บทที่ 2

ความทั่วไปเกี่ยวกับมาตรการบังคับทางอาญาและผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

2.1 มาตรการบังคับทางอาญา

2.1.1 แนวความคิดพื้นฐานเกี่ยวกับการลงโทษ

เนื่องด้วยมนุษย์เป็นสัตว์สังคมซึ่งรวมกลุ่มกันภายใต้กฎเกณฑ์ของกลุ่มที่ทุกคนในสังคมจะต้องปฏิบัติตาม ทั้งนี้เพื่อรักษาไว้ซึ่งความสงบเรียบร้อยของกลุ่มของสังคมนั้น เมื่อใดก็ตามที่บุคคลในสังคมมีการกระทำที่ฝ่าฝืนละเมิดกฎเกณฑ์อันเป็นระเบียบแห่งสังคม สังคมจะต้องหาวิธีการอย่างใดอย่างหนึ่งในการจัดการกับคนที่ฝ่าฝืนกฎเกณฑ์ดังกล่าว เหตุผลที่ต้องกระทำการเช่นนี้เนื่องมาจากหากสังคมไม่ดำเนินการอย่างใดอย่างหนึ่งกับบุคคลซึ่งฝ่าฝืนกฎเกณฑ์ของสังคมย่อมแสดงให้เห็นว่าสังคมยอมรับการกระทำความผิดดังกล่าว[1] ดังนั้นการลงโทษผู้ที่ฝ่าฝืนกฎเกณฑ์แห่งสังคมจึงเป็นรูปแบบอย่างหนึ่งของการอยู่ร่วมกันในสังคมมนุษย์โดยมีวิวัฒนาการมาตั้งแต่สมัยโบราณจนถึงปัจจุบัน ในยุคสมัยโบราณการปฏิบัติต่อผู้กระทำความผิดหรือประพฤติฝ่าฝืนกฎเกณฑ์ของสังคมมีลักษณะเป็นการเรียกร้องความยุติธรรมตามธรรมชาติในลักษณะตาต่อตา ฟันต่อฟัน (an eye for an eye, a tooth for a tooth) การลงโทษในยุคสมัยนั้นจึงเป็นการลงโทษเพื่อชดใช้ความเสียหายให้แก่ผู้เสียหาย[2] เป็นการลงโทษในแนวคิดด้านการแก้แค้นตอบแทน (revenge) กล่าวคือ เป็นการให้ลงโทษกันเองระหว่างผู้ประทุษร้ายกับผู้ถูกประทุษร้าย ซึ่งการลงโทษในลักษณะเช่นนี้มักจะทวีความรุนแรงขึ้นโดยต่างฝ่ายต่างมีญาติพี่น้องเพื่อนฝูงเข้าช่วย การ

---

[1] นัทธี จิตสว่าง, หลักทัณฑวิทยา, พิมพ์ครั้งที่ 3(กรุงเทพมหานคร: มูลนิธิพิบูลสงคราม กรมราชทัณฑ์, 2545), น.23.

[2] สหธน รัตนไพจิตร, “ความประสงค์ของการลงโทษอาญา : ศึกษาเฉพาะประเทศไทยสมัยใช้กฎหมายลักษณะอาญาและประมวลกฎหมายอาญา,” (วิทยานิพนธ์มหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2527), น.22-23.

แก้แค้นส่วนตัวจึงกลายเป็นความพยาบาทกันระหว่างตระกูลหรือระหว่างหมู่คณะซึ่งยืดเยื้อไม่รู้จักจบสิ้นและขยายขอบเขตกว้างใหญ่ออกไปทุกที จนในที่สุดอาจก่อให้เกิดความไม่สงบสุขหรือกระทบกระเทือนต่อความเป็นปึกแผ่นมั่นคงของสังคมนั้นได้[3]

ในยุคต่อมาจึงเริ่มมีคนกลาง (Impartial third party) เข้ามาเพื่อยุติความขัดแย้งกันทั้งสองฝ่าย โดยคนกลางจะเข้ามาทำหน้าที่ในการไกล่เกลี่ยตัดสินให้ฝ่ายถูกประทุษร้ายหรือฝ่ายที่ได้รับความเสียหายมากกว่าให้ได้รับการชดเชยทดแทนความเสียหายนั้น คนกลางซึ่งเข้ามาช่วยในการสมานรอยร้ายของทั้งสองฝ่ายและยังช่วยรักษาความสงบเรียบร้อยให้เกิดในสังคมจึงเป็นแนวทางที่ได้รับความนิยมมากยิ่งขึ้นและกลายเป็นหน้าที่ที่คล้ายกับเป็นตุลาการในการรักษาความสงบเรียบร้อยในสังคม[4] ต่อมาเมื่อสังคมมนุษย์มีความเจริญมากขึ้น มีการปกครองที่เป็นระเบียบเรียบร้อยมากขึ้น มีหัวหน้าหรือกษัตริย์ผู้ปกครองสังคมให้ได้รับความร่มเย็นเป็นสุข หัวหน้าของสังคมหรือกษัตริย์จึงได้รับอำนาจในการลงโทษผู้กระทำผิดต่อสังคมอย่างเป็นทางการและเป็นสถาบันขึ้น การลงโทษผู้กระทำผิดแทนที่จะเป็นการกระทำโดยคนหมู่มากลงมือกับผู้กระทำความผิดเสียเอง ก็เปลี่ยนเป็นการฟ้องร้องกล่าวโทษให้ผู้ที่มีอำนาจทำการตัดสิน เมื่อมีสถาบันซึ่งสังคมมอบอำนาจให้เช่นนี้แล้ว สมาชิกของสังคมก็จำต้องให้ความเคารพจะละเมิดมิได้ ต่อมาการกระทำหรือการประทุษร้ายกันระหว่างเอกชนนอกจากจะเป็นการทำลายความสงบเรียบร้อยแล้ว ยังเป็นการขาดความเคารพหรือละเมิดอำนาจของหัวหน้าหรือกษัตริย์ด้วย จึงถือเป็นความผิดต่อสถาบันของสังคม ซึ่งเท่ากับเป็นการกระทำความผิดต่อสังคมโดยส่วนรวมด้วย ฉะนั้นสังคมในยุคสมัยนี้จึงเข้ามามีบทบาทในการลงโทษผู้กระทำความผิดทำผิดต่อสังคม[5] ส่วนการที่สังคมจะดำเนินการลงโทษผู้กระทำความผิดอย่างไรนั้น ขึ้นอยู่กับความเชื่อของสังคมในแต่ละยุคแต่ละสมัย ทั้งนี้ขึ้นอยู่กับสาเหตุของการกระทำความผิดและเหตุผลซึ่งต้องจัดการหรือปฏิบัติต่อผู้กระทำผิดซึ่งเปลี่ยนไปตามยุคตามสมัยและตามสภาพการณ์ของแต่ละยุค กล่าวคือ สังคมในแต่ละยุคสมัยจะมีความมุ่งหมายในการลงโทษผู้กระทำความผิดเน้นไปในแนวทางแห่งวัตถุประสงค์และวิธีการที่จะปฏิบัติต่อผู้กระทำผิดที่แตกต่างกันออกไป[6] ยกตัวอย่างเช่น ในช่วงก่อนคริสตศตวรรษที่ 18 วัตถุประสงค์ใน

---

[3] ชาย เสวิกุล, อาชญาวิทยาและทัณฑวิทยา, (กรุงเทพมหานคร : โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2517), น.176-177.

[4] *เพิ่งอ้าง*, น.177.

[5] นัทธี จิตสว่าง, *อ้างแล้ว* เชิงอรรถที่ 1, น.21.

[6] ชาย เสวิกุล, *อ้างแล้ว* เชิงอรรถที่ 3, น.177-178.

การลงโทษจะมุ่งเน้นในด้านการแก้แค้นทดแทน ไกล่เกลี่ยชดเชยและการลงโทษเพื่อให้เข็ดหลาบหวาดกลัวไม่กล้ากระทำความผิดอีก แต่ต่อมานับตั้งแต่ปลายคริสตศตวรรษที่ 18 แนวความคิดในเรื่องการลงโทษเริ่มมีความตื่นตัวในด้านมนุษยธรรมมากยิ่งขึ้น โดยมีความพยายามในการปรับแนวคิดและวิธีการในการลงโทษให้เหมาะสมและมีมนุษยธรรมมากยิ่งขึ้น ซึ่งรายละเอียดเกี่ยวกับวัตถุประสงค์ในการลงโทษผู้เขียนจะอธิบายในลำดับถัดไป

2.1.2 วัตถุประสงค์ในการลงโทษ

การลงโทษผู้กระทำความผิดในสังคมแต่ละยุคแต่ละสมัยมีจุดเน้นในด้านวัตถุประสงค์และวิธีการปฏิบัติต่อผู้กระทำผิดหรือการลงโทษผู้กระทำผิดที่แตกต่างกันไป ดังที่ได้กล่าวไว้แล้วในเบื้องต้น ซึ่งการลงโทษผู้กระทำผิดไม่ว่าโดยรูปแบบหรือวิธีการอย่างหนึ่งอย่างใดอาจจะส่งผลสอดคล้องตามความมุ่งหมายหรือวัตถุประสงค์ของการลงโทษได้หลายประการร่วมกัน โดยวัตถุประสงค์ในการลงโทษในแต่ละรูปแบบมีรายละเอียดดังนี้

1. การลงโทษเพื่อแก้แค้นทดแทน[7]

การลงโทษเพื่อแก้แค้นทดแทน (retribution) ถือได้ว่าเป็นจุดประสงค์ในการลงโทษที่เก่าแก่มีมาตั้งแต่ในยุคที่มนุษย์ยังเป็นสังคมป่าเถื่อน การลงโทษในลักษณะเช่นนี้เป็นการลงโทษที่มีวัตถุประสงค์เพื่อตอบสนองความรู้สึกของผู้เสียหายรวมถึงคนในสังคมซึ่งต้องการจะเห็นคนที่ทำร้ายผู้อื่นได้รับผลร้ายด้วยเช่นกัน นอกจากนี้ยังมีวัตถุประสงค์เพื่อเป็นการชดเชยความเสียหายและเพื่อให้สาสมกับความผิดเพื่อให้เกิดความยุติธรรมตามหลักตาต่อตา ฟันต่อฟัน (An eye for an eye, a tooth for a tooth) โดยรูปแบบในการลงโทษซึ่งมีลักษณะที่รุนแรงป่าเถื่อน เช่น การตัดอวัยวะ การเฆี่ยนตี การทรมานและการประหารชีวิต เป็นต้น

อย่างไรก็ตามความมุ่งหมายในการลงโทษในปัจจุบันได้ลดความสำคัญของการลงโทษเพื่อการแก้แค้นทดแทนลง ทั้งนี้เนื่องจากวัตถุประสงค์ดังกล่าวมีจุดบกพร่องหลายประการ คือ ประการแรก การลงโทษเพื่อการแก้แค้นทดแทนไม่ได้พิจารณาในด้านประโยชน์ในอนาคต กล่าวคือ ไม่ได้ให้ความสำคัญในด้านการป้องกันสังคมจากการกระทำความผิดซ้ำในอนาคต ประการที่สอง การลงโทษเพื่อแก้แค้นทดแทนไม่ได้คำนึงถึงความจำเป็นของสังคม แต่คำนึงเฉพาะ

---

[7] นัทธี จิตสว่าง, *อ้างแล้ว* เชิงอรรถที่ 1, น.24-25.

ความเหมาะสมของโทษกับความผิดที่กระทำ ดังนั้นเมื่อได้ลงโทษผู้กระทำผิดตามอัตราโทษแล้วก็ต้องปล่อยตัวออกมาทั้ง ๆ ที่ยังเป็นอันตราต่อสังคมอยู่ ประการสุดท้าย เป็นเรื่องยากที่จะวัดขนาดความรุนแรงของโทษกับความผิดว่ามีความเท่าเทียมกันจริงหรือไม่ เพราะในสภาพความเป็นจริงยังไม่มีมาตรการใดที่จะสามารถลงโทษให้ได้สัดส่วนกับความผิดได้อย่างแท้จริง ปัญหาที่ตามมาคือ ผู้กระทำผิดถูกลงโทษอย่างยุติธรรมหรือผู้เสียหายได้รับการตอบแทนที่ยุติธรรมหรือไม่

2. <u>การลงโทษเพื่อข่มขู่ยับยั้ง</u>

การลงโทษเพื่อข่มขู่ยับยั้ง (deterrence) เป็นวัตถุประสงค์การลงโทษตามแนวความคิดของสำนักอาชญาวิทยาดั้งเดิม (Classiccal School) โดยเน้นรูปแบบการลงโทษเพื่อป้องกันอาชญากรรมหรือข่มขวัญยับยั้งมิให้เกิดการกระทำความผิดขึ้นอีกในอนาคต ทั้งนี้สามารถจำแนกลักษณะการข่มขู่ยับยั้งออกเป็น 2 ลักษณะ คือ การข่มขู่ยับยั้งโดยทั่วไป (General Deterrence) และการข่มขู่ยับยั้งเฉพาะราย (Specific Deterrence)

การข่มขู่ยับยั้งโดยทั่วไป คือ การลงโทษเพื่อข่มขวัญหรือป้องกันมิให้คนอื่นในสังคมกระทำความผิดแบบเดียวกัน หรือมิให้ประพฤติตนเป็นเยี่ยงอย่างซึ่งเข้าลักษณะที่ว่า “เชือดไก่ให้ลิงดู” เนื่องจากโดยธรรมชาติของมนุษย์ซึ่งหลีกเลี่ยงความเดือดร้อน ความเจ็บปวด เมื่อเห็นว่าการกระทำความผิดจะได้รับการลงโทษก็จะเกิดความรู้สึกเกรงกลัวไม่กล้าที่จะกระทำผิด ส่วนการข่มขู่ยับยั้งเฉพาะรายเป็นการลงโทษเพื่อให้ผู้กระทำความผิดรู้สึกเข็ดหลาบต่อการลงโทษและไม่กลับมากระทำความผิดซ้ำอีก ทั้งนี้เนื่องจากประสบการณ์ความยากลำบากและความเจ็บปวดที่ผู้กระทำผิดได้รับจากการถูกลงโทษ ย่อมทำให้ผู้กระทำผิดรู้สึกหลาบจำและไม่กล้าที่จะกระทำความผิดซ้ำอีกในอนาคต[8]

3. <u>การลงโทษเพื่อแสดงการไม่ยอมรับหรือประณามการกระทำความผิด</u>

การลงโทษเพื่อแสดงการไม่ยอมรับหรือประณามการกระทำความผิด (Expressive or Denunciatory Justification) แนวความคิดนี้เชื่อว่าการลงโทษผู้กระทำความผิดเป็นการไม่ยอมรับการกระทำนั้น เนื่องจากการลงโทษเพียงอย่างเดียวยังไม่เพียงพอ สังคมจึงต้องประณามการกระทำนั้นด้วย การประณามผู้กระทำผิดจะทำให้สังคมเกิดความเป็นปึกแผ่น (Social Cohesion)

---

[8] *เพิ่งอ้าง*, น.24-25.

