การประยุกต์ใช้การจัดทำเค้าร่างของอาชญากรกับการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ กรณีศึกษาการปลอมแปลงเว็บไซต์วารสารทางวิชาการ

Criminal Profiling as a Tool to Investigate Cybercrime : Hijacked Academic Journals' Websites and Fake Publishers

เบญญาภา มารินทร์ [1]

▣ บทนำ

ปัญหาอาชญากรรมในสังคมปัจจุบันมีหลายรูปแบบ ยิ่งโลกมีความเจริญก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยีมากขึ้นเท่าใด ก็ส่งผลให้การก่ออาชญากรรมมีความสลับซับซ้อนมากขึ้นเท่านั้น ปัญหาอาชญากรรมประเภทหนึ่งที่มีจำนวนมากและทวีความรุนแรงเพิ่มมากขึ้น ควบคู่ไปกับความเจริญรุดหน้าของเทคโนโลยี คือ ปัญหาอาชญากรรมทางคอมพิวเตอร์ประเภทต่าง ๆ อ้างอิงจากข้อมูลสถิติภาพรวมของอาชญากรรมทางคอมพิวเตอร์ที่รายงานโดย Symantec (บริษัทชั้นนำด้านซอฟต์แวร์ด้านความปลอดภัยคอมพิวเตอร์เป็นที่รู้จักจากผลิตภัณฑ์ ชื่อ Norton Anti Virus) เปิดเผยข้อมูลรายงานภัยคุกคามทางอินเทอร์เน็ต ทั่วโลกของปี 2557 ว่า *"เป็นปีที่พบช่องโหว่ในระบบอินเทอเน็ตมาก เพราะมีไฟล์ที่ถูกลักลอบเข้าไปในระบบเครือข่ายและคอมพิวเตอร์ส่วนบุคคล แล้วทำการกักไว้โดยการใส่รหัสเพื่อเรียกค่าไถ่ และมีการโจมตีด้วยโปรแกรมไม่พึงประสงค์มากขึ้น และส่งผลกระทบในวงกว้าง"* ข้อมูลสำคัญที่ทาง Symantec ได้เปิดเผยเพิ่มเติมว่า *"มีมัลแวร์ (Malware) ที่ถูกสร้างขึ้นมากกว่า 317 ล้านตัว หรือเกือบวันละ 1 ล้านตัว*

---

[1] *นักศึกษาปริญญาโท หลักสูตรรัฐประศาสนศาสตร์ มหาบัณฑิต สาขาอาชญาวิทยา และการบริหารงานยุติธรรม มหาวิทยาลัยรังสิต*

พบการโจมตีของไวรัสเรียกค่าไถ่ (Ransomware) มีจำนวนสูงขึ้นกว่าปีที่ผ่านมาร้อยละ 113 ขณะที่การโจมตีของไวรัสเรียกค่าไถ่แบบใส่รหัส (Crypto-ransom) เกิดขึ้นโดยมีจำนวนครั้งมากกว่าปีที่ผ่านมาสูงถึงร้อยละ 4,000" (SymantecCorporation, 2014) ดังนั้นเหยื่อของอาชญากรรมไซเบอร์จึงสามารถกระจายอยู่ทั่วโลก และอาชญากรรมประเภทนี้เหยื่อจะไม่สามารถยับยั้ง ป้องกันหรือแก้ไขได้ ยกเว้นยอมเสียข้อมูลในเครื่องคอมพิวเตอร์ที่ถูกลักลอบเข้ามาขโมยข้อมูลหรือกักไฟล์ไว้ ทำให้เกิดความเสียหายที่ไม่สามารถจะประเมินมูลค่าได้

สำหรับประเทศไทยก็พบเหตุการณ์ที่สอดคล้องกับสถานการณ์ระดับโลกเช่นเดียวกัน เมื่อข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ที่รายงานว่า "ปี 2556 มีผู้ใช้คอมพิวเตอร์ในไทยถูกโจมตีโดยมัลแวร์ที่เรียกว่า "GameOver" ซึ่งเป็นไวรัสเรียกค่าไถ่กว่า 3,000 ราย ขณะที่หน่วยงานของภาครัฐของไทยก็ตกเป็นเหยื่อของแฮกเกอร์ที่ส่งอีเมลหลอกลวงให้กดคลิกลิงค์กว่า 1,000 ครั้ง โดยระยะเวลาที่มีการส่งอีเมลหลอกลวงนั้นเพียงสองวัน แต่จากการกดคลิกลิงค์หลอกลวงนับพันครั้งนั้นส่งผลกระทบให้มีมัลแวร์ไปฝังตัวในคอมพิวเตอร์หรือบางกรณีเข้าไปล็อคไฟล์ต่าง ๆ ในหน่วยงานของรัฐที่มีการกดลิงค์ แล้วส่งอีเมล์มาเรียกค่าไถ่จากเจ้าของเครื่องคอมพิวเตอร์เพื่อให้ไฟล์ต่าง ๆ ที่เซฟไว้ในคอมพิวเตอร์ถูกปลดล็อคแล้วกลับมาใช้งานได้ตามปกติ" (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2557)

แต่ข้อมูลสถานการณ์เกี่ยวกับการก่ออาชญากรรมทางคอมพิวเตอร์ในประเทศไทยกลับแตกต่างออกไป เพราะหลังจากที่ได้มีการประกาศออกใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 สถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (2555) พบว่าประเภทของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้น สามารถจำแนกออกได้เป็น 2 ประเภทใหญ่ ๆ ด้วยกัน คือ

1. อาชญากรรมคอมพิวเตอร์ในรูปแบบดั้งเดิม ซึ่งเป็นการกระทำความผิดต่อตัวข้อมูลหรือระบบคอมพิวเตอร์โดยตรงตามมาตรา 5-13 อาทิ การเจาะระบบ การดักข้อมูล หรือการก่อวินาศกรรมคอมพิวเตอร์ด้วยการเผยแพร่โปรแกรมทำลาย

2. ความผิดที่ว่าด้วยตัวเนื้อหาของข้อมูลที่นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนสามารถเข้าถึงได้ตามมาตรา 14-16 เช่น การเผยแพร่ภาพลามก การเผยแพร่ข้อมูลที่ขัดต่อความมั่นคง หรือการหมิ่นประมาทด้วยการตัดต่อภาพ เป็นต้น (สถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์, 2555)

ลักษณะของการกระทำความผิดในประเทศไทยที่นำเสนอข้างต้นเป็นรูปแบบที่เกิดความเสียหายเฉพาะหน่วยงานหรือตัวบุคคล ส่วนใหญ่ไม่ส่งผลกระทบในวงกว้าง เช่นสถานการณ์ปัญหาที่เกิดขึ้นในระดับโลกที่ได้นำเสนอ แต่อย่างไรก็ตามข้อมูลจาก ThaiCERT ก็ได้แสดงให้เห็นถึงภัยที่กำลังเข้ามาคุกคามการใช้งานระบบคอมพิวเตอร์แบบออนไลน์ของผู้ใช้งานทุกสาขาอาชีพ และในอนาคตผู้ใช้งาน

ในประเทศไทยเองก็ย่อมหลีกเลี่ยงไม่ได้เช่นกัน

ทั้งนี้ นอกจากภัยคุกคามจากภายนอกของอาชญากรทางคอมพิวเตอร์ที่พร้อมจะโจมตีผู้ใช้ทุกคนที่มีช่องโหว่แล้ว ภัยอันน่ายำเกรงอีกประการหนึ่งของอาชญากรรมทางคอมพิวเตอร์ได้สะท้อนให้เห็นผ่านข้อมูลสถิติคดีความผิด (รวมทุกประเภทคดี) ตาม พรบ. ว่าด้วยการกระทำความผิดฯ จากกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) ปีพ.ศ. 2553-2558 (สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) สำนักงานตำรวจแห่งชาติ, 2558) ดังนี้

2553		2554		2555		2556		2557		2558	
จำนวน (คดี)	จับได้ (คดี)	จำนวน (คดี)	จับได้ (คดี)	จำนวน (คดี)	จับได้ (คดี)	จำนวน (คดี)	จับได้ (คดี)	จำนวน (คดี)	จับได้ (คดี)	จำนวน (คดี)	จับได้ (คดี)
123	25	98	34	93	23	89	36	164	44	346	120
รวมคดีที่มาแจ้งความ ปี 2553 – 2558 จำนวน 913 คดี											
รวมคดีที่สามารถจับกุมผู้ที่กระทำความผิดได้ ปี 2553 – 2558 จำนวน 282 คดี หรือ คิดเป็น ร้อยละ 30.89 ของคดีที่รับแจ้งความ											

ที่มา : กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.)

ข้อมูลจากตารางข้างต้นทำให้เห็นภาพว่าอาชญากรรมทางคอมพิวเตอร์มีการแจ้งความดำเนินคดีต่อปี จำนวนเฉลี่ย ปีละ 152 คดี ขณะที่การติดตามจับกุมผู้กระทำความผิดมาดำเนินคดี สามารถดำเนินการได้เฉลี่ยปีละ 47 คดี ขณะที่สัดส่วนของการจับกุมผู้กระทำความผิดมาดำเนินคดีได้นั้น คิดเป็นร้อยละ 30.89 เท่านั้น ทำให้เห็นได้ชัดว่าเกือบร้อยละ 70 ผู้กระทำความผิดไม่สามารถถูกติดตามตัวมารับโทษตามกฎหมายได้ ไม่ว่าด้วยเหตุผลด้านเทคนิคในการติดตามตัวผู้กระทำความผิดมาลงโทษ หรือเหตุผลอื่น

