รายงานวิจัยฉบับสมบูรณ์

โครงการการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปราม
อาชญากรรมทางเทคโนโลยี

โดย

ผู้ช่วยศาสตราจารย์พิเศษ พลตำรวจโท ดร.ณรงค์ กุลนิเทศ และคณะ

หลักสูตรปรัชญาดุษฎีบัณฑิต และวิทยาศาสตรมหาบัณฑิต
สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

กันยายน 2562

สัญญาเลขที่ RDG6140053

รายงานวิจัยฉบับสมบูรณ์
โครงการ
การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

คณะผู้วิจัย	สังกัด
1. ผู้ช่วยศาสตราจารย์พิเศษ พลตำรวจโท ดร.ณรงค์ กุลนิเทศ	ประธานหลักสูตรปรัชญาดุษฎีบัณฑิต และวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
2. รองศาสตราจารย์ พันตำรวจเอก วรธัช วิชชุวาณิชย์	รองศาสตราจารย์ (สบ.5) กลุ่มงานคณาจารย์ รองคณบดีคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
3. ผู้ช่วยศาสตราจารย์พิเศษ ดร.ศรีปริญญา ธูปกระจ่าง	อาจารย์ประจำหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการบริหารการพัฒนา มหาวิทยาลัยราชภัฏสวนสุนันทา
4. อาจารย์ ดร.ณิช วงศ์ส่องจ้า	หัวหน้าสาขาวิชานิติวิทยาศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา
5. พันตำรวจโทชาญชัย วิญญูรัตนะ	สารวัตรจราจร สถานีตำรวจนครบาลบางพลัด กองบัญชาการตำรวจนครบาล

สนับสนุนโดย

สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)

บทสรุปสำหรับผู้บริการ

1. ความสำคัญของปัญหา

จากการเจริญเติบโตอย่างรวดเร็วของเทคโนโลยีในปัจจุบัน ได้นำมาซึ่งความสะดวกสบายความรวดเร็วฉับไว ส่งผลให้ชีวิตประจำวันของผู้คนในยุคเทคโนโลยีสารสนเทศง่ายขึ้น นอกจากประโยชน์มหาศาลที่ได้รับจากเทคโนโลยีอันทันสมัยนี้ สิ่งที่แฝงมาด้วย คือ ภัยร้ายที่อาจคุกคามชีวิต และทำให้สูญเสียทรัพย์สินได้อย่างง่ายดายอีกด้วย ดังนั้น หลายหน่วยงานทั่วโลกรวมทั้งประเทศไทย จึงได้มีการทำการสำรวจสถิติความเสียหายที่เกิดขึ้น จากอาชญากรรมทางเทคโนโลยีเพื่อเป็นบันทึกข้อมูลที่เป็นประโยชน์ในการป้องกันและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีต่อไป ปัจจุบันมีหน่วยงานของต่างประเทศหลายหน่วยงานที่ทำการสำรวจข้อมูลสถิติเกี่ยวกับความเสียหายที่เกิดขึ้นจากอาชญากรรมทางเทคโนโลยี เช่น Crime Scene Investigation (CSI) และ International Prevention Research Institute (IPRI) ซึ่งจากรายงานการสำรวจความเสียหายที่เกิดขึ้นของ CSI ประเทศสหรัฐอเมริกา พบว่า ความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมา คือ การฉ้อโกงทางคอมพิวเตอร์ และการปล่อยไวรัส ตามลำดับ ในขณะที่ AusCert ซึ่งเป็นหน่วยงานที่ช่วยเหลือฉุกเฉิน (CERT) ในประเทศออสเตรเลีย และประเทศชั้นนำในภูมิภาคเอเชีย/แปซิฟิก ได้ทำการสำรวจความเสียหายที่เกิดจากการก่ออาชญากรรมทางเทคโนโลยี พบว่า ความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมาคือ การปล่อยไวรัสและการเข้าถึงอินเทอร์เน็ตหรือเมล์โดยไม่ได้รับอนุญาตจากคนในองค์กรตามลำดับเว็บไซต์ที่มีชื่อเสียงหลายเว็บไซต์ก็ได้ทำการสำรวจข้อมูลและผลกระทบของการก่ออาชญากรรมทางเทคโนโลยีเช่นเดียวกัน

จากการที่คอมพิวเตอร์มีคุณประโยชน์นานับปการ จึงมีผู้นำเทคโนโลยีเหล่านั้น มาเป็นช่องทางหรือเป็นเครื่องมือที่ใช้ในการกระทำความผิด ซึ่งลักษณะหรือรูปแบบของความสัมพันธ์ระหว่างคอมพิวเตอร์กับอาชญากรรมทางเทคโนโลยี พอสรุปได้ดังนี้

1. Computer as “Targets” Crimes คือ คอมพิวเตอร์เป็นเป้าหมายในการก่ออาชญากรรม เช่น การลักทรัพย์เครื่องคอมพิวเตอร์ หรือชิ้นส่วนของเครื่องคอมพิวเตอร์ โดยเฉพาะที่มีขนาดเล็กแต่มีราคาแพง

2. Facilitation of “Traditional” Crimes คือ คอมพิวเตอร์เป็นเครื่องอำนวยความสะดวกในการก่ออาชญากรรมในรูปแบบ “ดั้งเดิม” เช่น ใช้เครื่องคอมพิวเตอร์ในการเก็บข้อมูลลูกค้ายาเสพติด หรือในกรณี UNABOMBER ซึ่งอาชญากรใช้คอมพิวเตอร์ในการกำหนดตัวเหยื่อจาก on-line address แล้วส่งระเบิดแสวงเครื่องไปทางไปรษณีย์ โดยวัตถุประสงค์เพื่อสังหารบุคคลที่ชอบเทคโนโลยีชั้นสูง

3. Computer-unique Crime คือ อาชญากรรมที่เกิดกับคอมพิวเตอร์โดยเฉพาะ เช่น การสร้างให้ไวรัสคอมพิวเตอร์ (computer virus) แพร่ระบาดไปในระบบเครือข่ายคอมพิวเตอร์โดยมีเจตนาที่จะสร้าง

ความเสียหาย Nuke การลักลอบเข้าไปในระบบคอมพิวเตอร์ (hacking /cracking) การละเมิดทรัพย์สินทางปัญญาที่เกี่ยวกับคอมพิวเตอร์ (violation of computer intellectual properties)

4. Computer as “Instrumentality” of Crimes คอมพิวเตอร์เป็นเครื่องมือในการประกอบอาชญากรรม เช่น การใช้เครื่องคอมพิวเตอร์ในการโอนเงินจากบัญชีธนาคารจากบัญชีหนึ่งไปเข้าอีกบัญชีหนึ่งโดยมีเจตนาทุจริต ใช้เครื่องคอมพิวเตอร์ในการเป็นเจ้ามือรับพนันเอาทรัพย์สิน หรือ ใช้คอมพิวเตอร์ในการเผยแพร่เอกสาร สิ่งพิมพ์ รูปภาพ หรือ โฆษณาวัตถุ ลามก อนาจาร ผิดกฎหมาย