แต่อย่างไรก็ตามวัตถุประสงค์ในการประณามการกระทำความผิดจะไม่มีผลใด ๆ หากไม่มีการลงโทษเพื่อแก้แค้นทดแทนการกระทำความผิดนั้นควบคู่ไปด้วย[9]

4. การลงโทษเพื่อตัดโอกาสกระทำผิด

การลงโทษเพื่อตัดโอกาสกระทำผิด[10] (Incapacitation) มีวัตถุประสงค์ของการลงโทษที่คล้ายคลึงกับวัตถุประสงค์ของการลงโทษเพื่อข่มขู่ยับยั้ง กล่าวคือ คล้ายคลึงกันในแง่ของเป้าหมายในการป้องกันอาชญากรรม แต่มีความแตกต่างกันในแง่ของรูปแบบวิธีการ โดยหลักการลงโทษเพื่อข่มขู่ยับยั้งนั้นมุ่งก่อให้เกิดความเกรงกลัวไม่กล้าที่จะกระทำความผิดอีก ส่วนการลงโทษเพื่อตัดโอกาสมุ่งป้องกันการกระทำความผิดซ้ำโดยวิธีการทำให้ผู้กระทำผิดหมดโอกาสที่จะกระทำความผิด ยกตัวอย่างเช่น การประหารชีวิต เป็นรูปแบบหนึ่งของการลงโทษเพื่อตัดโอกาสในการกระทำความผิดอย่างถาวร กล่าวคือ ผู้กระทำผิดไม่อาจกระทำความผิดซ้ำได้อย่างสิ้นเชิง หรือใช้วิธีการโดยการเนรเทศออกไปจากสังคม ดังเช่นในกรณีที่ประเทศอังกฤษส่งตัวนักโทษไปไว้ที่ประเทศออสเตรเลีย หรืออาจใช้วิธีการตัดโอกาสของอาชญากรในการประกอบอาชญากรรม เช่น การลงโทษพวกลักขโมยโดยวิธีการตัดมือทำให้ผู้กระทำผิดหมดโอกาสในการลักขโมยของผู้อื่นได้อีก สำหรับโทษจำคุก ซึ่งเป็นโทษที่ใช้กันอย่างแพร่หลายในปัจจุบันนี้และยังเป็นรูปแบบหนึ่งของการลงโทษที่สอดคล้องกับวัตถุประสงค์นี้ กล่าวคือ การจำคุกเป็นการกันผู้กระทำผิดออกจากสังคมเท่ากับเป็นการตัดโอกาสในการกระทำผิดด้วยเช่นเดียวกัน

5. การลงโทษเพื่อแก้ไขฟื้นฟูผู้กระทำผิด

การลงโทษเพื่อแก้ไขฟื้นฟูผู้กระทำผิด (Rehabilitation) เป็นแนวคิดของสำนักอาชญาวิทยาปฏิฐานนิยม (Positive School) ซึ่งมีความเชื่อในเรื่องเจตจำนงกำหนด (Determinism) กล่าวคือ การกระทำของมนุษย์ถูกกำหนดจากปัจจัยต่าง ๆ มนุษย์ไม่สามารถเลือกกระทำได้อย่างอิสระ มนุษย์ถูกกดดันหล่อหลอมจากสิ่งแวดล้อมและปัจจัยต่าง ๆ จนมีบุคลิกภาพที่บกพร่องและหันไปสู่การกระทำผิด ดังนั้นการกระทำของมนุษย์จึงเป็นผลมาจากปัจจัยหลายอย่างรวมกัน ได้แก่ ปัจจัยทางจิตวิทยา ปัจจัยทางชีววิทยาและปัจจัยเกี่ยวกับสิ่งแวดล้อมทาง

---

[9] ประธาน วัฒนวาณิชย์, ความรู้เบื้องต้นเกี่ยวกับอาชญาวิทยา, (กรุงเทพมหานคร: สำนักพิมพ์ประกายพรึก, 2546), น.361-362.

[10] นัทธี จิตสว่าง, *อ้างแล้ว* เชิงอรรถที่ 1, น.28-29.

สังคม ปัจจัยเหล่านี้อยู่นอกเหนือการควบคุมของมนุษย์ ดังนั้นการกระทำความผิดจึงเกิดจากปัจจัยหลายอย่างร่วมกันด้วย ซึ่งอาจจะแตกต่างกันไปในแต่ละบุคคล การลงโทษจึงไม่ควรมุ่งเน้นที่การกระทำความผิดเป็นหลัก แต่ควรพิจารณาจากสาเหตุอันเป็นปัจจัยที่ทำให้เกิดการกระทำความผิดนั้นขึ้นแล้วจึงแก้ไขที่สาเหตุดังกล่าว[11]

การแก้ไขฟื้นฟูผู้กระทำความผิดในที่นี้ หมายถึง การแก้ไขฟื้นฟูและบำบัดรักษาทั้งร่างกายและจิตใจ รวมถึงปรับปรุงเปลี่ยนแปลงบุคลิกภาพเพื่อส่งเสริมให้ผู้ต้องโทษเป็นพลเมืองที่ดี เคารพกฎหมายเมื่อพ้นโทษและมีทัศนคติที่ดีต่อสังคม[12] แนวความคิดในการลงโทษเพื่อแก้ไขฟื้นฟูเป็นแนวคิดที่ให้โอกาสคนกลับตัว ให้โอกาสแก้ไขปรับปรุงตัวโดยการทำให้คนที่กระทำความผิดสำนึกในความผิดที่ตนได้กระทำลงไปและไม่ถลำตัวลึกไปสู่การกระทำความผิดมากขึ้น ทั้งนี้โดยพยายามหลีกเลี่ยงไม่ให้ผู้กระทำความผิดถูกลงโทษในลักษณะที่เป็นการทำลายคุณลักษณะหรือศักยภาพในการกลับคืนสู่สังคมของเขา โดยการใช้มาตรการลงโทษที่ไม่ทำให้เกิดรอยมลทินและได้รับการขัดเกลาจากผู้กระทำผิดอื่น ๆ วิธีการดังกล่าว ได้แก่ การใช้มาตรการเลี่ยงโทษจำคุก เช่น การรอการลงอาญาโดยมีการคุมประพฤติ การใช้โทษปรับและการใช้มาตรการในชุมชนอื่น ๆ ทั้งนี้เพื่อมิให้ผู้กระทำผิดได้รับผลกระทบในทางลบในเรือนจำ นอกจากจากนี้ยังใช้วิธีการเลี่ยงโทษจำคุกในกรณีที่ได้เข้าไปรับโทษในเรือนจำมาระดับหนึ่งแล้วก็ให้อยู่ในเรือนจำให้น้อยที่สุดเพื่อให้ได้รับผลกระทบน้อยที่สุดเช่นกัน โดยใช้วิธีการพักการลงโทษ การลดวันต้องโทษ หรือการทำงานสาธารณะและศูนย์ควบคุม ในขณะที่พวกที่ใช้วิธีการจำคุกในเรือนจำก็ให้ได้รับการอบรมแก้ไขโดยการฝึกวิชาชีพ ให้การศึกษา การอบรมทางศีลธรรมและศาสนา การจัดสวัสดิการ การให้การบำบัดแก้ไขเป็นกลุ่มและรายบุคคล ทั้งนี้เพื่อมุ่งแก้ไขสาเหตุที่ทำให้ผู้กระทำผิดมีความบกพร่องและเป็นเหตุให้กระทำผิด[13]

---

[11] *เพิ่งอ้าง*, น.29.

[12] ประธาน วัฒนวาณิชย์, *อ้างแล้ว* เชิงอรรถที่ 9, น.24-25.

[13] นัทธี จิตสว่าง, *อ้างแล้ว* เชิงอรรถที่ 1, น.30.

2.1.3 ทฤษฎีการลงโทษ

ทฤษฎีการลงโทษสามารถแบ่งออกเป็น 2 ทฤษฎีใหญ่[14] คือ ทฤษฎีทดแทน (retributive theory) และทฤษฎีอรรถประโยชน์ (Utilitarian theory) ทั้งนี้พื้นฐานในการแบ่งแยกความแตกต่างของทั้งสองทฤษฎีนี้ คือ มุ่งที่ความรับผิดชอบที่ผู้กระทำจะต้องมีต่อผู้เสียหายหรือต่อผู้อื่นกับผลของการลงโทษแก่ผู้กระทำผิดที่มีต่อผู้อื่น กล่าวคือ พื้นฐานการลงโทษตามทฤษฎีทดแทนนั้นมุ่งพิจารณาถึงการที่ผู้กระทำผิดจะต้องชดใช้ (paid) ต่อสิ่งที่เขากระทำลง ส่วนพื้นฐานของการลงโทษตามทฤษฎีอรรถประโยชน์นั้นมุ่งเน้นที่วิธีการป้องกันมิให้เกิดความผิดอาญาขึ้นในอนาคตอีก

1. ทฤษฎีทดแทน (Retributive Theory)

ทฤษฎีทดแทนเป็นทฤษฎีที่ผสานแนวความคิดในเรื่องการแก้แค้นกับหลักความยุติธรรมในปัจจุบันเข้าด้วยกัน โดยมีหลักการที่ว่าการลงโทษเป็นเรื่องของการทดแทนความเสียหายให้แก่ผู้เสียหายซึ่งได้รับผลกระทบจากการกระทำความผิดของผู้ละเมิดกฎหมาย ทั้งนี้เพื่อให้ผู้เสียหายมีความรู้สึกพอใจ ยอมรับการลงโทษโดยรัฐและเพื่อเป็นการย้ำให้คนในสังคมทุกคนเชื่อและปฏิบัติตามกฎหมายโดยถือว่าเป็นหนี้ที่ทุกคนต้องผูกพันในสังคม

หลักการลงโทษตามทฤษฎีทดแทนนี้จะต้องมีองค์ประกอบ 3 ประการ คือ ประการแรก จะต้องกระทำเพื่อแก้ไขความเสียหายที่ผู้กระทำก่อให้เกิดขึ้น หรือทดแทนความรู้สึกของผู้เสียหายที่สูญเสียไปอันเนื่องมาจากการกระทำความผิด ประการที่สอง การลงโทษจะต้องกระทำเพื่อให้เกิดความเป็นธรรม (fairness) และประการสุดท้าย การลงโทษจะต้องได้สัดส่วนกับความร้ายแรงของความผิด[15]

องค์ประกอบแรก การลงโทษต้องเป็นการทดแทนความเสียหาย (vindication) หมายถึง การลงโทษที่ชอบธรรมจะต้องเป็นการลงโทษที่มีขึ้นเพื่อเป็นการทดแทนหรือเป็นการแก้แค้นให้กับผู้เสียหายหรือเหยื่อแห่งอาชญากรรมซึ่งได้รับความเสียหายจากการกระทำความผิดของผู้ฝ่าฝืนกฎหมาย และนอกจากนี้จะต้องทำให้ผู้เสียหายมีความรู้สึกพึงพอใจและคิดว่าการลงโทษดังกล่าวเป็นการกระทำที่ยุติธรรมแล้ว หลักการตามทฤษฎีนี้ให้ความสำคัญกับความรู้สึก

---

[14] ณรงค์ ใจหาญ, กฎหมายอาญา ว่าด้วยโทษและวิธีการเพื่อความปลอดภัย, (กรุงเทพมหานคร : สำนักพิมพ์วิญญูชน, 2543), น.20-21.

[15] *เพิ่งอ้าง*, น.21-25.