สอดคล้องกับ Wori (2014) ที่ได้เขียนบทความซึ่งสรุปให้เห็นถึงความยากในการสืบสวนสอบติดและการติดตามผู้กระทำความผิดในประเภทคดีอาชญากรรมทางคอมพิวเตอร์มาดำเนินคดี ว่าประกอบด้วย 1) สถานที่เกิดเหตุกับที่อยู่ของอาชญากรทางคอมพิวเตอร์อยู่คนละแห่ง 2) อินเตอร์เน็ตเอื้อให้ผู้กระทำผิดมีสถานะนิรนาม 3) ไม่มีพยานรู้เห็นการกระทำความผิด 4) วัน/เวลา ที่กระทำความผิด และห้วงเวลาที่พบว่าเกิดเหตุเป็นคนละเวลา ง่ายต่อการหลบซ่อน/หลบหนีหรือทำลายหลักฐาน 5) รูปแบบของหลักฐาน อยู่ในรูปแบบดิจิตัล ต้องใช้ความเชี่ยวชาญของเจ้าหน้าที่ในการรวบรวม วิเคราะห์ สืบสวน 6) การขาดหรือมีน้อยของความรู้ ความเชี่ยวชาญ และประสบการณ์ในการดำเนินคดีของเจ้าหน้าที่ และ 7) นโยบายกฎหมาย ระเบียบ ปฏิบัติของแต่ละประเทศแตกต่างกัน อาจจะส่งผลให้ไม่สามารถติดตามผู้กระทำความผิดมาดำเนินคดีได้ (Wori, 2014) ดังนั้นผู้ที่ตกเป็นเหยื่อของอาชญากรรมทาง

คอมพิวเตอร์จึงต้องตระหนักในข้อเท็จจริงนี้ และทางเดียวในการป้องกันคือไม่ทำให้ตนเองตกเป็นเหยื่อตั้งแต่แรก

ด้วยรูปแบบการกระทำผิดทางคอมพิวเตอร์ที่มีหลายรูปแบบดังที่กล่าวถึงข้างต้นนั้น ส่งผลให้เหยื่อของอาชญากรรมประเภทนี้มีหลายกลุ่มเช่นเดียวกัน แต่เหยื่อกลุ่มหนึ่งที่มีความน่าสนใจที่จะศึกษา คือ การก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบของการปลอมแปลงเว็บไซต์วารสารทางวิชาการเพื่อหลอกเอาเงินค่าธรรมเนียมในการตีพิมพ์บทความวิชาการจากนักวิชาการ/นักวิจัย ตลอดจนอาจารย์ในสถาบันอุดมศึกษาและนักศึกษาระดับบัณฑิตศึกษา ถึงแม้จะไม่พบว่ามีรายงานปัญหานี้ว่าเกิดขึ้นในประเทศไทย แต่อาชญากรรมประเภทนี้ส่งผลกระทบอย่างสูงต่อความน่าเชื่อถือของแวดวงวิชาการทั่วโลก ซึ่งรวมถึงประเทศไทยด้วย เพราะการตีพิมพ์ผลงานทางวิชาการเป็นข้อกำหนดตามนโยบายของหน่วยงานที่กำดับดูแลด้านการศึกษาของไทย เพราะเป็นตัวชี้วัดการวัดคุณภาพการศึกษาและความก้าวหน้าของการจัดการศึกษาระดับอุดมศึกษา สถานการณ์ปัญหานี้จึงอาจจะเกิดขึ้นได้กับนักวิชาการของไทย เพราะนักวิชาการไทยยังจำเป็นต้องตีพิมพ์บทความในวารสารทางวิชาการ แต่เมื่ออาชญากรทำการโจมตีไปยังวารสารทางวิชาการเหล่านั้น ย่อมส่งผลต่อความเชื่อมั่นที่มีต่อวารสารทางวิชาการ รวมถึงความถูกต้องและน่าเชื่อถือของผลการวิจัยนั้น และยังอาจจะกระทบถึงการอ้างอิงผลงานวิจัยและการต่อยอดไปสู่การสร้างผลงานวิจัยใหม่ โดยเฉพาะผลงานวิจัยด้านวิทยาศาสตร์และทางการแพทย์ ทุกฝ่ายที่เกี่ยวข้องจึงต้องตระหนักถึงผลกระทบของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบนี้ แต่ข้อจำกัดตามที่ได้กล่าวมาแล้วข้างต้น คือ กระบวนการการติดตามสืบหาตัวอาชญากรทางคอมพิวเตอร์ที่กระทำความผิดทำได้ยาก เครื่องมือหรือวิธีการใหม่ ๆ จึงเป็นทางเลือกหนึ่งที่ท้าทายของหน่วยงานด้านการปราบปรามอาชญากรรม

■ ความสำคัญของปัญหา

นับตั้งแต่ปี พ.ศ. 2554 วงการวิชาการทั่วโลกต้องเผชิญกับอาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ที่เกิดขึ้น และมุ่งสร้างความเสียหายต่อแวดวงการวิชาการ คือ มีวารสารทางวิชาการในต่างประเทศที่น่าเชื่อถือและเก่าแก่จำนวนไม่ต่ำกว่า 100 วารสาร ถูกปลอมแปลงโดยอาชญากรทางคอมพิวเตอร์ที่มีความรู้ในการดัดแปลงหรือทำเว็บไซต์วารสารปลอมขึ้นมา ซึ่งอาชญากรเหล่านี้จะทำการขโมยเว็บไซต์ของวารสารที่ถูกกฎหมายแต่อาจจะมีช่วงที่ขาดต่ออายุเว็บไซต์จากผู้ให้บริการ (web host) เมื่อตรวจพบว่าเว็บไซต์ใดขาดต่ออายุ อาชญากรเหล่านี้จะทำการต่ออายุเว็บไซต์จากผู้ให้บริการแล้วเปลี่ยนแปลงข้อมูลการติดต่อมายังกลุ่มอาชญากรทางคอมพิวเตอร์เหล่านี้ และบางส่วนได้จัดทำเว็บไซต์ปลอมสำหรับวารสารทางวิชาการที่มีชื่อเสียงแต่ตีพิมพ์เฉพาะรูปวารสารแบบเล่ม แล้วเริ่มกระบวนการขโมยข้อมูลบทความทางวิชาการ และข้อมูลติดต่อของผู้เขียนหรืออาจารย์ในมหาวิทยาลัย (ซึ่งส่วนใหญ่กลุ่มเป้าหมายคือ ศาสตราจารย์ หรือนักวิชาการระดับต่าง ๆ รวมถึงผู้ที่กำลังศึกษาในระดับบัณฑิตศึกษาจากประเทศกำลังพัฒนา) เมื่อได้ข้อมูลจะทำการติดต่อไปยังนักวิชาการเหล่านั้น

โดยการส่ง Spam Mail จำนวนเป็นล้านฉบับไปยังกลุ่มเป้าหมาย (Jalalian, M., & Dadkhah, M., 2015) โดยยื่นข้อเสนอว่ายินดีจะตีพิมพ์บทความทางวิชาการให้ โดยไม่ต้องผ่านกระบวนการพิจารณาจากผู้ทรงคุณวุฒิ (Peer Review) และจะทำการตีพิมพ์ให้โดยเร็วที่สุด ทันทีที่ได้รับโอนเงินค่าตีพิมพ์วารสารจากนักวิชาการเหล่านั้น (Jalalian & Mahboobi, 2014) โดยเงินค่าธรรมเนียมในการตีพิมพ์ในวารสารทางวิชาการเหล่านี้ มีอัตราประมาณ 100-600 เหรียญสหรัฐต่อการตีพิมพ์หนึ่งบทความ (Bohannon J., 2015) (หรือคิดเป็นเงินบาทไทยที่อัตราแลกเปลี่ยน 35 บาท จะเป็นเงินประมาณ 3,500 บาท – 21,000 บาท) โดยอัตราค่าธรรมเนียมขึ้นอยู่กับความน่าเชื่อถือ ชื่อเสียง และ Impact Factors ของวารสารดังกล่าว ด้วยอัตราค่าธรรมเนียมที่ค่อนข้างสูงนี้ กลุ่มอาชญากรจะไม่ให้มีการโอนเงินไปยังระบบที่ตรวจสอบได้ เช่น บัญชีธนาคารที่จดทะเบียนด้วยชื่อคน หรือระบบจ่ายเงินแบบ PayPal ซึ่งตรวจสอบผู้รับเงินได้ แต่จะใช้การโอนเงินโดยตัดยอดจากบัตรเครดิต ซึ่งยากที่จะติดตามหาผู้รับเงินจริง (Jalalian, M., & Dadkhah, M. ,2015) จึงทำให้เชื่อได้ว่ากลุ่มอาชญากรทางคอมพิวเตอร์เหล่านี้ได้รับเงินจากการก่ออาชญากรรมประเภทนี้ค่อนข้างสูง

ดังที่กล่าวมาแล้วข้างต้นว่าแม้ว่าในประเทศไทยยังไม่ได้รับรายงานการแจ้งความดำเนินคดีกรณีที่มีเหยื่อถูกหลอกหลวงให้โอนเงินโดยเว็บไซต์วารสารทางวิชาการที่ถูกปลอมแปลงเหล่านี้ แต่ย่อมมีความเป็นไปได้ที่นักวิชาการไทยก็สามารถจะตกเป็นเหยื่อของอาชญากรรมประเภทนี้ และย่อมได้รับผลกระทบเช่นเดียวกัน ทั้งในแง่ของการสูญเสียเงินและความน่าเชื่อถือของผลงานทางวิชาการ ด้วยสาเหตุนี้ทำให้เหยื่อที่เป็นนักวิชาการไม่แจ้งความว่าถูกหลอกลวงจากเว็บไซต์วารสารทางวิชาการที่ถูกปลอมแปลงเหล่านี้ สอดคล้องกับการสืบค้นข้อมูลพบว่ามีนักวิชาการจำนวนไม่น้อยที่ได้รับอีเมลเชิญชวนให้มีการตีพิมพ์จากเว็บไซต์วารสารทางวิชาการเหล่านี้ บางกรณีมีรายงานว่าแม้แต่ในเว็บไซต์ Web of Science (WOS) ซึ่งดำเนินการโดย Thomson Reuters ก็ยังถูกหลอกให้นำที่อยู่เว็บไซต์ที่ถูกปลอมแปลงมาลิงค์ไว้เว็บไซต์ดังกล่าว จนต้องแจ้งไปยัง Thomson Reuters ให้เอาลิงค์ของเว็บไซต์ที่ทำปลอมแปลงขึ้นเหล่านั้นออกจากเว็บไซต์ (Jalalian,Mahboobi, 2014; Jalalian, 2014a) ในต่างประเทศจึงมีความตื่นตัวและตระหนักถึงปัญหานี้ โดยเริ่มมีการทำวิจัยและตีพิมพ์บทความทางวิชาการจำนวนหนึ่งเกี่ยวกับวารสารทางวิชาการที่ถูกทำเว็บไซต์ปลอมขึ้นเพื่อหลอกลวงเอาเงินค่าธรรมเนียมในการตีพิมพ์ เช่นผลงานวิชาการของ Jalalian, M., & Dadkhah, M. (2015) บอกว่ามีวารสารที่น่าเชื่อถือและมีชื่อเสียงในศาสตร์ต่าง ๆ ถึงอย่างน้อย 90 วารสารที่เว็บไซต์ถูกปลอมแปลงสอดคล้องกับรายการของรายชื่อวารสารที่เว็บไซต์ถูกปลอมแปลงของ Jeffrey Beall (2016) เป็นบรรณารักษ์และรองศาสตราจารย์มหาวิทยาลัยโคโรราโด เมืองเดนเวอร์ ประเทศสหรัฐอเมริกาที่จัดทำรายการวารสารที่เว็บไซต์ถูกปลอมแปลงเผยแพร่ผ่านเว็บไซต์ของเขาเอง ซึ่งมีวารสารที่ตรวจสอบแล้วว่าเป็นวารสารที่เว็บไซต์ถูกปลอมแปลง จำนวนถึง 114 วารสาร