โดยปัญหาของอาชญากรรมทางเทคโนโลยีนั้น สาเหตุส่วนใหญ่ที่ทำให้เป็นปัญหา และไม่ได้รับความสนใจ เช่น

1) อาชญากรรมทางเทคโนโลยีโดยธรรมชาติจะมีความไม่เป็นส่วนตัว (Impersonal) จึงไม่มีผลกระทบต่อจิตใจและความรู้สึก (emotion) ของประชาชนโดยทั่วไปและถูกมองข้ามไป

2) อาชญากรรมทางเทคโนโลยีเช่น การละเมิดทรัพย์สินทางปัญญา (Theft of Intellectual Property), การโอนเงินโดยผิดกฎหมาย (Unlawful Transfer of Money) การฉ้อโกงด้านการสื่อสาร (Telecommunication Fraud) มีความแตกต่างกับอาชญากรรมแบบดั้งเดิมที่เจ้าหน้าที่ตำรวจมีความคุ้นเคยและเข้าใจเป็นอย่างดี เช่น การลักทรัพย์ ทำร้ายร่างกาย

3) เจ้าหน้าที่ตำรวจมักจะมองไม่เห็นว่าอาชญากรรมทางเทคโนโลยีนี้ เป็นปัญหาที่กระทบต่อประสิทธิภาพการปฏิบัติงานของตนจึงไม่ให้ความสนใจ

4) อาชญากรรมทางเทคโนโลยีแตกต่างจากอาชญากรรมรุนแรง (Violent crime) จึงทำให้เจ้าหน้าที่ผู้รับผิดชอบมีความจำเป็นที่จะต้องทุ่มเท สรรพกำลังไปในการแก้ไขปัญหาอาชญากรรมในรูปแบบทั่วไป

5) อาชญากรรมทางเทคโนโลยีมีความเกี่ยวพันอย่างยิ่งกับเทคโนโลยีสมัยใหม่ ซึ่งจะทำให้บุคคลที่ไม่มีความรู้เกี่ยวกับเทคโนโลยีที่เกี่ยวข้องเกิดความไม่กล้า (Intimidated) ในการที่จะเข้าไปยุ่งเกี่ยวข้องด้วย

6) บุคคลโดยส่วนมากจะมองอาชญากรรมทางเทคโนโลยีในลักษณะมิติเดี่ยว (Unidimensionally) ในลักษณะสภาวะของเหตุการณ์ที่เกิดขึ้นเป็นครั้ง ๆ ไป โดยอาจไม่นึกถึงผลกระทบ ความรุนแรงการแพร่กระจายและปริมาณของความเสียหายที่เกิดขึ้น ในการก่ออาชญากรรมแต่ละครั้งนั้น

7) เทคโนโลยีที่เกี่ยวข้อง และประสิทธิภาพในการใช้เทคโนโลยีของอาชญากรมีการพัฒนาที่รวดเร็ว ทำให้ยากต่อการเรียนรู้ถึงความเปลี่ยนแปลงในวงการของอาชญากรรมประเภทนี้

8) ผู้เสียหายกลับจะตกเป็นผู้ที่ถูกประณามว่า เป็นผู้เปิดช่องโอกาสให้กับอาชญากรในการกระทำผิดกฎหมาย เช่น ผู้เสียหายมักถูกตำหนิว่าไม่มีการวางระบบการรักษาความปลอดภัยที่เหมาะสมกับโครงข่ายงานคอมพิวเตอร์ บางครั้งจึงมักไม่กล้าเปิดเผยว่า ระบบของตนถูกบุกรุกทำลาย

9) ทรัพย์สินทางปัญญาโดยทั่วไปจะไม่สามารถประเมินราคาความเสียหายได้อย่างแน่ชัด จึงทำให้คนทั่วไปไม่รู้สึกถึงความรุนแรงของอาชญากรรมประเภทนี้

10) พนักงานเจ้าหน้าที่ที่เกี่ยวข้องอาจไม่มีความรู้ ความชำนาญ หรือความสามารถพอเพียงที่จะสอบสวนดำเนินคดีกับอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ

11) บุคคลทั่วไปมักมองเห็นว่า อาชญากรรมทางเทคโนโลยีนี้ไม่ได้เกิดขึ้นบ่อยครั้ง จึงไม่ควรค่าต่อการให้ความสนใจ

12) เจ้าหน้าที่ตำรวจมักใช้ความรู้ความเข้าใจในอาชญากรรมแบบดั้งเดิมนำมาใช้ในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี ซึ่งเป็นเหตุให้อาชญากรรมประเภทนี้ไม่ครบองค์ประกอบความผิดตามอาชญากรรมแบบดั้งเดิม และถูกมองข้ามไปโดยไม่พบการกระทำผิด

13) เจ้าหน้าที่ตำรวจโดยทั่วไปไม่มีการเตรียมการเพื่อรองรับอาชญากรรมทางเทคโนโลยีอย่างจริงจัง

14) ในปัจจุบันนี้อาชญากรรมทางเทคโนโลยีไม่ใช่อาชญากรรมที่มีผลกระทบต่อความมั่นคงทางการเมือง เมื่อเทียบกับอาชญากรรมที่เกี่ยวกับทรัพย์ หรือ ชีวิตร่างกาย ซึ่งทำให้ประชาชนเกิดความรู้สึกไม่ปลอดภัยในชีวิตและทรัพย์สิน (ญาณพล ยั่งยืน, 2555)

ด้วยปัญหาทางด้านอาชญากรรมทางเทคโนโลยีมีปัญหาอยู่หลายประการที่กล่าวมาข้างต้นนั้น ประเด็นปัญหาที่สำคัญโครงสร้างทางกฎหมายทำให้เกิดปัญหาด้านการสืบสวนสอบสวนทางด้านอาชญากรรมทางเทคโนโลยีกฎหมาย และความรู้ของพนักงานสอบสวน ตลอดจนการรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล ยังก้าวไปไม่ทันต่อการกระทำผิดทางด้านอาชญากรรมทางเทคโนโลยี เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจาก ความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน (Globalization) ความรู้ทางด้านอาชญากรรมทางเทคโนโลยีของเจ้าหน้าที่รัฐยังไม่เพียงพอ การศึกษา การค้นหา การเก็บรวบรวมพยานหลักฐาน และการพิสูจน์หลักฐานดิจิตอล เป็นอีกเรื่องหนึ่งที่เจ้าหน้าที่รัฐยังไม่มีความรู้เพียงพอ การหาแนวทางและวิธีการตรวจพิสูจน์ให้มีวิธีการที่ทันสมัยมากยิ่งขึ้น เป็นเรื่องที่ต้องดำเนินการ (ณรงค์ กุลนิเทศ, 2557)