ของผู้เสียหายเป็นพิเศษ โดยชี้ให้เห็นว่าการละเลยในเรื่องของความรู้สึกของผู้เสียหายที่ต้องการจะแก้แค้นกับผู้กระทำผิดเป็นสิ่งที่ไม่ถูกต้อง เนื่องจากจะทำให้ผู้เสียหายรวมทั้งญาติพี่น้องของเขารู้สึกเสื่อมศรัทธาต่อรัฐว่าไม่อาจเยียวยาความเสียหายให้แก่เขาได้และจะนำไปสู่ความวุ่นวายอันเนื่องมาจากการแก้แค้นโดยเอกชนด้วยกันเอง ดังนั้นหากทำให้ผู้เสียหายเกิดความพึงพอใจในการลงโทษโดยรัฐแล้ว ผู้เสียหายจะยอมรับการลงโทษอันชอบธรรมโดยรัฐและยอมรับว่าการแก้แค้นผู้กระทำผิดไม่ใช้หน้าที่ของเอกชนแต่เป็นหน้าที่ของรัฐ

องค์ประกอบที่สอง การลงโทษต้องกระทำเพื่อให้เกิดความเป็นธรรม (fairness) เนื่องจากกฎหมายเป็นกฎเกณฑ์ของสังคมซึ่งคนในสังคมทุกคนจะต้องปฏิบัติตาม ผู้ที่กระทำความผิดโดยฝ่าฝืนบทบัญญัติแห่งกฎหมายจึงเป็นผู้ที่เอาเปรียบบุคคลอื่นซึ่งเคารพต่อกฎหมาย ดังนั้นผู้ที่ละเมิดต่อกฎหมายจะต้องได้รับการลงโทษ โดยการลงโทษแก่ผู้กระทำความผิดควรมีความรุนแรงเทียบเท่ากับความได้เปรียบที่ผู้กระทำผิดได้รับจากการฝ่าฝืนกฎหมายนั้น โดยถือว่าผู้กระทำผิดได้จ่ายหนี้อันเกิดจากการกระทำผิดให้แก่คนทุกคนที่เชื่อฟังกฎหมายซึ่งเป็นสมาชิกในสังคมนั้นและเมื่อจ่ายแล้วเขาก็กลับคืนสู่สังคมในฐานะที่เป็นพลเมืองดีและมีฐานะเท่าคนอื่น[16]

องค์ประกอบประการสุดท้าย การลงโทษจะต้องได้สัดส่วนกับความผิด (proportionality of punishment) หมายถึง จำนวนโทษที่ผู้กระทำผิดควรจะได้รับจะต้องเท่ากันกับความเสียหายที่เขาได้กระทำลงไปจากการกระทำผิดนั้น แต่อย่างไรก็ตามหลักดังกล่าวมีข้อยกเว้นอยู่ 2 กรณี คือ กรณีแรก การลงโทษที่สูงกว่าความเสียหายที่ผู้กระทำได้ก่อขึ้นนั้นสามารถทำได้ในกรณีการลงโทษจำคุกตลอดชีวิตแก่ผู้ที่กระทำผิดที่เป็นอันตรายต่อสังคม ทั้งนี้เพื่อเป็นการป้องกันสังคมให้ปลอดภัยยิ่งขึ้น และกรณีที่สอง คือ การลงโทษอาจต่ำกว่าสัดส่วนแห่งความผิด ในกรณีที่ผู้กระทำผิดไม่มีโอกาสที่จะกระทำผิดได้อีก ดังนั้น ผู้กระทำจะได้รับการลดโทษหรือรอการลงโทษและให้อยู่ภายใต้เงื่อนไขการคุมประพฤติ ส่วนหลักการในการพิจารณาสัดส่วนของโทษจะต้องพิจารณาถึงสภาพและความหนักเบาของความผิดซึ่งประกอบด้วยความร้ายแรงของความเสียหายจากการกระทำความผิดและผลต่อสังคมอันเกิดจากการกระทำความผิดนั้น[17]

---

[16] *เพิ่งอ้าง*, น.21-22.

[17] *เพิ่งอ้าง*, น.22-23.

2. ทฤษฎีอรรถประโยชน์ (Utilitarian Theories)

ทฤษฎีอรรถประโยชน์เป็นทฤษฎีที่มีหลักการตรงกันข้ามกับทฤษฎีทดแทน กล่าวคือ ทฤษฎีทดแทนจะมุ่งเน้นการเยียวยาความเสียหายอันเกิดจากความผิดซึ่งได้เกิดขึ้นแล้วในอดีต แต่ทฤษฎีอรรถประโยชน์จะมุ่งเน้นผลในอนาคตของการลงโทษโดยมุ่งประสงค์จะลดอาชญากรรมที่เกิดขึ้นในสังคม โดยถือว่าการลงโทษเป็นวิธีการที่จะทำให้บุคคลผู้กระทำผิดเกิดความรู้สึกกลัวและไม่กล้าที่จะกระทำความผิดนั้นอีก รวมถึงทำให้บุคคลอื่น ๆ ในสังคมกลัวการถูกลงโทษเช่นเดียวกันกับผู้กระทำผิด การลงโทษเป็นการตัดความสามารถของผู้กระทำผิดที่จะก่ออาชญากรรมขึ้นอีก และนอกจากนี้การลงโทษยังเป็นวิธีการแก้ไข ฟื้นฟูจิตใจของผู้กระทำผิดให้สำนึกผิดและกลับตัวเป็นคนดีของสังคมได้ จากหลักการดังกล่าวจะเห็นได้ว่า ทฤษฎีอรรถประโยชน์ถือว่าการลงโทษเป็นวิธีการซึ่งก่อให้เกิดผลดีซึ่งจะทำให้อาชญากรรมในสังคมลดลง โดยผลดีดังกล่าวประกอบด้วยประการแรก การลงโทษจะมีผลยับยั้ง (deterrence) มิให้มีการกระทำผิดอาญาโดยจะมีผลเป็นการยับยั้งทั้งแก่ตัวผู้กระทำผิดและแก่บุคคลทั่วไป ประการที่สอง การลงโทษจะมีผลเป็นการแก้ไข (reformative effect) และฟื้นฟู (rehabilitative effect) ผู้กระทำผิดโดยทำให้ผู้กระทำผิดเปลี่ยนทัศนคติและค่านิยมที่จะเชื่อฟังและไม่ฝ่าฝืนกฎหมาย ประการสุดท้าย การลงโทษจะมีผลเป็นการตัดโอกาสมิให้ผู้นั้นกระทำความผิด (incapacitive effect) โดยการลงโทษจำคุกผู้กระทำผิดจึงไม่มีโอกาสก่ออาชญากรรมขึ้นในสังคมได้อีก[18]

การข่มขู่หรือยับยั้งผู้กระทำความผิดมิให้กระทำความผิดอาญาขึ้นอีกในอนาคต เป็นผลดีอย่างหนึ่งของการลงโทษซึ่งนอกจากจะเป็นการข่มขู่เฉพาะตัวผู้กระทำความผิด (specific deterrence) ให้เกิดความรู้สึกกลัวไม่กล้าที่จะกระทำความผิดในลักษณะเดียวกันนั้นอีก ยังสามารถส่งผลดีในการข่มขู่โดยทั่วไป (general deterrence) อีกด้วย กล่าวคือ การลงโทษบุคคลผู้กระทำผิดเพื่อให้เป็นเยี่ยงอย่างแก่บุคคลอื่นในสังคม ส่งผลให้คนในสังคมเกิดความเกรงกลัวต่อการลงโทษและไม่กล้าที่จะกระทำความผิด[19]

การลงโทษเพื่อแก้ไขหรือฟื้นฟูจิตใจของผู้กระทำความผิดเป็นวัตถุประสงค์ในการแก้ไขเยียวยาจิตใจของผู้กระทำผิดให้ลดความรู้สึกต่อต้านกฎหมายและกลับมามีความเห็นดีเห็นชอบด้วยกับการปฏิบัติตามกฎหมาย ตลอดจนมีความสามารถยับยั้งตนเองมิให้คิดหรือกระทำการอันเป็นความผิดอีกต่อไป โดยวิธีการในการลงโทษเพื่อการแก้ไขหรือฟื้นฟูจิตใจของผู้กระทำ

---

[18] *เพิ่งอ้าง*, น.25-26.

[19] *เพิ่งอ้าง*, น.28-31.

ความผิดสามารถกระทำได้หลายวิธี ทั้งนี้ขึ้นอยู่กับลักษณะและพื้นฐานทางจิตใจของผู้กระทำความผิดในแต่ละราย ยกตัวอย่างเช่น พยายามหลีกเลี่ยงการลงโทษจำคุกในระยะเวลาอันสั้นและให้ใช้วิธีการอื่นแทน เช่น กักขัง รอการลงโทษหรือปรับ เป็นต้น ทั้งนี้เพราะการลงโทษจำคุกในระยะเวลาอันสั้นนั้นนอกจากจะไม่ก่อให้เกิดผลเป็นการแก้ไขพฤติกรรมของผู้กระทำความผิดแล้ว ยังก่อให้เกิดผลเสียต่อผู้ต้องโทษเพราะถูกตราหน้าว่าเป็นคนคุกมาก่อน หรืออาจใช้วิธีการแก้ไขปรับปรุงผู้ต้องโทษในขณะอยู่ในเรือนจำ เช่น ฝึกหัดอาชีพ อบรมทางการศึกษาและศีลธรรมหรือให้การรักษาพยาบาลเพื่อให้จิตใจของผู้กระทำความผิดมีทัศนคติที่สอดคล้องกับปทัสถานของสังคมเมื่อถูกปล่อยตัวออกจากเรือนจำไปแล้ว[20]

การลงโทษเพื่อตัดโอกาสมิให้ผู้กระทำผิดมีโอกาสที่จะกระทำความผิดในลักษณะเช่นนั้นอีก เป็นลักษณะของการลงโทษเพื่อป้องกันความปลอดภัยให้แก่สังคมมิให้ได้รับผลกระทบจากการกระทำความผิดซ้ำของผู้ต้องโทษ โดยวิธีการที่จะทำให้ผู้กระทำความผิดหมดโอกาสในการกระทำความผิดซ้ำจะต้องเป็นวิธีการที่ทำให้ผู้นั้นหมดโอกาสกระทำผิดตลอดไป เช่น การประหารชีวิต การเนรเทศหรือการจำคุกโดยมีกำหนดเวลาจนกว่าจะแน่ใจว่าผู้นั้นไม่เป็นอันตรายแก่สังคมอีก เป็นต้น[21]

2.2 ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ

2.2.1 คำนิยามคำว่า “แฮกเกอร์”

คำว่า “แฮกเกอร์” (Hacker) เป็นคำที่มีที่มาจากปรากฏการณ์ความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยีด้านคอมพิวเตอร์ โดยในยุคเริ่มต้นของวงการคอมพิวเตอร์ คำว่า “แฮกเกอร์” นี้ถูกนำมาใช้เรียกบุคคลซึ่งมีความรู้ความเชี่ยวชาญพิเศษในด้านคอมพิวเตอร์จนสามารถแก้ไขเปลี่ยนแปลงการทำงานของเครื่องคอมพิวเตอร์ให้เป็นไปตามที่ต้องการได้ คำว่า “แฮกเกอร์” ในยุคสมัยนั้นยังคงเป็นที่รู้จักกันแต่เฉพาะในกลุ่มของนักคอมพิวเตอร์ ทั้งนี้เนื่องจากในยุคสมัยนั้นการใช้งานคอมพิวเตอร์ยังไม่เป็นที่แพร่หลายมากนัก ต่อมาเมื่อการใช้งานคอมพิวเตอร์เริ่มเป็นที่นิยมมากยิ่งขึ้น ประกอบกับข่าวสารจากสื่อสารมวลชนเกี่ยวกับผู้เชี่ยวชาญด้าน

---

[20] *เพิ่งอ้าง*, น.31-34.

[21] *เพิ่งอ้าง*, น.34.

