไป หรือกรณีที่เจ้าของเครื่องที่ตกเป็นเหยื่อทราบว่ามีม้าโทรจันหรือสปายแวร์ติดตั้งหรือฝังตัวอยู่ในเครื่องแล้วทำการกำจัด (Clean) ออกไปจากระบบแต่ระหว่างการกำจัดได้เกิดความเสียหายกับข้อมูลที่อยู่ภายในเครื่อง (ซึ่งถ้าหากไม่เกิดจากการถูกเข้าถึงจากม้าโทรจันหรือสปายแวร์จนต้องทำการกำจัด ดังกล่าวแล้วข้อมูลก็คงไม่เกิดความเสียหายขึ้น) เป็นต้น

3.5 ปัญหาปลีกย่อยอื่นๆ ได้แก่ (1) มาตรา 21 อาจถูกใช้เป็นเครื่องมือให้กับพนักงานเจ้าหน้าที่ไปในทางมิชอบได้ (2) ความหมาย "ชุดคำสั่งไม่พึงประสงค์" ที่ว่า "ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้" นั้น ในกรณีที่เป็นบั๊ก (Bug) ของโปรแกรมหรือชุดคำสั่งต่าง ๆ จะจัดให้อยู่ในความหมายดังกล่าวหรือไม่

▣ บทสรุปและข้อเสนอแนะ

จากผลการศึกษาและการวิเคราะห์ปัญหาในการบังคับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 รวมทั้งการศึกษาถึงมาตรการทางกฎหมายของต่างประเทศหรือขององค์การระหว่างประเทศที่เกี่ยวกับชุดคำสั่งไม่พึงประสงค์แล้วพบว่า หลักการที่สำคัญต่าง ๆ ในกฎหมายต่างประเทศหรือขององค์การระหว่างประเทศได้ถูกนำมาบัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของประเทศไทยเกือบทั้งหมดแล้ว เพียงแต่ยังมีข้อบกพร่องในการบัญญัติกฎหมายในส่วนที่เกี่ยวกับความหมายของคำว่า "เข้าถึง (access)" และมาตรการป้องกันการเข้าถึงโดยไม่มีอำนาจ (Illegal access) ที่ยังไม่ชัดเจนเพียงพอ ผู้เขียนจึงขอเสนอแนะวิธีการแก้ไขปัญหาเหล่านั้น ดังนี้

1. การที่จะให้พนักงานเจ้าหน้าที่ทำการตรวจสอบชุดคำสั่งไม่พึงประสงค์ตามมาตรา 21 วรรคหนึ่ง ต้องเป็นกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามกฎหมายนี้และเป็นไปเพื่อประโยชน์ในการสืบสวนและสอบสวนตามที่บัญญัติไว้ในมาตรา 18 ก่อน กล่าวคือ ผู้เขียนจะขอเชื่อมโยงไปที่พฤติการณ์ของผู้ที่จะกระทำการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ตามมาตรา 13 ซึ่งย่อมจะมีการจัดเก็บชุดคำสั่งไม่พึงประสงค์ไว้ในสื่อบันทึกข้อมูลอื่นเพื่อความสะดวกในการจำหน่ายหรือเผยแพร่เสมอ ดังนั้น หากพนักงานเจ้าหน้าที่ไปตรวจพบชุดคำสั่งไม่พึงประสงค์ในสื่อบันทึกข้อมูลอื่นและมีเหตุอันควรเชื่อได้ว่ามีการจำหน่ายหรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์นั้นซึ่งถือเป็นความผิดตามมาตรา 13 แล้ว พนักงานเจ้าหน้าที่ก็จะสามารถอาศัยอำนาจตามมาตรา 18 เพื่อการยื่นคำร้องต่อศาลตามมาตรา 21 วรรคหนึ่งได้ต่อไป

นอกจากนี้ การบัญญัติให้มาตรา 21 วรรคหนึ่ง ให้เชื่อมโยงไปยังมาตรา 18 ก็ยังมีผลดีอีกประการหนึ่งก็คือ หากเป็นกรณีที่พนักงานเจ้าหน้าที่ได้ใช้อำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อ

ได้ว่ามีการกระทำความผิด หรือได้ยึดระบบคอมพิวเตอร์ไว้เพื่อการตรวจสอบ พนักงานเจ้าหน้าที่ก็จะสามารถตรวจสอบได้ว่ามีชุดคำสั่งไม่พึงประสงค์ปะปนอยู่ในระบบคอมพิวเตอร์ด้วยหรือไม่ ซึ่งการกำหนดเช่นนั้น ย่อมจะทำให้เกิดความรอบคอบมากขึ้นและเป็นการป้องกันมิให้พนักงานเจ้าหน้าที่ใช้อำนาจในมาตรา 21 ไปในทางมิชอบได้ เนื่องจากพนักงานเจ้าหน้าที่จะต้องได้รับอนุญาตจากศาลตามมาตรา 19 ก่อนที่จะดำเนินการตามมาตรา 18 (4) (5) (6) (7) และ (8) เสมอ ทั้งนี้ ผู้เขียนขอเสนอให้แก้ไขเพิ่มเติมมาตรา 21 วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นดังนี้