แม้ว่าการป้องกันการเกิดอาชญากรรมประเภทนี้จะดำเนินการได้ยาก และผู้ที่อยู่ใน

กลุ่มเสี่ยงของอาชญากรรมประเภทนี้ต้องระมัดระวังในการป้องกันตนเองไม่ให้ตกเป็นเหยื่อตามที่กล่าวมาแล้วข้างต้น เพราะอัตราความสำเร็จในการติดตามสืบสวนเพื่อจับกุมอาชญากรทางคอมพิวเตอร์มาดำเนินคดีในประเทศไทยนั้นมีเพียงร้อยละ 30 ยังไม่นับรวมถึงข้อจำกัดของกฎหมายที่จะเอาผิดการกระทำความผิดที่ก่อขึ้นโดยอาชญากรหรือกลุ่มอาชญากรที่อยู่ต่างประเทศนั้น กฎหมายที่มีอยู่ในประเทศหนึ่ง ๆ ย่อมไม่ครอบคลุมถึงการลงโทษผู้กระทำความผิด กรณีที่ผู้กระทำความผิดอาศัยอยู่ในต่างประเทศ (ซึ่งบางกรณีอาจจะไม่มีข้อตกลงความร่วมมือตามหลักการส่งผู้ร้ายข้ามแดน) ดังนั้นจึงมีความจำเป็นที่จะต้องทบทวนเกี่ยวกับการกำหนดนโยบายใหม่ หรือมีกฎหมายที่จะเตรียมรับมือ และมีแนวทางหรือเครื่องมือใหม่ ๆ ในการป้องกันกับภัยจากอาชญากรรมทางคอมพิวเตอร์ในรูปแบบใหม่เหล่านี้ด้วย

จากการสืบค้นข้อมูลพบว่ายังมีแนวทางที่เป็นไปได้ในทางการแก้ไขปัญหานี้ โดยมุ่งเน้นไปที่การสืบสวนจับกุมของเจ้าหน้าที่ที่เกี่ยวข้อง โดยเฉพาะการพัฒนาขีดความสามารถและองค์ความรู้ ตลอดจนความเชี่ยวชาญในการสอบสวนสืบสวนคดีอาชญากรรมประเภทนี้ที่จำเป็นต้องใช้องค์ความรู้ใหม่ “การจัดทำเค้าร่างของอาชญากร (Criminal Profiling)” อาจจะเป็นอีกวิธีการหนึ่งในการใช้เพื่อสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ได้ บทความนี้จึงมุ่งเน้นการค้นคว้าข้อมูลจากเอกสารและผลงานวิจัยเพื่อนำเสนอแนวทางของการประยุกต์ใช้การจัดทำเค้าร่างของอาชญากรมาใช้กับการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ กรณีศึกษาการปลอมแปลงเว็บไซต์วารสารทางวิชาการ โดยจะนำเสนอข้อมูลและองค์ความรู้องค์ความรู้เพื่อทำความเข้าใจเกี่ยวกับการจัดทำเค้าร่างของอาชญากร การประยุกต์ใช้การจัดทำเค้าร่างของอาชญากรกับการสืบสวนอาชญากรรมทางคอมพิวเตอร์ทั่วไปและกรณีการปลอมแปลงเว็บไซต์วารสารทางวิชาการ

▣ การจัดทำเค้าร่างของอาชญากร

นิยาม

การจัดทำเค้าร่างของอาชญากร (Criminal Profiling) สฤษดิ์ สืบพงษ์ศิริ (2559) ได้รวบรวมนิยามความหมายไว้ในเอกสารประกอบการบรรยายเรื่องการจัดทำเค้าร่างของอาชญากรเบื้องต้นไว้ ดังนี้

- กระบวนการในการอนุมานจากคุณลักษณะบุคลิกภาพที่มีลักษณะพิเศษของบุคคล สำหรับในสิ่งที่อาชญากรได้ลงมือกระทำลงไป (Turvey, 2002 อ้างอิงใน สฤษดิ์ สืบพงษ์ศิริ, 2559)
- วิธีการจำแนกผู้กระทำผิดที่ก่ออาชญากรรมโดยใช้การวิเคราะห์ถึงธรรมชาติของการกระทำผิด และวิธีการกระทำในสิ่งที่ชั่วร้าย (Teten, 1995 อ้างอิงใน สฤษดิ์ สืบพงษ์ศิริ, 2559)

นอกจากนี้ยังได้รวบรวมเพิ่มเติมจากบทความของนักวิชาการคนอื่นที่ได้ให้คำจำกัดความของการจัดทำเค้าร่างของอาชญากรไว้เพิ่มเติม ดังนี้

- วิธีการสำหรับแยกแยะลักษณะส่วนบุคคลและพฤติกรรมของผู้กระทำผิดที่

ยังไม่รู้ว่าเป็นใคร โดยใช้กระบวนการวิเคราะห์ธรรมชาติของการกระทำผิด และลักษณะของการกระทำผิดนั้น (Canter, D., et al., 2004)

- กระบวนการหนึ่งของการสืบสวนที่ใช้การประเมินสถานที่เกิดเหตุ รวบรวมข้อมูลเกี่ยวกับเหยื่อและหลักฐาน ทำการอนุมานลักษณะเฉพาะของผู้กระทำความผิด และทำการตีความโดยการคาดการณ์ลักษณะของผู้กระทำผิด รูปแบบการกระทำความผิดบนฐานของงานวิจัย ข้อเท็จจริง และประสบการณ์ที่เคยเกิดขึ้น ซึ่งช่วยให้สามารถจำกัดกลุ่มของผู้ต้องสงสัยให้มีจำนวนน้อยลง รวมถึงให้ทิศทางในการสืบสวนต่อไปได้ โดยใช้กระบวนการวิเคราะห์ทางจิตวิทยาเป็นตัวช่วยที่สำคัญ (Hadley, 2005)
- แก่นของการจัดทำเค้าร่างของอาชญากร คือ การทำความเข้าใจอาชญากรรมจากมุมมองของผู้กระทำความผิดและเหยื่อ โดยทำการแยกแยะและคาดการณ์จากหลักฐานต่าง ๆ ว่าใครคือคนที่น่าจะเป็นผู้กระทำผิด และใครที่เสี่ยงจะตกเป็นเหยื่อ (Kocsis, 2008)

โดยสรุปการจัดทำเค้าร่างของอาชญากรเป็นวิธีการหนึ่งของกระบวนการทางนิติวิทยาศาสตร์ที่ใช้กระบวนการวิเคราะห์ข้อมูลต่าง ๆ จากหลักฐานที่จัดเก็บได้ ทั้งจากสถานที่เกิดเหตุและการเปรียบเทียบกับอาชญากรรมที่เคยเกิดขึ้นที่มีลักษณะใกล้เคียงกัน เพื่อทำการวิเคราะห์ลักษณะส่วนบุคคลและพฤติกรรมเพื่อหาความผิดปกติหรือความแตกต่าง จนสามารถที่จะจำกัดและให้ข้อมูลเกี่ยวกับผู้กระทำผิด รวมถึงแรงจูงใจ/ความตั้งใจในการก่อเหตุอาชญากรรม รูปแบบของอาชญากรรม และประเภทของเหยื่อ เพื่อให้ข้อมูลกลุ่มผู้ต้องสงสัยที่แคบลง และมีทิศทางในการสืบสวนเพื่อหาตัวผู้กระทำผิดที่แท้จริงมาลงโทษ

พัฒนาการ และวัตถุประสงค์ของการจัดทำเค้าร่างของอาชญากร

การจัดทำเค้าร่างของอาชญากรจากบทความของ Wori (2014) อาจกล่าวได้ว่าเริ่มต้นจากหนังสือคู่มือเรื่อง “Malleus Maleficarum” ที่ตีพิมพ์เมื่อปี 1486 ซึ่งคู่มือดังกล่าวได้มีข้อมูลที่เป็นคำแนะนำเกี่ยวกับการแยกแยะกลุ่มบุคคลที่ต้องสงสัย สำหรับนักล่าแม่มดมืออาชีพ (Turvey, 2002) ต่อมาในต้นช่วงศตวรรษที่ 19 การรวบรวมลักษณะทางกายภาพของบุคคลที่ Jacob Fries และ Cesare Lombroso ดำเนินการก็อาจนับได้ว่าเป็นความพยายามที่จะรวบรวมและวิเคราะห์ลักษณะของอาชญากรได้ แม้ในยุคนั้นจะยังไม่ได้เรียกว่าการจัดทำเค้าร่างของอาชญากรก็ตาม แต่การจัดทำเค้าร่างของอาชญากรถูกบันทึกอย่างเป็นทางการเมื่อ FBI ได้จัดตั้งหน่วยพฤติกรรมศาสตร์ (Behavioral Sciences Unit) ขึ้นในช่วงปี 1970 และได้พัฒนาเทคนิคและองค์ความรู้เกี่ยวกับการจัดทำเค้าร่างของอาชญากรขึ้น (Patherick, 2005 อ้างอิงใน สฤษดิ์ สืบพงษ์ศิริ, 2559) และเมื่อปี 1983 ได้พัฒนาระบบรายงานผลด้วยโปรแกรมคอมพิวเตอร์ หรือชื่อว่าโปรแกรม ViCAP (Violent Criminal Apprehension Program) ขึ้นเพื่อบันทึกข้อมูลคดีอาชญากรรมที่มีความรุนแรงที่เกิดขึ้นไว้เป็นฐานข้อมูล และเมื่อเกิดคดีที่คล้ายคลึงกันสามารถใช้สืบค้นหาข้อมูลคดีและค้นหาตัวผู้ต้องสงสัยที่มีพฤติกรรมใกล้เคียงกันได้ นับเป็นตัวช่วยในการสืบหา