คอมพิวเตอร์ที่สามารถอาศัยความรู้ทางคอมพิวเตอร์ของตนในการเข้าถึงหรือแทรกแซงการทำงานของระบบคอมพิวเตอร์ได้ พร้อมกันนี้ยังได้นำเอาคำว่า “แฮกเกอร์” มาใช้เรียกบุคคลซึ่งมีพฤติกรรมดังกล่าว ในที่สุดคำว่า “แฮกเกอร์” จึงถูกนิยามเพิ่มเติมสาระในส่วนของพฤติกรรมในด้านลบจนกลายเป็นคำสามัญซึ่งคนทั่วไปเข้าใจความหมายตามที่สื่อสารมวลชนได้นำเสนอไป[22]

นอกเหนือจากคำนิยามของคำว่า “แฮกเกอร์” ตามความหมายดั้งเดิมและความหมายในปัจจุบัน ยังปรากฏคำอื่นซึ่งถูกนำมาใช้กันอย่างสับสน อาทิ คำว่า “แครกเกอร์” (Cracker) ซึ่งมีความหมายในทำนองเดียวกับคำว่า “แฮกเกอร์” ตามคำนิยามที่สื่อสารมวลชนนำมาใช้ในปัจจุบัน กล่าวคือ เป็นบุคคลซึ่งใช้ความรู้ ทักษะด้านคอมพิวเตอร์ในทางที่ผิดก่อให้เกิดความเดือดร้อนเสียหายให้แก่ผู้อื่น โดยคำว่า “แครกเกอร์” นี้เป็นคำที่นำมาใช้ในการแบ่งแยกพฤติกรรมระหว่างบุคคลที่เป็นแฮกเกอร์ตามความหมายดั้งเดิมกับบุคคลที่ถูกเรียกว่าแฮกเกอร์ตามความหมายในปัจจุบัน แต่อย่างไรก็ตามสื่อสารมวลชนในปัจจุบันยังคงนิยมใช้คำว่า “แฮกเกอร์” มากกว่าคำว่า “แครกเกอร์” ในการสื่อความหมายถึงบุคคลซึ่งมีพฤติกรรมในด้านลบหรือผู้ที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์[23]

เนื่องด้วยคำนิยามของคำว่า “แฮกเกอร์” ที่มีความคลุมเครือระหว่างความหมายดั้งเดิมกับความหมายที่ใช้ในปัจจุบัน ฉะนั้นการใช้คำว่า “แฮกเกอร์” ในวิทยานิพนธ์นี้ผู้เขียนประสงค์ให้มีความหมายในเชิงสถานะทางบุคคลซึ่งเป็นผู้ที่มีความรู้ความเชี่ยวชาญและทักษะในด้านคอมพิวเตอร์ โดยไม่คำนึงว่าบุคคลดังกล่าวจะมีความเกี่ยวพันกับพฤติกรรมอาชญากร (criminal behavior) หรือไม่ก็ตาม ส่วนกรณีผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์โดยอาศัยเทคนิคทางคอมพิวเตอร์ ผู้เขียนจะใช้คำว่า “ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ” แทนการใช้คำว่า “แครกเกอร์” หรือคำว่า “แฮกเกอร์” ตามความหมายที่ใช้ในปัจจุบัน อนึ่งการใช้คำว่า “ผู้กระทำผิดฐานเข้าถึงข้อมูลของผู้อื่นโดยมิชอบ” ผู้เขียนมิได้มีวัตถุประสงค์ที่จะจำกัดการศึกษาแต่เฉพาะการกระทำความผิดในฐานความผิดดังกล่าวเท่านั้น แต่หากเป็นเพียงการนำเอารูปแบบหนึ่งของการกระทำความผิดอันเป็นสามัญหรือเป็นที่เข้าใจของคนทั่ว ๆ ไปมาใช้เป็นการสื่อความหมายถึงความเป็น “อาชญากรคอมพิวเตอร์” (cyber criminal) หรือผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งในสภาพความเป็นจริงบุคคลดังกล่าวอาจมีพฤติกรรมการกระทำผิดใน

---

[22] Slatalla, Michelle. “A Brief History of Hacking.” <http://tlc.discovery.com/convergence/hackers/articles/history.html>

[23] *Ibid.*

ฐานความผิดเกี่ยวกับคอมพิวเตอร์อื่น ๆ รวมอยู่ด้วย เช่น การดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ หรือการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เป็นต้น[24]

2.2.2 ประวัติความเป็นมาของแฮกเกอร์

จากการศึกษาของผู้เขียนพบว่า วิวัฒนาการของการบังเกิดขึ้นของแฮกเกอร์ในสังคมแห่งเทคโนโลยี ไม่ได้มีหลักฐานหรือรายละเอียดที่ปรากฏอย่างเด่นชัดว่า เริ่มมีการเจาะระบบเกิดขึ้นครั้งแรกเมื่อใดและที่ใด แต่อย่างไรก็ตาม อาจจะกล่าวได้ว่า แฮกเกอร์น่าจะเกิดขึ้นมาพร้อมๆ กับความเจริญก้าวหน้าทางเทคโนโลยีด้านคอมพิวเตอร์ กล่าวคือ เมื่อสังคมใดเริ่มมีการใช้งานระบบคอมพิวเตอร์ สังคมนั้นย่อมมีแฮกเกอร์ปรากฏอยู่เสมอ คำกล่าวในลักษณะเช่นนี้ เท่ากับเป็นการยอมรับว่า แฮกเกอร์ เป็นปรากฏการณ์ทั่วไปของสังคมที่มีความเจริญก้าวหน้าทางเทคโนโลยี ประวัติความเป็นมาของแฮกเกอร์ สามารถจัดแบ่งออกได้เป็น 6 ยุค[25] ดังนี้

1. ยุคก่อนประวัติศาสตร์ (Prehistory Age)

คำว่า “ก่อนประวัติศาสตร์” ในที่นี้หมายถึง ช่วงของการเริ่มต้นก่อนที่จะก้าวเข้าสู่ยุคแห่งข้อมูล (Information Age) คือ ในระหว่าง ค.ศ. 1878 – 1969 ซึ่งอาจนับได้ว่าเป็นจุดเริ่มต้นของการปรากฏตัวขึ้นของกลุ่มแฮกเกอร์กลุ่มแรก ในยุคเริ่มแรกแห่งวงการคอมพิวเตอร์ กลุ่มแฮกเกอร์จะอยู่ในกลุ่มของนักศึกษาของสถาบันเทคโนโลยีแห่งมลรัฐแมสซาชูเซตส์ หรือ MIT (Massachusitts Institutes of Techonology) ซึ่งในช่วงทศวรรษที่ 1960 นักศึกษาของสถาบันแห่งนี้เป็นกลุ่มที่มีโอกาสที่จะสามารถเข้าถึงคอมพิวเตอร์เมนเฟรม (mainframe computer) ของสถาบันได้ และด้วยเหตุนี้เองทำให้กลุ่มแฮกเกอร์ในยุคแรกๆ ล้วนมาจากการศึกษาเรียนรู้วิชาจาก

---

[24] *Ibid.*

[25] Jordana Heaton, “History of Hacker,” <http://www.slais.ubc.ca/people/students/student-projects/J_Heaton/index.htm>,see also Michelle Slatalla, “A Brief History of Hacking,” <http://tlc.discovery.com/convergence/hacker/articles/history.html> and Robert Trigaux, “A history of hacking,” <http://www.sptimes.com/Hackers/history.hacking.html>

สถาบันแห่งนี้ ทั้งนี้เพราะมีโอกาสในการใช้งานคอมพิวเตอร์ที่ทันสมัยที่สุดในยุคนั้น พวกเขาจึงทุ่มเทเวลาในการศึกษาเรียนรู้ระบบของคอมพิวเตอร์อย่างลึกซึ้งและเริ่มมีการดัดแปลง ปรับแต่งการทำงานของระบบคอมพิวเตอร์ให้สามารถทำงานได้เกินกว่าขีดจำกัดที่มีการออกแบบเอาไว้แต่เดิม การกระทำเหล่านี้ถูกเรียกโดยคำที่ใช้กันในกลุ่มว่า “การแฮก” (hacking) ดังนั้น คำว่า “hacker” ในยุคสมัยนี้จึงมีความหมายในแง่บวก คือ หมายถึงผู้ที่มีความรู้ความสามารถเกี่ยวกับระบบคอมพิวเตอร์อย่างแตกฉานจนสามารถดัดแปลงแก้ไขการทำงานของระบบให้ดีขึ้นกว่าขีดจำกัดเดิมได้ นอกจากนี้กลุ่มนักศึกษาที่เป็นแฮกเกอร์ของ MIT ยังมีคุณลักษณะที่เหมือนกันในเรื่องความเชื่อเกี่ยวกับความเป็นอิสระของข้อมูลและเทคโนโลยี (freedom of information and technology) ซึ่งเป็นลักษณะดังกล่าวนี้ได้สืบทอดต่อๆ กันมาจนถึงแฮกเกอร์ในยุคปัจจุบันนี้[26]

2. <u>ยุคฟรีกเกอร์ (Phreaker Age)</u>[27]

ยุคนี้อยู่ในช่วงทศวรรษที่ 1970 โดยคำว่า “ฟรีกเกอร์” (phreaker) เป็นคำที่เกิดจากการเล่นคำระหว่างคำว่า “freak” ซึ่งหมายถึง ความคิดที่นอกลู่นอกทาง คำว่า “phone” ซึ่งหมายถึง โทรศัพท์ และคำว่า “free” หมายถึง ไม่เสียค่าใช้จ่าย เมื่อรวมคำเหล่านี้เข้าด้วยกัน คำว่า “ฟรีกเกอร์” จึงหมายถึง พวกที่มีหัวคิดแบบนอกลู่นอกทาง ในการหาวิธีการแปลกๆ เพื่อทำให้สามารถใช้โทรศัพท์โดยไม่เสียค่าใช้จ่าย

นายจอห์น เดรปเปอร์ (John Draper) หรือฉายา กัปตันครั๊นช์ (Captain Crunch) เป็นตัวอย่างของฟรีกเกอร์ที่มีชื่อเสียงในยุคสมัยนั้น เขาเป็นคนที่ค้นพบวิธีการนำเอานกหวีดซึ่งแถมมากับขนมธัญพืชอบกรอบ ยี่ห้อกัปตันครั๊นช์ (Cap’n Crunch Cereal) มาเป่าเพื่อให้เกิดเสียงที่มีช่วงความถี่ 2600 เฮิร์ซ ซึ่งเป็นช่วงความถี่เสียงที่ทำให้สามารถใช้บริการโทรศัพท์ทางไกลได้โดยไม่เสียค่าใช้จ่าย

นอกจากนี้ จอห์น เดรปเปอร์ ได้หาวิธีการฟรีก (phreaking) ในรูปแบบอื่นๆ โดยไม่ได้มีวัตถุประสงค์เพียงเพื่อให้สามารถใช้โทรศัพท์ได้โดยไม่เสียค่าใช้จ่ายเพียงเท่านั้น แต่เขายังพยายามเข้าถึง (access) และควบคุมจัดการ (manipulate) ระบบคอมพิวเตอร์ที่ทำงานอยู่เบื้องหลังระบบโทรศัพท์อีกด้วย และจากวัฒนธรรมรอง (subculture) ของกลุ่มฟรีกเกอร์ในยุคนี้

---

[26] *Ibid.*

[27] *Ibid.*

จึงได้ถ่ายทอดและพัฒนาไปสู่กลุ่มของแฮกเกอร์ในยุคต่อมา โดยเฉพาะอย่างยิ่งในเรื่องของอิสรภาพของเทคโนโลยี (The Liberation of Technology)

3. ยุคทอง (Golden Age)[28]

ยุคนี้เป็นยุคที่คอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC) ได้มีการประดิษฐ์และผลิตออกวางจำหน่ายในทวีปอเมริกาเหนือและยุโรปในช่วง ปี ค.ศ. 1980 – 1985 เป็นจำนวนมากในยุคก่อนหน้าที่จะมีคอมพิวเตอร์ส่วนบุคคลเกิดขึ้น ปรากฏการณ์ของการเจาะระบบคอมพิวเตอร์จะถูกจำกัดอยู่แต่เฉพาะการฟรีก หรือการเข้าถึงระบบคอมพิวเตอร์เมนเฟรมในหน่วยงานใหญ่ๆ หรือในมหาวิทยาลัยเพียงเท่านั้น ดังนั้นเมื่อคอมพิวเตอร์ส่วนบุคคลเริ่มได้รับความนิยม บุคคลทั่วไปสามารถซื้อเครื่องคอมพิวเตอร์ไปใช้งานในบ้านได้ในราคาที่ไม่แพงมากนัก จึงทำให้ปรากฏการณ์ของการเจาะระบบเริ่มมีการแพร่หลายออกไปในวงกว้าง

เรื่องราวของการเจาะระบบคอมพิวเตอร์ ต่อมาถูกนำเสนอในรูปแบบของภาพยนตร์เรื่อง “War Games” ซึ่งฉายในปี ค.ศ. 1983 จุดนี้เองที่ทำให้คำว่า “hacker” หรือคำว่า “hacking” เริ่มถูกนำมาอธิบายในแง่ลบ กล่าวคือ เนื้อหาของภาพยนตร์เรื่องนี้เป็นเรื่องที่เกี่ยวกับ เด็กอัจฉริยะด้านคอมพิวเตอร์ที่สามารถเจาะระบบของคอมพิวเตอร์ของโรงเรียนของเขาได้ สามารถจองเที่ยวบินฟรีไปกรุงปารีสและสามารถจุดชนวนสงครามนิวเคลียร์ให้เกิดขึ้นได้โดยที่เขาเพียงแค่นั่งอยู่ในห้องเท่านั้น ต่อมาภาพยนตร์เรื่องนี้จึงกลายเป็นแรงบันดาลใจที่สำคัญให้กับแฮกเกอร์ที่มีชื่อเสียงหลายคน

การเติบโตมากยิ่งขึ้นของวัฒนธรรมรองของกลุ่มแฮกเกอร์ในยุคนี้ จะเห็นได้จากระบบกระดานข่าว หรือ Bullention Board System ที่เพิ่มมากขึ้น โดยแฮกเกอร์จะใช้ช่องทางนี้ในการแลกเปลี่ยนเรื่องราวและเทคนิคต่างๆ การที่บุคคลใดๆ จะสามารถเข้าถึงหรือจะถูกปฏิเสธในการใช้กระดานข่าวเหล่านี้จะขึ้นอยู่กับระดับความเชี่ยวชาญทางเทคนิค (technical proficiency) หรือชื่อเสียงของแต่ละคน นอกจากนี้ยังมีสื่อโดยทางอื่นอีก คือ จดหมายข่าวอิเล็กทรอนิกส์ (electronics newsletter) นอกจากนี้ในยุคนี้ยังมีการเปิดตัวของสื่อทางอิเล็กทรอนิกส์ที่เกี่ยวกับแฮกเกอร์แห่งแรก คือ “2600 : The Hacker Quaterly” (www.2600.com) โดยก่อตั้งขึ้นในปี ค.ศ. 1984 และยังได้รับความนิยมอย่างมากจากกลุ่มแฮกเกอร์ทั่วโลกตราบจนถึงทุกวันนี้