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

2. การกำหนดนิยามคำว่า "เข้าถึง (access)" เพิ่มเติมเข้าไปในมาตรา 3 แห่งพระราชบัญญัติฯ เพื่ออุดช่องว่างของกฎหมายในกรณีที่มีการกระทำความผิดฐานเข้าถึงโดยไม่มีอำนาจจากชุดคำสั่งไม่พึงประสงค์ในทุกรูปแบบ โดยจะเป็นการแก้ไขปัญหาแบบครบวงจร ทั้งในส่วนของกฎหมายสารบัญญัติ (โดยเฉพาะความผิดตามมาตรา 5 และมาตรา 7) และส่วนของกฎหมายวิธีสบัญญัติ กล่าวคือ เพื่อให้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยสามารถบังคับใช้ได้กับการโจมตี หรือภัยคุมคามที่เกิดจากชุดคำสั่งไม่พึงประสงค์ได้ในทุกรูปแบบซึ่งรวมทั้งม้าโทรจันและสปายแวร์ด้วย โดยมีหลักการการบัญญัตินิยามคำว่า "เข้าถึง" ดังนี้

"เข้าถึง" หมายความว่า การกระทำอย่างใดอย่างหนึ่ง ดังต่อไปนี้

(1) การทำให้สามารถเข้าสู่ระบบคอมพิวเตอร์ การสั่งการให้คอมพิวเตอร์ปฏิบัติการ หรือดำเนินการอื่นใดเพื่อให้สามารถสื่อสารข้อมูลกับหน่วยประมวลผล หน่วยบันทึกผลของระบบคอมพิวเตอร์ได้ หรือ

(2) การแสดงผลข้อมูลคอมพิวเตอร์โดยระบบคอมพิวเตอร์ หรือข้อมูลอื่นใดจากระบบคอมพิวเตอร์ หรือ

(3) การทำซ้ำหรือโอนย้ายข้อมูลคอมพิวเตอร์ไปยังหน่วยความจำอื่นในระบบคอมพิวเตอร์นั้นเอง หรืออุปกรณ์สำหรับบันทึกข้อมูลคอมพิวเตอร์อื่น หรือ

(4) การกระทำอื่นใดเพื่อแสวงหาประโยชน์จากข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์

3. การออกกฎกระทรวงเพื่อเพิ่มเติมความหมายของ "ชุดคำสั่งไม่พึงประสงค์" ตามที่พระราชบัญญัติฯ ได้ให้อำนาจไว้ภายใต้หลักการที่สำคัญว่า "ชุดคำสั่งไม่พึงประสงค์นอกจากจะหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้แล้ว ยังให้หมายความรวมถึงชุดคำสั่งที่มีผลทำให้มีการเข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์โดยมิชอบด้วย" ก็จะทำให้ความหมายของชุดคำสั่งไม่พึง

ประสงค์มีความหมายครอบคลุมถึงลักษณะของการกระทำความผิดในประเด็นปัญหาดังกล่าวข้างต้นได้ทุก ๆ ประเด็น ซึ่งจะส่งผลในการป้องกันและปราบปรามการกระทำความผิดดังกล่าวให้มีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

4. การดำเนินการเพื่อแยกแยะชุดคำสั่งไม่พึงประสงค์ที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนด ออกจากชุดคำสั่งไม่พึงประสงค์ที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าว โดยการจัดทำเป็นประกาศของรัฐมนตรีว่าการกระทรวงเทคโนโลยีและการสื่อสาร และประกาศในราชกิจจานุเบกษา เพื่อให้ประชาชนรับรู้เป็นการทั่วกัน ก็จะสามารถเป็นเครื่องมือของพนักงานเจ้าหน้าที่ในการแก้ไขปัญหาในประเด็นดังกล่าวข้างต้นได้เป็นอย่างดีอีกทางหนึ่งด้วย