คนร้ายได้อีกทางหนึ่ง ปัจจุบันในต่างประเทศมีการพัฒนาองค์ความรู้เกี่ยวกับการจัดทำเค้าร่างของอาชญากรทั้งอาชญากรรมที่มีความรุนแรง และการจัดทำเค้าร่างอาชญากรเกี่ยวกับคดีอาชญากรรมทางคอมพิวเตอร์ (Digital Profiling) เพราะมีความก้าวหน้าทางเทคโนโลยีสามารถสร้างเครื่องมือและเทคนิคใหม่ ๆ เพื่อสนับสนุนการสืบสวนของเจ้าหน้าที่ได้

สำหรับวัตถุประสงค์ของการจัดทำเค้าร่างของอาชญากร สฤษดิ์ สืบพงษ์ศิริ (2559) บอกว่าเป็นไปเพื่อสนับสนุนกระบวนการยุติธรรมให้สามารถที่จะประเมินผู้กระทำความผิดได้ โดยให้ข้อมูลทางสังคม และจิตวิทยาที่เป็นคุณสมบัติประจำตัวของผู้กระทำผิด รวมถึงเชื้อชาติ อายุ เพศ ประเภทของอาชีพ ศาสนา สถานภาพสมรส และการศึกษา นอกจากนี้ยังช่วยขอบเขตของการสืบสวนของตำรวจโดยใช้การคาดการณ์ลักษณะของการจู่โจม และประเภทของเหยื่อที่เป็นไปได้ รวมถึงการให้ข้อมูลเรื่องของสถานที่ก่อคดี และสนับสนุนแนวทางในการสัมภาษณ์หรือสอบสวนผู้กระทำผิดให้มีประสิทธิภาพ และมีความสัมพันธ์กับรูปแบบเฉพาะของผู้กระทำผิด เพราะไม่มีผู้กระทำผิดคนใดที่จะมีการตอบคำถามไปในแนวทางเดียวกันเสมอ จึงต้องการกลยุทธ์ในการสัมภาษณ์ที่แตกต่างกันไป

รูปแบบของการจัดทำเค้าร่างของอาชญากร

สฤษดิ์ สืบพงษ์ศิริ (2559) กล่าวว่ามีรูปแบบของการจัดทำเค้าร่างของอาชญากรใน 2 รูปแบบ คือ

- รูปแบบการใช้เหตุผลแบบอุปมาน (Inductive Criminal Profiling) เป็นการใช้ข้อมูลทางสถิติมาทำการวิเคราะห์ เช่น เมื่อเกิดเหตุการณ์ขึ้น ก็ใช้การสังเกตและรวบรวมข้อมูลและสถิติที่มีเข้ามาสนับสนุน ซึ่งมาจากปรากฏการณ์ย่อย ๆ ที่เคยเกิดขึ้นในลักษณะคล้ายคลึงหรือมีแบบแผนเดียวกัน แล้วนำข้อมูลที่ได้ทั้งหมดมาทำการสรุปวิเคราะห์เพื่อตั้งสมมติฐานเพื่อทำการทดสอบต่อไป (เริ่มจากหลักทั่วไปสู่เรื่องเฉพาะ) โดยหลักการใช้สถิติหรือข้อมูลประกอบไปด้วย การค้นหาความคล้ายคลึงกัน การทำนาย การประมาณ และการตัดสินใจจากข้อมูลที่ปรากฏในขั้นต้น ข้อมูลที่ใช้เป็นสถิติจากการรวบรวมลักษณะทางกายภาพ และจากการสัมภาษณ์ผู้กระทำความผิด ลักษณะของข้อมูล เช่น เป็นชาย ผิวขาว โสด ฉลาดหรือมีสติปัญญาสูงกว่าปกติ แต่ไม่ตั้งใจเรียน ทำให้ทำงานแบบใช้แรงงาน มาจากครอบครัวที่มีปัญหา ถูกพ่อทอดทิ้งตั้งแต่เด็กโดยมีแม่เป็นผู้ดูแล เมื่อยังเด็กถูกทารุณกรรม ทั้งทางร่างกาย ทางเพศ และทางจิตใจ จากการที่ต้องอยู่อาศัยภายใต้การบังคับของแม่ ทำให้กลายเป็นผู้เกลียดชังผู้หญิง และมักจะกระทำรุนแรงต่อผู้หญิง เป็นต้น

ข้อดีของเทคนิคการใช้เหตุผลแบบอุปมาน คือ เป็นข้อมูลที่ใช้ง่าย เห็นผลชัดเจน เหมาะสำหรับผู้ที่ยังไม่มีความรู้พิเศษด้านนิติวิทยาศาสตร์หรือด้านการอบรมทางพฤติกรรมอาชญากร หรือการสืบสวนคดีอาชญากรรมมาก่อน และไม่จำเป็นต้องเป็นผู้ที่ได้รับการฝึกอบรมมาทางด้านนิติวิทยาศาสตร์หรือในด้านจิตวิทยาอาชญากรรม จิตวิทยาอปกติ และไม่จำเป็นต้อง

มีประสบการณ์ในการสืบสวนอาชญากรรมรุนแรงเลยก็ได้ ส่วนข้อด้อยของวิธีการทำเค้าร่างอาชญากรแบบนี้ คือ ความไม่เป็นวิทยาศาสตร์ที่ให้เหตุผลในลักษณะนี้ เนื่องจากข้อมูลที่ใช้ประกอบการให้เหตุผลเป็นข้อมูลแบบกว้าง ๆ ที่มาจากกลุ่มตัวอย่างที่มีอยู่จำกัด และไม่มีความเฉพาะเจาะจงในเรื่องของความสัมพันธ์กับคดีอื่น จึงเป็นการนำเสนอคุณลักษณะแบบกว้าง ๆ และเป็นการเฉลี่ยจากกลุ่มบุคคลกลุ่มเล็ก ๆ จากผู้กระทำความผิดที่ถูกควบคุมไว้ได้เท่านั้น ซึ่งอาจจะเป็นกลุ่มตัวอย่างที่เหมาะสมหรือไม่เหมาะสมขึ้นอยู่กับความรู้ความสามารถของผู้เก็บรวบรวมข้อมูล รวมถึงอาจจะไม่เพียงพอหรือถูกต้องแม่นยำกับจำนวนอาชญากรที่มีอยู่มากมายในปัจจุบัน และหากผู้ที่จัดทำเค้าร่างของอาชญากรไม่มีความเชี่ยวชาญ อาจจะเกิดความผิดพลาดต่อผู้บริสุทธิ์ได้

- รูปแบบการใช้เหตุผลแบบอนุมาน (Deductive Criminal Profiling) วิธีการนี้จะใช้ทฤษฎีที่เกี่ยวข้องมาตั้งเป็นสมมติฐานแล้วกำหนดรูปแบบการศึกษาวิจัยให้เหมาะสม เพื่อทดสอบสมมติฐาน แล้วจึงเริ่มเก็บรวบรวมข้อมูลและนำข้อมูลมาวิเคราะห์ ลักษณะของผู้กระทำผิดที่ได้จากวิธีการนี้จะมาจากสมมติฐานที่ตั้งไว้โดยตรงและเกี่ยวกับรูปแบบที่จำเพาะของพฤติกรรม เป็นการวิเคราะห์พยานหลักฐานด้านพฤติกรรม เพราะเชื่อว่าไม่มีการกระทำความผิดใดที่ปราศจากแรงจูงใจ ผู้กระทำผิดแต่ละคนสามารถแสดงออกถึงพฤติกรรมที่คล้ายคลึงกันแต่ทำไปด้วยเหตุผลที่แตกต่างกันโดยสิ้นเชิง การใช้เหตุผลแบบอนุมานจะเริ่มจากข้อมูลจากการวิเคราะห์ลำดับย้อนเหตุการณ์ โดยอาศัยพยานหลักฐานทางนิติวิทยาศาสตร์ ลักษณะเฉพาะของสถานที่เกิดเหตุเพื่อเชื่อมโยงระหว่างผู้กระทำผิดกับสถานที่เกิดเหตุ หากมีลักษณะเฉพาะก็จะทำให้สามารถหาข้อสรุปเกี่ยวกับแรงจูงใจของผู้กระทำผิด แผนประทุษกรรม และเหยื่อ

ข้อดีของการใช้การให้เหตุผลแบบอนุมานในการวิเคราะห์ คือ สามารถจับต้องได้เพราะมีการตรวจสอบด้านเหยื่อวิทยาอย่างละเอียด การวิเคราะห์เรื่องเหยื่อกับผู้กระทำผิด เพื่อวิเคราะห์แรงจูงใจของผู้กระทำผิด การวิเคราะห์พยานหลักฐานจากวัตถุพยาน เหยื่อ หรือสถานที่เกิดเหตุ ส่วนข้อจำกัดของวิธีการอนุมาน คือ ต้องใช้เวลานาน และความพยายามสูง ตลอดจนเจ้าหน้าที่ต้องมีทักษะแบบสหวิทยาการ อาจจะทำให้เจ้าหน้าที่ฝ่ายสืบสวนไม่สนใจเรียนรู้วิธีการนี้ นอกจากนี้ยังเป็นเทคนิคที่ไม่สามารถระบุอย่างเฉพาะเจาะจงได้ว่าบุคคลนั้นเป็นผู้กระทำผิด หากไม่มีหลักฐานหรือลักษณะเฉพาะที่ชี้ไปยังผู้กระทำความผิดได้อย่างแน่ชัดก่อน