---

[28] *Ibid.*

นอกเหนือจากนี้ยังมีแฮกเกอร์หลายคนได้รวมตัวกันเป็นกลุ่มขึ้น หนึ่งในนั้น คือ กลุ่ม 414 (414 Group) โดยชื่อของกลุ่มมีที่มาจากรหัสพื้นที่ (area code) ในเมือง Wisconsin และนอกจากนี้ยังมีกลุ่มที่มีชื่อเสียงมากอีกกลุ่มหนึ่ง คือ Legion of Doom ที่เติบโตขึ้นอย่างรวดเร็วในปี ค.ศ.1984 โดยการนำของแฮกเกอร์ ชื่อ เล็กซ์ ลูเธอร์ (Lex Luther) ในแต่ละกลุ่มของแฮกเกอร์จะมีการติดต่อสื่อสารกันผ่านทางกระดานข่าวของกลุ่มนั้นๆ โดยจะมีแฮกเกอร์ที่อยู่ในระดับหัวกะทิเพียงสิบคนเท่านั้นที่เป็นแกนนำของกลุ่ม นอกจากนั้นจะเป็นพวกฝึกหัดที่สนใจการเจาะระบบที่เข้ามาหาความรู้จากแฮกเกอร์ในกระดานข่าวเหล่านี้[29]

ต่อมาเป้าหมายเบื้องต้นในการสำรวจโลกแห่งเทคโนโลยีของเหล่าแฮกเกอร์ได้เริ่มต้นขึ้น เมื่อ ARPANET ได้เริ่มการเชื่อมต่อเครือข่ายคอมพิวเตอร์ระหว่างมหาวิทยาลัย จนก่อให้เกิดระบบอินเทอร์เน็ตในเวลาต่อมา

4. <u>ยุคพฤติกรรมอาชญากร (Criminal Behavior Age)</u>[30]

ในช่วงของยุคนี้อยู่ระหว่างปี ค.ศ.1985 – 1990 เป็นยุคที่แฮกเกอร์เข้าสู่เส้นทางของพฤติกรรมอาชญากร (criminal behavior) มากยิ่งขึ้น โดยแฮกเกอร์บางคนได้ใช้ความรู้ความสามารถทางด้านคอมพิวเตอร์ของตนมาเป็นประโยชน์ในการกระทำความผิด ถึงแม้ว่าในยุคทองที่ผ่านมาจะมีแฮกเกอร์บางคนที่กระทำความผิดและถูกจับดำเนินคดีตามกฎหมาย อย่างเช่นในกรณีของ Pat Riddle หรือ Captain Zap ซึ่งเป็นแฮกเกอร์คนแรกของประเทศสหรัฐอเมริกาที่ถูกดำเนินคดีในข้อหาขโมยสินค้าหรือบริการทางโทรศัพท์ ในปี ค.ศ.1981 แต่อย่างไรก็ตาม กฎหมายที่ใช้บังคับอยู่ในยุคนั้นยังมีจุดบกพร่องหลายประการที่ทำให้ไม่สามารถดำเนินคดีกับการเจาะระบบคอมพิวเตอร์ได้ ดังนั้นในยุคนี้จึงได้มีการแก้ไขจุดบกพร่องหรือช่องว่างของกฎหมายขึ้นในปี ค.ศ.

---

[29] นอกจากนี้ยังมีกลุ่มแฮกเกอร์กลุ่มอื่น ๆ ที่รวมตัวกันก่อตั้งขึ้นมา ยกตัวอย่างเช่น กลุ่ม Chaos Computer Club อยู่ที่กรุงเบอร์ลิน ประเทศเยอรมันนี (http://www.ccc.de/?language=en) กลุ่มลัทธิวัวตาย (Cult of the Dead Cow) ในมลรัฐเท็กซัส ประเทศสหรัฐอเมริกา (http://www.cultdeadcow.com/cms/main.php3) กลุ่ม L0pht Heavy Industries ในมลรัฐแมสซาชูเซ็ตส์ ประเทศสหรัฐอเมริกา และกลุ่มแฮกเกอร์อื่น ๆ ทั่วโลกอีกหลายกลุ่ม เช่น กลุ่ม L0pht, กลุ่ม Youth International Party Line/Technology Assistance Program (YIPL/TAP), กลุ่ม LOD/H และกลุ่ม Masters of Deception เป็นต้น

[30] Jordana Heaton, *supra note* 25.

1985 และ ค.ศ.1986 โดยมีการแก้ไขประมวลกฎหมายอาญาของประเทศแคนาดา และออกพระราชบัญญัติว่าด้วยการฉ้อโกงและความผิดเกี่ยวกับคอมพิวเตอร์ (The Computer Fraud And Abuse Act) ในประเทศสหรัฐอเมริกา

การเพิ่มจำนวนมากขึ้นของแฮกเกอร์ในยุคนี้ ก่อให้เกิดปัญหาตามมา คือ แฮกเกอร์หลายคนนำความรู้ของตนมาใช้ในลักษณะของอาชญากรมากยิ่งขึ้น มีการแจกจ่ายโปรแกรมคอมพิวเตอร์และเกมส์เถื่อนกันอย่างมากมาย แฮกเกอร์บางคนได้กล่าวถึงปรากฏการณ์ในยุคนี้ว่า แฮกเกอร์ในยุคนี้เริ่มไม่สนใจในเรื่องหลักความเป็นอิสรภาพของเทคโนโลยีเหมือนเช่นในอดีต แต่พวกเขาสนใจแต่เฉพาะผลประโยชน์ส่วนตนเท่านั้น ด้วยเหตุนี้แฮกเกอร์ที่แท้จริงจึงมีการแบ่งแยกพวกตนออกจากกลุ่มแฮกเกอร์ที่เรียกว่า “แครกเกอร์” (cracker) ซึ่งหมายถึงพวกแฮกเกอร์กลุ่มใหม่ที่มีเจตนาประสงค์ร้ายเป็นอย่างมาก แต่อย่างไรก็ตามการแบ่งแยกความแตกต่างในเรื่องนี้กลับไม่ได้รับความสนใจจากสื่อมวลชนมากเท่าที่ควร เพราะสื่อมวลชนยังคงนำเสนอข่าวและเรื่องราวเกี่ยวกับการกระทำความผิดของบุคคลที่เรียกว่า “แฮกเกอร์” ในความหมายเช่นเดียวกับพวก “แครกเกอร์”

นอกจากนี้ในยุคนี้ ยังปรากฏไวรัสคอมพิวเตอร์เกิดขึ้นเป็นครั้งแรก ในปี ค.ศ.1987 โดยเข้าไปโจมตีระบบคอมพิวเตอร์ของมหาวิทยาลัย Delaware ส่งผลให้ระบบคอมพิวเตอร์ของมหาวิทยาลัยขัดข้องชั่วคราว แม้ว่าไวรัสคอมพิวเตอร์ตัวแรกนี้จะไม่ได้ก่อความเสียหายอย่างถาวร แต่หนังสือพิมพ์และนิตยสารจำนวนหนึ่งเริ่มนำเรื่องนี้ออกมาตีแผ่ โดยชี้ให้เห็นถึงภัยรูปแบบใหม่ที่อยู่ในรูปของโปรแกรมคอมพิวเตอร์ที่สามารถทำซ้ำตัวมันเองได้ คล้ายกับลักษณะการแพร่พันธุ์ของเชื้อไวรัส และในเดือนพฤศจิกายน ปี ค.ศ.1988 ไวรัสคอมพิวเตอร์สายพันธุ์ใหม่ได้ปรากฏตัวขึ้นในระบบคอมพิวเตอร์ของ ARPANET ผู้เชี่ยวชาญด้านคอมพิวเตอร์เรียกไวรัสสายพันธุ์นี้ว่า “หนอน” (worm) เนื่องจากลักษณะการทำงานของมันแตกต่างไปจากไวรัสคอมพิวเตอร์ทั่วๆ ไป โดยหนอนตัวนี้ได้แพร่กระจายไปในระบบคอมพิวเตอร์ของ ARPANET, หน่วยงานของรัฐและมหาวิทยาลัยต่างๆ ภายในเวลาเพียงไม่กี่ชั่วโมง ต่อมาสืบสวนพบว่า หนอนตัวนี้ถูกสร้างขึ้นโดยนาย Robert Morris ซึ่งเป็นลูกชายของหัวหน้าทีมนักวิจัยของศูนย์ความปลอดภัยของคอมพิวเตอร์แห่งชาติ (National Computer Security Center)

5. ยุคกวาดล้างแฮกเกอร์ (Hacker Crackdown Age)[31]

หลังจากผ่านจากช่วงของยุคมืด เมื่อย่างเข้าสู่ทศวรรษที่ 1990 พฤติกรรมอาชญากรของแฮกเกอร์เริ่มปรากฏให้เห็นเด่นชัด และทวีความรุนแรงมากยิ่งขึ้น หน่วยงานของรัฐเริ่มมีการวางมาตรการตอบโต้พฤติกรรมของเหล่าบรรดาแฮกเกอร์ที่ประพฤติตัวเฉกเช่นอาชญากรในโลกของอิเล็กทรอนิกส์ ทั้งนี้ผลพวงประการหนึ่งที่ทำให้แฮกเกอร์ในยุคนี้ถูกจับตัวได้มากยิ่งขึ้น อาจจะมาจากงานเขียน เรื่อง “Hacker Crackdown” เขียนโดยแฮกเกอร์ที่ชื่อ Bruce Sterling ในหนังสือเล่มนี้ได้เขียนเรื่องราวเปิดโปงพฤติกรรมในด้านมืดของแฮกเกอร์ในหลากหลายรูปแบบ และจากเนื้อหาในหนังสือเล่มนี้เองทำให้ผู้คนเริ่มเข้าใจพฤติกรรมของพวกแฮกเกอร์มากยิ่งขึ้น ต่อมาสมาชิกในกลุ่มของแฮกเกอร์ต่างๆ โดยเฉพาะอย่างยิ่ง กลุ่ม Legion of Doom จึงเริ่มกลายเป็นเป้าหมายที่สำคัญที่ถูกจับตามองจากเจ้าหน้าที่ของรัฐ ในยุคนี้มีแฮกเกอร์สองคนที่มีชื่อเหมือนกันและต่างมีชื่อเสียงและความสามารถในด้านการเจาะระบบเป็นอย่างมาก แต่สุดท้ายทั้งสองต้องถูกเจ้าหน้าที่จับกุมและดำเนินคดี คนแรกคือ นายเควิน มิตนิค (Kevin Mitnick) และอีกคนหนึ่ง คือ นายเควิน พอลเซ่น (Kevin Poulsen)

2.2.3 การจัดประเภทของแฮกเกอร์

เมื่อภัยในสังคมอิเล็กทรอนิกส์เริ่มทวีความรุนแรงมากยิ่งขึ้น สังคมในโลกแห่งความเป็นจริงจึงเริ่มตระหนักถึงปัญหาต่าง ๆ เหล่านี้ที่เกิดขึ้นจากการกระทำของบุคคลซึ่งถูกขนานนามว่าเป็นแฮกเกอร์ โดยมีการศึกษาเพื่อทำความเข้าใจพฤติกรรมของบุคคลที่เป็นแฮกเกอร์ในสังคมปัจจุบันว่ามีลักษณะ รูปแบบที่เหมือนกันหรือแตกต่างกันหรือไม่ อย่างไร ทั้งนี้เพื่อประโยชน์ในการจำแนกประเภทแฮกเกอร์ออกเป็นกลุ่ม ๆ ได้อย่างชัดเจน อย่างไรก็ดีจากการศึกษาพบว่า การจำแนกประเภทของแฮกเกอร์ที่มีปรากฏอยู่ทั้งในตำราและเอกสารทางวิชาการในปัจจุบันยังไม่มีหลักเกณฑ์ในการจำแนกที่แน่นอน ชัดเจน การจำแนกประเภทแฮกเกอร์ที่มีปรากฏในปัจจุบันนี้จึงเป็นเพียงการจัดแบ่งประเภทตามความเห็นของนักวิจัยนั้น ๆ แต่อย่างไรก็ตามผู้ศึกษาเห็นว่าโดยภาพรวมสามารถจำแนกรูปแบบของการจัดแบ่งประเภทของแฮกเกอร์ออกเป็น 3 กลุ่มใหญ่ คือ การจำแนกตามเจตนาของแฮกเกอร์ การจำแนกตามระดับความสามารถของแฮกเกอร์และการจำแนกตามแรงจูงใจของแฮกเกอร์

---

[31] *Ibid.*

1. การจำแนกตามเจตนาของแฮกเกอร์

ดังที่ได้กล่าวไว้แล้วว่าความหมายดั้งเดิมของแฮกเกอร์ คือ บุคคลที่มีความรู้และประสบการณ์ด้านคอมพิวเตอร์เป็นพิเศษ เป็นผู้อุทิศตนให้กับงานที่ทำอย่างเต็มที่ รวมทั้งทำประโยชน์ให้แก่วงการคอมพิวเตอร์ แต่ต่อมาภาพลักษณ์ที่ดีนี้เริ่มเปลี่ยนแปลงไปเมื่อมีพฤติกรรมในด้านไม่ดีเข้ามาแทนที่ ส่งผลให้มีการแบ่งฝักแบ่งฝ่ายออกเป็น 2 กลุ่ม[32] โดยอาศัยเจตนาของแฮกเกอร์เป็นเกณฑ์ กล่าวคือ หากเป็นแฮกเกอร์ฝ่ายดีตามความหมายดั้งเดิม จะถูกเรียกว่า “แฮกเกอร์หมวกขาว” (white hat) และหากเป็นพวกแฮกเกอร์ที่มีเจตนาร้าย จะเรียกพวกนี้ว่า “แฮกเกอร์หมวกดำ” (black hat) ทั้งนี้อาจมีที่มาจากภาพยนตร์ตะวันตกซึ่งฝ่ายพระเอกที่เป็นฝ่ายดีมักจะสวมหมวกคาวบอยสีขาวและฝ่ายคนร้ายมักจะสวมหมวกสีดำ[33]

