2.2.4 สาเหตุในการกระทำความผิด

ผลกระทบจากพฤติกรรมอาชญากรรมของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบก่อให้เกิดความเสียหายเป็นวงกว้างและคิดเป็นจำนวนมหาศาล รวมทั้งยังส่งผลกระทบต่อความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภัยจากแฮกเกอร์จึงกลายเป็นปัญหาใหญ่สำหรับยุคแห่งเทคโนโลยีสารสนเทศ ด้วยเหตุนี้จึงมักจะมีคำถามตามมาเสมอว่า เหตุใดคนกลุ่มนี้จึงกระทำความผิดในลักษณะเช่นนี้ หรือมีปัจจัยอะไรที่เป็นแรงจูงใจในการกระทำความผิด การหาคำตอบเกี่ยวกับสาเหตุการกระทำความผิด ได้มีการศึกษาประเด็นดังกล่าวนี้หลากหลายแนวทางทั้งในด้านอาชญาวิทยา สังคมวิทยาและจิตวิทยา ผลการศึกษาในแต่ละด้านได้แสดงให้เห็นถึงปัจจัยอันเป็นเหตุแห่งพฤติกรรมอาชญากรรมของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่มีอยู่หลายปัจจัยแตกต่างกันออกไป ดังนี้

การศึกษาของ The German Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA[67]) ในปี ค.ศ.1999 ซึ่งทำการศึกษาเกี่ยวกับพฤติกรรมพื้นฐานทางสังคมและแรงจูงใจในการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบปรากฏผลออกมาว่าแรงจูงใจหลักในการกระทำความผิด ได้แก่ ผลประโยชน์ในทางการเงิน (51.3 %) รองลงมา คือ เพื่อความท้าทาย (33.1%) โดยรายละเอียดของปัจจัยในด้านอื่นๆ มีดังนี้

---

[67] Fötinger, Christian S. and Ziegler, Wolfgang, Understanding a hacker's mind – A psychological insight into the hijacking of identities, <http://www.donau-uni.ac.at/de/studium/fachateilungen/tim/zentren/zpi/DanubeUniversityHackersStudy.pdf>

ตารางที่ 2.6

ตารางแสดงแรงจูงใจในการกระทำความผิด

แรงจูงใจ	จำนวน	คิดเป็นร้อยละ
เหตุผลทางการเงิน	307	51.3
ลองผิดลองถูก (ความท้าทาย)	198	33.1
โอกาสทางเทคนิค	72	12
เหตุผลอื่น	49	8.2
เรื่อยเปื่อย(ไม่แน่นอน)	16	2.7
การยอมรับของกลุ่ม	9	1.5
การแข่งขัน	6	1
การยอมรับในสังคมอินเตอร์เน็ต	4	0.7
ต้องการใช้บริการ	2	0.3
เพื่อสืบหาความลับของผู้อื่น	-	0
เพื่อทำความเสียหายแก่ผู้อื่น	-	0

ที่มา: http://www.donau-uni.ac.at/de/studium/fachateilungen/tim/zentren/zpi/DanubeUniversityHackersStudy.pdf

ข้อมูลเชิงสถิติจากองค์การตำรวจสากล (Interpol[68]) ปรากฏผลว่า แรงจูงใจในการกระทำความผิดของอาชญากรคอมพิวเตอร์มาจากเหตุผลทางการเงิน ร้อยละ 66 เหตุผลทางการเมือง ร้อยละ 17 ความต้องการอยากรู้อยากเห็น ร้อยละ 7 แรงจูงใจแบบพวกอันธพาลต้องการก่อกวน ร้อยละ 5 และต้องการแก้แค้น ร้อยละ 4

Max Kilger[69] ได้นำเสนอโครงสร้างแรงจูงใจในการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ โดยเรียกว่า “MEECES” ซึ่งตัวอักษรแต่ละตัวมีที่มาจากอักษร

---

[68] Vladimir Golubev, “Criminalistics Characteristic of Cybercrimes’ Committers,” <http://www.crime-research.org/library/Golubev_mar.html>

[69] Adam Sutton, David Tait, Shane Mckenzie and Fiora Bavinton, “Internet Crime Prevention,” <http://www.aic.gov.au/conferences/internet/sutton.pdf>

ตัวแรกของปัจจัยแต่ละประการ ได้แก่ เงิน (Money) อัตตา (Ego) ความบันเทิง (Entertainment) มูลเหตุ (Cause) การเข้าสู่ (Entrance) และสถานะ (Status)

ปัจจัยด้านการเงิน นับว่าเป็นแรงจูงใจหลักในปัจจุบันที่ทำให้แนวโน้มในการกระทำความผิดทางคอมพิวเตอร์สูงขึ้นเรื่อย ๆ ทั้งในรูปแบบของการจารกรรมข้อมูลทางอิเล็กทรอนิกส์โดยวัตถุประสงค์ในทางการค้าเพื่อนำไปเสนอขายให้แก่คู่แข่งอีกฝ่ายหนึ่ง หรือเพื่อข่มขู่เจ้าของข้อมูลในการเรียกเอาทรัพย์สินหรือที่เข้าใจในภาษาชาวบ้านว่า “การขโมยไฟล์เพื่อเรียกค่าไถ่” (ransom-ware) การกระทำความผิดในลักษณะเช่นนี้เริ่มปรากฏให้เห็นมากยิ่งขึ้น[70] นอกจากนี้ยังปรากฏว่ามีการว่าจ้างแฮกเกอร์ที่มีฝีมือ โดยผู้ว่าจ้างอาจจะเป็นทั้งนิติบุคคลซึ่งเป็นคู่แข่งทางการค้าหรืออาจเป็นองค์กรอาชญากรรมที่อาศัยแฮกเกอร์เป็นเครื่องมือในการกระทำความผิด[71]

ปัจจัยด้านอัตตา คือ ความต้องการส่วนตัวของผู้กระทำผิดโดยมิได้หวังผลประโยชน์ในทางการเงินแต่อย่างใด ซึ่งได้แก่ ต้องการความรู้ ทำความเข้าใจระบบคอมพิวเตอร์ของเหยื่อ การเจาะระบบคอมพิวเตอร์ตามแนวความคิดของคนกลุ่มนี้จึงเปรียบเสมือนการท้าทายความรู้ความสามารถทางสติปัญญา (intellectual challenge) ดังนั้นยิ่งระบบคอมพิวเตอร์ของเหยื่อมีความซับซ้อนและความมั่นคงมากเท่าใด ก็ยิ่งกระตุ้นแรงจูงใจในด้านอัตตาของกลุ่มแฮกเกอร์ได้มากยิ่งขึ้น[72]

ปัจจัยด้านความบันเทิง คือ แรงจูงใจอันเนื่องมาจากความสนุกที่ได้จากการเจาะระบบคอมพิวเตอร์ของผู้อื่น แฮกเกอร์บางกลุ่มจึงมีความคิดว่าการเจาะระบบคอมพิวเตอร์เป็นเพียงเกมส์อย่างหนึ่งเท่านั้น[73]

ปัจจัยด้านมูลเหตุ ปัจจัยนี้มีอิทธิพลอย่างมากต่อแรงจูงใจของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่มีพื้นฐานทางความคิดเกี่ยวกับการเมือง โดยกลุ่มแฮกเกอร์ในลักษณะนี้จะให้ความสำคัญกับเรื่องชาตินิยมและเสรีภาพการแสดงความคิดเห็น ยกตัวอย่างเช่น กลุ่มต่อต้านอิสราเอล (USG – Unix Security Guards) กลุ่มปากีสถาน (WFD – Worlds Fantabulous

---

[70] “ระวังแรนซอมแวร์เรียกค่าไถ่ไฟล์ 200 เหรียญฯ,” <http://www.arip.co.th/news.php?id=404143>, 25 พฤษภาคม 2548.

[71] Adam Sutton, David Tait, Shane Mckenzie and Fiora Bavinton, *supra note* 69.

[72] *Ibid.*

[73] *Ibid.*

Defacers) กลุ่ม Anti-India Crew (AIC) และกลุ่มต่อต้านแฮกเกอร์สหรัฐอเมริกา (Al-Qaeda Muslim Alliance) เป็นต้น[74]

ปัจจัยด้านการเข้าสู่ คือ แรงจูงใจจากการเข้าสู่สังคมของแฮกเกอร์ ซึ่งรูปแบบปฏิสัมพันธ์ในสังคมออนไลน์ของแฮกเกอร์ไม่เพียงแต่มีการส่งเสริมความรู้และเทคนิคในการเจาะระบบคอมพิวเตอร์โดยแฮกเกอร์รุ่นพี่ซึ่งมีทักษะและประสบการณ์มากกว่าเท่านั้น แต่ยังมีการเอื้อเฟื้อเครื่องมือในการเจาะระบบ (hack tool) ให้แก่แฮกเกอร์มือใหม่ที่สนใจสามารถดาวน์โหลดไปทดลองใช้ได้ฟรีอีกด้วย ดังนั้นในปัจจุบันนี้จึงปรากฏว่ามีแฮกเกอร์หน้าใหม่ก้าวเข้าสู่สังคมใต้ดินนี้เพิ่มขึ้นเรื่อย ๆ[75]

ปัจจัยด้านสถานะ คือ แรงจูงใจในการยกระดับสถานะของตนให้สูงขึ้น เปรียบเสมือนกับพนักงานบริษัทซึ่งต้องการทำผลงานให้โดดเด่นจึงจะมีสิทธิได้เลื่อนขึ้นหรือเลื่อนตำแหน่งในสังคมของแฮกเกอร์ก็เช่นเดียวกัน ชนชั้นของแฮกเกอร์จัดแบ่งตามทักษะความสามารถในการเจาะระบบคอมพิวเตอร์ ดังนั้นผู้ที่มีความรู้และประสบการณ์สูงเท่านั้นจึงจะได้รับการยกย่องนับถือและเป็นที่ยอมรับในสังคมแฮกเกอร์[76]

นอกจากนี้ยังมีการศึกษาสาเหตุแห่งพฤติกรรมอาชญากรรมของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในแนวทางอาชญาวิทยา ซึ่งมีรายละเอียดดังต่อไปนี้

งานวิจัยของ Hollinger (1988)[77] ได้ศึกษาวิจัยโดยวิธีการสัมภาษณ์นักศึกษา 3 คนที่เคยเจาะระบบคอมพิวเตอร์ของมหาวิทยาลัยฟลอริดา และได้ทำลายข้อมูลคอมพิวเตอร์ในระบบ นอกจากนี้ยังได้สัมภาษณ์โดยการสุ่มเลือกนักศึกษาจากคณะวิทยาศาสตร์คอมพิวเตอร์ จำนวน 8 คน ซึ่งจากการศึกษาในครั้งนี้เขาได้ข้อสรุปว่า กลุ่มของเพื่อนมีส่วนในการทำให้บุคคลเข้ามาเกี่ยวข้องกับการกระทำความผิด กล่าวคือ หากบุคคลนั้นมีกลุ่มเพื่อนที่เกี่ยวข้องกับการกระทำความผิดด้านนี้แล้ว อาจเป็นไปได้ที่บุคคลนั้นจะเข้ามาเกี่ยวข้องกับกับการกระทำความผิดในลักษณะนี้ได้ ซึ่งจากข้อสรุปดังกล่าวนี้สอดคล้องกับแนวคิดตามทฤษฎีการคบหาสมาคมที่แตกต่าง (Differential association theory) ของ เอ็ดวิน เอช ซัตเทอร์แลนด์

---

[74] *Ibid.*

[75] *Ibid.*

[76] *Ibid.*

[77] Marc Rogers, *supra note* 35.