ในปัจจุบันมีหน่วยงานหลักหลายหน่วยงานที่มีภารกิจที่บังคับใช้กฎหมาย อำนวยความยุติธรรม ป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงการตรวจพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ที่มีภารกิจป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี รับแจ้งแบะแสจากประชาชน ตลอดจนให้คำปรึกษาแนะนำ ตลอดจนรวบรวมสภาพปัญหา เพื่อเสนอแนะแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยี และสนับสนุนการปฏิบัติงานของหน่วยงานอื่น ตลอดจนประสานความร่วมมือระหว่างหน่วยงานภายในประเทศและต่างประเทศในการป้องกันอาชญากรรมทางเทคโนโลยี เป็นต้น และหน่วยงานที่สำคัญ คือ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจที่มีหน้าที่และความรับผิดชอบเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐานและของกลางในคดีที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยี และสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) สำนักงานตำรวจแห่งชาติ ที่มีหน้าที่ศึกษา วิเคราะห์ วิจัย และพัฒนาระบบงานเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจน

ฝึกอบรมเทคโนโลยีสารสนเทศและการสื่อสารให้แก่ข้าราชการตำรวจ ซึ่งภารกิจ และหน้าที่ความรับผิดชอบของแต่ละหน่วยงานมีการทำงานที่คล้ายคลึงกัน ทำให้เกิดปัญหาในด้านต่าง ๆ เช่น อำนาจหน้าที่รับผิดชอบหรือการครอบครองวัตถุพยานที่อาจจะมีปัญหาในการตรวจพิสูจน์

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 (พ.ศ. 2560-2564) มุ่งเสริมสร้างกลไกการพัฒนาให้มีประสิทธิภาพและสอดคล้องกับสถานการณ์ที่เป็นปัจจุบันมากขึ้นทั้งกลไกที่เป็นกฎหมายและกฎระเบียบต่างๆ และกลไกการทำงานในรูปแบบของคณะกรรมการ หรือหน่วยงานที่รับผิดชอบการขับเคลื่อนยุทธศาสตร์ในทุกระดับให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ ลดความซ้ำซ้อนทั้งในระดับประเทศและระดับพื้นที่ให้ดำเนินงานได้อย่างมีประสิทธิภาพ และในขณะเดียวกันก็เพิ่มบทบาทของกลไกภาคองค์ความรู้ เทคโนโลยี นวัตกรรม และความคิดสร้างสรรค์ให้เป็นเครื่องมือหลักในการขับเคลื่อนการพัฒนาในทุกภาคส่วน โดย ข้อ 1.3 (สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักนายกรัฐมนตรี, 2558, หน้า 3) ระบุว่าประเทศไทยต้องเผชิญกับแรงกดดันและความเสี่ยงมากขึ้นภายใต้สถานการณ์ที่ กระแสโลกาภิวัตน์เข้มข้นมากขึ้น เป็นโลกไร้พรมแดน โดยมีการเคลื่อนย้ายคน เงินทุน องค์ความรู้ เทคโนโลยี ข่าวสาร สินค้าและบริการอย่างเสรีทำให้การแข่งขันในตลาดโลกรุนแรงขึ้น ส่งผลให้มีการรวมตัวด้านเศรษฐกิจ ของกลุ่มต่างๆ ในโลกมีความเข้มข้นขึ้น ประเทศเศรษฐกิจใหม่มีขีดความสามารถในการแข่งขันมากขึ้น เช่น จีน อินเดีย ละตินอเมริกา และเวียดนาม ซึ่งมีแรงงานราคาถูกและมีมาตรการอื่นๆประกอบในการดึงดูดการลงทุน จากต่างประเทศได้เพิ่มขึ้น นอกจากนั้นการพัฒนาการสื่อสารด้วยเทคโนโลยีสมัยใหม่ทำให้สังคมโลกมีความเชื่อมโยงกันอย่างใกล้ชิดมากขึ้น เกิดภัยคุกคามและความเสี่ยง เช่น การก่อการร้าย โรคระบาด อาชญากรรมข้ามชาติ เป็นต้น

จากความเป็นมาดังกล่าวข้างต้น ผู้วิจัยมีความสนใจที่จะการศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยศึกษาจากเอกสารงานวิจัยที่เกี่ยวข้องทั้งภายในประเทศ และต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีในแต่ละหน่วยงาน เพื่อรวบรวมข้อมูลเกี่ยวกับการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำมาพัฒนางาน รวมทั้งการสัมภาษณ์ผู้ที่ปฏิบัติงานที่เกี่ยวข้องกับ งานทางด้านดังกล่าว เพื่อให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้ง คุ้มครองสิทธิและเสรีภาพด้วย ความรวดเร็ว เที่ยงตรง และเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้เป็นที่ยอมรับศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

2. คำถามในการวิจัย

1) การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จะสามารถแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีได้เป็นอย่างไร

2) องค์ความรู้ในการจัดทำคู่มือการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จะสามารถนำมาใช้ประโยชน์ได้เป็นอย่างไร

3. วัตถุประสงค์ของการวิจัย

1) เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) เพื่อกำหนดรูปแบบการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

3) เพื่อสร้างองค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

4. ขอบเขตของการวิจัย

การวิจัยครั้งนี้ เป็นการศึกษาเกี่ยวกับการวิจัยเชิงคุณภาพมาดำเนินการ เพื่อนำข้อค้นพบที่ได้รับมาถอดบทเรียน โดยนำแนวคิดทฤษฎีที่เกี่ยวข้องที่ได้จากการศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้องกับ การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และข้อมูลสำคัญและนำมาถอดบทเรียน โดยมีประเด็นหลัก ๆ ดังนี้

ประเด็นที่ 1 หน่วยงานตำรวจที่ปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 2 การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 3 การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 4 องค์ความรู้ และความชำนาญงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 5 การพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 6 การสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยี

5. ผลที่คาดว่าจะได้รับ

1) ได้ทราบถึงแนวทางในการพัฒนานโยบายการบริหาร การจัดการ รวมทั้งปัญหาอุปสรรคในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การบูรณาการการทำงานของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และข้อกฎหมายและระเบียบที่เหมาะสมต่อการนำไปใช้ในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) ได้คู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ใช้ในการปฏิบัติงานของหน่วยงานตำรวจ

6. ผลที่คาดว่าจะได้รับเมื่อสิ้นสุดการวิจัย

1) Output

1.1) ทำให้เกิดองค์ความรู้และความเข้าใจที่จัดทำในรูปแบบคู่มือการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

1.2) ทำให้เกิดการพัฒนาประสิทธิภาพงานของหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) Outcome