อย่างไรก็ดีในการใช้งานจริงยังไม่มีข้อสรุปว่าวิธีการจัดทำเค้าร่างของอาชญากรแบบใดที่ถูกต้องกว่าหรือดีกว่า ทั้งสองวิธีต่างมีข้อดีและข้อเสีย ในการใช้งานจึงต้องเลือกวิธีการที่เหมาะสมกับวิธีคิดของผู้ปฏิบัติงาน และอาจจะมีการใช้ทั้งสองวิธีการนี้สลับกันไปมาแบบไม่รู้ตัวอยู่ตลอดเวลาอยู่แล้ว และข้อมูลจากสฤษดิ์ สืบพงษ์ศิริ (2559) ได้วิเคราะห์ว่าการจัดทำเค้าร่างของอาชญากรที่ในปัจจุบันยังไม่ได้ถูกใช้เป็นที่แพร่หลายในประเทศไทย เพราะเป็น

องค์ความรู้ใหม่ที่ยังไม่ได้มีการสอน หรือถ่ายทอดองค์ความรู้ผ่านสถาบันการศึกษาที่กว้างขวาง กรณีของโรงเรียนนายร้อยตำรวจเองที่เป็นส่วนหนึ่งของวิชานิติวิทยาศาสตร์ ยังไม่มีการนำไปใช้อบรมให้กับเจ้าหน้าที่ตำรวจฝ่ายสืบสวน และที่สำคัญที่สุด คือ องค์ความรู้ด้านการจัดทำเค้าร่างของอาชญากรยังไม่สามารถสร้างความน่าเชื่อถือ หรือมีกรณีตัวอย่างคดีที่ประสบความสำเร็จจำนวนมากพอที่จะถูกนำมาพัฒนาใช้เป็นแนวทางหลักที่สำคัญแนวทางหนึ่งในการสืบสวนคดี แต่ด้วยจำนวนคดีอาชญากรรมทางคอมพิวเตอร์ที่เพิ่มจำนวนขึ้นในปัจจุบัน การพัฒนาองค์ความรู้ ตัวแบบ (Model) และพัฒนาโปรแกรมต่าง ๆ เพื่อใช้จัดทำเค้าร่างของอาชญากรโดยใช้คอมพิวเตอร์ถูกนำมาประยุกต์ใช้โดยการนำอุปกรณ์ทางคอมพิวเตอร์เข้ามาช่วยในการวิเคราะห์แยกแยะ และประมวลข้อมูลมากขึ้น

การจัดทำเค้าร่างของอาชญากรสำหรับอาชญากรรมทางคอมพิวเตอร์ (Digital Profiling)

อาชญากรรมทางคอมพิวเตอร์ตามคำจำกัดความของ Britz (2008) คือ *"การกระทำความผิดที่กระทำต่อบุคคลหรือกลุ่มบุคคลโดยใช้เครือข่ายการสื่อสารโทรคมนาคมที่ทันสมัย เช่น อินเตอร์เน็ตและมือถือ"* ซึ่งมีผลงานวิจัยจำนวนมากที่ค้นหาขอบเขตและประเภทของอาชญากรรมทางคอมพิวเตอร์และขั้นตอนในการฟ้องร้องเพื่อดำเนินคดีของอาชญากรรมประเภทนี้ เช่น จากบทความทางวิชาการของ Wori (2014) ได้ทำการทบทวนวรรณกรรมของนักวิชาการจำนวนหนึ่ง เช่น Cohen and Felson (1979) Hindelang, Gottfredson & Garafalo (1978) และ Gottfredson & Hirschi (1990) ที่เสนอมุมมองและแนวคิดเรื่องรูปแบบการใช้ชีวิต (Lifestyles) และกิจวัตรประจำวัน (Routine Activities) และทฤษฎีเรื่องอาชญากรรม (The Theories of Crime) เพื่อแสดงเหตุผลของการก่ออาชญากรรมทางคอมพิวเตอร์และวิเคราะห์เหยื่อของอาชญากรรมประเภทนี้ แต่ข้อเสนอแนะจากการทบทวนวรรณกรรมนี้ พบว่าไม่เพียงแต่ต้องทำการวิเคราะห์สถานการณ์ที่เกิดขึ้นเท่านั้นแต่ต้องวิเคราะห์ปัจจัยส่วนบุคคลด้วย เพราะที่ผ่านมายังไม่สามารถที่จะชี้ชัดได้ถึงลักษณะของบุคคลหรือกลุ่มบุคคลกลุ่มเป้าหมายที่จะตกเป็นเหยื่อของอาชญากรรมทางคอมพิวเตอร์ได้ ขณะที่การศึกษาวิจัยของ Bossler & Holt (2010) ได้หมายเหตุไว้ว่าการขาดการควบคุมตนเอง (Self Control) เป็นปัจจัยหนึ่งที่ทำให้บุคคลหรือกลุ่มบุคคลนั้นตกเป็นเหยื่อของอาชญากรรมประเภทนี้ ส่วนผู้กระทำความผิดจากการศึกษาของ Hochmuch (2004) สะท้อนว่าในปัจจุบันมุ่งหมายต่อเงินมากขึ้น ขณะที่ Gudaitis (2005) เปรียบอาชญากรรมทางคอมพิวเตอร์ว่าเป็นเหมือนกับการปล้นธนาคารที่ในยุคก่อนที่กลุ่มผู้กระทำความผิดจะมีการจัดเตรียมความพร้อมเป็นอย่างดี เพียงแต่ในวันนี้ผู้กระทำผิดนั้นไม่ได้อยู่ในสถานที่เกิดเหตุ แต่อยู่ในประเทศที่ห่างไกลออกไป เช่น ประเทศจีน ประเทศอินเดีย ประเทศรัสเซีย ประเทศโรมาเนีย และในทวีปละตินอเมริกา ซึ่งอยู่นอกเหนือจากกฎหมายของประเทศที่สถานเกิดเหตุจะเอาผิดได้ อาชญากรทางคอมพิวเตอร์เหล่านี้จึงได้อาศัยความ

ได้เปรียบของอินเตอร์เน็ตที่ผู้กระทำผิดอยู่ห่างไกลจากสถานที่เกิดเหตุ และไม่มีผู้รู้ตัวตนในการก่อเหตุมากขึ้น ดังนั้นจึงจำเป็นที่จะต้องมีความเข้าใจเกี่ยวกับกลุ่มอาชญากรเหล่านี้และค้นหาแรงจูงใจในการก่อเหตุให้ได้ (Wori, 2014)

จากการทบทวนวรรณกรรมของ Wori (2014) ยังเสนอเพิ่มเติมอีกว่าในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ไม่ควรตั้งสมมติฐานว่าอาชญากรรมและตัวอาชญากรผู้ก่อเหตุในแต่ละคดีมีความคล้ายคลึงกัน เพราะที่แท้จริงนั้นแต่ละคดีมีความแตกต่างกันทั้งแรงจูงใจ ความตั้งใจ และผลลัพธ์ของการก่อเหตุ เช่นเดียวกับอาชญากรรมที่กระทำต่อร่างกาย แต่สิ่งที่อาชญากรรมทางคอมพิวเตอร์มีความแตกต่างจากอาชญากรรมที่กระทำต่อร่างกาย คือ รูปแบบของหลักฐาน เพราะหลักฐานของอาชญากรรมประเภทนี้ไม่ใช่สิ่งที่จับต้องได้เหมือนอาชญากรรมในโลกแห่งความเป็นจริง (Heiser & Kruse, 2002) ดังนั้นนักสืบที่เคยทำงานกับหลักฐานที่จับต้องได้ เช่น การมีพยานหรือคำรับสารภาพ เพื่อคลี่คลายคดีก็จะเปลี่ยนแปลงไป เพราะหลักฐานส่วนใหญ่ของอาชญากรรมทางคอมพิวเตอร์จะอยู่ในรูปแบบดิจิตัล (Rogers, 2003) ซึ่งผู้กระทำผิดจะทิ้งหลักฐานบางรูปแบบไว้ในสถานที่เกิดเหตุ และนำหลักฐานอีกบางส่วนที่เชื่อมโยงกับอาชญากรรมไปด้วย (Safestein, 2001) แต่หลักฐานที่เจ้าหน้าที่สามารถจัดเก็บมาได้จากสถานที่เกิดเหตุนั้นยังไม่สามารถที่จะแปรความหมายได้ จำเป็นต้องมีนักนิติวิทยาศาสตร์ด้านดิจิตัลที่ทำหน้าที่ในการรวบรวมและนำข้อมูลมาวิเคราะห์เพื่อทำให้เกิดความหมายขึ้น (Wori, 2014)

การสืบสวนคดีประเภทนี้จึงต้องอาศัยความรู้ความเข้าใจในการสืบสวนโดยเน้นกระบวนการทางนิติวิทยาศาสตร์ โดยสามารถใช้การจัดทำเค้าร่างของอาชญากรเป็นเครื่องมือหนึ่งในการสืบสวนโดยสืบจากหลักฐานที่เก็บไว้ในรูปแบบไฟล์ดิจิตัลที่ถูกบันทึกไว้ใน Hard Drive หรือ Flash Drive ตัวไฟล์ดิจิตัลสามารถอยู่ในหลากหลายรูปแบบ ทั้งโค้ดที่เขียนขึ้น แบบเนื้อหา เนื้อหาในแบบตาราง เนื้อหาแบบเข้ารหัส หรือแม้แต่รูปภาพ บางกรณีเป็นรูปภาพขนาดเล็กที่ประกอบเป็นส่วนหนึ่งของรูปภาพขนาดใหญ่ ซึ่งนักนิติวิทยาศาสตร์ดิจิตัล เรียกว่า การอำพรางข้อมูล (Steganography) (Wori, 2014)

นอกจากนี้ Wori (2014) นำเสนอว่าขณะที่นิติวิทยาศาสตร์เป็นเครื่องมือที่มีประโยชน์ในการค้นหาหลักฐาน แต่ก็ยังต้องใช้เทคนิคอื่น ๆ อีกมากในการสืบสวนเพื่อคลี่คลายคดี กรณีนี้การจัดทำเค้าร่างของอาชญากรน่าจะสามารถนำมาปรับใช้ได้ เพราะอาชญากรรมทางคอมพิวเตอร์นั้น อาชญากรจะสร้างสถานการณ์ที่เป็นเอกลักษณ์ ทางเดียวในการสืบสวน คือ การใช้รูปแบบการวิเคราะห์ตามแนวทางในการจัดทำเค้าร่างของอาชญากรเพื่อวิเคราะห์พฤติกรรมของผู้กระทำผิดแต่ละคนที่ได้มาจากข้อมูลเชิงเทคนิคระดับสูง เช่น System Logs และ System Level Reconstruction เพื่อวิเคราะห์พฤติกรรมการโจมตีของอาชญากรทางคอมพิวเตอร์ หรือการที่ผู้กระทำความผิดอาศัยอยู่ในอีกซีกโลกหนึ่งขณะที่ก่ออาชญากรรมในอีกประเทศหนึ่ง วิธีการสืบสวนแบบใหม่