งานวิจัยของ Chantler (1996)[78] ศึกษาแฮกเกอร์ในเชิงที่ลึกยิ่งขึ้น กล่าวคือ การศึกษาของเขามีวัตถุประสงค์ในการอธิบายสภาพแวดล้อมของแฮกเกอร์, ลักษณะเฉพาะของคนที่เป็นแฮกเกอร์และตั้งสมมติฐานว่าด้วยบ่อเกิดของแฮกเกอร์ โดยเน้นการศึกษาทางด้านมนุษยศาสตร์เกี่ยวกับธรรมชาติของความเป็นมนุษย์และวัฒนธรรมของแฮกเกอร์ เป็นการศึกษาวิจัยในเชิงคุณภาพ โดยใช้วิธีการสัมภาษณ์ทั้งทางตรงคือ สัมภาษณ์แบบตัวต่อตัว และการสัมภาษณ์ทางอีเมล์ รวมทั้งได้ศึกษาโปรแกรม อุปกรณ์ของเหล่าแฮกเกอร์ด้วย

จำนวนของกลุ่มประชากรในการศึกษาวิจัยนี้ มีจำนวน 164 คน ซึ่งประกอบด้วยแฮกเกอร์จากประเทศออสเตรเลีย (เนื่องจาก Chantler ดำรงตำแหน่งเป็นหัวหน้าของหน่วยรักษาความปลอดภัยระบบคอมพิวเตอร์ของกองทัพบกออสเตรเลีย) นอกจากนี้รวมถึงแฮกเกอร์อื่น ๆ จากทั่วโลก โดยการติดต่อกันทางอีเมล์

เครื่องมือที่ใช้ในการวิจัย ได้แก่ การสังเกตการณ์บนเครือข่ายคอมพิวเตอร์และกระดานข่าว (BBSs : Computer bullentin boards) , แบบสอบถามออนไลน์ , การสัมภาษณ์โดยตรงและโดยทางอีเมล์ โทรศัพท์ แฟกซ์ นอกจากนี้ยังรวมถึงข้อมูลที่ได้จากการสังเกตการณ์ของเขาเกี่ยวกับการติดต่อสื่อสารกันของแฮกเกอร์ ซึ่งเขาได้เก็บรวบรวมข้อมูลไว้ในช่วงระยะเวลากว่า 12 ปี ประเด็นที่น่าสนใจ คือ แบบสอบถามออนไลน์ของเขามีลักษณะเฉพาะโดยจัดทำเป็น 2 ชุด แบบสอบถามชุดหนึ่งพิมพ์อักษร “s” แทนที่โดย “z” ซึ่งเป็นลักษณะเฉพาะที่นิยมกันมากในกลุ่มของแฮกเกอร์ ยกตัวอย่างเช่น คำว่า “softwares” ในกลุ่มของแฮกเกอร์มักจะนิยมใช้คำว่า “warez” ซึ่งจะเป็นที่รู้กันในวงการว่าหมายถึงอุปกรณ์หรือโปรแกรมคอมพิวเตอร์ของกลุ่มแฮกเกอร์ เป็นต้น แบบสอบถามทั้งสองชุดจะประกอบด้วย คำถามปลายเปิด และคำถามปลายปิด[79] 90 ข้อ เกี่ยวกับรายละเอียดที่อยู่,คำถามเกี่ยวกับการเจาะระบบคอมพิวเตอร์, ข้อมูลทางบ้าน, โรงเรียน

---

[78] *Ibid.*

[79] <u>คำถามปลายเปิด (openended questions)</u> คือ คำถามที่เปิดโอกาสให้ตอบอย่างเสรี เป็นคำถามที่ตั้งขึ้นเพื่อให้ผู้ตอบตอบตามสบาย มักใช้กันมากในแบบสัมภาษณ์ เช่น ท่านประกอบอาชีพนี้มาแล้วกี่ปี ท่านสอนวิชานี้มาแล้วกี่ปี เป็นต้น

<u>คำถามปลายปิด (closed questions)</u> คือ คำถามแบบจัดคำตอบให้เลือกตายตัว เป็นคำถามที่มีคำตอบให้เลือกทางใดทางหนึ่ง เช่น เห็นด้วย ไม่เห็นด้วย มาก ปากกลาง น้อย หรือมีคำตอบให้เลือก 5 คำตอบ โดยเลือกตอบได้เพียงหนึ่งคำตอบ เป็นต้น (บุญธรรม จิตต์อนันต์, 2536, น.99.)

หรือมหาวิทยาลัย หรือที่ทำงาน, การใช้คอมพิวเตอร์และกลุ่มแฮกเกอร์ ส่วนบทสัมภาษณ์ ได้สัมภาษณ์แฮกเกอร์ทั้งหมด 23 คน และบุคลากรที่เกี่ยวข้อง เช่น ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยคอมพิวเตอร์ จำนวน 41 คน โดยการสัมภาษณ์นี้จะเน้นไปที่พื้นฐานการศึกษา, ข้อมูลพื้นฐานของแฮกเกอร์ เช่น สภาพแวดล้อมที่บ้าน และที่ทำงาน , ความรู้ , แรงจูงใจ , การดำเนินการเกี่ยวกับข้อมูลในการโจมตีระบบคอมพิวเตอร์, ระดับในการโจมตีระบบคอมพิวเตอร์ และประเภทของแฮกเกอร์[80]

บทสรุปจากงานวิจัยของ Chantler สรุปได้ว่า แฮกเกอร์มีลักษณะจำเพาะหลายประการที่จะนำมาใช้ในการแบ่งแยกประเภทของแฮกเกอร์ เช่น ลักษณะของการเจาะระบบ, ความห้าวหาญ (prowess)ในการเจาะระบบ, ความรู้ , ทักษะ ความสามารถในการเจาะระบบ, แรงจูงใจ และระยะเวลาที่ใช้ในการเจาะระบบ จากการศึกษาของ Chantler เขาสรุปว่า ในสังคมของแฮกเกอร์นั้นประกอบด้วย แฮกเกอร์ในกลุ่มแรกคิดเป็นร้อยละ 30 , ในกลุ่มที่สอง มีจำนวนมากที่สุด คิดเป็นร้อยละ 60 และที่เหลือคือกลุ่มสุดท้ายมีเพียงร้อยละ 10 เท่านั้น[81]

นอกจากนี้เขายังได้สรุปผลการวิจัยนี้ว่า ไม่มีบุคคลใด ๆ ที่มีส่วนสนับสนุนแฮกเกอร์ในการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่น เพราะพวกเขากระทำเนื่องมาจากแรงจูงใจส่วนตัวของเขาเท่านั้น การยืนยันเช่นนี้ นับว่าเป็นการขัดแย้งการงานวิจัยของ Hollinger ดังที่ได้กล่าวไว้ในเบื้องต้น ทั้งนี้ Chantler ยังได้สรุปผลการวิจัยของเขาอีกว่า ไม่มีแนวความคิดในทางทฤษฎีใดในปัจจุบันที่จะนำมาใช้อ้างอิงเป็นพื้นฐานในการอธิบายผลการวิจัยของเขาได้[82]

งานวิจัยของ Dr. Marcus K. Rogers[83] เป็นบุคคลที่มีชื่อเสียงในด้านการศึกษาวิจัยเกี่ยวกับเรื่องอาชญากรคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งนักเจาะระบบ ท่านมีผลงานทางวิชาการที่เกี่ยวกับการศึกษาพฤติกรรมของแฮกเกอร์หลายเรื่อง ผลงานที่น่าสนใจของท่านได้แก่ วิทยานิพนธ์ระดับดุษฎีบัณฑิต มหาวิทยาลัยมานิโทบา (University of Manitoba) ประเทศ แคนาดา ซึ่งศึกษาวิจัยเชิงสำรวจ (Exploratory Study) เกี่ยวกับเรื่อง “การวิเคราะห์พฤติกรรมของอาชญากรคอมพิวเตอร์โดยอาศัยทฤษฎีการเรียนรู้สังคม (Social Learning Theory) และ Moral Disengagement “ นอกจากนี้ยังมีบทความ เรื่อง ทฤษฎีจิตวิทยา ว่าด้วยอาชญากรรมและการ

---

[80] Marc Rogers, *supra note* 35.

[81] *Ibid.*

[82] *Ibid.*

[83] *Ibid.*

เจาะระบบคอมพิวเตอร์ (Psychological Theories of Crime and “ Hacking “)[84] A New Hacker Taxonomy[85] และ Modern-day Robin Hood or Moral Disengagement : Understanding the Justification for Criminal Computer Activity[86]

ในด้านของงานวิจัยท่านศึกษาโดยวิเคราะห์พฤติกรรมของแฮกเกอร์ ภายใต้พื้นฐานทางทฤษฎีการเรียนรู้สังคม ซึ่งประกอบด้วย 2 ทฤษฎีย่อย คือ ทฤษฎีการคบหาสมาคมที่แตกต่างกัน (Differential Association) และทฤษฎีแรงสนับสนุนที่แตกต่าง (Differential Reinforcement) สรุปผลการศึกษาวิจัยของท่าน พบว่า อาชญากรคอมพิวเตอร์มีลักษณะการดำเนินชีวิต กระทำกิจกรรมไม่ต่างจากคนทั่วไป แต่เมื่อเทียบกับอาญากรทั่วไปแล้ว มีความ แตกต่างกันเพียงเล็กน้อย และที่สำคัญคือ พฤติกรรมของอาชญากรคอมพิวเตอร์ได้รับอิทธิพลจากการคบหาสมาคมกับเพื่อนหรือกลุ่มคนที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นไปตามทฤษฎีการคบหาสมาคมที่แตกต่าง, ทฤษฎีการสนับสนุนที่แตกต่าง[87]

เหตุผลที่ท่านนำเอาทฤษฎีการเรียนรู้สังคม การคบหาสมาคมที่แตกต่างและการสนับสนุนที่แตกต่างมาวิเคราะห์ถึงพฤติกรรมของกลุ่มแฮกเกอร์นั้น เพราะว่าในสภาพของความเป็นจริงที่เกิดขึ้นในปัจจุบัน จะเห็นได้ว่าแฮกเกอร์มีปฏิสัมพันธ์กัน มีการติดต่อสื่อสาร แลกเปลี่ยนความรู้ เทคนิคใหม่ ๆ มีการแนะนำให้ความรู้แก่พวกที่กำลังเริ่มฝึกหัด พร้อมทั้งแจกจ่ายอุปกรณ์อันได้แก่ ซอฟต์แวร์หรือโปรแกรมที่ใช้ในการเจาะระบบคอมพิวเตอร์ ให้แก่ผู้ที่สนใจสามารถดาวน์โหลดจากอินเตอร์เน็ตได้โดยไม่ต้องเสียค่าใช้จ่ายใด ๆ การปฏิสัมพันธ์ของเหล่าแฮกเกอร์นั้นมีทั้งที่ปรากฏในรูปแบบทางอิเล็กทรอนิกส์ เช่น กระดานข่าว (Webboard หรือ Forum) หรือห้องสนทนาออนไลน์ (Chat room) เป็นต้น นอกจากนี้ยังมีการรวมตัวกันเป็นกลุ่ม เป็นชมรมของนักเจาะระบบ ยกตัวอย่างเช่น ลัทธิวัวตาย (Cult of the Dead Cow : cDc) หรือ Legion of Doom

---

[84] Marc Rogers, “Psychological Theories of Crime and Hacking - Rogers, 2000”, <http://www.cerias.purdue.edu/homes/mkr/crime.doc>

[85] Marc Rogers, “A New Hacker Taxonomy "REVISED VERSION"- Rogers, 2000”, <http://www.cerias.purdue.edu/homes/mkr/hacker.doc>

[86] Marc Rogers, “Modern-day Robin Hood or Moral Disengagement : Understanding the Justification for Criminal Computer Activity”, <http://citeseer.ist.psu.edu/374648.htm>

[87] Marc Rogers, *supra note* 35.