2.1) ทำให้เกิดการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

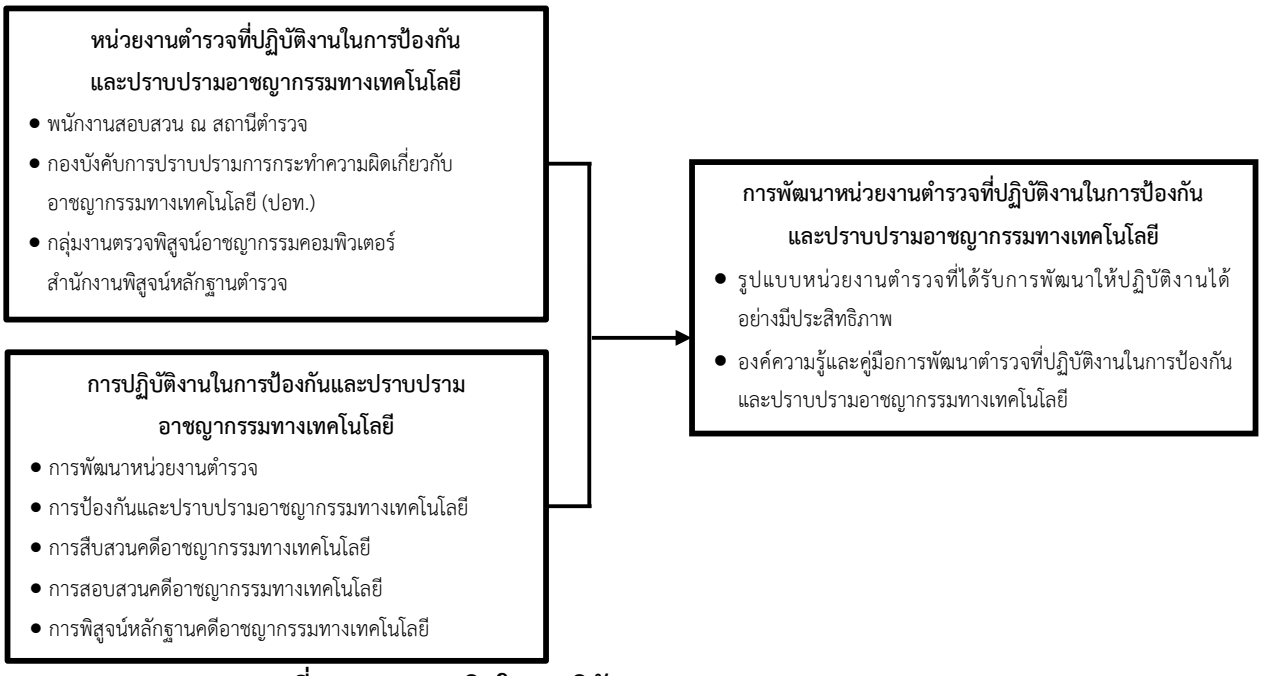
3) Impact

3.1) ทำให้เกิดแนวความคิดขององค์ความรู้และความเข้าใจที่ในการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

3.2) ทำให้การเกิดอาชญากรรมทางเทคโนโลยีของประเทศไทยมีปริมาณลดลง และหน่วยงานตำรวจที่ปฏิบัติงานสามารถปฏิบัติหน้าที่ในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากขึ้น

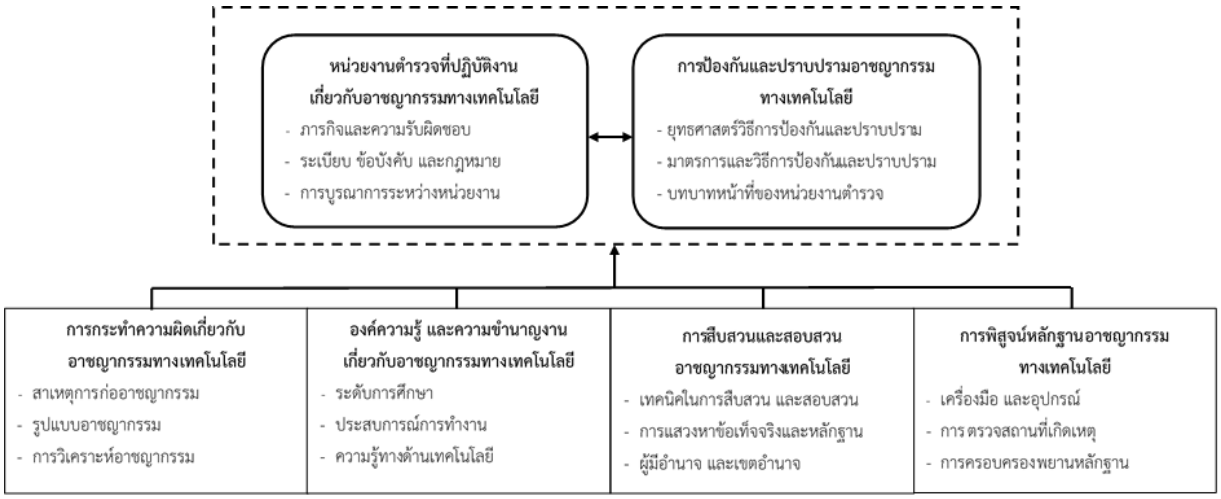
7. กรอบแนวคิดในการวิจัย (Conceptual Framework)

คณะผู้วิจัยได้นำที่มาและความสำคัญ และการทบทวนเอกสารเชิงสังเคราะห์ในการวิจัย แนวคิดต่าง ๆ รวมถึงงานวิจัยที่เกี่ยวข้องมาสังเคราะห์ และนำมารวบรวมให้เกิดกรอบแนวคิดของการวิจัย และกรอบวิเคราะห์ในการวิจัย ได้ดังนี้



ภาพที่ 1 กรอบแนวคิดในการวิจัย (Conceptual Framework)

8. กรอบวิเคราะห์ในการวิจัย (Analysis Framework)



ภาพที่ 2 กรอบวิเคราะห์ของการวิจัย (Analysis Framework)

9. ระเบียบวิธีวิจัย

แนวทางที่ใช้ในการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยใช้แนวทางการวิจัยเชิงคุณภาพ (Qualitative Research) โดยทำการศึกษาเก็บข้อมูล เชิงลึกกับกลุ่มตัวอย่าง ผู้วิจัยได้กำหนดวิธีการวิจัยที่จะนำมาใช้ในการวิจัยครั้งนี้ เพื่อให้ได้มาซึ่งข้อมูลตามวัตถุประสงค์ของการวิจัยที่ถูกต้องและเชื่อถือได้ ประกอบด้วยการค้นคว้าจากเอกสารและบทความทางวิชาการที่เกี่ยวข้องจากหลายแห่ง

ประชากรและกลุ่มตัวอย่างของการวิจัย

ผู้วิจัยคัดเลือกจากประชากรซึ่งมีประสบการณ์เกี่ยวกับการทำสำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี รวมทั้ง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยเลือกจากผู้ที่มีความรู้และประสบการณ์ที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี การวิจัยประเภทนี้ จะเป็นกลุ่มตัวอย่างที่เป็นผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญพิเศษเฉพาะด้านที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี สอดคล้องกับประเภทของอาชญากรรมไซเบอร์ ซึ่งแบ่งออกเป็น 2 กลุ่ม ดังนี้

1) กลุ่มตัวอย่างที่ใช้ในการสัมภาษณ์เชิงลึก ได้แก่

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) พนักงานสอบสวน ฝ่ายสืบสวน และฝ่ายป้องกันและปราบปรามของสถานีตำรวจนครบาล และสถานีตำรวจภูธร

(3) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

(4) อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมทางเทคโนโลยี

2) กลุ่มตัวอย่างที่ใช้ในการประชุมกลุ่มย่อย (Focus Group) ได้แก่

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) เจ้าหน้าที่ตำรวจกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจ

(3) เจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(4) เจ้าหน้าที่ตำรวจสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.)