เทคนิค IP Tracing หรือตามรอย IP ของเครื่องคอมพิวเตอร์ที่ออนไลน์ผ่านอินเตอร์เน็ต ซึ่งจะช่วยให้รู้ว่าการกระทำความผิดนั้นกระทำในจุดใด เมือง หรือประเทศใด ห่างไกลจากสถานที่เกิดเหตุจริงเพียงใด แต่ด้วยเหตุที่มีความซับซ้อนของสถานที่เกิดเหตุ และจุดที่ผู้กระทำผิดลงมือแยกจากกันนั้น ย่อมส่งผลต่อการเข้าถึงและการกำหนดช่วงเวลาในการสืบสวนอาชญากรรม ดังนั้นจึงแทบจะเป็นไปไม่ได้เลยที่จะใช้หลักฐานทางกายภาพเพียงอย่างเดียวในการชี้ตัวอาชญากรเพราะเป็นอินเตอร์เน็ตช่วยทำให้ผู้ก่อเหตุนั้นเป็นบุคคลนิรนาม (Wori, 2014)

ในการสืบสวนอาชญากรรมทางคอมพิวเตอร์โดยใช้การสร้างเค้าร่างของอาชญากรนั้น Wori (2014) ได้ทบทวนวิธีการที่พัฒนาโดย Shoemaker and Kenedy ซึ่งได้มีพื้นฐานมาจากวิธีการจัดทำเค้าร่างของอาชญากรของ FBI และการวิเคราะห์หลักฐานทางพฤติกรรมของ Turvey (Turvey's Behavioral Evidence Analysis) โดยสรุปออกมาเป็น 5 ขั้นตอนตามลำดับของกระบวนการจัดทำเค้าร่างของอาชญากรทางคอมพิวเตอร์ ดังนี้

1) การรวบรวมหลักฐาน (Assimilation Phase or Equivocal Forensic Analysis) : เป็นขั้นตอนแรกในการรวบรวมหลักฐานทางนิติวิทยาศาสตร์ซึ่งไม่ต่างจากการเก็บรวบรวมหลักฐานจากคดีอาชญากรรมประเภทอื่น ๆ

2) การวิเคราะห์ที่เจาะจงไปที่การสังเกตเกี่ยวกับความสัมพันธ์ของพฤติกรรมที่ชี้ให้เห็นถึงรูปแบบ หรือลักษณะเฉพาะของอาชญากรรม: ขั้นตอนนี้ต้องใช้ข้อมูลที่ได้จากการรวบรวมในขั้นตอนแรกมาทำการวิเคราะห์เพื่อระบุตัวผู้กระทำผิดจากพฤติกรรมที่เขาแสดงออกผ่านหลักฐานที่จัดเก็บ

3) เหยื่อวิทยา (Victimology): ข้อมูลของเหยื่อสามารถบอกได้เกี่ยวกับประเภทของผู้กระทำผิดโดยพิจารณาจากเอกลักษณ์เฉพาะ (Signature) ของผู้กระทำผิดแต่ละราย/กลุ่มจากพฤติกรรมการก่ออาชญากรรมที่ผ่านมา ซึ่งทำให้สามารถจำกัดกลุ่มผู้กระทำผิดได้

4) การวิเคราะห์รูปแบบการก่ออาชญากรรม (Crime Pattern Analysis): ในขั้นตอนนี้การวิเคราะห์ด้วยทฤษฎีจะมีความเป็นเหตุเป็นผลมากขึ้น โดยจะนำปัจจัยต่าง ๆ เข้ามาวิเคราะห์ร่วมด้วย เช่น ปัจจัยทางภูมิศาสตร์ (Geography) และช่วงเวลา (Timing) ของการก่ออาชญากรรม ทำให้สามารถบอกได้ว่าการก่ออาชญากรรมคอมพิวเตอร์นั้นคนที่ลงมือทำไปเพื่ออะไร และทำอย่างไร ขั้นตอนนี้เหมือนการสอบสวนคดีอาชญากรรมตามปกติที่จะต้องมีการตั้งสมมติฐานแล้วมีหลักฐานและข้อเท็จจริงของการก่ออาชญากรรมมาสนับสนุนเพื่อจะดำเนินการจับกุมตัวผู้กระทำความผิด

5) การสร้างเค้าร่างของอาชญากร (Profile Development): เมื่อมีข้อมูลเกี่ยวกับการก่ออาชญากรรมมากเพียงพอที่จะชี้ได้ว่าผู้กระทำผิดอาจจะเป็นคนใด/กลุ่มใด ลักษณะการก่ออาชญากรรมเป็นแบบใด และเหยื่อเป็นใครตลอดจนเวลาที่ก่ออาชญากรรม ความเสียหายที่เกิดขึ้น ข้อมูลด้านพฤติกรรมต่าง ๆ ที่จะสนับสนุนการจัดทำเค้าร่างจะถูกพัฒนาขึ้นโดยใช้วิธีการให้เหตุผลแบบอนุมานเกี่ยวกับลักษณะของการกระทำผิด แต่ในทางกลับกันหากมีข้อมูลที่มีการจำแนกประเภทแบบอุปมานในมือก็จะช่วยในการแปลความหมายของรูปแบบการก่ออาชญากรรมได้ด้วย

ทั้งนี้ เนื่องจากในปัจจุบันมีความเจริญรุดหน้าทางด้านเทคโนโลยีเป็นอย่างมาก ในการสร้างเค้าร่างของอาชญากรสามารถดำเนินการโดยใช้โปรแกรมทางคอมพิวเตอร์ช่วยดำเนินการสืบค้นหาร่องรอยผู้กระทำความผิดและแผนประทุษกรรมของผู้กระทำความผิด (modus operandi) ได้ จากการวิจัยของ Clara Colombini & Antonio Colella (2011) ได้กำหนดเทคนิคการจัดทำเค้าร่างของอาชญากรโดยใช้ระบบคอมพิวเตอร์ช่วยในการวิเคราะห์ไฟล์ดิจิตัล 6 ขั้นตอนตามลำดับ ดังนี้

1) ระบุเป้าหมายว่ามองหาอะไรจากหลักฐานที่เก็บรวบรวมมาได้ กรณีนี้หมายถึงเมื่อได้อุปกรณ์ต่าง ๆ ที่บันทึกข้อมูลดิจิตัลจากสถานที่เกิดเหตุ ก่อนจะทำการประมวลผลข้อมูลโดยใช้โปรแกรมคอมพิวเตอร์ต้องระบุว่าต้องการค้นหาข้อมูลอะไรเกี่ยวกับการกระทำความผิดนั้น

2) รวบรวมและประมวลผลข้อมูลที่เก็บจากหลักฐานที่บันทึกไว้ในแหล่งต่าง ๆ โดยใช้โปรแกรมคอมพิวเตอร์ในการระบุตัวแปรที่ต้องการค้นหาเพื่อสืบค้น เปรียบเทียบข้อมูลและแยกแยะข้อมูลที่ตรงตามวัตถุประสงค์ของการค้นหาข้อมูล

3) เลือกข้อมูลที่เกี่ยวข้องและสกัดข้อมูลออกมาตามตัวชี้วัดที่กำหนดไว้ ขั้นตอนนี้สามารถกำหนดให้โปรแกรมสืบค้นและแยกแยะตามตัวชี้วัด ซึ่งการศึกษานี้กำหนดองค์ประกอบของตัวชี้วัดเพื่อให้ได้ข้อมูลต่าง ๆ เช่น ชนิดของอุปกรณ์จัดเก็บข้อมูล องค์ประกอบของไฟล์ สถานที่จัดเก็บไฟล์ ชนิดของไฟล์ที่เกี่ยวข้อง เป็นต้น

4) ตรวจสอบข้อมูลให้ถูกต้องตรงตามตัวชี้วัดที่กำหนดไว้ ขั้นตอนนี้จะสามารถกำหนดรูปแบบของข้อมูลดิจิตัลที่จัดเก็บในอุปกรณ์บันทึกข้อมูลที่เกี่ยวข้องกับการกระทำความผิดและตรวจสอบซ้ำเพื่อเปรียบเทียบกับข้อมูลจากอุปกรณ์บันทึกข้อมูลอื่น ๆ เช่น การตรวจสอบวันที่มีการสร้าง แก้ไข และลบไฟล์ เพื่อให้เข้าใจเกี่ยวกับการกระทำเกี่ยวกับข้อมูลที่ถูกบันทึกไว้ในอุปกรณ์ของผู้กระทำผิด เพื่อให้เป็นไปตามวัตถุประสงค์ของการค้นหาข้อมูล

5) รวบรวมข้อมูลและจัดทำเป็นเค้าร่างของอาชญากร เมื่อได้รูปแบบของการดำเนินการเกี่ยวกับข้อมูลที่ถูกบันทึกไว้ จะถูกนำมาจัดทำเป็นเค้าร่างของอาชญากรโดยข้อมูลที่นำเสนอจะผ่านการวิเคราะห์ ทั้งเชิงปริมาณ เช่น สถิติของความเป็นไปได้ที่จะเกิดเหตุบังเอิญเช่นนี้ และวิเคราะห์เชิงคุณภาพ เช่น ข้อมูลที่ได้มาสอดคล้องกับตัวชี้วัดที่วางไว้และมีความน่าเชื่อถือมากเพียงใด

6) แปลความหมายของผลที่ได้รับ แล้วเปรียบเทียบกับเป้าหมายที่กำหนดไว้ในขั้นตอนแรก เมื่อจัดทำเค้าร่างอาชญากรเสร็จสิ้น ต้องนำมาตีความหมายของข้อมูลให้สอดคล้องกับเป้าหมายที่ต้องการตามข้อ 1)