เป็นต้น นอกจากนี้ยังมีการพบปะพูดคุย จัดประชุมกันเพื่อแลกเปลี่ยนข้อมูล ข่าวสาร ความคิด เทคนิคการเจาะระบบต่าง ๆ ยกตัวอย่างเช่น Defcon ในเมืองลาสเวกัส ประเทศสหรัฐอเมริกา เป็นต้น[88]

2.2.5 รูปแบบการกระทำความผิด

การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจหรือการเจาะระบบคอมพิวเตอร์เป็นรูปแบบที่พื้นฐานที่สุดที่แฮกเกอร์นำมาใช้และยังเป็นพฤติกรรมที่คนทั่วไปรับทราบเรื่องราวเกี่ยวกับพฤติกรรมเหล่านี้ของแฮกเกอร์มากที่สุดเนื่องจากเมื่อพูดถึงข่าวสารเกี่ยวกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบซึ่งเจาะระบบหรือแฮกระบบคอมพิวเตอร์ของเหยื่อ บุคคลทั่ว ๆ ไปย่อมเข้าใจถึงลักษณะของการกระทำเช่นนั้นในทำนองเดียวกัน คือ เป็นการใช้ความรู้และเทคนิคทางคอมพิวเตอร์เพื่อทำให้สามารถเข้าไปควบคุมหรือใช้งานระบบคอมพิวเตอร์ในส่วนที่ตนไม่มีอำนาจในการเข้าถึง กล่าวคือ เป็นส่วนที่ได้มีการกำหนดมาตรการป้องกันบุคคลภายนอกเอาไว้ เช่น กำหนดให้มีการระบุชื่อทะเบียน (user name) และรหัสผ่าน (password) ก่อนใช้งาน เป็นต้น แต่อย่างไรก็ตามในความเป็นจริงแล้ว คำว่า “การเข้าถึง” (access) ในที่นี้อาจมีความหมายรวมถึงการเข้าถึงระบบคอมพิวเตอร์ในระดับกายภาพด้วย ยกตัวอย่างเช่น กรณีที่มีการกำหนดรหัสผ่านเพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้มาซึ่งรหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง ทั้งนี้ไม่จำเป็นต้องเข้าถึงระบบคอมพิวเตอร์ซึ่งอยู่ห่างโดยระยะทางกับผู้กระทำผิดเหมือนดังเช่นความเข้าใจของคนทั่ว ๆ ไป[89]

รูปแบบหรือวิธีการในการเข้าถึงระบบคอมพิวเตอร์โดยปราศจากอำนาจมีอยู่ด้วยกันหลายรูปแบบหลายวิธีการ[90] ทั้งนี้ขึ้นอยู่กับปัจจัยหลายประการ เช่น ทักษะและประสบการณ์ด้าน

---

[88] *Ibid.*

[89] สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์, (กรุงเทพมหานคร: สำนักงานเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, 2546), น.20-22.

[90] รักษ์พงษ์ ฉันท์ภาวัต, “Internet Mafia : การรุกรานครั้งใหม่ของมาเฟียอินเทอร์เน็ต ,” CHIP (มิถุนายน 2549): น.118-123.

คอมพิวเตอร์ของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบคนนั้น ระบบปฏิบัติการที่เหยื่อใช้ การปรับปรุงซ่อมแซมจุดบกพร่องหรือช่องโหว่ของระบบคอมพิวเตอร์ของเหยื่อ และระบบความปลอดภัยทางคอมพิวเตอร์ของเหยื่อ เป็นต้น โดยภาพรวมหลัก ๆ ของการเข้าถึงระบบคอมพิวเตอร์สามารถสรุปขั้นตอนได้ 3 ขั้นตอน ดังนี้

ขั้นตอนแรก การวางแผนและเตรียมพร้อม กระบวนการแรกที่ผู้กระทำผิดจะต้องดำเนินการ คือ การหาข้อมูลที่เกี่ยวกับเหยื่อให้ได้มากที่สุด ซึ่งข้อมูลสำคัญที่มีความจำเป็น ได้แก่

- ระบบปฏิบัติการและเวอร์ชั่นที่เหยื่อใช้
- IP address
- ชื่อโฮสต์
- ชื่อและเบอร์โทรศัพท์

ข้อมูลต่าง ๆ เหล่านี้ผู้กระทำผิดจะมีวิธีการในการได้มาหลากหลายวิธี ยกตัวอย่างเช่น การค้นหาข้อมูลทางอินเทอร์เน็ต โดยเฉพาะอย่างยิ่งอาศัยเครื่องมือในการค้นหา คือ google.com หรืออาจจะหาข้อมูลจากขยะเอกสารที่ทิ้งจากหน่วยงานหรือองค์กรนั้น ซึ่งอาจจะมีข้อมูลที่เป็นประโยชน์หลงเหลืออยู่ หรืออาจจะสอบถามจากพนักงานในองค์กรที่มีหน้าที่รับผิดชอบในส่วนของเครือข่ายคอมพิวเตอร์ขององค์กรนั้นๆ โดยวิธีการล้วงเอาข้อมูลจากบุคคลที่รับผิดชอบงานเช่นนี้เรียกว่า “การแฮกตัวบุคคล” (Social Engineering)[91]

ขั้นตอนที่สอง การสแกนระบบและประเมินช่องโหว่ หลังจากที่ผู้กระทำผิดมีข้อมูลเกี่ยวกับเป้าหมายเพียงพอแล้ว ขั้นตอนต่อไปผู้กระทำผิดจะดำเนินการตรวจสอบการทำงานของระบบคอมพิวเตอร์ของเหยื่อ รวมทั้งช่องโหว่ของระบบคอมพิวเตอร์ที่จะสามารถเข้าถึงได้ โดยในขั้นตอนนี้จำเป็นต้องอาศัยความรู้ทางเทคนิคและประสบการณ์ของผู้กระทำผิดในการดำเนินการ หากเป็นแฮกเกอร์มือใหม่อาจจะต้องเสียเวลาในการตรวจสอบในขั้นตอนนี้เป็นเวลานานมาก แต่หากเป็นแฮกเกอร์ที่มีทักษะสูงจะเสียเวลาในขั้นตอนนี้เพียงเล็กน้อยเท่านั้น

ขั้นตอนสุดท้าย การลงมือเจาะระบบ เมื่อผู้กระทำผิดสามารถค้นพบช่องโหว่ที่ตนสามารถเข้าถึงระบบคอมพิวเตอร์ของเหยื่อได้แล้ว ขั้นตอนสุดท้ายคือการลงมือเจาะระบบ

---

[91] Social Engineering เป็นวิธีการ “หลอกลวงซึ่งหน้า” ทางโทรศัพท์ เพื่อล้วงเอาข้อมูลสำคัญที่เกี่ยวข้องกับความปลอดภัยของระบบคอมพิวเตอร์ การหลอกลวงซึ่งหน้านี้เป็นกลอุบายที่พวกนักคอมพิวเตอร์ใต้ดิน (แฮกเกอร์หรือแครกเกอร์) ใช้เพื่อให้ได้มาซึ่งข้อมูลสำคัญหรือวิธีการเล็ดลอดเข้าไปในระบบ

คอมพิวเตอร์ของเหยื่อ และเมื่อผู้กระทำผิดสามารถเข้าไปควบคุมระบบคอมพิวเตอร์ของเหยื่อได้แล้วจะดำเนินต่อไปอย่างไรนั้น ขึ้นอยู่กับวัตถุประสงค์ของผู้กระทำผิดคนนั้น ๆ ว่ามีเจตนาเช่นไร

2.2.6 ความเสียหายที่เกิดจากการกระทำความผิด

1. ความเสียหายต่อปัจเจกชน

ความเสียหายอันเกิดจากผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่ส่งผลให้เห็นเด่นชัดที่สุด คือ ความเสียหายที่มีต่อเอกชนซึ่งเป็นเจ้าของระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือแม้กระทั่งข้อมูลคอมพิวเตอร์ ผลกระทบที่เกิดกับเอกชนจะมีความรุนแรงมากหรือน้อยขึ้นอยู่กับรูปแบบของการกระทำและเจตนาของผู้กระทำผิด ยกตัวอย่างเช่น การเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยปราศจากอำนาจ ลำพังแต่กระบวนการเข้าถึงระบบคอมพิวเตอร์อาจไม่ส่งผลเสียหายในทางทรัพย์สินต่อเจ้าของระบบคอมพิวเตอร์ เว้นเสียแต่ผู้บุกรุกจะแฝงด้วยเจตนาร้ายโดย อาจจะขโมยข้อมูลที่สำคัญ เปลี่ยนแปลงแก้ไขข้อมูล ทำลายหรือรบกวนการทำงานของระบบคอมพิวเตอร์หรืออาจจะวางแผนโดยแอบเปิดช่องโหว่ในระบบคอมพิวเตอร์ของเหยื่อให้ตนสามารถเข้าถึงในภายหลังได้โดยง่าย นอกจากความเสียหายในทางทรัพย์สินที่ปัจเจกชนจะได้รับจากการกระทำของเหล่าผู้บุกรุกแล้ว ยังมีความเสียหายต่อสิทธิส่วนบุคคล (privacy right) ที่เอกชนได้รับผลกระทบ ยกตัวอย่างเช่น การเจาะระบบคอมพิวเตอร์ของผู้อื่นเพื่อเข้าถึงข้อมูลส่วนบุคคล แอบอ่านจดหมายอิเล็กทรอนิกส์หรืออีเมล์ของเหยื่อ ใช้โปรแกรมสอดแนมที่เรียกว่า “Key logger” ในการสอดส่องพฤติกรรมการใช้งานคอมพิวเตอร์ของเหยื่อ หรือแม้กระทั่งเจาะเข้าไปในระบบคอมพิวเตอร์ของเหยื่อเพื่อควบคุมเว็บแคมของเหยื่อแล้วแอบบันทึกภาพชีวิตส่วนตัวของเหยื่อภายในห้องโดยที่เหยื่อไม่รู้ตัว[92]

2. ความเสียหายต่อสังคม

ความเสียหายที่เกิดขึ้นจากผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบที่มีต่อสังคม มีทั้งที่ปรากฏในสังคมในโลกแห่งความเป็นจริงและสังคมในเครือข่ายคอมพิวเตอร์ ในด้าน

---

[92] กรุง เหลืองมโนธรรม, “การศึกษาประเด็นทางกฎหมายเกี่ยวกับการจัดการความไม่มั่นคงของระบบคอมพิวเตอร์ในสังคมไทย: ศึกษาเฉพาะภัย ไวรัสคอมพิวเตอร์ แฮกเกอร์ และสแปมเมล์,” (สารนิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), น.33.