(5) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES)

10. ผลที่คาดว่าจะได้รับเมื่อสิ้นสุดการวิจัย

1. Output

- ทำให้เกิดองค์ความรู้และความเข้าใจที่จัดทำในรูปแบบคู่มือการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
- ทำให้เกิดการพัฒนาประสิทธิภาพงานของหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2. Outcome

- ทำให้เกิดประสิทธิภาพในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

3. Impact

- ทำให้เกิดแนวความคิดและมาตรฐานขององค์ความรู้และความเข้าใจที่ในการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
- ทำให้การเกิดอาชญากรรมทางเทคโนโลยีของประเทศไทยมีปริมาณลดลง และหน่วยงานตำรวจที่ปฏิบัติงานสามารถปฏิบัติหน้าที่ในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากขึ้น

11. สรุปผลการวิจัย

1) การศึกษาพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

แนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น คือ

(1) ด้านบุคลากร พบว่า สตช.ยังขาดแคลนบุคลากรที่มีความรู้ ความสามารถในการดำเนินคดีอาชญากรรมทางเทคโนโลยีเป็นอย่างยิ่ง แต่ทราบว่า สตช.ได้พยายามเพิ่มอัตรากำลัง และฝึกอบรมบุคลากรด้านนี้เพิ่มเติมอยู่ ควรมีการกำหนดกรอบอัตราจำนวนที่เพียงพอต่อการปฏิบัติหน้าที่และกระจายบุคลากรออกไปในส่วนภูมิภาคอย่างทันต่อเหตุการณ์มิใช่กระจุกตัวอยู่ในส่วนกลาง

(2) ด้านการฝึกอบรม พบว่า การจัดอบรมให้กับเจ้าหน้าที่ตำรวจยังมีน้อย เมื่อเทียบกับความจำเป็นเร่งด่วนในการสร้างบุคลากรให้ทันต่อการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ควรจัดให้มีการอบรมตามรอบระยะเวลาที่เหมาะสมมีหลักสูตรระดับต้น กลาง สูง เพื่อสริมสร้างทักษะความรู้ต่างๆ ให้ทันต่อเหตุการณ์ การเรียนรู้ อาจมีทั้งการอบรมหรือศึกษาด้วยตนเอง

(3) ด้านงบประมาณ พบว่า ควรเพิ่มงบประมาณให้เพียงพอแก่การประชาสัมพันธ์ให้ประชาชนได้รับทราบให้มากที่สุด สื่อที่ใช้ควรมีหลายรูปแบบ เพื่อให้เข้าถึงประชาชนทุกกลุ่ม

(4) ด้านเครื่องมือ และอุปกรณ์ พบว่า สตช.ยังขาดแคลนงบประมาณในการจัดหาเครื่องมือ และอุปกรณ์ ให้เพียงพอต่อการดำเนินคดีอาชญากรรมทางเทคโนโลยี ในภูมิภาคต่างๆ ทั่วประเทศ ควรเพิ่มอุปกรณ์เครื่องมือทำงานสืบสวนหาทางจัดเก็บวัตถุพยานต่างๆ ให้มีประสิทธิภาพ น่าเชื่อถือเป็นไปตามมาตรฐานของต่างประเทศ ข้อมูลหรือผลลัพธ์ที่ได้ สามารถนำไปใช้ได้ต่างได้ทั่วโลก

(5) ด้านเทคโนโลยี พบว่า สตช.ควรนำเทคโนโลยีใหม่ๆ มาช่วยเจ้าหน้าที่ตำรวจทั้งด้านสืบสวน และสอบสวน เพื่อลดภาระในการทำงาน โดยเฉพาะในปัจจุบันที่เทคโนโลยีการสื่อสาร และการทำธุรกรรมต่างๆ ทำให้พยานหลักฐานแต่ละเรื่อง กระจายอยู่ในหลายท้องที่ ซึ่งมีความยุ่งยากในการรวบรวม รวมทั้งควรมีการติดตั้งปรับปรุง Software ที่ทันสมัยมากกว่าอาชญากรรมคอมพิวเตอร์ เพื่อให้พัฒนาขีดความสามารถได้เท่าทันอาชญากรรมเทคโนโลยี

(6) ด้านบริหารการจัดการ พบว่า ผู้บังคับบัญชาควรมีความรู้พื้นฐานเกี่ยวกับเรื่องอาชญากรรมทางคอมพิวเตอร์ เพื่อที่จะได้เข้าใจการทำงานของผู้ใต้บังคับบัญชา และเป็นผู้ให้คำชี้แนะแก่ผู้ใต้บังคับบัญชาหากเกิดปัญหาขัดข้อง

(7) ด้านโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า มีการกำหนดนโยบายที่ชัดเจน มีเป้าหมายที่แน่นอนมีแนวทางปฏิบัติหน้าที่เป็นขั้นเป็นตอนสอดคล้องกับนโยบายหลัก เพื่อให้การขับเคลื่อนขององค์กรเป็นไปในทิศทางเดียวกัน

(8) ด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน พบว่า การมีส่วนร่วมของหน่วยงานภาครัฐอื่น และภาคเอกชน มีความสำคัญในการช่วยเหลือเจ้าหน้าที่ตำรวจทั้งฝ่ายสืบสวน และสอบสวนได้มาก แต่ค่านิยมของคนไทย และสภาพสังคม ทำให้หน่วยงานภาครัฐอื่น และภาคเอกชน มักมองว่าเป็นหน้าที่ของเจ้าหน้าที่ตำรวจแต่เพียงฝ่ายเดียว ขาดการใส่ใจช่วยเหลือ ทั้งกรณีที่เป็นหน้าที่ตามกฎหมาย และกรณีที่สมควรจะช่วยเหลือได้ แม้ไม่มีหน้าที่โดยตรง การใช้มาตรการทางสังคมที่จะส่งเสริมให้ภาคเอกชน เข้ามามีส่วนร่วมในการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ตำรวจ จะช่วยเสริมประสิทธิภาพในการดำเนินคดีได้

มีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐทุกแห่งที่มีส่วนเกี่ยวข้อง รวมทั้งมีการบูรณาการร่วมกันระหว่างภาครัฐและภาคประชาชนหรือภาคเอกชน จะได้มุมมองที่กว้างและเป็นการรับฟังความคิดเห็นของภายนอกด้ว