อย่างไรก็ตามการจำแนกประเภทในลักษณะเช่นนี้เป็นการจัดแบ่งประเภทที่กว้างจนเกินไป และบางกรณีอาจมีปัญหาในการจำแนกเจตนาที่แท้จริงของแฮกเกอร์คนนั้น ๆ ว่ามีเจตนาดีหรือเจตนาร้าย จนบางครั้งอาจต้องจัดอยู่ในกลุ่มใหม่ที่เรียกว่า “แฮกเกอร์หมวกเทา” (gray hat) ซึ่งเป็นพวกที่อาจมีทั้งเจตนาดีและเจตนาร้ายปะปนกันจนไม่อาจแบ่งแยกได้[34]

2. การจำแนกตามระดับความสามารถของแฮกเกอร์

เนื่องจากรูปแบบหรือวิธีการในการกระทำความผิดของแฮกเกอร์มีวิธีการที่หลากหลายและต้องอาศัยทั้งความรู้ ทักษะ รวมถึงความเชี่ยวชาญทางด้านคอมพิวเตอร์ในระดับที่แตกต่างกันออกไป จึงส่งผลให้ความสามารถและศักยภาพของแฮกเกอร์แต่ละคนขึ้นอยู่กับระดับ

---

[32] ทรงเกียรติ ภาวดี, เปิดโปงแฮกเกอร์ เล่ม 1 , (กรุงเทพมหานคร: ซีเอ็ดยูเคชั่น, 2548), น.7-19.

[33] เควิน บีเวอร์, แฮก ฟอร์ ดัมมี่ส์, แปลโดย อัฏฐพล ส่งแสงและมานิตา เจริญปรุ, (กรุงเทพมหานคร: กริฟฟอน มีเดีย, 2548), น.9-10. และโปรดดู สุภัทท์ บุญญานนท์, “แฮกเกอร์ (Hacker) คือใคร ?,” สรรพากรสาส์น (กุมภาพันธ์ 2546): น.63-77.

[34] นอกจากนี้ยังมีการจัดแบ่งประเภทแฮกเกอร์อีกกลุ่มหนึ่ง คือ กลุ่มแฮกเกอร์หมวกเหลือง (yellow hat hacker) ซึ่งเป็นกลุ่มแฮกเกอร์ที่ทำเพื่อเงินเท่านั้น ไม่ว่าจะเป็นการรับจ้างเจาะระบบหรือแม้กระทั่งขายวิธีการในการเจาะระบบคอมพิวเตอร์ของหน่วยงานต่าง ๆ โปรดดูรายละเอียดใน จีระศักดิ์ ศรีรัตน์, “Hacker Hunting ตามล่าอาชญากรบนโลกไซเบอร์,” COMPUTER.TODAY ฉบับที่ 256 (กุมภาพันธ์ 2548): น.71-75.

ของความรู้ ทักษะและประสบการณ์เฉพาะด้านของแฮกเกอร์คนนั้น ด้วยเหตุนี้ผู้ที่ทำการศึกษาและวิจัยเกี่ยวกับพฤติกรรมอาชญากรรมของแฮกเกอร์หลายท่านจึงนำเอาระดับทักษะของแฮกเกอร์มาเป็นหลักเกณฑ์ในการกำหนดกรอบในการจัดแบ่งประเภทของแฮกเกอร์ โดยจำแนกจากกลุ่มที่มีทักษะความรู้น้อยไปจนถึงกลุ่มที่มีความรู้ความเชี่ยวชาญสูง จากการศึกษาของผู้เขียนพบว่า การจำแนกประเภทของแฮกเกอร์ในลักษณะเช่นนี้ได้มีการศึกษาและจัดแบ่งประเภทไว้ดังต่อไปนี้[35]

Landreth[36] แบ่งออกเป็น 6 ประเภท ได้แก่

1. novice เป็นพวกที่มีประสบการณ์และความรู้ทางคอมพิวเตอร์น้อยที่สุด มักจะสร้างความเดือดร้อนเล็กๆ น้อยๆ

2. student เป็นพวกนักเรียนนักศึกษาที่สนใจในการสำรวจระบบคอมพิวเตอร์ของบุคคลอื่นมากกว่าที่จะมาสนใจเรื่องการเรียนของตนเอง

3. tourist พวกนี้รู้สึกว่าการเจาะระบบคอมพิวเตอร์เป็นการผจญภัย โดยมีความรู้สึกตื่นเต้น (thrill) เป็นรางวัลในการเจาะระบบคอมพิวเตอร์

4. crasher เป็นพวกแฮกเกอร์ที่เป็นภัย โดยมีเจตนาสร้างความเสียหายให้แก่ข้อมูลและระบบคอมพิวเตอร์

5. thief เป็นพวกแฮกเกอร์ที่พบน้อยที่สุด โดยเป็นพวกที่แสวงหากำไรจากการเจาะระบบคอมพิวเตอร์และจัดเป็นพวกที่มีความเชี่ยวชาญทางด้านคอมพิวเตอร์มากที่สุด

Hollinger[37] จัดแบ่งออกเป็น 3 ประเภท ได้แก่

1. pirate เป็นพวกที่มีความรู้ความเชี่ยวชาญต่ำที่สุด และมักจะกระทำความผิดโดยการละเมิดลิขสิทธิ์ (piracy[38])

---

[35] Marc Rogers, “Doctoral Thesis: A Social Learning Theory and Moral Disengagment Analysis of Criminal Computer Behavior: An Exploratory Study - Rogers 2001,” <http://homes.cerias.purdue.edu/~mkr/cybercrime-thesis.pdf>

[36] *Ibid.*

[37] *Ibid.*

2. browser เป็นพวกที่มีความรู้ความเชี่ยวชาญอยู่ในระดับกลาง สามารถเจาะระบบคอมพิวเตอร์และเข้าถึงข้อมูลของผู้อื่นได้ แต่พวกเขามักจะไม่ทำลายหรือคัดลอกไฟล์ข้อมูลจากเครื่องคอมพิวเตอร์ของคนอื่น

3. cracker เป็นแฮกเกอร์ที่มีความรู้ความสามารถมากที่สุด ส่วนใหญ่จะก่อความเสียหายอย่างร้ายแรง เช่น คัดลอกหรือทำลายข้อมูลคอมพิวเตอร์ของบุคคลอื่น

Chantler[39] จัดแบ่งออกเป็น 3 ประเภท ได้แก่

1. elite group เป็นผู้ที่มีความรู้ความสามารถอยู่ในระดับสูง มีแรงจูงใจ คือ ความปรารถนาเพื่อให้ได้มาซึ่งสิ่งที่ตนต้องการ, ต้องการสำรวจระบบคอมพิวเตอร์ของคนอื่น รวมทั้งความตื่นเต้นและความท้าทาย

2. neophyte เป็นพวกที่มีความรู้ในระดับปานกลาง ส่วนใหญ่อยู่ในขั้นกำลังเรียนรู้เพื่อก้าวเข้าสู่ขั้น elite group ต่อไปในอนาคต

3. loser และ lamer เป็นกลุ่มที่มีความรู้น้อยมาก โดยพวกเขาจะมีแรงจูงใจ คือ ความปรารถนาเพื่อผลกำไร, การแก้แค้น, การจารกรรม ฯลฯ

นอกจากนี้ Chantler ยังได้ให้ข้อมูลด้วยว่า ในสังคมของแฮกเกอร์นั้น ประกอบด้วย elite group ประมาณร้อยละ 30 กลุ่ม neophyte ประมาณร้อยละ 60 และกลุ่ม loser และ lamer ประมาณร้อยละ 10

Power[40] จัดแบ่งออกเป็น 3 ประเภท ได้แก่

---

[38] piracy หรือ software piracy เป็นการใช้งาน สำเนาหรือแจกจ่ายซอฟต์แวร์โดยผิดกฎหมาย รวมถึงการที่ซอฟต์แวร์บางตัวอาจกำหนดให้ผู้ใช้ติดตั้งได้แค่ครั้งเดียว หรือติดตั้งได้แค่บนคอมพิวเตอร์เครื่องเดียว หากใช้เกินจำนวนเครื่องที่ระบุก็ถือว่ากระทำผิดกฎหมายเช่นเดียวกัน (วิโรจน์ ชัยมูลและคณะ, 2548, น.298.) ในวงการคอมพิวเตอร์เรียกกระบวนการในการละเมิดสิทธิ์ดังกล่าวว่า การแคร็กโปรแกรม โปรดดูรายละเอียดเพิ่มเติมใน Rigistry Xpert, “แคร็กยกกำลัง3 ต่ออายุโปรแกรมทดลองใช้ให้ใช้งานได้ตลอดไป,” PC Today ฉบับที่ 24 (เมษายน 2549): น.46 - 57.

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

[40] *Ibid.*

1. sport intruder เป็นพวกแฮกเกอร์ในระบบอินเทอร์เน็ตที่เจาะเข้าไปในระบบคอมพิวเตอร์หรือเปลี่ยนหน้าเว็บไซต์ต่างๆหรือกระทำการก่อให้เกิดความเสียหายอย่างอื่น

2. competitive intelligence เป็นพวกแฮกเกอร์ที่มีคุณธรรมโดยหลีกเลี่ยงการกระทำที่ผิดกฎหมาย

3. foreign intelligence เป็นพวกกลุ่มที่มีเป้าหมาย คือ ความปลอดภัยของชาติ หรือผลประโยชน์ในทางเศรษฐกิจ ส่วนมากมักจะเป็นเงินของประเทศอื่น

Parker[41] จัดแบ่งออกเป็น 7 ประเภท ได้แก่

1. prankster เป็นแฮกเกอร์ที่เข้าถึงระบบคอมพิวเตอร์ของคนอื่นโดยไม่ได้มีเจตนาก่อความเสียหายอย่างถาวร

2. hackster เป็นแฮกเกอร์ตามความหมายเดียวกับคำนิยามที่ให้ไว้โดย Levy กล่าวคือ แฮกเกอร์ในยุคแรกๆ มักจะสำรวจระบบคอมพิวเตอร์ของบุคคลอื่นเพื่อการศึกษา ความอยากรู้อยากเห็น การแข่งขัน หรือเพื่อความยุติธรรมในสังคม (social justice)

3. malicious hacker เป็นแฮกเกอร์ตามความหมายเดียวกันกับคำว่า “แครกเกอร์” (cracker) โดยกลุ่มนี้จะเป็นพวกที่มีเจตนาก่อให้เกิดความเสียหายแก่ระบบหรือข้อมูลคอมพิวเตอร์ของผู้อื่น ตัวอย่างในกลุ่มนี้ ได้แก่ ผู้สร้างไวรัสคอมพิวเตอร์

4. personal problem solver เป็นพวกที่อาศัยปัญหาของระบบคอมพิวเตอร์ (ช่องโหว่) ในการก่ออาชญากรรม โดยพวกเขาเห็นว่า อาชญากรรมคอมพิวเตอร์ เป็นวิธีที่ง่ายและรวดเร็วในการแก้ปัญหาเหล่านี้ จากการวิจัยของ Parker พบว่ากลุ่มนี้เป็นรูปแบบที่พบได้มากที่สุด

5. career criminals เป็นกลุ่มที่มีส่วนเกี่ยวข้องกับพฤติกรรมของอาชญากร บางคนมีงานอื่นทำไปด้วย บางคนเข้าไปมีส่วนเกี่ยวข้องกับองค์กรอาชญากรรม

6. extreme advocate กลุ่มนี้เป็นพวกผู้ก่อการร้าย โดยเป็นกลุ่มที่มีมุมมองทางสังคม ทางการเมืองและทางศาสนาที่รุนแรง พวกเขาจะพยายามเปลี่ยนเงื่อนไขต่างๆ โดยการก่ออาชญากรรม

7. malcontent, addict, และ irrational และ incompetent people กลุ่มนี้เป็นกลุ่มที่อธิบายยากที่สุด ทั้งยังป้องกันได้ยาก เนื่องจากมีลักษณะอาการป่วยทางจิต (mentally ill) ลักษณะที่เกี่ยวข้องทางเคมีและความประมาทในการก่ออาชญากรรม

---

[41] *Ibid.*

Rogers[42] แบ่งประเภทของแฮกเกอร์ โดยจัดแบ่งตามทักษะทางด้านคอมพิวเตอร์ เป็น 7 ประเภท ได้แก่ Novice (Newbies / Script Kiddies), Cyber-punks, Insiders, Coders, Old Guard, Professionals และ Cyber-Terrorists

ตารางที่ 2.1

การจำแนกประเภทของแฮกเกอร์โดย Rogers[43]

ประเภทของแฮกเกอร์	คุณลักษณะ
1. Novice (Newbies / Script Kiddies)	- มีทักษะด้านคอมพิวเตอร์น้อยมาก - เป็นมือใหม่ - ต้องอาศัยโปรแกรมแฮก (hack tool) ที่มีแพร่หลายในอินเทอร์เน็ต - มักจะก่อความเดือดร้อนด้วยวิธีการโจมตีแบบ DOS[44] (Denial of Service) - สามารถก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ได้อย่างใหญ่หลวงทั้งๆที่พวกเขายังไม่มีความเข้าใจเลยว่าการโจมตีเช่นนั้นมีการทำงานอย่างไร - การกระทำของกลุ่มนี้อยู่ในความสนใจของสื่อมวลชน
2. Cyber-punks	- มีทักษะด้านคอมพิวเตอร์เป็นอย่างดี - แต่ความรู้ในด้านโปรแกรม (Programming) มีค่อนข้างน้อย - มีความเข้าใจในเรื่องการทำงานของการโจมตีเป็นอย่างดี - มีเจตนาของอาชญากร (Criminal Intent) หรือพฤติกรรมมุ่งร้าย (malicious behavior), ฉ้อโกงบัตรเครดิต (credit frauds) ฯลฯ - การกระทำของกลุ่มนี้อยู่ในความสนใจของสื่อมวลชน

[42] Marc Rogers, “A New Hacker Taxonomy,” <http://homes.cerias.purdue.edu/~mkr/hacker.doc>

[43] *Ibid.*

[44] “รูปแบบการโจมตีแบบ Denial of Service ในอดีตและแนวโน้มในอนาคต,” <http://www.thaicert.nectec.or.th/paper/DoS.php>, 28 ธันวาคม 2544.