ของสังคมในโลกแห่งความเป็นจริงภัยของผู้บุกรุกทางอิเล็กทรอนิกส์ได้กลายเป็นนวัตกรรมแห่งอาชญากรรมซึ่งเป็นลู่ทางใหม่ของการประกอบอาชญากรรมและกลายเป็นเครื่องมือที่ทรงประสิทธิภาพที่จะเอื้อประโยชน์ให้กับภาคธุรกิจที่มีเจตนาชั่วร้าย รวมไปถึงองค์กรอาชญากรรมที่จำต้องอาศัยความก้าวหน้าทางเทคโนโลยีในการอำนวยความสะดวกสำหรับการกระทำความผิด ซึ่งไม่เพียงแต่จะทำให้องค์กรเหล่านี้ประกอบอาชญากรรมได้อย่างสะดวกมากยิ่งขึ้นเท่านั้น แต่ยังปรากฏหลักฐานในการพิสูจน์ได้ยากยิ่งขึ้นอีกด้วย เมื่ออัตราอาชญากรรมซึ่งเกิดจากองค์กรเหล่านี้เติบโตขึ้น ย่อมส่งผลกระทบต่อสังคมโดยรวมให้ได้รับความเสียหายในด้านอื่น ๆ ตามมา[93]

ในด้านของสังคมอิเล็กทรอนิกส์หรือสังคมในโลกไซเบอร์ ซึ่งโดยสภาพไม่ต่างไปจากโลกในความเป็นจริง กล่าวคือกลายเป็นสังคมที่ปราศจากความมั่นคงและความปลอดภัย ภัยคุกคามอันเกิดจากฝีมือของเหล่าผู้บุกรุกทางอิเล็กทรอนิกส์กลายเป็นปัญหาใหญ่ในปัจจุบันที่ส่งผลกระทบต่อหน่วยงานหลายฝ่ายทั่วโลก รวมถึงปัญหาจากสังคมของแฮกเกอร์ วัฒนธรรมกลุ่มของแฮกเกอร์ที่ก่อตัวขึ้นและขยายวงกว้างในโลกไซเบอร์ ได้กลายเป็นอีกปัญหาหนึ่งที่จะทำให้ผู้ใช้อินเทอร์เน็ตโดยเฉพาะกลุ่มเด็กวัยรุ่นซึมซับเอาแนวความคิด ทัศนคติของสังคมแฮกเกอร์ และบั่นทอนจริยธรรมในการใช้เทคโนโลยีสารสนเทศ

3. ความเสียหายทางเศรษฐกิจ

เมื่อคอมพิวเตอร์และเทคโนโลยีสารสนเทศเข้ามามีบทบาทในด้านเศรษฐกิจมากยิ่งขึ้นภัยจากผู้บุกรุกทางอิเล็กทรอนิกส์จึงส่งผลกระทบในทางเศรษฐกิจด้วยเช่นเดียวกัน จากการสำรวจในประเทศสหรัฐอเมริกา พบว่ามีความเสียหายที่เกิดขึ้นจากอาชญากรรมคอมพิวเตอร์ ในปี ค.ศ.2005 เป็นจำนวนเงินถึง 130,104,542 เหรียญสหรัฐ[94] การสำรวจความเสียหายจากอาชญากรรมคอมพิวเตอร์ในประเทศออสเตรเลีย ในปี ค.ศ. 2006 เป็นจำนวนเงิน 48,471,208 เหรียญออสเตรเลีย[95] การสำรวจความเสียหายจากอาชญากรรมคอมพิวเตอร์ในเขตปกครองพิเศษฮ่องกง

---

[93] International News, “องค์กรอาชญากรรมบุกไซเบอร์สเปซเพื่อทำเงิน,” COMPUTERWORLD (16-30 กันยายน 2547), น.17-20.

[94] Lawrence A. Gordon, Martin P. Loeb,William Lucyshyn and Robert Richardson, “2005 CSI/FBI computer Crime and Security Survey,” <http://www.usdoj .gov/criminal/cybercrime/FBI2005.pdf>

[95] “Computer Crime & Security Survey,”<http://www.auscert.org.au/images

ในปี ค.ศ. 2004 เป็นจำนวนเงิน 13,136,646 เหรียญฮ่องกง และในปี ค.ศ. 2005 เป็นจำนวนเงิน 7,818,798 เหรียญฮ่องกง[96] จากรายงานความเสียหายดังกล่าวข้างต้น เป็นแต่เพียงสถิติส่วนหนึ่งของความเสียหายที่เกิดขึ้นจริง ทั้งนี้เนื่องจากยังมีความเสียหายบางส่วนที่ยังไม่รับการประเมินซึ่งอาจจะมีสาเหตุมาจากเจตนาของผู้เสียหายที่ไม่ต้องการรายงานความเสียหายของตนให้หน่วยงานนั้น ๆ ทราบเพราะเกรงว่าอาจจะส่งผลกระทบต่อภาพลักษณ์ขององค์กรและความเชื่อมั่นในทางธุรกิจ

นอกจากมูลค่าความเสียหายอันมหาศาลที่เกิดจากการกระทำของเหล่าแฮกแกอร์ดังกล่าวข้างต้นแล้ว พฤติกรรมของผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ยังส่งผลกระทบโดยอ้อมต่อภาคธุรกิจได้เช่นเดียวกัน กล่าวคือ ด้วยความร้ายแรงของผลเสียหายที่เกิดจากฝีมือของเหล่าผู้บุกรุกทางอิเล็กทรอนิกส์ส่งผลให้ภาคธุรกิจจะต้องมีการวางแผนดำเนินการป้องกันความเสี่ยงซึ่งอาจจะเกิดขึ้นกับองค์กรของตนได้ตลอดเวลา โดยวิธีการจัดการความเสี่ยงดังกล่าว ได้แก่ การติดตั้งระบบรักษาความปลอดภัยทางคอมพิวเตอร์ การจ้างผู้ดูแลระบบรักษาความปลอดภัยทางคอมพิวเตอร์และการทำประกันภัยคอมพิวเตอร์ ซึ่งการดำเนินการดังกล่าวนี้จำเป็นต้องเสียค่าใช้จ่ายเป็นจำนวนมาก[97] และนอกจากนี้ยังส่งผลกระทบต่อความเชื่อมั่นทางการค้าทั้งภายในและภายนอกประเทศ เมื่อนักธุรกิจนักลงทุนไม่มีความเชื่อมั่นในการดำเนินธุรกิจโดยเฉพาะอย่างยิ่งภาคธุรกิจที่มีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ทั้งนี้เนื่องจากเกรงว่าภัยจากผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์จะส่งผลต่อการดำเนินธุรกิจของตนและการดำเนินการเพื่อป้องกันความเสี่ยงดังกล่าวไม่คุ้มค่า อาจทำให้นักธุรกิจนักลงทุนหันไปทำธุรกิจในที่ที่มีความ ปลอดภัยสูงกว่า ซึ่งอาจทำให้ประเทศไทยต้องสูญเสียโอกาสในทางเศรษฐกิจไปเป็นจำนวนมหาศาล

4. <u>ความเสียหายต่อความมั่นคงของประเทศ</u>

เนื่องจากกลุ่มแฮกเกอร์บางกลุ่มมีทัศนคติและแนวคิดฝักใฝ่ในด้านชาตินิยม พฤติกรรมบางอย่างอาจแสดงออกมาโดยมีแรงจูงใจในทางการเมืองร่วมด้วย ยกตัวอย่างเช่น การ

/ACCSS2006.pdf>

[96] “InfoSec - Information Security & Prevention of Computer Related Crime,” < http://www.infosec.gov.hk/engtext/general/crc/statistics_3.htm >

[97] “Computer Security Spending Statistics,” < http://www.securitystats.com /sspend.html >

โจมตีเว็บไซต์ของหน่วยงานราชการโดยเข้าไปแก้ไขข้อมูลในหน้าเว็บไซต์เพื่อโจมตีรัฐบาลหรือผู้นำประเทศ ซึ่งที่ผ่านมาปรากฏว่ามีการโจมตีเว็บไซต์แล้วแก้ไขหน้าเว็บไซต์ (Website defacement) โดยมีวัตถุประสงค์ในทางการเมืองเป็นจำนวนมาก[98] สำหรับประเทศไทยมีการโจมตีของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในลักษณะเช่นนี้ด้วยเช่นกัน อาทิเช่น กรณีการโจมตีเว็บไซต์ของกระทรวงวิทยาศาสตร์และเทคโนโลยีสารสนเทศ โดยนำรูปควายไปแทนที่รูปของผู้บริหาร[99] และกรณีการเปลี่ยนที่อยู่เว็บไซต์ที่นายกรัฐมนตรีไปประชุมด้านเศรษฐกิจโดยเปลี่ยนไปเป็นที่อยู่ของเว็บไซต์ลามกอนาจาร[100] นอกจากนี้ยังพบว่ามีการโจมตีทางการเมืองโดยอาศัยผู้บุกรุกทางอิเล็กทรอนิกส์เป็นเครื่องมือในการโจมตีฝ่ายตรงข้าม ดังเช่นในกรณีเว็บไซต์ของผู้จัดการออนไลน์ซึ่งถูกผู้กระทำผิดโจมตีโดยวิธีการที่เรียกว่า “Denial of Service” (DoS) ส่งผลให้เว็บไซต์ดังกล่าวล่มไม่สามารถให้บริการได้[101]

นอกเหนือจากการอาศัยแฮกเกอร์เป็นเครื่องมือในทางการเมืองแล้ว สำหรับกลุ่มผู้ก่อการร้ายยังอาศัยแฮกเกอร์เป็นอาวุธอันทรงประสิทธิภาพในการล้วงความลับ ก่อวินาศกรรมระบบคอมพิวเตอร์ของฝ่ายตรงข้าม รวมทั้งหลบเลี่ยงการถูกตรวจจับจากเจ้าหน้าที่ของรัฐซึ่งกำลังสอดส่องพฤติกรรมของตน[102]

---

[98] Zone-H : Attackers Special Top List, <http://www.zone-h.org/component/option,com_topatt/ Itemid,49/>

[99] “มือดีลองของแฮกเว็บไอซีทีโพสต์รูปควายเย้ยผู้บริหาร,” <http://www.police.go.th/policenews/show.php?news_id=269&cat=CRC1&id=135>, 20 พฤษภาคม 2546.

[100] “แฮกเกอร์เปลี่ยนลิงค์เว็บที่ “ทักษิณ”ไปประชุมเศรษฐกิจไปเว็บโป๊,” <http://www.police.go.th/policenews/show.php?news_id=77&cat=CRC1&id=64>, 11 พฤศจิกายน 2545.