การจัดทำเค้าร่างของอาชญากรโดยใช้โปรแกรมทางคอมพิวเตอร์อาจจะเป็นปัจจัยหนึ่งที่ช่วยสนับสนุนการทำงานของเจ้าหน้าที่สืบสวนในการวิเคราะห์หาความเป็นไปได้ของการกระทำความผิดและการระบุตัวผู้กระทำความผิดได้ในระยะเวลาที่สั้นลง ทำให้ผู้เสียหายได้รับความยุติธรรมได้เร็วขึ้น สำหรับประเทศไทยหน่วยงานที่รับผิดชอบการสืบสวนคดีอาชญากรรม

ทางคอมพิวเตอร์ เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สังกัดกองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ หรือกรมสอบสวนคดีพิเศษ มีการใช้โปรแกรมคอมพิวเตอร์ในการวิเคราะห์ข้อมูลและสร้างเค้าร่างอาชญากรเช่นเดียวกัน

ทั้งนี้ ข้อมูลที่ได้จากกลุ่มตรวจพิสูจน์หลักฐานทางอิเลคทรอนิกส์ กองนิติวิทยาศาสตร์บริการ สถาบันนิติวิทยาศาสตร์ (รายงานวิชาสัมมนา, 2559) เจ้าหน้าที่ได้ให้ข้อมูลว่ากลุ่มงานนี้ได้ใช้โปรแกรมคอมพิวเตอร์ในการตรวจวิเคราะห์ข้อมูลดิจิตัลที่ได้จากการเก็บรวบรวมหลักฐานทางคดี ซึ่งขั้นตอนการตรวจวิเคราะห์มีดังนี้

1) รับวัตถุพยานจากหน่วยงานต้นสังกัด และพิจารณาเหตุผลในการส่งตรวจเพื่อจะดำเนินการให้สอดคล้องกับเหตุผลในการส่งตรวจหรือการกระทำผิดนั้น ๆ ซึ่งเจ้าหน้าที่ที่ปฏิบัติงานจะพิจารณาว่าคดีที่ดำเนินการเป็นคดีที่เกี่ยวข้องกับอะไร เหตุผลที่ต้องการค้นหาข้อเท็จจริงในเรื่องใด

2) ทำสำเนาข้อมูล

3) ทำการวิเคราะห์ข้อมูลที่ได้จากการสำเนาที่ตรงตามเหตุผลที่ส่งตรวจตามข้อ 1

4) ออกรายงานให้กับหน่วยงานที่ส่งตรวจ ประกอบด้วย รายงานที่ตอบวัตถุประสงค์การส่งตรวจ และข้อมูลภาพรวมเอกสารที่ตรวจเจอ เว็บไซต์และข้อมูลต่าง ๆ ที่เกี่ยวข้อง

อย่างไรก็ดี แม้ว่าองค์ความรู้และขั้นตอนการดำเนินงานโดยใช้กระบวนการสร้างเค้าร่างของอาชญากรเพื่อสืบสวนคดีอาชญากรรมคอมพิวเตอร์จะยังไม่มีความชัดเจนมากนัก แต่จากกรณีตัวอย่างที่ยกขึ้นมา ทำให้เห็นว่าในต่างประเทศได้มีการศึกษาวิจัยและนำเสนอตัวแบบของการจัดทำเค้าร่างของอาชญากรโดยใช้ระบบคอมพิวเตอร์จำนวนไม่น้อย ประกอบกับมีการปฏิบัติงานจริงโดยหน่วยงานในกระบวนการยุติธรรมของประเทศไทย หากมีการศึกษาวิจัยอย่างต่อเนื่อง รวมถึงการปฏิบัติการจริงของหน่วยงานเหล่านี้ กระบวนการถ่ายทอดกรณีตัวอย่างการสืบสวนที่ประสบความสำเร็จจำนวนมากพอ จะทำให้มีการนำไปประยุกต์ใช้กับกรณีอาชญากรรมทางคอมพิวเตอร์รูปแบบอื่น ๆ ต่อไป

การประยุกต์ใช้การจัดทำเค้าร่างของอาชญากรสำหรับอาชญากรรมทางคอมพิวเตอร์ (Digital Profiling) กรณีศึกษาการปลอมแปลงเว็บไซต์วารสารทางวิชาการ

กรณีการปลอมแปลงเว็บไซต์วารสารทางวิชาการ Mehrdad Jalalian และ Hamidreza Mahboobi (2015) เปิดเผยเกี่ยวกับข้อมูลเชิงลึกของเว็บไซต์วารสารทางวิชาการที่ถูกปลอมแปลงขึ้นมาโดยให้ข้อมูลเจาะลึกเกี่ยวกับอาชญากรกลุ่มนี้ ตลอดจนให้ข้อมูลของวิธีการที่พวกเขาให้หาเหยื่อ วิธีการหลอกลวงเหยื่อให้มาตีพิมพ์ในเว็บไซต์วารสารทางวิชาการที่ปลอมแปลงขึ้นเพื่อให้ได้เงินค่าธรรมเนียมในการตีพิมพ์ และการซ่อนตัวตนให้พ้นจากการถูกติดตามจับกุม ซึ่งจากการศึกษานี้สามารถระบุกลุ่มอาชญากรได้เป็น 3 กลุ่ม คือ 1) ผู้ช่วยศาสตราจารย์ด้านเทคโนโลยีสารสนเทศจากประเทศซาอุดิอารเบียกับพวกที่เป็นผู้เชี่ยวชาญ

จากประเทศปากีสถานทำการปลอมแปลงเว็บไซต์วารสารทางวิชาการอย่างน้อย 6 วารสาร สำหรับอาชญากรรายนี้มีภูมิลำเนามาจากปากีสถาน เขาได้รับปริญญาดุษฎีบัณฑิตจากประเทศมาเลเซีย และใช้คอมพิวเตอร์โน้ตบุ๊คยี่ห้อ *HP* ในช่วงปี 2556-2558 ด้วยความทุ่มเทในการทำผลงานทางวิชาการทำให้เขาได้ดำรงตำแหน่งด้านการบริหารของมหาวิทยาลัยในประเทศซาอุดิอาระเบีย 2) อาชญากรที่ใช้ชื่อปลอมว่า *James Robinson* และใช้ที่อยู่ปลอมว่าอาศัยอยู่ที่ประเทศสหรัฐอาหรับเอมิเรตส์ รายนี้ทำการปลอมแปลงเว็บไซต์วารสารกว่า 20 วารสาร 3) อาชญากรที่เป็นชาวยุโรปและใช้ชื่อปลอมว่า *Ruslan Boranbaev* เขาใช้คอมพิวเตอร์โน้ตบุ๊คยี่ห้อ *"Sony"* และทำการปลอมแปลงวารสารกว่า 25 วารสาร โดยการดำเนินงานของเขานั้นมีการทำการปลอมแปลงอย่างเป็นระบบมากจนถูกเรียกว่าเป็น *The King of Hijacked Journals* ผลงานที่โดดเด่นของเขาคือ การทำช่องทางปลอมของ ของ *Web of Sciences* เพื่อเปิดรับบทความทางวิชาการโดยใช้เซิร์ฟเวอร์ในประเทศฝรั่งเศส เพื่อทำให้มีความน่าเชื่อถือและเหยื่อจะได้ส่งบทความมาตีพิมพ์ยังเว็บไซต์วารสารวิชาการถูกปลอมแปลงนั้น นอกจากนี้ยังส่งลิงค์เว็บไซต์วารสารวิชาการปลอมให้กับ *Thomson Reuters* เพื่อทำลิงค์มายังเว็บไซต์ปลอม และเขายังได้สร้างช่องทางในการจ่ายเงินออนไลน์จำนวนมากเพื่อรอรับเงินค่าธรรมเนียมในการตีพิมพ์บทความจากเว็บไซต์ปลอมที่สร้างขึ้นจำนวนมากอีกด้วย

ข้อมูลที่ Mehrdad Jalalian และ Hamidreza Mahboobi (2015) เปิดเผยข้างต้น มาจากการสืบค้นข้อมูลผ่านเว็บไซต์ของวารสารทางวิชาการที่ถูกปลอมแปลงเหล่านั้น โดยทำการวิเคราะห์จากไฟล์ที่แสดงในเว็บไซต์ รวมถึงข้อมูลการจดทะเบียนโดเมนและข้อมูลสำหรับการติดต่อช่องทางต่าง ๆ ของผู้ปลอมแปลงเว็บไซต์ จนทำให้ได้ข้อมูลที่ชัดเจนเกี่ยวกับกลุ่มอาชญากรที่นำเสนอข้างต้น จะเห็นได้ว่าแม้แต่วิชาการที่มีความเชี่ยวชาญด้านเทคโนโลยีและสารสนเทศ ยังสามารถทำการสืบค้นข้อมูลจนสามารถระบุกลุ่มอาชญากรเหล่านี้ได้ จึงเป็นไปได้ที่เจ้าหน้าที่ฝ่ายสืบสวนมีทั้งอำนาจตามกฎหมาย เครื่องมือที่เหมาะสม รวมถึงความเชี่ยวชาญและประสบการณ์จะสามารถนำองค์ความรู้การจัดทำเค้าร่างของอาชญากรสำหรับอาชญากรรมทางคอมพิวเตอร์ที่กล่าวมาข้างต้นมาประยุกต์ใช้กับสืบสวนอาชญากรรมทางคอมพิวเตอร์รูปแบบนี้ได้ รวมถึงหากได้ทดลองดำเนินการจริงจะทำให้เกิดการพัฒนาองค์ความรู้นี้เพื่อการต่อยอดไปสู่การปฏิบัติได้จริง

กรณีศึกษาที่ยกมานี้เป็นรูปแบบอาชญากรรมทางคอมพิวเตอร์ไม่เป็นที่รับรู้ในวงกว้างมากนัก นอกเหนือจากประเด็นของการที่ผู้กระทำความผิดอาศัยอยู่นอกราชอาณาจักรไทยแล้ว ประเด็นอุปสรรคสำคัญอีกประการหนึ่ง คือ ยังไม่ปรากฏข้อมูลทั้งระดับนานาชาติและประเทศไทยว่ามีเหยื่อที่ไปแจ้งความว่าได้รับความเสียหายโดยจ่ายเงินให้กับอาชญากรกลุ่มนี้เพื่อตีพิมพ์บทความในเว็บไซต์ที่ถูกปลอมแปลง ทั้งที่มีข้อมูลประมาณการว่าอาชญากรทางคอมพิวเตอร์ได้รับเงินค่าธรรมเนียมในการตีพิมพ์บทความเป็นเงินหลายล้านเหรียญดอลลาร์สหรัฐ (*Jalalian & Mahboobi, 2014; Kolata, 2013* อ้างถึงใน *Jalalian M. & Bimler D., 2014*) สาเหตุเพราะกลุ่มเป้าหมายที่เจาะจงไปยัง