3. Insiders	- เป็นผู้ที่ศึกษาทางด้านคอมพิวเตอร์มาโดยเฉพาะหรือศึกษาในสาขาวิชาที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ - มักจะปรากฏในรูปแบบของลูกจ้างที่ไม่พอใจนายจ้างหรือหน่วยงานที่ตนสังกัดอยู่ (Disgruntled employee) หรืออดีตลูกจ้างที่โดนไล่ออก (Ex-employee) - สามารถปฏิบัติการโจมตีระบบคอมพิวเตอร์ของหน่วยงานนั้นๆ ได้โดยง่ายเนื่องจากมีอภิสิทธิ์เหนือระบบคอมพิวเตอร์ของหน่วยงานซึ่งตนมีหน้าที่รับผิดชอบ - เป็นปัญหาด้านระบบความปลอดภัยของคอมพิวเตอร์ที่ใหญ่ที่สุด คือ ประมาณ 70-80% ของปัญหาที่เกิดขึ้นทั้งหมด
4. Coders	- เป็นผู้มีทักษะทางด้านเทคนิคเป็นอย่างดี - สามารถเขียนสคริปต์ หรือชุดคำสั่งและเขียนโปรแกรมเจาะระบบได้ - มักจะทำตัวเป็นที่ปรึกษา (mentor) ให้แก่พวกมือใหม่ (newbies) - มีแรงจูงใจเพื่ออำนาจและชื่อเสียง - มักจะเป็นที่เคารพยกย่อง (revered) - มีการโจมตีที่อันตราย เช่น การแฝงตัวอยู่ในระบบคอมพิวเตอร์, การใช้ม้าโทรจัน (Trojan Horse) ฯลฯ
5. Old Guard	- ไม่มีเจตนาของอาชญากร - เป็นพวกที่ทำประโยชน์มากกว่าก่อความเสียหาย เหมือนเช่นแฮกเกอร์ในยุคแรกๆ - คอยดูแลช่องโหว่ของระบบคอมพิวเตอร์ เมื่อพบแล้วจะแจ้งให้เจ้าของทราบทันที - เป็นผู้ให้คำปรึกษา - คอยปกป้อง ต่อต้านและจำกัดมุมมองที่ไม่ดีของสังคมแฮกเกอร์ (hacker community)
6. Professionals	- เป็นพวกอาชญากร (criminal), หัวขโมย (Thieves) - เป็นพวกกลุ่มจารกรรม (corporate espionage) - เป็นพวกรับจ้างเจาะระบบ

	- มีแรงจูงใจสูง มีการฝึกฝนมาเป็นอย่างดี - มีข้อมูลเกี่ยวกับกลุ่มนี้น้อยมาก
7. Cyber-Terrorists	- กลุ่มนี้มักจะมีกองทุนสนับสนุนเป็นอย่างดี - มีแรงจูงใจสูง - มักจะรวมเอาลัทธิความเชื่อทางการเมืองกับพฤติกรรมอาชญากรไว้ด้วยกัน - ก่อสงครามทางสารสนเทศ (Information Warfare) - มีข้อมูลในส่วนนี้น้อยมาก

จากข้อมูลเท่าที่มีอยู่พบว่า cyber-punks มีลักษณะโดยทั่วไป คือ เป็นคนผิวขาว (Caucasian) อายุระหว่าง 12-30 ปี ครอบครัวอยู่ในระดับชนชั้นกลาง ชอบอยู่ตัวคนเดียว จึงทำให้มีปัญหาในการปรับตัวเข้ากับสังคมหรือกับบุคคลอื่น ที่สำคัญพวกเขามีพรสวรรค์ในด้านคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ[45] นอกจากนี้ยังปรากฏข้อมูลเพิ่มเติมว่าลักษณะพิเศษของคนที่เป็นแฮกเกอร์ คือ มักจะเป็นเพศชาย อายุน้อย และไม่ยากจน เนื่องจากพวกนี้มักจะมีเงินซื้อตำรา ซื้อคอมพิวเตอร์และซอฟต์แวร์ ซึ่งต่างจากอาชญากรปกติที่ส่วนใหญ่จะยากจน จนต้องประกอบอาชญากรรม นอกจากนี้ยังมีความฉลาดหลักแหลม มีความพยายามและความอดทนสูง สามารถทำงานติดต่อกันครั้งละนาน ๆ โดยไม่ลุกไปไหน มีความหยิ่งยโสโอหัง คิดว่าตัวเองเก่งเหนือกว่าคนอื่น มักเป็นนักสะสมข้อมูลข่าวสารต่าง ๆ มักเป็นผู้ที่ไม่ค่อยมีความรับผิดชอบต่อการกระทำของตนเอง มักไม่ค่อยมีมนุษย์สัมพันธ์ ไม่มีระเบียบ มักง่าย อาจเป็นเพราะมัวแต่คิดหมกมุ่นเรื่องการเจาะระบบ[46]

ภาพของแฮกเกอร์ที่ปรากฏตามสื่อต่างๆ พบว่าแตกต่างไปจากผลการศึกษานี้ กล่าวคือ ปรากฏว่ามีลักษณะต่อต้านทางสังคม (sociopath) หรืออาการป่วยทางจิต (psychopath) น้อยมาก โดยสังคมขนาดใหญ่ของแฮกเกอร์จะประกอบด้วยกลุ่ม (group) หรือชมรม (club) จำนวนมาก นอกจากนี้ยังมีการจัดการประชุมประจำปีเพื่ออภิปรายเกี่ยวกับการเจาะระบบคอมพิวเตอร์ รวมทั้งการบังคับใช้กฎหมายที่จะส่งผลกระทบต่อการเจาะระบบของพวกเขา ส่วนช่องทางในการ

---

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

[46] ญาณพล ยั่งยืน และ ศรีดา ตันทะอธิพานิช, <u>อินเทอร์เน็ตเข้าใจง่าย</u>, (กรุงเทพมหานคร: เอทีเอ็นโปรดักชั่น, 2546), น.47-50.

ติดต่อสื่อสารทางอิเล็กทรอนิกส์ กลุ่มแฮกเกอร์จะติดต่อโดยผ่านทางกลุ่มข่าว (newsgroup) ห้องสนทนา (chat channel) และนิตยสาร เช่น 2600 (www.2600.com) เป็นต้น[47]

พวก cyber-punks มักจะชอบคุยโวเกี่ยวกับผลงานการเจาะระบบคอมพิวเตอร์ของตนต่อกลุ่มเพื่อนแฮกเกอร์คนอื่นๆ และการคุยโวเหล่านี้มักจะนำมาสู่การดำเนินการทางคดี แต่อย่างไรก็ตามพวกเขายังคุยโวในความสามารถของตนต่อไปแม้ในขณะที่ถูกคุมขังและในระหว่างการสัมภาษณ์ของเจ้าหน้าที่[48]

จากผลการวิจัยของ Post พวกแฮกเกอร์อ้างว่า แรงจูงใจของพวกเขา คือ ความท้าทาย ความตื่นเต้นในความสำเร็จและความต้องการเรียนรู้ความพึงพอใจในทางสติปัญญาของตน (intellectual satisfaction) ซึ่งเหล่านี้ดูเหมือนกับแรงจูงใจของแฮกเกอร์ในยุคสมัยแรกๆ แต่อย่างไรก็ตามบางคนอ้างว่า แรงจูงใจของพวกเขารวมถึงความอาฆาตพยาบาท (vengeance) ความต้องการก่อกวน ก่อวินาศกรรม (sabotage) และต้องการฉ้อโกงด้วย นอกจากนี้จากการศึกษากลุ่ม cyber-punks พบว่า มีลักษณะที่ปรากฏว่าได้รับอิทธิพลมาจากสื่อ มีแรงจูงใจในการกระทำเกิดมาจากความละโมบ (greed) ความต้องการแก้แค้น (revenge) ความมุ่งร้าย (maliciousness) และต้องการอำนาจ (power) แม้ว่าบางส่วนจะอ้างว่าเกิดจากอาการทางจิตที่เสพติดการเจาะระบบคอมพิวเตอร์ของบุคคลอื่น (psychological addiction to hacking) ด้วยก็ตาม แต่ข้อเท็จจริงในเรื่องนี้ยังไม่มีผลการศึกษามาสนับสนุน[49]

3. <u>การจำแนกตามแรงจูงใจของแฮกเกอร์</u>

นอกจากการจัดแบ่งจำแนกประเภทของแฮกเกอร์ตามเจตนาและระดับความเชี่ยวชาญในการกระทำความผิดตามกรณีดังได้กล่าวไว้ในข้างต้นแล้ว ยังมีการจัดแบ่งแฮกเกอร์ในฐานะรูปแบบหนึ่งของอาชญากรคอมพิวเตอร์ (computer criminal) โดยมีการจำแนกประเภทของ

---

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

[48] *Ibid.*

[49] *Ibid.*

อาชญากรคอมพิวเตอร์ตามลักษณะของแรงจูงใจในการกระทำความผิดออกเป็น 3 ประเภท[50] ได้แก่

1. แครกเกอร์ (Cracker)[51]
2. อาชญากร (Criminal)
3. พวกชอบทำลาย (Vandal)

แม้ว่าการจำแนกประเภททั้งสามประเภทจะมีลักษณะบางอย่างที่คล้าย ๆ กัน แต่อย่างไรก็ตามการจำแนกประเภทตามแรงจูงใจในลักษณะนี้ต้องการที่จะเน้นไปที่แรงจูงใจหลักที่แตกต่างกัน กล่าวคือ แรงจูงใจหลักของกลุ่มแครกเกอร์ คือ การเข้าถึง (access) ระบบหรือข้อมูลคอมพิวเตอร์ แรงจูงใจหลักของกลุ่มอาชญากร ได้แก่ ผลกำไรหรือผลประโยชน์ทางการเงิน ส่วนแรงจูงใจของกลุ่มพวกชอบทำลาย คือ การทำลาย[52]

ประเภทแรก แครกเกอร์ (Cracker) แม้ว่านักเจาะระบบคอมพิวเตอร์ทั้งสามประเภทดังกล่าวข้างต้น อาจมีพฤติกรรมในการเจาะระบบ (cracking) แต่สำหรับแครกเกอร์จัดเป็นกลุ่มที่มีลักษณะเฉพาะแตกต่างกันออกไป คือ มีแรงจูงใจจากความท้าทายทางสติปัญญา (intellectual challenge) โดยพวกเขามักจะออกปฏิบัติการในช่วงเวลากลางคืน เนื่องจากในตอนกลางวันพวกเขาต้องเรียนหนังสือหรือต้องทำงานที่มีความตื่นเต้นน้อยกว่าการเจาะระบบ แต่อย่างไรก็ตามแม้พวกเขาจะปฏิบัติการในตอนกลางคืน แต่สามารถเข้าถึงระบบคอมพิวเตอร์ในแต่ละเขตเวลาของโลก (time zone) ได้[53]

นักเจาะระบบคอมพิวเตอร์ หรือ แครกเกอร์หลายคนเป็นเด็กวัยรุ่น ถึงแม้ว่าพวกเขาจะมีอายุน้อย แต่พวกเขากลับสามารถเข้าถึงระบบคอมพิวเตอร์ทุกระบบได้อย่างสบาย อาทิ ระบบ

---

[50] David Icove, Karl Seger and William VonStorch, Computer Crime : A Crimefighter's Handbook, (United States of America : O'Reilly & Associates, 1995), pp.61-69.

[51] ความหมายของคำว่า "แครกเกอร์" ในที่นี้ คือ บุคคลที่เข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ซึ่งตรงกับความหมายเดียวกับคำว่า "แฮกเกอร์" ตามที่สื่อนำมาใช้อย่างผิดเพี้ยนไป ซึ่งโดยความจริงแล้วแฮกเกอร์ คือ โปรแกรมเมอร์ผู้มีพรสวรรค์ด้านคอมพิวเตอร์และกระทำการโดยชอบด้วยกฎหมาย

[52] David Icove, Karl Seger and William VonStorch, *supra note* 50, pp.61-62.