[101] “มือมืดยิง “รีเควสต์เทียม” ถล่มเว็บผู้จัดการหนัก!!,” <http://www.manager.co.th/Cyberbiz/ViewNews.aspx?NewsID=9490000116887>, 15 กันยายน 2549.

[102] “มุสลิมหัวรุนแรงใช้อีเมล์เข้ารหัสติดต่อวางแผนโจมตีสหรัฐ,” <http://www.police.go.th/policenews/show.php?news_id=83&cat=CRC1&id=69>, 11 พฤศจิกายน 2545.

เช่นเดียวกับการโจมตีทางการทหาร ในปัจจุบันได้เปลี่ยนรูปแบบมาสู่การทำสงครามทางสารสนเทศ[103] กล่าวคือ เป็นการโจมตีระบบคอมพิวเตอร์ทางการทหารของฝ่ายตรงข้าม ทั้งนี้เพื่อให้ได้มาซึ่งข้อมูลด้านกำลังพล อาวุธยุทโธปกรณ์ สถานที่ตั้งทางทหาร ยุทธวิธีการรบหรือสภาพภูมิศาสตร์ เนื่องจากข้อมูลเหล่านี้เป็นข้อมูลที่สำคัญในการทำสงคราม ทั้งนี้รวมถึงการโจมตีทำลายระบบคอมพิวเตอร์หรือระบบสาธารณูปโภคเพื่อขัดขวางมิให้มีการติดต่อสื่อสาร หรือตัดกำลังเสบียงของฝ่ายตรงข้ามเพื่อสร้างความวุ่นวายและทำลายขวัญกำลังใจของกำลังทหารฝ่ายตรงข้าม[104] ตัวอย่างเช่น ในปี ค.ศ.1998 หน่วยข่าวกรองของอดีตสหภาพโซเวียต (KGB) ได้เจาะระบบการป้องกันเข้ามาล้วงเอาความลับทางทหารของประเทศสหรัฐอเมริกา ซึ่งได้แก่ ข้อมูลทางการทหาร ข้อมูลนิวเคลียร์ ข้อมูลเกี่ยวกับอาวุธเชื้อโรคและอาวุธเคมี และข้อมูลเกี่ยวกับการสร้างระบบรักษาความปลอดภัยในห้วงอวกาศ ทำให้ประเทศสหรัฐอเมริกาได้รับความเสียหายอย่างมหาศาล[105]

2.3 มาตรการป้องกันและปราบปรามผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

เนื่องจากผลกระทบที่เกิดจากผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบนั้นได้ก่อให้เกิดความเสียหายในหลาย ๆ ด้าน สร้างความสูญเสียในทางการเงินคิดเป็นจำนวนมหาศาล และส่งผลกระทบต่อสังคมเป็นวงกว้าง หลายฝ่ายทั้งในส่วนของภาครัฐและภาคเอกชนต่างหาแนวทางหรือมาตการในการจัดการปัญหาเหล่านี้ทั้งในมิติของการป้องกันหรือยับยั้งไม่ให้ปัญหาเกิดขึ้นและมิติของการจัดการปราบปรามลงโทษผู้ก่อปัญหา หรือผู้ที่กระทำความผิดสำเร็จแล้ว โดยมาตรการ ต่าง ๆ สามารถจำแนกออกเป็น 3 มาตรการหลัก คือ มาตรการทางเทคโนโลยี มาตรการด้านบุคคล และมาตรการทางกฎหมาย

---

[103] Bruce Berkowitz, โฉมใหม่ของสงครามยุคดิจิตอล THE NEW FACE OF WAR, แปลโดย สรศักดิ์ สุบงกช (กรุงเทพมหานคร: Animate Group, 2547), น.41-42.

[104] บุญเรือง หอมขจร, “CYBER-THREAT/ ภัยคุกคามคอมพิวเตอร์มหันตภัยตัวใหม่ที่ไม่ควรมองข้าม,” นาวิกาธิปัตย์สาร (กุมภาพันธ์-พฤษภาคม 2544): น.60-69.

[105] ณรงค์ชัย นิมิตบุญอนันต์, Computer Security for E-Commerce, (กรุงเทพมหานคร: Sum System Company Limited, 2542), น.3.

2.3.1 มาตรการทางเทคโนโลยี

มาตรการป้องกันทางเทคโนโลยีเป็นแนวทางหนึ่งในการจัดการปัญหาความปลอดภัยทางคอมพิวเตอร์ ซึ่งปัจจุบันองค์กรไม่ว่าจะเป็นภาครัฐหรือเอกชนต่างนำเอาแนวทางนี้มาปรับใช้กับระบบคอมพิวเตอร์ของตน ทั้งนี้เพื่อเป็นมาตรการในการป้องกันภัยจากผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ รวมทั้งช่วยลดความเสี่ยงอันเกิดจากความเสียหายที่จะเกิดขึ้นกับระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ขององค์กรนั้น ๆ โดยมาตรการทางเทคโนโลยีที่นำมาใช้ในการป้องกันและรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ สามารถจำแนกออกเป็น 3 รูปแบบดังต่อไปนี้

(ก) ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ คือ อุปกรณ์ซึ่งใช้ติดตั้งในเครือข่ายคอมพิวเตอร์ เพื่อรักษาความปลอดภัยโดยการกลั่นกรองข้อมูลที่เข้าออกเครือข่าย โดยมักจะติดตั้งไฟร์วอลล์ระหว่างเครือข่ายภายในกับเครือข่ายภายนอก (อินเทอร์เน็ต) ซึ่งคำว่า “ไฟร์วอลล์” นั้นหมายถึงการปกป้องความปลอดภัยในตัวเอง เสมือนกำแพงกันไฟซึ่งทนความร้อนและใช้ป้องกันไม่ให้ไฟลุกลามจากบริเวณหนึ่งไปยังบริเวณอื่น ในมุมมองด้านความปลอดภัยสำหรับคอมพิวเตอร์นั้น อินเทอร์เน็ตเป็นแหล่งที่เต็มไปด้วยภัยอันตรายแอบแฝงอยู่ ดังนั้นไฟร์วอลล์จึงเป็นทางออกหนึ่งในการปกป้องเครือข่ายภายในให้มีความปลอดภัย[106]

(ข) ระบบตรวจจับการบุกรุก (IDS : Intrusion Detection System)

ระบบตรวจจับการบุกรุก คือ เครื่องมือที่มีความสามารถตรวจพบความผิดปกติของระบบคอมพิวเตอร์ที่เกิดขึ้นเนื่องมาจากการบุกรุกของบุคคลหรือระบบอัตโนมัติใดที่อาจสร้างความเสียหายแก่ระบบ ซึ่งการบุกรุกดังกล่าวอาจถูกตรวจจับได้ด้วยวิธีต่างกัน หากจำแนกระบบตรวจจับการบุกรุกตามวิธีการวิเคราะห์การบุกรุกจะจัดแบ่งได้เป็น 2 ประเภท คือ ระบบตรวจจับการ

---

[106] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, รายงานผลการศึกษา : นโยบายความปลอดภัยของเครือข่ายสำหรับประเทศไทย, (กรุงเทพมหานคร: ฝ่ายพัฒนานโยบายและกฎหมาย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547), น. 37.

บุกรุกผ่านจุดอ่อน (Misuse Detection) และระบบตรวจจับพฤติกรรมที่ผิดปกติ (Anomaly Detection)[107]

สาเหตุที่ต้องมีระบบตรวจจับการบุกรุกเนื่องจากความปลอดภัยของคอมพิวเตอร์นั้นเป็นเรื่องยากในการมองภาพที่ชัดเจนว่าอะไรที่จะบ่งบอกได้ว่าการใช้งานคอมพิวเตอร์มีความปลอดภัย ความปลอดภัยของคอมพิวเตอร์จึงเป็นสิ่งที่จับต้องไม่ได้และเป็นเรื่องยากต่อการวัด การติดตั้งไฟร์วอลล์ให้กับระบบเครือข่ายคอมพิวเตอร์แต่เพียงอย่างเดียวก็ไม่อาจสร้างความปลอดภัยให้แก่เครือข่ายคอมพิวเตอร์ได้ ทั้งนี้เนื่องจากการติดตั้งไฟร์วอลล์ให้กับระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนการสร้างรั้วหรือกำแพงเพื่อตรวจสอบบุคคลที่จะบุกรุกเข้ามาในสถานที่ที่รักษาความปลอดภัย แต่หากมีบุคคลใดซึ่งไม่หวังดีสามารถปีนรั้วหรือกำแพงเข้ามาได้แล้ว การรักษาความปลอดภัยโดยใช้รั้วหรือกำแพงก็หมดความหมาย ดังนั้นการใช้ระบบตรวจจับการบุกรุกจึงเป็นการเพิ่มความปลอดภัยให้แก่ระบบคอมพิวเตอร์อีกชั้นหนึ่งต่อจากการป้องกันโดยใช้ไฟร์วอลล์[108]

ตัวอย่างระบบตรวจจับการบุกรุกในปัจจุบัน ได้แก่

- Snort
- CMDS
- NetRanger
- VCC/TripwireTM
- INTOUCH NSA (Network Security Agent)
- POLYCENTER Security Intrusion Detector

อย่างไรก็ตามแม้ว่าเทคโนโลยีด้านความปลอดภัยของระบบสารสนเทศในการตรวจจับการบุกรุกและการป้องกันระบบคอมพิวเตอร์โดยใช้ไฟร์วอลล์จะพัฒนาก้าวหน้าไปอย่างรวดเร็ว แต่ก็มิอาจป้องกันภัยร้ายจากผู้ไม่ประสงค์ดีต่อระบบคอมพิวเตอร์ได้อย่างสมบูรณ์แบบ ทั้งนี้เนื่องจากเทคโนโลยีด้านความปลอดภัยเหล่านี้มักจะพัฒนาตามหลังเทคนิคใหม่ ๆ ของบรรดาผู้บุกรุกอยู่ก้าวหนึ่งเสมอ[109] และด้วยเหตุนี้เอง เพื่อที่จะสามารถเรียนรู้เทคนิคของผู้บุกรุกและสามารถรับมือ

---

[107] *เพิ่งอ้าง,* น.29.

[108] ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย, “ระบบตรวจจับการบุกรุก (Intrusion Detection System),” <http://www.thaicert.nectec.or.th/paper/ids/ids.php>.