(9) ด้านการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยี และด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า ในระยะเร่งด่วน ควรสร้างองค์ความรู้พื้นฐานของคดีอาชญากรรมทางเทคโนโลยีประเภทต่างๆ แบบสำเร็จรูป ให้ง่ายต่อการทำความเข้าใจ และมีตัวอย่าง คำแนะนำ และแนวทางแก้ปัญหาให้เจ้าหน้าที่ตำรวจในหน่วยงานย่อยท้องที่ต่างๆ สามารถศึกษาและจัดการคดีอาชญากรรมทางเทคโนโลยีในระดับที่ไม่ยุ่งยากซับซ้อนด้วยตัวเองได้ ในระยะยาว ควรเพิ่มเติมองค์ความรู้เฉพาะทางของคดีอาชญากรรมทางเทคโนโลยีประเภทต่างๆ ให้แก่หน่วยงานเฉพาะด้านของ สตช. ที่มีภารกิจเฉพาะด้าน และหน่วยงานในท้องถิ่น เพื่อรับมือกับคดีอาชญากรรมทางเทคโนโลยีทุกระดับที่จะเพิ่มปริมาณขึ้นในอนาคต รวมถึงการสร้างบุคลากรของหน่วยงานให้สามารถเติบโตได้อย่างมีความพร้อมในการปฏิบัติหน้าที่ และมีขวัญกำลังใจเพื่อทำงานในหน่วยงานเฉพาะด้านระยะยาวได้ และการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยีให้มีอิสระสามารถขับเคลื่อนองค์กรไปได้ตามภารกิจให้เกิดประสิทธิภาพสูงสุด บุคลากรของหน่วยงานควรได้รับการส่งเสริมให้มีความก้าวหน้าในหน่วย ตำแหน่งบริหารของหน่วยงาน ควรเป็นบุคลากรภายใน เพื่อเป็นขวัญกำลังใจของคนในหน่วย

จากการศึกษาการปฏิบัติงานของหน่วยงานทางด้านอาชญากรรมทางเทคโนโลยีของต่างประเทศ พบว่ามีขยายออกทั่วประเทศ คณะผู้วิจัยจึงมีความเห็นว่า ในการพัฒนางานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยการปรับปรุงโครงสร้างหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีใน 3 ระดับ คือ

(1) หน่วยงานระดับสถานีตำรวจ – เพิ่มงานพนักงานสอบสวน ผู้เชี่ยวชาญทางด้านอาชญากรรมทางเทคโนโลยีอยู่ในงานสอบสวนในสถานีตำรวจ

(2) หน่วยงานระดับกองบัญชาการ คือ กองบังคับการอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และกองบังคับการอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ขยายหน่วยงานเป็นกองบัญชาการอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.) ขยายหน่วยงานออกเป็นศูนย์ ซึ่งเป็นหน่วยงานเทียบเท่ากองบังคับการ ออกสู่ส่วนภูมิภาคเป็น 10 ศูนย์ คือ ศูนย์ ปอทศ. 1 (ปทุมธานี) ศูนย์ ปอทศ. 2 (ชลบุรี) ศูนย์ ปอทศ. 3 (นครราชสีมา) ศูนย์ ปอทศ. 4 (ขอนแก่น) ศูนย์ ปอทศ. 5 (ลำปาง) ศูนย์ ปอทศ. 6 (พิษณุโลก) ศูนย์ ปอทศ. 7 (นครปฐม) ศูนย์ ปอทศ. 8 (สุราษฎร์ธานี) ศูนย์ ปอทศ. 9 (สงขลา) และศูนย์ ปอทศ. 10 (ยะลา) เช่น เดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

(3) หน่วยงานศูนย์พิสูจน์หลักฐาน สำนักงานพิสูจน์หลักฐานตำรวจ พบว่า ทางสำนักงานพิสูจน์หลักฐานได้ดำเนินการวางแผนทางด้านบุคลากร และเครื่องมือสำหรับตรวจพิสูจน์ โดยมีบุคลากรที่ปฏิบัติงานทั้ง 11 แห่งไว้ครบแล้ว แต่อุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์มีเพียง 3 แห่ง คือ กองพิสูจน์หลักฐานกลาง, ศูนย์พิสูจน์หลักฐาน 7 (นครปฐม) และศูนย์พิสูจน์หลักฐาน 10 (ยะลา)

เท่านั้น ยังคงขาดเครื่องมือสำหรับตรวจพิสูจน์ที่ศูนย์พิสูจน์หลักฐานอีก 8 แห่ง จึงควรสนับสนุนงบประมาณในการจัดซื้ออุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์ให้ครบทั้ง 11 แห่ง

2) การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญงานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีรายละเอียดและสาระสำคัญโดยสรุป คือ ภัยคุกคามความปลอดภัยข้อมูลเกี่ยวกับอาชญากรรม ขั้นตอนการบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการรวบรวมพยานหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการบริหารจัดการและขนส่งพยานหลักฐาน ขั้นตอนการบริหารจัดการและจัดเก็บพยานหลักฐาน ขั้นตอนการเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน แนวทางคำถามสำหรับคดีด้านอาชญากรรมทางเทคโนโลยี และการตรวจพิสูจน์อาชญากรรมทางเทคโนโลยี

3) องค์ความรู้และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญทางด้านการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์องค์ความรู้ และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีรายละเอียด และสาระสำคัญโดยสรุป คือ สภาพการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ วิธีการและขั้นตอนการสืบสวนและสอบสวนเกี่ยวกับอาชญากรรมทางเทคโนโลยี กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี รายการอาชญากรรมทางเทคโนโลยี และพยานหลักฐานทางดิจิตอล หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ แนวทางบริหารจัดการและจัดเก็บพยานหลักฐาน ปัญหาข้อขัดข้องในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ การบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ การปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการปฏิบัติเพื่อบรรจุพยานหลักฐานลงบรรจุภัณฑ์ในสถานที่เกิดเหตุ การบริหารจัดการขนส่งพยานหลักฐาน การบริหารจัดการและจัดเก็บพยานหลักฐาน การเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน การทำลายข้อมูลในสื่อเก็บข้อมูล องค์ประกอบพื้นฐานของระบบเน็ตเวิร์คในบ้าน รายการอุปกรณ์และเครื่องมือสำหรับการปฏิบัติงาน และห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์

12. ข้อเสนอแนะ

12.1 ข้อเสนอแนะเชิงนโยบาย

12.1.1 รัฐบาลควรมีนโยบายโดยการใช้มาตรการทางสังคมที่ส่งเสริมให้ภาคเอกชนเข้ามามีส่วนร่วมในการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ โดยมีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐและ

ภาคประชาชน หรือภาคเอกชน เช่น ปัญหาในเรื่องการขอข้อมูลจากผู้ให้บริการประเภทต่าง ๆ ทั้งที่เกี่ยวกับระบบคอมพิวเตอร์ และธุรกรรมการเงินที่โต้แย้งอำนาจเจ้าหน้าที่ของรัฐอย่างไม่สมเหตุสมผล หรือให้ข้อมูลล่าช้า หรือปฏิเสธการให้ข้อมูลรวมทั้งการเรียกรับค่าใช้จ่ายจากเจ้าหน้าที่ของรัฐ ฯลฯ อาจหามาตรการจูงใจต่าง ๆ เพื่อให้ผู้บริการเต็มใจให้ความร่วมมือกับเจ้าหน้าที่ของรัฐ เช่น การให้คำรับรองหรือประกาศชมเชยว่าเป็นหน่วยงานที่มีความรับผิดชอบทางสังคม