[53] *Ibid*, pp.62-63.

คอมพิวเตอร์ของธนาคาร บริษัทต่าง ๆ รวมถึงระบบคอมพิวเตอร์ทางทหารด้วย นอกจากนี้อาจพบว่าแครกเกอร์อาจมีการกระทำเป็นกลุ่ม แต่ส่วนมากแล้วมักจะกระทำโดยลำพังเพียงคนเดียว แม้ว่าพวกแครกเกอร์จะเป็นเด็กที่มีสติปัญญาที่ชาญฉลาดในโลกอิเล็กทรอนิกส์ แต่ในโรงเรียนกลับตรงกันข้าม พวกเขาจึงมีเพื่อนน้อยมาก เว้นแต่กลุ่มเพื่อนแครกเกอร์ด้วยกันเอง ด้วยเหตุนี้การปฏิสัมพันธ์มักจะเป็นไปในลักษณะของการสื่อสารผ่านทางกระดานข่าวในโลกอินเทอร์เน็ตมากกว่าในโลกของความเป็นจริง[54]

แรงจูงใจของแครกเกอร์ คือ ผลประโยชน์ส่วนตัว (personal gain) หรือค้นหาความท้ายทายทางสติปัญญาหรือหนทางในการโจมตีระบบ โดยการกระทำของพวกเขาเสมือนได้แสร้งเป็นผู้กระทำการอย่างโรบินฮู้ด[55] ผู้ต่อสู้เพื่อความถูกต้อง ยุติธรรมและเสรีภาพ ทั้งนี้กลุ่มของแครกเกอร์มีแนวโน้มที่ไม่เป็นทางการมากยิ่งขึ้น กล่าวคือ มีการรวมกลุ่มเพื่ออภิปรายหรือทำงานร่วมกัน โดยใน ปี ค.ศ. 1990 มีการจัดการประชุมนานาชาติของกลุ่มแครกเกอร์ในยุโรป แครกเกอร์จากทั่วทุกมุมโลกต่างเข้าร่วมเพื่อแลกเปลี่ยนแนวความคิด เรียนรู้วิธีการเจาะระบบคอมพิวเตอร์ในประเทศอื่น และฝึกฝนทักษะของตนเอง นับตั้งแต่นั้นเป็นต้นมา ได้มีการจัดการประชุมแครกเกอร์ในประเทศสหรัฐอเมริกาและในประเทศอื่น ๆ ปัจจุบันแครกเกอร์หลายคนได้ก้าวเข้าสู่อาชีพนี้อย่างเต็มตัว โดยการรับจ้างเจาะระบบคอมพิวเตอร์ตามความต้องการของผู้ว่าจ้าง หรือผู้ที่ให้ราคาประมูล (bidder) สูงสุด การขโมยข้อมูลสารสนเทศไม่ว่าจะเป็นของบริษัทคู่แข่งทางการค้า หรือ

---

[54] *Ibid.*

[55] Robin Hood of the Balkans ในปี 1998 แฮกเกอร์ชาวยุโรปที่เรียกตัวเองว่า “Eastern Prowler” เจาะเข้าไปในระบบของแก๊งค์อาชญากรรมในบัลกาเรียและโรมาเนีย และได้เก็บบันทึกข้อมูลทางการเงินต่างๆ ของแก๊งค์ดังกล่าวแล้วส่งไปให้อัยการในเมืองนั้นๆ นอกจากนี้เขายังได้ขโมยเงินกว่า 3.2 ล้านเหรียญสหรัฐมาจากแก๊งค์ดังกล่าวและแจกจ่ายเงินจำนวนดังกล่าวให้กับองค์กรการกุศลสำหรับเด็กในประเทศโรมาเนียและบัลกาเรีย ด้วยการโอนเงินผ่านทางธนาคารโดยใช้หมายเลขบัญชีมากกว่า 17 หมายเลข ซึ่งทำให้ไม่มีใครสามารถตามรอยเขาได้ ในเวลาต่อมาเขาจึงถูกขนานนามว่าเป็น Robin Hood of the Balkans โดยที่เขาได้มีส่วนในการแกะรอยและจับกุมแก๊งค์ต่างๆ มากกว่า 37 แก๊งค์ ไม่ว่าจะเป็นแก๊งค์ที่หาเงินโดยผิดกฎหมาย แก๊งค์ลักพาตัว แก๊งค์ขนของหนีภาษี รวมถึงพวกนักฆ่าอีกด้วย ข้อมูลจาก Golden IT, “เจาะตำนาน 10 สุดยอดแฮคเกอร์(อัจฉริยะหรือผู้ร้ายที่ต้องปราบ),” อีซี่คอม 8(มิถุนายน 2548): น.93-95.

ข้อมูลทางการทหารของศัตรู หรือแม้กระทั่งหมายเลขบัตรเครดิต บัตรโทรศัพท์ ได้กลายเป็นตลาดทางธุรกิจขนาดใหญ่ในสังคมของแครกเกอร์[56]

ประเภทที่สอง อาชญากรคอมพิวเตอร์ (Computer Criminal) แม้ว่านักเจาะระบบทั้งสามประเภท อาจจัดอยู่ในกลุ่มพวกอาชญากรได้เช่นเดียวกัน แต่รูปแบบของอาชญากรในประเภทนี้จะจำกัดพฤติกรรมอาชญากรใน 2 ลักษณะ คือ การจารกรรม (espionage) และ การฉ้อโกงและใช้คอมพิวเตอร์ในทางที่ผิด (fraud and abuse)[57]

การจารกรรมทางคอมพิวเตอร์ ส่วนใหญ่มักจะเป็นการขโมยข้อมูลสารสนเทศอันเป็นความลับของชาติหรือความลับในทางการค้า ทั้งนี้อาจจะรวมถึงการกระทำของสายลับต่างชาติและคู่สัญญาที่ขโมยความลับของคู่แข่งหรือฝ่ายตรงกันข้าม หรืออาชญากรที่ขโมยข้อมูลหรือข่าวสารจากคอมพิวเตอร์ของหน่วยงานบังคับใช้กฎหมาย ส่วนการฉ้อโกงและการใช้คอมพิวเตอร์ในทางที่ผิดนั้น เป็นปัญหาใหญ่ในวงการธุรกิจและอุตสาหกรรม ไม่ว่าจะเป็นอาชญากรหรือองค์กรอาชญากรรมต่างเปลี่ยนรูปแบบและวิธีการกระทำความผิดโดยนำเอาเทคโนโลยีทางคอมพิวเตอร์เข้ามามีส่วนช่วยมากยิ่งขึ้น เช่น การฟอกเงินที่ได้จากการค้ายาเสพติด การฉ้อโกงเงินจำนวนมากโดยใช้คอมพิวเตอร์เป็นเครื่องมือ เป็นต้น[58]

ประเภทสุดท้าย คือ พวกชอบทำลาย (vandal) นักเจาะระบบในประเภทพวกชอบทำลายนี้มักจะไม่ได้ก่ออาชญากรรมด้วยแรงจูงใจหรือแรงกระตุ้นทางสติปัญญาเหมือนเช่นในประเภทแครกเกอร์ รวมทั้งไม่มีแรงจูงใจทางการเงินหรือทางการเมืองเหมือนเช่นประเภทอาชญากร แต่พวกชอบทำลายนี้มักจะมีแรงจูงใจอันเนื่องมาจากความโกรธแค้น โดยสามารถจำแนกกลุ่มนี้ออกเป็น 2 กลุ่ม คือ ผู้ใช้ (user) หรือคนในองค์กรที่มีอำนาจในการใช้ระบบคอมพิวเตอร์ขององค์กรนั้น ๆ แต่กระทำความผิดโดยเข้าถึงส่วนอภิสิทธิ์ (root หรือ superuser) ซึ่งไม่มีอำนาจ อีกประเภทหนึ่ง คือ คนนอกองค์กร (stranger) ซึ่งเป็นผู้ที่ไม่มีอำนาจในการใช้ระบบคอมพิวเตอร์ขององค์กรไม่ว่ากรณีใด ๆ ก็ตาม[59]

นักเจาะระบบในรูปแบบของคนในองค์กร มักจะเป็นลูกจ้างที่พยายามหาทางเข้าถึงระบบคอมพิวเตอร์ในส่วนที่ตนไม่มีอำนาจ เพื่อที่จะขยายอภิสิทธิ์ในการจัดการต่อระบบ

---

[56] David Icove, Karl Seger and William VonStorch, *supra note* 50, p.63.

[57] *Ibid*, p.63.

[58] *Ibid*, pp.63-64.

[59] *Ibid*, p.64.

คอมพิวเตอร์ขององค์กร สามารถที่จะเข้าถึงข้อมูลสำคัญ ๆ เช่น ข้อมูลการจ่ายเงินเดือน ข้อมูลรหัสผ่านของพนักงาน เป็นต้น ทั้งนี้อาจจะได้รับแรงจูงใจอันเนื่องมาจากการถูกไล่ออก ถูกตัดเงินเดือนหรือถูกนายจ้างต่อว่า จึงต้องการที่จะแก้แค้นองค์กรหรือนายจ้างโดยใช้ความสามารถของตนทำลาย แก้ไขเปลี่ยนแปลงระบบคอมพิวเตอร์หรือขโมยข้อมูลสำคัญขององค์กรนั้น ๆ ไปขายให้แก่คู่แข่งทางการค้า[60]

ส่วนนักเจาะระบบในรูปแบบคนนอกองค์กร มักมีลักษณะที่ใกล้เคียงกับประเภทแครกเกอร์หรือประเภทอาชญากร แต่ต่างกันในแง่ของแรงจูงใจที่มุ่งทำลายและก่อความเสียหายแก่ระบบคอมพิวเตอร์ของเป้าหมายเป็นหลัก ทั้งนี้มีวิธีการที่หลากหลาย อาทิ การสวมรอย (masquerading) เป็นคนในองค์กร หรืออาจใช้เครื่องมือดักจับรหัสผ่าน (password sniffer) รวมถึงการข่มขู่บังคับหรือติดสินบนพนักงานในองค์กรนั้น ๆ ด้วย[61]

การจำแนกประเภทดังกล่าวข้างต้นนี้ ยังมีการอธิบายถึงคุณลักษณะของอาชญากรคอมพิวเตอร์ในแต่ละประเภท โดยเรียกว่า “The Computer Crime Adversarial Matrix” ซึ่งใช้เป็นเครื่องมือในการสืบสวนเจ้าหน้าที่เอฟบีไอ โดยได้มีการจำแนกคุณลักษณะในแต่ละประเภทออกเป็น 4 คุณลักษณะ[62] ได้แก่

1. คุณลักษณะด้านองค์กร (Organization Characteristics)
2. คุณลักษณะด้านการปฏิบัติการ (Operational Characteristics)
3. คุณลักษณะด้านพฤติกรรม (Behavioral Characteristics)
4. คุณลักษณะด้านแหล่งข้อมูล (Resource Characteristics)

คุณลักษณะด้านองค์กร จะอธิบายถึงการก่อตั้งของกลุ่มอาชญากรคอมพิวเตอร์ในแง่ของโครงสร้างของกลุ่ม (organization) แรงจูงใจในการเข้าร่วมกลุ่ม (recruitment/attraction) รวมถึงรูปแบบการปฏิบัติการของกลุ่มว่ามีจุดเกาะเกี่ยวในทางระหว่างประเทศ (international connections) หรือไม่ เพียงใด[63]

---

[60] *Ibid.*

[61] *Ibid.*

[62] *Ibid*, pp.65-69.

[63] *Ibid*, p.65.

คุณลักษณะด้านการปฏิบัติการ จะอธิบายถึงวิธีการก่ออาชญากรรมคอมพิวเตอร์ว่า มีการวางแผน (planning) อย่างละเอียดรอบคอบก่อนลงมือหรือไม่ มีระดับความเชี่ยวชาญในการก่ออาชญากรรมแค่ไหน (Level of Expertise) รวมถึงมีกลยุทธ์และวิธีการในการก่ออาชญากรรมคอมพิวเตอร์อย่างไรบ้าง (tactics/method used)[64]

คุณลักษณะด้านพฤติกรรม จะอธิบายถึงแรงจูงใจ (motivation) ของอาชญากรคอมพิวเตอร์ในแต่ละประเภท รวมถึงลักษณะของอาชญากรคอมพิวเตอร์ (personal characteristics) และจุดอ่อน (weakness) ในการก่ออาชญากรรมซึ่งอาจทำให้สามารถสืบสวนหาตัวอาชญากรคอมพิวเตอร์ได้[65]

คุณลักษณะด้านแหล่งข้อมูล เป็นการอธิบายถึงการฝึกฝนทักษะ (training skills) ในการก่ออาชญากรรมคอมพิวเตอร์ของอาชญากรคอมพิวเตอร์ในแต่ละประเภท อุปกรณ์หรือเครื่องมือขั้นต่ำที่จำเป็นต้องใช้ในการก่ออาชญากรรมคอมพิวเตอร์ (minimum equipment required) และบุคคลหรือองค์กรที่ให้การสนับสนุนในการก่ออาชญากรรมคอมพิวเตอร์ (support structure)[66]

---

[64] *Ibid*, p.66.

[65] *Ibid*, pp.66-67.

[66] *Ibid*, p.67.