[109] ไตรรัตน์ พุทธรักษา, “รู้จักกับ Honeypot,” <http://www.thaicert.nectec.or.th/

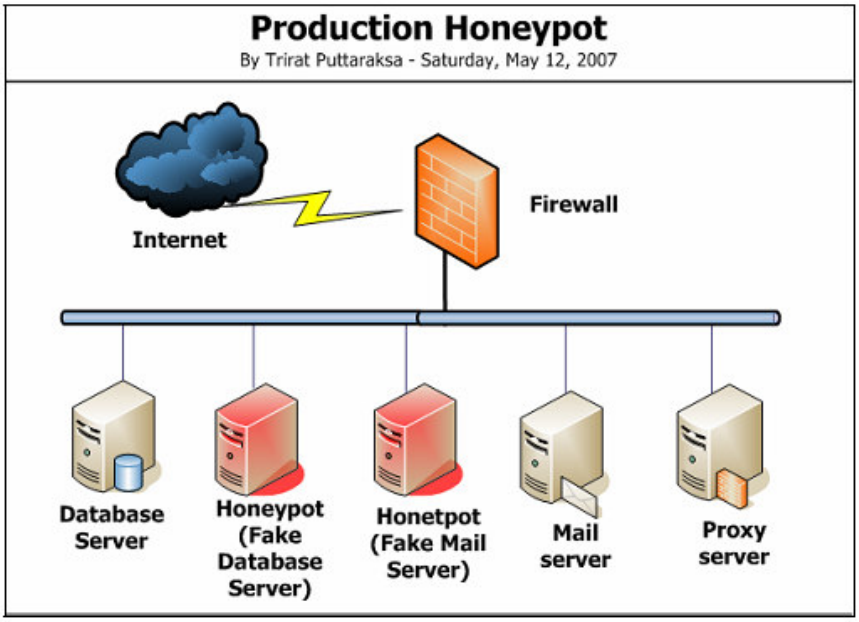
กับการโจมตีรูปแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ หน่วยงานที่ทำการวิจัยด้านความปลอดภัยระบบสารสนเทศจึงได้มีแนวความคิดที่จะนำเอาเทคโนโลยีรูปแบบใหม่มาประยุกต์ใช้ โดยเรียกเทคโนโลยีนี้ว่า “Honeypot”[110]

Honeypot คือ คอมพิวเตอร์หรือกลุ่มของคอมพิวเตอร์ที่ถูกติดตั้งไว้สำหรับลวงให้ผู้บุกรุกทำการโจมตี เพื่อเรียนรู้เทคนิคที่ผู้บุกรุกใช้ และใช้ความรู้เหล่านั้นหาทางป้องกันการโจมตีใหม่ ๆ ที่เกิดขึ้น นอกจากนี้ honeypot ยังสามารถใช้ลดความเสี่ยงของเซิร์ฟเวอร์ในระบบที่อาจถูกโจมตีหรือใช้เป็นระบบตรวจจับการบุกรุกได้อีกทางหนึ่งด้วย

Honeypot ถูกนำมาใช้งาน 2 รูปแบบ คือ การนำไปใช้ในงานวิจัย (Research Honeypot) และการนำไปใช้เพื่อลดความเสี่ยงจากการถูกโจมตี (Production Honeypot)

ภาพที่ 2.2

การนำ Honeypot ไปใช้เพื่อลดความเสี่ยงจากการถูกโจมตี



ที่มา : http://www.thaicert.nectec.or.th/paper/ids/Honeypot.pdf

อย่างไรก็ตามการนำเอาเทคโนโลยี Honeypot มาใช้ในด้านความปลอดภัยทางคอมพิวเตอร์ยังมีข้อควรระวังบางประการ ประการแรก การใช้งาน Honeypot อาจเป็นการเพิ่ม

---

paper/ids/Honeypot.pdf>, 15 พฤษภาคม 2550.

[110] *เพิ่งอ้าง.*

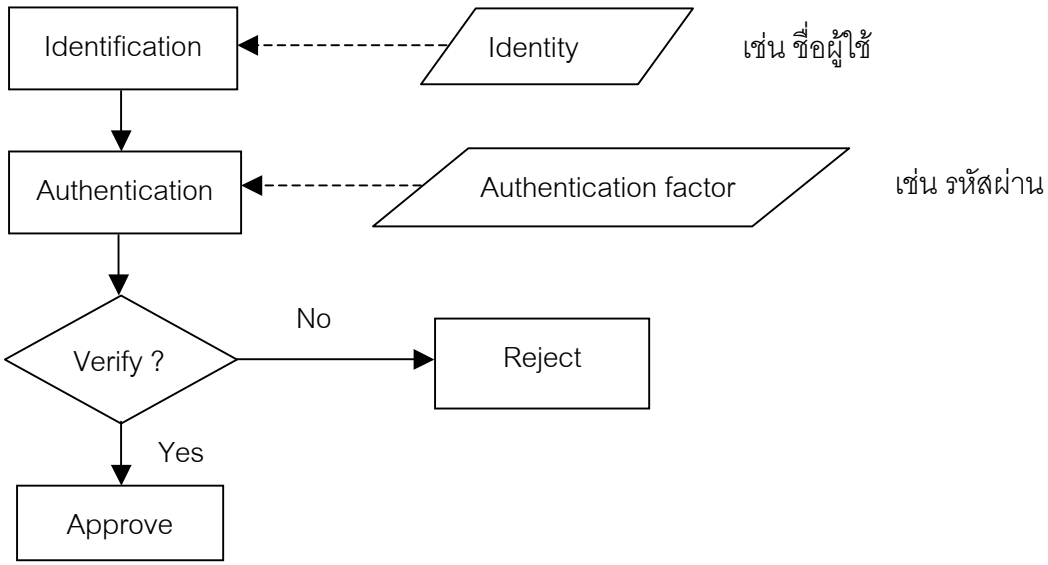
ความเสี่ยงให้กับระบบคอมพิวเตอร์ขององค์กรได้ หากผู้บุกรุกอาศัย Honeypot เป็นเครื่องมือในการโจมตีเครือข่ายอื่น อีกประการหนึ่ง เนื่องจากในบางประเทศนั้นการใช้งาน Honeypot เข้าข่ายการกระทำผิดกฎหมาย เพราะเป็นการลวงหลอกให้ผู้อื่นกระทำความผิด และเป็นการละเมิดสิทธิส่วนบุคคล[111]

(ค) การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้าง ในทางปฏิบัติแบ่งออกเป็น 2 ขั้นตอน ได้แก่ การระบุตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (username) และการพิสูจน์ตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น การใช้รหัสผ่าน (password)

ภาพที่ 2.3

แผนผังแสดงกระบวนการพิสูจน์ตัวตน[112]



---

[111] *เพิ่งอ้าง.*

[112] สิริพร จิตต์เจริญธรรม เสาวภา ปานจันทร์ และเลอศักดิ์ ลิ้มวิวัฒน์กุล, “ความรู้เบื้องต้นเกี่ยวกับการพิสูจน์ตัวตน,” <http://www.thaicert/or.th/paper/authen/authentication_guide.php>, 11 มิถุนายน 2547.

จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้ คือ การระบุตัวตน (Identification) และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน (Authentication) หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้ว ถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้อง ผู้ใช้จะถูกปฏิเสธจากระบบ ในปัจจุบันรูปแบบของการพิสูจน์ตัวตนมีปรากฏหลากหลายรูปแบบ ได้แก่ การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Password) การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN) การพิสูนตัวตนโดยใช้ Password Authenticators หรือ Tokens การพิสูจน์ตัวตนโดยใช้ลักษณะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits) การพิสูจน์ตัวตนโดยการเข้ารหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password : OTP) การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-Key Cryptography) และการพิสูจน์ตัวตนโดยใช้การถามตอบ (Zero-knowledge proofs)[113]

2.3.2 มาตรการด้านบุคคล

นอกเหนือจากมาตรการทางเทคโนโลยีในการป้องกันความปลอดภัยทางคอมพิวเตอร์ มาตรการในด้านบุคคลก็เป็นอีกแนวทางหนึ่งที่จะมีส่วนช่วยเสริมให้มาตรการป้องกันภัยทางคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้เนื่องจากในสภาพความเป็นจริง พบว่า ปัจจัยส่วนหนึ่งที่ทำให้เกิดการกระทำความผิดทางคอมพิวเตอร์มาจากพฤติกรรมในการใช้งานคอมพิวเตอร์ที่ไม่ถูกต้องเหมาะสม แม้ว่าระบบคอมพิวเตอร์จะมีการวางมาตรการทางเทคโนโลยีที่ทันสมัยมากเพียงใดก็ตาม หากผู้ใช้งานหรือบุคลากรขององค์กรนั้น ๆ ขาดความรู้ความเข้าใจในการเตรียมพร้อมรับมือกับภัยทางคอมพิวเตอร์ มาตรการในการป้องกันความปลอดภัยทางคอมพิวเตอร์ก็ไม่อาจประสบผลสำเร็จได้ หรือไม่อาจจัดการกับปัญหาดังกล่าวได้อย่างมีประสิทธิภาพ ดังนั้นมาตรการป้องกันทางเทคโนโลยีควรที่จะนำมาปรับใช้ควบคู่ไปกับการให้ความรู้ความเข้าใจแก่บุคลากรหรือผู้ใช้งานคอมพิวเตอร์เกี่ยวกับแนวทางความปลอดภัยในการใช้งานคอมพิวเตอร์อย่างถูกต้อง

---

[113] *เพิ่งอ้าง.*

เหมาะสม เพื่อป้องกันภัยหรือช่วยลดความเสี่ยงจากความเสียหายอันเกิดขึ้นจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์[114]

ตัวอย่างที่เห็นได้ชัดในกรณีช่องโหว่ของมาตรการด้านบุคคล คือ การกำหนดรหัสผ่าน (password) ที่เปราะบางและคาดเดาได้ง่าย โดยธรรมชาติของมนุษย์ที่ชอบความสะดวกสบายจนทำให้มองข้ามความปลอดภัยในการกำหนดรหัสผ่าน ด้วยเหตุผลที่ต้องการให้สามารถจำรหัสผ่านได้ง่าย จึงเลือกที่จะใช้คำที่คุ้นเคยหรือคำใกล้ตัว เช่น ชื่อจริง ชื่อเล่น นามสกุล ชื่อสัตว์เลี้ยง เบอร์โทรศัพท์ หรือแม้แต่วันเดือนปีเกิด เป็นต้น[115] นอกจากนี้การกำหนดรหัสผ่านที่สั้นเกินไปอาจเพิ่มความเสี่ยงที่จะทำให้ผู้ไม่หวังดีสามารถถอดรหัสได้ง่ายยิ่งขึ้น ซึ่งจากการศึกษาพบว่า รหัสลับ 1 ตัวอักษร ใช้เวลาในการถอดรหัสเพียง 6 นาที ถ้ามีความยาว 2 ตัวอักษร ใช้เวลาในการถอดรหัส 4 ชั่วโมง ความยาว 3 ตัวอักษร จะใช้เวลาในการถอดรหัส 5 วัน ดังนั้นยิ่งรหัสผ่านมีความยาวมากเพียงใด ยิ่งช่วยลดความเสี่ยงในการถูกถอดรหัสได้มากขึ้นเท่านั้น[116]

2.3.3 มาตรการทางกฎหมาย

มาตรการทางด้านกฎหมายโดยวิธีการออกกฎหมายเพื่อป้องปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นมาตรการที่สำคัญอีกประการหนึ่งนอกเหนือจากมาตรการป้องกันทางเทคโนโลยีและมาตรการด้านบุคคลในการรักษาความปลอดภัยทางคอมพิวเตอร์ หลาย ๆ ประเทศได้มีการบัญญัติหรือตรากฎหมายเพื่อกำหนดฐานความผิดและโทษทางอาญาสำหรับการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ไว้ตามลักษณะ รูปแบบของการกระทำความผิด ซึ่งกฎหมายที่เกี่ยวข้องกับผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบเพื่อป้องปรามอาชญากรรมคอมพิวเตอร์ของประเทศต่าง ๆ มักมีสาระสำคัญโดยรวมร่วมกันคือ การกำหนดการกระทำต่อระบบคอมพิวเตอร์ที่ถือเป็นความผิดทางอาญาและบทลงโทษต่อการกระทำดังกล่าว เช่น การเข้า

---

[114] SME SECURITY, “รับมือกับภัยคุกคามระบบสำหรับองค์กรขนาดกลางและขนาดย่อม,” COMPUTERWORLD (16-31 มกราคม 2549): น.25-26.