12.1.2 รัฐควรมีนโยบายหรือใช้มาตรการทางภาษีให้กับหน่วยงานที่ให้บริการ หากให้ความร่วมมือกับเจ้าหน้าที่ อาจให้มีสิทธิในการนำไปคิดเป็นค่าใช้จ่าย โดยลดภาษีให้ หากไม่ให้ความร่วมมือกับเจ้าหน้าที่หรือให้ความร่วมมือล่าช้า อาจใช้กฎหมายสรรพากรไปใช้บังคับ ในกรณีที่ผู้ให้บริการไม่ให้ความร่วมมือ ถูกเรียกเก็บภาษีเพิ่ม หรือถูกปรับทางภาษีเพิ่มเติม

12.1.3 รัฐบาลควรมีนโยบายให้มีการบูรณาการร่วมกันอย่างชัดเจนระหว่างหน่วยงาน เพราะหน่วยงานที่ปฏิบัติงานทางด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีหลายหน่วยงานทั้งกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เช่น ให้กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคมออกกฎหมายรองรับการทำงานของเจ้าหน้าที่ตำรวจ รวมทั้งให้หน่วยงานที่เกี่ยวข้องปรับปรุงภารกิจ และความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง การเสนอขอแก้ไขกฎหมายข้อบังคับ ระเบียบที่เกี่ยวข้อง ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี

12.1.4 รัฐบาลควรมีนโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีการกำหนดนโยบายที่มีความชัดเจน รวมทั้งมีการวิเคราะห์บทบาทของหน่วยงานให้สอดคล้องกับการปฏิบัติงานจริง เพื่อให้การขับเคลื่อนขององค์กรเป็นไปในทิศทางเดียวกัน โดยเฉพาะการแก้ไขกฎหมายเพิ่มเติมขีดความสามารถ และอำนาจที่จะให้เข้าถึงข้อมูลต่าง ๆ ด้านเทคโนโลยีให้กับเจ้าหน้าที่ได้อย่างรวดเร็วเพื่อป้องกันปราบปรามและสืบสวนการกระทำผิด

12.1.5 รัฐบาลควรมีนโยบายให้ปรับปรุงโครงสร้างหน่วยงานที่ปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของสำนักงานตำรวจแห่งชาติใน 3 ระดับ คือ

(1) หน่วยงานระดับสถานีตำรวจ เพิ่มงานพนักงานสอบสวนผู้เชี่ยวชาญด้านอาขญากรรมทางเทคโนโลยี โดยรับจากผู้มีวุฒิทางด้านคอมพิวเตอร์เข้ามาปฏิบัติงานอยู่ในสถานีตำรวจ

(2) กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.) ปรับปรุงโครงสร้างเป็นกองบัญชาการ โดยขยายออกเป็นส่วนภูมิภาค 10 ศูนย์ เช่นเดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

(3) สำนักงานพิสูจน์หลักฐานตำรวจ เพิ่มงบประมาณในการจัดซื้อเครื่องมือสำหรับการตรวจพิสูจน์อาชญากรรมทางเทคโนโลยีในส่วนภูมิภาคให้ครบทั้ง 10 ศูนย์ ให้สามารถช่วยพนักงานสอบสวนในการพิสูจน์หลักฐานข้อเท็จจริง รวมทั้งการกำหนดวิธีการตรวจให้รัดกุม การเก็บหลักฐานให้เป็นระบบ

12.2 ข้อเสนอแนะเชิงปฏิบัติการ

12.2.1 ในเรื่องอำนาจการสอบสวนมีปัญหามากระหว่างสถานตำรวจกับ บก.ปอท. และ บก.ปอศ. จึงควรเพิ่มเจ้าหน้าที่ลงในสถานีตำรวจรับจากผู้ที่มีความรู้จริง อย่างน้อยปริญญาตรีทางคอมพิวเตอร์ แล้ว

นำมาอบรม ส่วน บก.ปอท. และ บก.ปอศ. ซึ่งเป็นหน่วยงานระดับกองบังคับการ ควรขยายโครงสร้างของหน่วยงานเป็นระดับกองบัญชาการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.) ขยายงานออกตามส่วนภูมิภาคออกเป็น 10 ศูนย์ เช่นเดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

12.2.2 พนักงานสอบสวนยังขาดความรู้ความเข้าใจในเรื่องอาชญากรรมทางเทคโนโลยี เมื่อมีผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที เพราะไม่รู้ถึงกระบวนการในการทำงานที่เกิดขึ้น ซึ่งเป็นปัญหาใหญ่ที่จะต้องมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยี และกฎหมายที่เกี่ยวข้อง โดยเฉพาะประเดนการตั้งคำถามของพนักงานสอบสวนเป็นเพราะขาดความรู้ ทำให้ตั้งคำถามอย่างไม่มีทิศทาง ทั้งนี้ รวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติด้วย แต่อย่างไรก็ตามคณะผู้วิจัยได้จัดทำคู่มือในการปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยีให้กับเจ้าหน้าที่ผู้ปฏิบัติ ซึ่งคาดว่าน่าจะแก้ไขปัญหาในเรื่องนี้อยู่ในระดับหนึ่ง รวมถึงการจัดการฝึกอบรมในหลักสูตรต่างๆ ที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี

12.2.3 ควรจัดแบ่งคดีอาชญากรรมทางเทคโนโลยี ออกเป็นประเภทต่างๆ รวมทั้งแบ่งระดับความยากง่าย เช่น ประเภทที่การกระทำผิดอยู่ในระบบเทคโนโลยี โดยตรง (เช่น ฉ้อโกงขายสินค้าทางอินเทอร์เน็ต ลักลอบทำธุรกรรม E-Banking ฯลฯ) กับประเภทที่การกระทำผิดไม่ได้อยู่ในระบบเทคโนโลยี แต่ใช้เทคโนโลยีเฉพาะการสื่อสาร หรือการทำธุรกรรมที่เกี่ยวข้อง (เช่น การขายสิ่งของผิดกฎหมาย แล้วมีการติดต่อสื่อสารกันด้วยโทรศัพท์หรือโปรแกรมสนทนาผ่านอินเตอร์เน็ต ฯลฯ) แล้วแยกระดับความยากง่าย

- การทำแบบฟอร์มสำเร็จรูป ละกำหนดช่องทางรวบรวมพยานหลักฐานจากผู้ให้บริการต่างๆ จะช่วยให้เจ้าหน้าที่ตำรวจได้รับความสะดวกมากยิ่งขึ้น สามารถใช้กับคดีที่ไม่ยุ่งยากซับซ้อน ลดภาระค่าใช้จ่ายและระยะเวลาทำคดีได้

12.2.4 ควรจัดแบ่งเจ้าหน้าที่ออกเป็นกลุ่ม เพื่อรับมือกับคดีทางด้านอาชญากรรมทางเทคโนโลยีที่มีความยากง่ายต่างๆ กัน เช่น

(1) ระดับที่ใช้ความรู้อย่างเดียว หรือใช้เทคโนโลยีที่มีอยู่ทั่วไปในการบริหารจัดการคดีได้

(2) ระดับที่ต้องใช้เครื่องมือพิเศษที่จะต้องมีความรู้เป็นการเฉพาะในการทำงาน เช่น การใช้โปรแกรมตรวจพิสูจน์