กลุ่มนักวิชาการเกรงผลกระทบต่อความน่าเชื่อถือทางวิชาการและผลกระทบต่อสถาบันที่สังกัดทำให้ปกปิดข้อมูลการตกเป็นเหยื่อไว้ แต่ปรากฏการณ์ของการที่มีเว็บไซต์วารสารทางวิชาการที่ถูกปลอมแปลงเกิดขึ้นจำนวนมากนี้ย่อมส่งผลกระทบโดยตรงต่อคุณภาพ ความถูกต้องของผลงานวิจัยและคุณภาพด้านการผลิตบุคลากรทางการศึกษาของประเทศ จึงทำให้แม้ว่ายังไม่พบกรณีปัญหาในประเทศไทย แต่ก็เห็นความจำเป็นที่จะต้องเตรียมการเพื่อรับมือกับปัญหานี้ การประยุกต์ใช้องค์ความรู้เรื่องการจัดทำเค้าร่างอาชญากรทางคอมพิวเตอร์กับการสืบหาตัวผู้กระทำความผิดจึงเป็นทางเลือกหนึ่งของการเตรียมความทางด้านการพัฒนาองค์ความรู้ใหม่

การนำองค์ความรู้เรื่องการจัดทำเค้าร่างอาชญากรมาประยุกต์ใช้กับกรณีศึกษาการปลอมแปลงเว็บไซต์ของวารสารทางวิชาการยังคงมีปัญหาอุปสรรคดังที่ได้นำเสนอข้างต้น ซึ่งทำให้เกิดความตระหนักว่าองค์ความรู้ในเรื่องนี้ยังจำเป็นต้องมีการพัฒนาทั้งด้านองค์ความรู้ การทดลองนำไปสู่การปฏิบัติจริงเพื่อนำไปสู่การกำหนดนโยบาย การออกกฎหมายและแนวทางที่รองรับ เพราะการจัดทำเค้าร่างของอาชญากรนั้น ข้อมูลที่ได้สามารถนำมาใช้ในการจัดทำมาตรการเชิงรุก คือ ให้ข้อมูลรูปแบบการก่ออาชญากรรมของผู้กระทำผิดกลุ่มนี้กับกลุ่มเหยื่อ หรือหน่วยงานที่เกี่ยวข้องเพื่อประกาศสู่วงกว้าง เพื่อการเฝ้าระวังไม่ให้ตกเป็นเหยื่อ ตลอดจนให้ข้อมูลกับหน่วยงานในกระบวนการยุติธรรมที่เกี่ยวข้องถึงรูปแบบ เพื่อให้เตรียมการด้านกฎหมายต่าง ๆ ตลอดจนเทคนิค กระบวนการและวิธีการติดตามสืบสวนเพื่อจับกุม เพราะหากมีเหตุเกิดขึ้นในประเทศไทยก็สามารถที่จะดำเนินการทางคดีได้โดยไม่ต้องเสียเวลาในการไปดำเนินการเรื่องกฎหมายหรือส่วนที่เกี่ยวข้องต่าง ๆ ในภายหลัง นับเป็นการเตรียมการรับมือกับรูปแบบของคดีที่อาจจะเกิดขึ้นได้ในอนาคต

▣ บทสรุป

การจัดทำเค้าร่างของอาชญากร เป็นองค์ความรู้ใหม่สำหรับประเทศไทย ในช่วงที่ผ่านมาพบว่ากองบัญชาการตำรวจสอบสวนกลางได้มีการนำมาใช้ในการสืบสวนบางคดีที่เป็นคดีที่ร้ายแรงมีการกระทำผิดต่อร่างกายซึ่งสอดคล้องกับประเภทของคดีอาชญากรรมที่เหมาะสมกับการจัดทำเค้าร่างของอาชญากร เช่น คดีการทำร้ายทางเพศ การตัดอวัยวะภายในของเหยื่อ การกระทำรุนแรงและตัดอวัยวะศพ การวางเพลิงที่ไม่มีเหตุจูงใจ หรือการฆาตรกรรมอย่างรุนแรงทารุณโหดร้าย (สฤษดิ์ สืบพงษ์ศิริ, 2559) อย่างไรก็ตามการรูปแบบของการกระทำความผิดในปัจจุบันมีหลากหลายขึ้น อาชญากรรมทางคอมพิวเตอร์เป็นอีกรูปแบบหนึ่งที่มีความหลากหลาย ซับซ้อน และหาตัวผู้กระทำความผิดมาลงโทษได้ยาก การจัดทำเค้าร่างของอาชญากรสามารถนำมาประยุกต์ใช้กับการสืบหาตัวคนกระทำผิดได้ โดยใช้เทคนิควิธีการจัดทำเค้าร่างของอาชญากรที่เป็นพื้นฐานในการวิเคราะห์เกี่ยวกับพฤติกรรม เหยื่อ สถานที่เกิดเหตุ หลักฐานในที่เกิดเหตุ แล้วนำมาพัฒนาโดยใช้เครื่องมือ เช่น ระบบคอมพิวเตอร์ต่าง ๆ เข้ามาช่วยจนสามารถพัฒนาเป็นแนวทางการจัดทำเค้าร่างของอาชญากรทางคอมพิวเตอร์ได้ (Digital Profiling) ซึ่งในต่างประเทศได้มี

การศึกษาอย่างหลากหลาย ในประเทศไทยสามารถสนับสนุนให้มีการศึกษาเพิ่มเติมหรือนำตัวแบบมาทดลองและปรับใช้กับการสืบสวนอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่ง คือ การปลอมแปลงเว็บไซต์วารสารทางวิชาการได้ การใช้การจัดทำเค้าร่างอาชญากรนี้จะเป็นเสมือนการพัฒนาองค์ความรู้และเทคนิค ตลอดจนรูปแบบการรวบรวมหลักฐานและวิธีการสืบสวนใหม่ ๆ เพื่อเป็นเครื่องมือที่ช่วยในการเตรียมการเพื่อป้องกันเหตุไม่ให้เกิดขึ้น และถือเป็นมาตรการเชิงรุกเพื่อรับมือกับอาชญากรรมรูปแบบนี้ที่อาจเกิดขึ้นได้ในอนาคต

▣ บรรณานุกรม

มหาวิทยาลัยรังสิต, สถาบันอาชญาวิทยาและการบริหารงานยุติธรรม. (2559). **รายงานสรุปวิชาสัมมนาปัญหาอาชญากรรมในปัจจุบัน**

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2557). **รายงานประจำปีไทยเซิร์ต 2556.** กรุงเทพฯ: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

สฤษฎ์ สืบพงศ์ศิริ. (2559). **การจัดทำเค้าร่างของอาชญากรเบื้องต้น** [PowerPoint slides].

สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) สำนักงานตำรวจแห่งชาติ. (2557). **ข้อมูลสถิติคดีความผิดตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.** สืบค้นเมื่อ 11 มีนาคม 2559, จาก https://docs.google.com/viewer-?a=v&pid=sites&srcid=aGlnaHRlY2hjcmltZS5vcmd8d3d3fGd4OjE3Njg4MzQ0ZGRmNzBlMA

ictkm.info. (2555). **สถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์.** สืบค้นเมื่อ 11 มีนาคม 2559, จาก audit.hss.moph.go.th/uploadFiles/document/D00000001216_25552.pdf

Bohannon, J. (2015). **How to hijack a journal.** Retrieved December 10, 2015 from http://www.sciencemag.org/news/2015/11/feature-how-hijack-journal Bohannon, J. (2015). How to hijack a journal. Retrieved from science website: http://www.sciencemag.org/news/2015/11/feature-how-hijack-journal doi: 10.1126/science.aad7463

Britz, M. T. (2008). **Computer Forensics and Cyber Crime: An Introduction.** Upper Saddle River, NJ: Prentice Hall.

Canter, D., Alison, L., Alison, E., and Wentink, N. **The Organized/Disorganized Typology of Serial Murder: Myth or Model?** Psychology, Public Policy, and Law. 2004. 10; 293-320.

Colombini, C. & Colella, A. (2011). **Digital Profiling: A Computer Forensics Approach,** pp. 330–343,

Hadley, M., (2005). **Criminal Profiling as a Psychologically Influenced Aid to Criminal Investigations.** Senior Honors Theses. Paper 77.Hijacked Journals, July 26, 2016, https://scholarlyoa.com/other-pages/hijacked-journals/, Jeffrey Beall

Hochmuth, P., 2004: **Profiling Cybercrime–"Network Threats and Defence Strategies",** Network World, www.

networkworld.com, November 29, 2004, 1–2, accessed 12/2006.

Jalalian, M., & Dadkhah, M. (2015). The Full Story of 90 Hijacked Journals from August 2011 to June 2015. **Geographica Pannonica,** 19(2), 73–87.

Jalalian, M., & Mahboobi, H. (2014). **Hijacked Journal and Predatory Publishers: Is there a Need to Re-Think How to Assess the Quality of Academic Research?.** Walailak Journal, 11(5), 389-394.

Kocsis, R. & Palermo, G. (2008). Contemporary Problems in Criminal Profiling, **Chapter 16, Criminal Profiling: International Theory, Research, and Practice.** Edited by: R. N. Kocsis , Humana Press Inc., Totowa, New JerseyPetherick, W., 2005: The Science of Criminal Profiling. Barnes and Noble, New York. SymantecCorporation. (2014). Internet Security Threat Report Appendices. 20.

Turvey, B., (2002). **Criminal Profiling: An Introduction to Behavioural Evidence Analysis.** 2nd Ed. Academic Press, New York.

Wori, O. (2014). Computer Crimes: Factors of Cybercriminal Activities. **International Journal of Advanced Computer Science and Information Technology,** 3(1), 51-67