[115] เควิน บีเวอร์, *อ้างแล้ว เชิงอรรถที่* 25, น.81-82.

[116] พรชัย ยิ่งปัญญาโชค, “โจรกรรมในยุคเทคโนโลยีสารสนเทศ HACKER or CRACKER ?,” วารสารนักบริหาร 18, 2(เมษายน – มิถุนายน 2541): น.46-47.

ถึงคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต (illegal access) และการใช้อุปกรณ์ในทางที่ผิด (misuse of device) เช่น การผลิต จำหน่าย เผยแพร่ฮาร์ดแวร์ ซอฟต์แวร์ รหัสผ่านที่ใช้ในการกระทำความผิดดังกล่าวข้างต้น นอกจากนี้ยังมีการบัญญัติรายละเอียดในส่วนของขั้นตอนทางกฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ที่เกี่ยวข้องในการดำเนินการรวบรวมพยานหลักฐานที่เกี่ยวข้องอย่างรวดเร็ว เช่น การกำหนดให้มีการเก็บรักษาข้อมูลในคอมพิวเตอร์ และข้อมูลที่ติดต่อสื่อสารกันทางเครือข่ายที่อยู่ในข่ายต้องสงสัยว่าเกี่ยวข้องกับการก่ออาชญากรรม การเรียกขอข้อมูลจากผู้ครอบครองหรือผู้ให้บริการโทรคมนาคมต่าง ๆ ที่เกี่ยวข้อง การตรวจ ค้นและยึด (search and seizure) ข้อมูลในระบบคอมพิวเตอร์ หรือการกระทำอื่น ๆ เพื่อป้องกันการเปลี่ยนแปลงแก้ไขพยานหลักฐาน และการดักจับและรวบรวมข้อมูลสื่อสารโดยเจ้าหน้าที่ หรือการสั่งให้ผู้ให้บริการโทรคมนาคมต่าง ๆ ให้ความร่วมมือในการดังกล่าว[117]

2.4 แนวคิดในการลงโทษผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

รูปแบบการกระทำความผิดของผู้บุกรุกทางอิเล็กทรอนิกส์เป็นมิติใหม่ของภัยสังคมในยุคเทคโนโลยีสารสนเทศซึ่งการกระทำดังกล่าวอาจส่งผลกระทบที่รุนแรงและกว้างขวางกว่าการกระทำความผิดแบบดั้งเดิมซึ่งได้กระทำในโลกแห่งความเป็นจริง ด้วยเหตุนี้มาตรการทางกฎหมายโดยเฉพาะอย่างยิ่งการลงโทษ รวมถึงมาตรการบังคับทางอาญาอื่น ๆ ซึ่งต้องนำมาปรับใช้กับผู้กระทำผิดในลักษณะเช่นนี้จึงอาจมีปัญหาในการกำหนดโทษแก่ผู้กระทำผิดว่าควรจะลงโทษผู้กระทำผิดอย่างไร กล่าวคือ ควรจะลงโทษจำนวนเท่าใด และด้วยวิธีการใด[118]

จากงานเสวนาทางวิชาการ เรื่อง “ทัศนคติของหน่วยงานในกระบวนการยุติธรรมไทยต่อปัญหาความมั่นคงบนอินเทอร์เน็ต” ในวันที่ 28 มิถุนายน พ.ศ. 2545 ณ ห้องประชุมศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ มีการถกประเด็นปัญหาใน

---

[117] “ความปลอดภัยของเครือข่ายอินเทอร์เน็ต,” <http://www.police.go.th/pisc/cybercrime.pdf>

[118] มณฑนา สีตสุวรรณ, “การกระทำของมนุษย์บนอินเตอร์เน็ตที่เป็นภัยต่อมนุษย์ในสังคมไทย : แนวคิดในการจัดการ,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546), น.54.

เรื่องจำนวนโทษที่จะลงแก่ผู้กระทำความผิดบนอินเทอร์เน็ต โดยมีความเห็นที่แตกต่างกัน 2 ฝ่าย คือ

ฝ่ายแรก[119] เห็นว่า เนื่องจากการกระทำความผิดบนอินเทอร์เน็ตส่งผลกระทบที่รุนแรงกว่าการกระทำในโลกแห่งความเป็นจริง ดังนั้นผู้กระทำผิดบนอินเทอร์เน็ตจึงสมควรที่จะต้องได้รับโทษที่หนักกว่าผู้กระทำผิดทั่วไป

ฝ่ายที่สอง[120] เห็นว่า การลงโทษหนักนั้นไม่ก่อให้เกิดประโยชน์ใด ๆ ดังนั้นควรพิจารณาจากวัตถุประสงค์ของการลงโทษมากกว่า ในกรณีที่ผู้กระทำผิดมิได้มีจิตใจเป็นอาชญากรโดยกำเนิด การลงโทษเบาก็สามารถทำให้ผู้กระทำผิดเข็ดหลาบได้เช่นกัน

ส่วนประเด็นในเรื่องรูปแบบหรือวิธีการลงโทษผู้กระทำผิดบนอินเทอร์เน็ตจะต้องสอดคล้องกับวัตถุประสงค์ของการลงโทษ เช่น การลงโทษจำคุก อาจไม่ก่อให้เกิดประโยชน์ใด ๆ การให้ทำงานบริการสังคมหรือเพื่อสาธารณประโยชน์น่าจะเหมาะสมกว่า เป็นต้น[121] แต่อย่างไรก็ตามวิธีการลงโทษย่อมแตกต่างกันออกไปตามมุมมองของความยุติธรรมทางอาญา ซึ่งสามารถสรุปได้เป็น 6 มุมมองใหญ่[122] คือ

---

[119] ได้แก่ รศ.ดร. พันธุ์ทิพย์ กาญจนะจิตรา สายสุนทร และคุณสกนธ์ ปั้นตะ จากงานเสวนาทางวิชาการ เรื่อง “ทัศนคติของหน่วยงานในกระบวนการยุติธรรมไทยต่อปัญหาความมั่นคงบนอินเทอร์เน็ต” ในวันที่ 28 มิถุนายน พ.ศ. 2545 ณ ห้องประชุมศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

[120] ได้แก่ พ.ต.อ. ญาณพล ยั่งยืน, รศ.ณรงค์ ใจหาญ และคุณจุมพล ภิญโญสินวัฒน์ จากงานเสวนาทางวิชาการ เรื่อง “ทัศนคติของหน่วยงานในกระบวนการยุติธรรมไทยต่อปัญหาความมั่นคงบนอินเทอร์เน็ต” ในวันที่ 28 มิถุนายน พ.ศ. 2545 ณ ห้องประชุมศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

[121] พ.ต.อ. ญาณพล ยั่งยืน,งานเสวนาทางวิชาการ เรื่อง “ทัศนคติของหน่วยงานในกระบวนการยุติธรรมไทยต่อปัญหาความมั่นคงบนอินเทอร์เน็ต” ในวันที่ 28 มิถุนายน พ.ศ. 2545 ณ ห้องประชุมศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

[122] ชาญเชาว์ ไชยานุกิจ, งานเสวนาทางวิชาการ เรื่อง “ทัศนคติของหน่วยงานในกระบวนการยุติธรรมไทยต่อปัญหาความมั่นคงบนอินเทอร์เน็ต” ในวันที่ 28 มิถุนายน พ.ศ. 2545 ณ ห้องประชุมศาสตราจารย์จิตติ ติงศภัทิย์ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

มุมมองที่ 1 Crime Control Perspective มองว่าความยุติธรรมทางอาญาต้องลงโทษให้หนัก ต้องบังคับใช้กฎหมายอย่างมีประสิทธิภาพ ต้องเป็นการข่มขู่ไม่ให้ใครกระทำความผิดอีก และต้องปกป้องอย่างเต็มที่ จำกัดสิทธิผู้ต้องหาได้แล้วต้องตัดโอกาสผู้กระทำผิดให้อยู่ในคุก

มุมมองที่ 2 Rehabilitation Perspective มองความยุติธรรมทางอาญาที่สาเหตุโดย มุมมองนี้จะต้องเร่งบำบัดแก้ไขคนทำผิด ต้องมุ่งเน้นตัวผู้กระทำผิดให้มาก หาสาเหตุการกระทำผิดนั้นให้ได้ รวมถึงปรับปรุงแก้ไขให้คำปรึกษาและเยียวยามิให้กระทำผิดซ้ำอีก

มุมมองที่ 3 Due Process Perspective เน้นเรื่องกระบวนการทางด้านกฎหมาย การหาพยานหลักฐานต้องปราศจากข้อสงสัย ภาระการพิสูจน์ต้องตกอยู่กับอัยการโจทก์อย่างเต็มที่ เมื่อไม่มีประจักษ์พยานแล้วจะลงโทษจำเลยไม่ได้ นอกจากนี้ยังเน้นกระบวนการและเข้มงวดในเรื่องของการรับฟังพยานมาก

มุมมองที่ 4 Non-Intervention Perspective มุมมองนี้พยายามลดมลทินของผู้กระทำผิด โดยมองที่เป้าหมายว่าไม่อยากให้คนที่กระทำผิดแล้วกลับมาทำผิดใหม่ จะต้องเบี่ยงเบนคดีออกมา อย่าให้ผู้กระทำผิดมีมลทินติดตัว กล่าวคือ อย่าปล่อยให้ผู้กระทำผิดเดินเข้าไปในกระบวนการยุติธรรมจนสุดทาง ต้องเอาเขาออกมาแล้วบำบัด การลงโทษแบบนอกระบบหมายความว่า โทษอาญา ได้แก่ ประหารชีวิต จำคุก กักขัง ปรับ ริบทรัพย์สิน ไม่ควรนำมาใช้ทั้งหมด

มุมมองที่ 5 Justice Model Perspective มุมมองนี้ต้องการลดดุลพินิจของศาล ดุลพินิจของคนในกระบวนการยุติธรรมออกไปให้หมด เน้นความเสมอภาค กล่าวคือ เมื่อกระทำผิดแบบใดก็สมควรได้รับโทษเช่นนั้นเหมือนกันโดยไม่มีการลดหย่อนผ่อนโทษ ไม่มีการนำความประพฤติในอดีตของผู้กระทำความผิด หรือปัจจัยว่าผู้เสียหายได้รับความเสียหายจากการกระทำความผิดนั้นหรือไม่มาพิจารณาในการลดโทษ และไม่สนใจว่าต่อไปในอนาคตผู้กระทำผิดจะกลับไปกระทำความผิดซ้ำหรือไม่

มุมมองที่ 6 Restorative Justice Perspective มุมมองนี้เน้นสังคมที่สมานฉันท์ เน้นการกลับคืนสู่สังคม รวมถึงเน้นจิตสำนึกของผู้กระทำผิดให้รู้สึกสำนึกผิดในกระทำของตน และในด้านของผู้เสียหายจะต้องได้รับการเยียวยาอย่างพอใจ ต้องมีการเจรจาไกล่เกลี่ยกันระหว่างผู้กระทำผิด ผู้เสียหายและเจ้าหน้าที่เพื่อให้เกิดความสมานฉันท์ขึ้นในสังคม

สำหรับแนวความคิดในการลงโทษการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในปัจจุบันยังไม่มีหลักเกณฑ์ที่ปรากฏชัดเจน แน่นอนตายตัว หลายประเทศได้มีการประกาศใช้บังคับกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์เพื่อเอาผิดและลง

โทษผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ที่มีพฤติกรรมฝ่าฝืนกฎหมายและในบางประเทศ อาทิ ประเทศอังกฤษ มาเลเซียและสิงคโปร์ ต่างกำหนดกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ไว้อย่างเข้มงวด แต่ก็ไม่อาจลดอัตราการเกิดอาชญากรรมทางคอมพิวเตอร์ในประเทศเหล่านี้ได้[123] ซึ่งข้อเท็จจริงดังกล่าวแสดงให้เห็นว่าการลงโทษหนักสำหรับกรณีนี้มิอาจส่งผลในเชิงยับยั้งพฤติกรรมการกระทำความผิดได้อย่างแท้จริง[124]

เหตุผลประการหนึ่งที่ทำให้มาตรการลงโทษผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบไม่อาจบรรลุวัตถุประสงค์ในการควบคุมอาชญากรรมทางคอมพิวเตอร์ได้ คือ การขาดความรู้ความเข้าใจเกี่ยวกับพฤติกรรม สังคมและวัฒนธรรมของกลุ่มแฮกเกอร์ ตัวอย่างที่เห็นได้ชัดในกรณีนี้ คือ การดำเนินคดีและลงโทษอย่างหนักสำหรับการกระทำความผิดของแฮกเกอร์ประเภท script – kiddies หรือพวกแฮกเกอร์มือใหม่ โดยผู้กระทำผิดในจำพวก script – kiddies นี้เป็นกลุ่มที่มีระดับทักษะในด้านคอมพิวเตอร์ต่ำกว่ากลุ่มอื่น ๆ ซึ่งส่วนใหญ่มักจะปรากฏในรูปของเยาวชนหรือวัยรุ่นที่มีความอยากรู้อยากเห็น ต้องการแสดงอำนาจของตนและต้องการเป็นที่ยอมรับในสังคมด้วยความอ่อนด้อยในด้านวุฒิภาวะจึงทำให้พวกเขากระทำการบางสิ่งบางอย่างไปโดยมิได้คำนึงถึงความเสียหายที่จะตามมาจากการกระทำนั้น ๆ ของตน[125] ผู้กระทำผิดในกลุ่มนี้จะเป็นเป้าหมายหลักที่เจ้าหน้าที่ของรัฐจะสามารถแกะรอยหาตัวผู้กระทำผิดมาดำเนินคดีได้ง่าย เนื่องจากมีระดับทักษะด้านคอมพิวเตอร์ที่น้อยมากจึงทำให้ปรากฏมีหลักฐานในการกระทำความผิดได้ แต่อย่างไรก็ตามการลงโทษสถานหนักกับผู้กระทำความผิดในกลุ่มนี้ย่อมไม่ก่อให้เกิดประโยชน์ ในทางตรงกันข้ามอาจส่งผลกระทบระยะยาวทั้งต่อตัวผู้กระทำผิดและต่อการควบคุมปัญหาอาชญากรรมคอมพิวเตอร์ในอนาคตได้

การศึกษาพฤติกรรมของผู้กระทำผิดเป็นสิ่งที่สำคัญในการทำความเข้าใจบริบทของอาชญากรรมนั้น ๆ ได้เป็นอย่างดี จากการศึกษาเกี่ยวกับจิตวิทยาของแฮกเกอร์ มีผู้ให้ความเห็นว่าโทษทางอาญาอาจจะไม่สามารถยับยั้งพฤติกรรมการกระทำความผิดของแฮกเกอร์ได้[126] Indira

---

[123] Reid Skibell, “CYBERCRIMES & MISDEMEANORS : A REEVALUATION OF THE COMPUTER FRAUD AND ABUSE ACT,” <www.law.berkeley.edu/journals/btlj/articles/vol18/Skibell.pdf>

[124] *Ibid.*

[125] *Ibid.*

[126] *Ibid.*

Carr และ Katherine Williams[127] ให้เหตุผลว่า พวกแฮกเกอร์ถูกดึงดูดโดยความท้าทายทางจิตใจให้เอาชนะระบบความปลอดภัยในคอมพิวเตอร์ ด้วยเหตุนี้พวกเขาจึงแสดงออกซึ่งความสามารถและศักยภาพของตนโดยการเจาะระบบคอมพิวเตอร์ ทั้งนี้ได้กระทำไปโดยไม่ได้คำนึงถึงผลประโยชน์อื่นใดและไม่ได้คำนึงถึงผลลัพธ์ที่จะตามมา Paul Taylor[128] ซึ่งศึกษาเกี่ยวกับสังคมของแฮกเกอร์ พบว่าแฮกเกอร์มีแรงจูงใจที่หลากหลายแต่ไม่ปรากฏว่ามีแรงจูงใจเพื่อผลประโยชน์จากการเจาะระบบคอมพิวเตอร์ ซึ่งโดยทั่วไปแล้วแฮกเกอร์จะกระทำไปโดยมีแรงจูงใจในเชิงบวก (benign motivation) เช่น ความอยากรู้อยากเห็น ต้องการแสดงออกซึ่งอำนาจและต้องการเป็นที่ยอมรับในสังคม[129] มีเพียงกลุ่มที่ลักษณะตรงข้ามที่เรียกว่า cracker เท่านั้น ที่กระทำไปด้วยหวังผลประโยชน์จากการเจาะระบบคอมพิวเตอร์ แต่อย่างไรก็ตามพวก cracker มักจะมีลักษณะพื้นฐานที่ไม่ต่างไปจากแฮกเกอร์ กล่าวคือ ถูกดึงดูดด้วยความท้าทายทางจิตใจให้เจาะระบบคอมพิวเตอร์เช่นเดียวกัน โดยมีผลประโยชน์ที่ได้จากการเจาะระบบคอมพิวเตอร์เป็นเพียงผลพลอยได้ที่ตามมา[130]

นอกจากนี้แฮกเกอร์และแครกเกอร์หลายคนยังได้อธิบายถึงแรงดึงดูดภายในจิตใจซึ่งมิอาจควบคุมได้ส่งผลให้พวกเขาต้องเจาะระบบคอมพิวเตอร์ โดยเรียกลักษณะเช่นนี้ว่า “อาการติดการเจาะระบบคอมพิวเตอร์” (hacking addiction)[131] ประเด็นนี้แม้ว่าในปัจจุบันยังไม่มีข้อมูลทาง

---

[127] Indira Carr and Katherine S. Williams, “A Step Too Far in Controlling Computer?: The Singapore Computer Misuse (Amendment) Act 1998,” INT’L J.L. & INFO. TECH. 48,56(2000), cited by Reid Skibell, “CYBERCRIMES & MISDEMEANORS : A REEVALUATION OF THE COMPUTER FRAUD AND ABUSE ACT,” <www.law.berkeley.edu/journals/btlj/articles/vol18/Skibell.pdf>

[128] Paul A. Taylor, “HACKERS: CRIME IN THE DIGITAL SUBLIME,” (1999), cited by Reid Skibell, “CYBERCRIMES & MISDEMEANORS : A REEVALUATION OF THE COMPUTER FRAUD AND ABUSE ACT,” <www.law.berkeley.edu/journals/btlj/articles/vol18/Skibell.pdf>

[129] Reid Skibell, *supra note* 124.

[130] *Ibid.*

[131] Reid Skibell, *supra note* 124; see also Majid Yar, “Computer Hacking: Just Another Case of Juvenile Delinquency?,” The Haward Journal Vol.44 No.4

วิชาการที่จะสามารถนำมาอ้างอิงยืนยันได้ แต่ก็นำมาสู่ประเด็นข้อโต้แย้งของฝ่ายจำเลยในการพิจารณาคดีผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบในต่างประเทศ 2 คดี คือ คดีแรก เป็นคดีชื่อดังในประเทศสหรัฐอเมริกา คือ นายเควิน มิตนิก แต่ในคดีนี้ศาลไม่ได้รับฟังประเด็นข้อโต้แย้งดังกล่าวเนื่องจากไม่มีเหตุผลเพียงพอที่จะรับฟังได้[132] ส่วนในคดีที่สอง เป็นคดีผู้กระทำผิด ชื่อ Paul Bedworth ในประเทศอังกฤษ คดีนี้เป็นคดีแรกภายใต้กฎหมาย Computer Misuse Act ที่ศาลยอมรับฟังข้อโต้แย้งของฝ่ายจำเลยในประเด็นนี้ โดยจำเลยในคดีนี้มีอาการติดการเจาะระบบคอมพิวเตอร์ถึงขนาดขังตัวเองอยู่แต่ในห้อง และนั่งอยู่แต่หน้าจอคอมพิวเตอร์ทั้งวันจนกระทั่งอ่อนเพลียหมดแรงลง[133] คดีของ Paul Bedworth เป็นตัวอย่างหนึ่งที่ทำให้เห็นว่า การกระทำความผิดของอาชญากรคอมพิวเตอร์โดยพื้นฐานมิได้มาจากแรงจูงใจที่เกี่ยวข้องกับผลประโยชน์ในทางทรัพย์สิน ฉะนั้นสำหรับกรณีเช่นนี้โทษในทางอาญาอาจไม่ส่งผลในทางข่มขู่ยับยั้งพฤติกรรมของผู้กระทำผิดได้ตามวัตถุประสงค์ในการลงโทษ

แต่อย่างไรก็ตาม ในปัจจุบันคดีอาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งในส่วนที่เป็นการกระทำความผิดของผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบได้เข้าสู่กระบวนพิจารณาของศาลในต่างประเทศซึ่งมีกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์บังคับใช้แล้วหลายคดี ศาลในแต่ละประเทศได้นำเอามาตรการลงโทษต่าง ๆ มาใช้กับอาชญากรทางคอมพิวเตอร์เหล่านี้ในหลากหลายรูปแบบ ทั้งในรูปแบบของโทษทางอาญา เช่น ประหารชีวิต จำคุก ปรับและริบทรัพย์สิน รวมไปจนถึงคำสั่งศาลอันเป็นมาตรการบังคับทางอาญาในการควบคุมพฤติกรรมของจำเลยมิให้มีโอกาสในการกระทำความผิดซ้ำ ทั้งยังเป็นการป้องกันความปลอดภัยให้แก่สังคมหลังจากที่ปล่อยตัวผู้กระทำผิดออกมาแล้ว อย่างไรก็ดีมาตรการต่าง ๆ ของศาลที่นำมาใช้กับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบันก่อให้เกิดคำถามตามมาถึงความเหมาะสมและสอดคล้องกับวัตถุประสงค์ในการลงโทษอย่างแท้จริงหรือไม่ เพียงใด ซึ่งประเด็นปัญหาดังกล่าวจะได้ศึกษาในลำดับต่อไป

(September, 2005), pp. 392-393.

[132] *Ibid.*

[133] *Ibid.*