สำหรับวิธีการที่จะออกประกาศนั้นก็มีปัญหาที่ควรนำมาพิจารณาประกอบด้วยว่า จะทราบได้อย่างไรว่ามีชุดคำสั่งไม่พึงประสงค์ใดออกมาบ้าง ประเด็นนี้ผู้เขียนเห็นว่า ควรมีการสร้างพันธมิตรขึ้นระหว่างภาครัฐและภาคเอกชนที่เป็นผู้ประกอบการในอุตสาหกรรมซอฟท์แวร์ประเภทแอนตี้ไวรัสหรือกำจัดมัลแวร์ชนิดต่าง ๆ ซึ่งส่วนใหญ่แล้วผู้ประกอบการเหล่านี้จะมีผู้รับผิดชอบโดยตรงเพื่อคอยสอดส่องและติดตามเกี่ยวกับชุดคำสั่งไม่พึงประสงค์ที่เกิดขึ้นใหม่ในแต่ละวัน รวมทั้งอาจมีทีมงานสำหรับการวิจัยเกี่ยวกับชุดคำสั่งไม่พึงประสงค์โดยตรงอยู่แล้วด้วย ซึ่งหากสามารถร่วมกันทำงานในรูปแบบของการบูรณาการทั้งภาครัฐและเอกชนเหล่านั้นอย่างเป็นรูปธรรม โดยมีการแต่งตั้งคณะทำงานและกำหนดภารกิจและการติดตามผลไว้อย่างชัดเจน ก็จะทำให้สามารถสร้างระบบหรือกลไกในการแยกแยะชุดคำสั่งไม่พึงประสงค์ได้อย่างสมบูรณ์และมีประสิทธิภาพ และนำไปสู่การออกประกาศรับรองชุดคำสั่งไม่พึงประสงค์ที่มุ่งหมายในการป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวได้สมตามเจตนารมณ์ของกฎหมาย ทั้งนี้สำหรับวิธีการหรือเทคนิคในการออกประกาศรับรองอาจจะรับรองเป็นตระกูลและรุ่นหรือเวอร์ชั่นของซอฟท์แวร์ก็ได้ เช่น ตระกูลของเทรนด์ไมโคร (Trend micro) ตระกูลของนอร์ตั้น (Norton) หรือตระกูลของแม็คเอฟี (McAfee) ซึ่งถือเป็นผู้ประกอบการอุตสาหกรรมซอฟท์แวร์ประเภทแอนตี้ไวรัสหรือกำจัดมัลแวร์รายใหญ่ เป็นต้น

4. สำหรับประเด็นของบั๊กที่ว่า จะถือเป็นชุดคำสั่งไม่พึงประสงค์หรือไม่นั้น ผู้เขียนเห็นว่าต้องนำหลักการของความรับผิดทางอาญาซึ่งเป็นองค์ประกอบภายใน (เจตนา) ในการกระทำความผิดมาประกอบการวินิจฉัยดังกล่าวด้วย กล่าวคือ การเกิดบั๊กในโปรแกรมต่าง ๆ นั้นโดยปกติมักจะเกิดจากความพลั้งเผลอหรือความไม่รอบคอบของโปรแกรมเมอร์หรือผู้เขียนโปรแกรม ซึ่งมิได้มีเจตนาในการทำให้เกิดบั๊กในโปรแกรมที่ตนได้พัฒนาขึ้น ดังนั้นโปรแกรมที่เกิดบั๊กขึ้นโดยปกติจึงมิอาจถือได้ว่าเป็นชุดคำสั่งไม่พึงประสงค์ เว้นแต่จะพิสูจน์ได้ว่าผู้พัฒนาโปรแกรมมีเจตนาให้เกิดบั๊กขึ้น ก็อาจถือได้ว่าโปรแกรมที่เกิดจากเจตนาให้เกิดบั๊กขึ้นนั้นเป็นชุดคำสั่งไม่พึงประสงค์

บรรณานุกรม

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

คำพิพากษาศาลฎีกาที่ 5161/2547.

คำให้สัมภาษณ์ของนายสิทธิชัย โภไคย-อุดม 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

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.)" นิติศาสตรมหาบัณฑิต 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 เขตอุตสาหกรรมซอฟต์แวร์ 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

บันทึกสำนักงานคณะกรรมการกฤษฎีกา ประกอบร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... เรื่องเสร็จที่ 257/2548.

ประมวลกฎหมายแพ่งและพาณิชย์.

ประมวลกฎหมายอาญา.

บล็อก (Blog) ในเว็บไซต์ http://www.BioLawCom.De กฎหมาย ที่ร่างกันแบบไม่เร่งแต่ผ่านกันแบบรีบ ๆ (ตอน 1)" *(ออนไลน์)* ค้นคืนเมื่อวันที่ 24 ธันวาคม 2553

ปริญญา หอมอเนก (2552) The Latest Update Computer Crime Law Implementation Status in Thailand "สรุปความเคลื่อนไหวเกี่ยวกับ พรบ. ว่าด้วยการกระทำผิดฯ หลังมีผลบังคับใช้" "The Latest Update Computer Crime Law Implementation Status in Thailand สรุปความเคลื่อนไหวเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 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) ค้นคืน เมื่อวันที่ 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

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 ห้องพิมานเมฆแกรนด์บอลรูม ชั้น 3 โรงแรม เดอะแกรนด์ กรุงเทพฯ

_____.(2546) แนวทางการจัดทำกฎหมายอาชญากรรมคอมพิวเตอร์ กรุงเทพมหานคร

สราวุธ เบญจกุล (2550) ""E-crime" อาชญากรรมทางอิเล็กทรอนิกส์ มหันตภัยในโลกยุคใหม่" *บทความออนไลน์พิเศษในเว็บไซต์ผู้จัดการออนไลน์ 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

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 Information Law of August 17, 1991.

Cyber Crime Law-Code of Maryland.

Electronic Commerce Act 2000.

Penal Code ประเทศฝรั่งเศส.

Penal Code ประเทศฟินแลนด์.

Penal Code ประเทศสวิตเซอร์แลนด์.

Penal Code ประเทศอิตาลี.