(3) ระดับที่ต้องใช้ทั้งเครื่องมือพิเศษ และความรู้พิเศษในการจัดการคดีที่มีความยุ่งยาก ซับซ้อนทางเทคโนโลยีโดยตรง เช่น การลักลอบเข้าถึงระบบคอมพิวเตอร์ ของหน่วยงานภาครัฐ หรือสถาบันการเงินก่อความเสียหายในรูปแบบต่าง ๆ

สภาพปัญหาในส่วนนี้ คือ การแก้ไขปัญหาโดยเข้าใจว่า คดีอาชญากรรมทางเทคโนโลยีมีความยุ่งยากซับซ้อนสูง ต้องรอให้มีผู้เชี่ยวชาญพิเศษพร้อมเครื่องมือและงบประมาณจึงจะทำคดีได้ กลายเป็นว่าคดีที่ไม่มีความยุ่งยากเพียงแต่ต้องอาศัยความรู้เบื้องต้น เจ้าหน้าที่ส่วนใหญ่ก็ยังไม่สามารถทำคดี หรือวางแผนการรวบรวมพยานหลักฐานได้

12.2.5 ผู้บังคับบัญชาในแต่ละหน่วยต้องหาแนวทางในการดำเนินคดีที่มีประสิทธิภาพลดกระบวนการทำงานที่ไม่จำเป็น หรือกระบวนการที่ไม่สามารถทำได้ เช่น การขอความร่วมมือระหว่างประเทศ

ในเรื่องทางอาญาหลายกรณีที่ไม่ทันเวลา หรือไม่ได้รับความร่วมมือจากต่างประเทศ แล้วใช้บุคลากรดำเนินคดีด้วยแนวทางที่เหมาะสมในแต่ละสถานการณ์

12.2.6 ควรพิจารณาแนวทางการสอบสวนในรูปแบบใหม่ๆ ที่จะช่วยลดภาวะด้านเวลาค่าใช้จ่ายให้แก่เจ้าหน้าที่ฝ่ายสืบสวนและพนักงานสอบสวน เช่น

- การสอบปากคำผ่านระบบ Video Conference
- การแบ่งงานบางส่วนให้ฝ่ายสืบสวน รวยรวมพยานหลักฐานในรูปแบบที่สามารถนำไปใช้เป็นพยานหลักฐานในการทำสำนวนการสอบสวนได้
- การจัดทำแบบฟอร์มมาตรฐานในการสอบปากคำ หรือขอข้อมูลเพื่ออำนวยความสะดวกสำหรับผู้เสียหายหรือพยานตามประเภท
- การใช้เอกสารอิเล็กทรอนิกส์ที่มีความน่าเชื่อถือและชอบด้วยกฎหมาย ในการติดต่อขั้นตอนต่างๆ สามารถนำมาใช้เป็นพยานหลักฐานและมีสภาพบังคับตามกฎหมายได้
- การใช้อาสาสมัครหรือนักศึกษาฝึกงานมาช่วยให้คำแนะนำแก่ผู้เสียหายในการจัดเตรียมข้อมูลและพยานหลักฐานเบื้องต้นให้แก่พนักงานสอบสวน

12.2.7 พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์ในหลายกรณีไม่มีความน่าเชื่อถือ เนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of Custody) หน่วยงานที่เกี่ยวข้องจึงต้องมีระเบียบข้อบังคับที่ชัดเจนในการบันทึกหลักฐานตามลำดับเวลาเพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอน และพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้นๆ สำหรับในเรื่องนี้ คณะผู้วิจัยได้จัดทำคู่มือในการปฏิบัติงานของพนักงานสอบสวน รวมถึงขั้นตอนเกี่ยวกับพยานหลักฐานไว้ส่วนหนึ่ง

12.3 ข้อเสนอแนะในการวิจัยครั้งต่อไป

12.3.1 หน่วยงานที่ดำเนินคดีอาชญากรรมทางเทคโนโลยี มีมากแต่ไม่มีการช่วยเหลือกันในหน่วยงานและระหว่างหน่วยงานเพื่อแก้ไขปัญหาต่างๆ อย่างเป็นระบบ ไม่เฉพาะแต่สำนักงานตำรวจแห่งชาติที่มีปัญหา แต่หน่วยงานอื่นๆ ก็มีปัญหาเหล่านี้ ทั้ง กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม (MDES) กรมสอบสวนคดีพิเศษ สำนักงานศาลและอัยการสูงสุด เป็นต้น จึงควรเข้าไปทำการศึกษาในเรื่องการมีส่วนร่วมระหว่างหน่วยงานที่เกี่ยวข้องเพื่อหาความเชื่อมโยง การสร้างเครือข่ายและการบูรณาการในการทำงานร่วมกันระหว่างหน่วยงาน ทำให้เกิดประสิทธิภาพของระบบการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

12.3.2 ระบบการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ ซึ่งในการศึกษาวิจัยครั้งนี้ ได้พยายามเข้าไปศึกษาถึงลักษณะการทำงานและโครงสร้างของหน่วยงานที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของต่างประเทศ ทั้งในอเมริกา ยุโรป และเอเชีย แต่ข้อมูลที่ได้อยู่ในระดับหนึ่งที่ยังไม่ละเอียดเท่าที่ควร จึงควรเข้าไปทำการศึกษาในเรื่องการป้องกันและปราบปรามอาชญากรรมเทคโนโลยีของต่างประเทศอย่างละเอียด โดยเฉพาะงานวิจัยทางด้านอาชญากรรม ทางด้านเทคโนโลยีของต่างประเทศ

12.3.3 ศึกษาถึงการวางรูปแบบในการขอข้อมูลจากหน่วยงานเอกชนที่ให้บริการประเภทต่างๆ ที่หน่วยงานรัฐประสบปัญหาทางด้านความล่าช้าและไม่ได้รับความร่วมมือ ทั้งการปฏิเสธและโต้แย้งอำนาจของเจ้าหน้าที่รัฐ ซึ่งอาจใช้มาตรการทางภาษี หรือใช้มาตรการของสรรพกร เพื่อนำมาแก้ไขปัญหา เพราะการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่จะได้ผลดีนั้น ต้องได้รับความร่วมมือจากหน่วยงานเอกชนที่ให้บริการ การศึกษาจะช่วยทำให้เกิดแนวทางในการปฏิบัติมากยิ่งขึ้น ส่งผลต่อประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

คำนำ

หลักสูตรปรัชญาดุษฎีบัณฑิต และวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา โครงการวิจัย เรื่อง “การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีจุดมุ่งหมายเพื่อศึกษาการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กำหนดรูปแบบที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และสร้างองค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยได้รับการสนับสนุนงบประมาณในการดำเนินงานจากสำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.) และได้รับคำแนะนำจาก พลตำรวจโท ดร.อดุลย์ ณรงค์ศักดิ์ ผู้ประสานงานของสำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.) จัดทำขึ้นจากการสกัดความรู้โดยผ่านกระบวนการประชุมกลุ่มย่อย และการสัมภาษณ์เจาะลึกจากทฤษฎีสู่การปฏิบัติเพื่อให้ได้ความรู้ใหม่ สามารถนำไปปฏิบัติงานได้อย่างเป็นระบบ โดยได้รับความร่วมมือจากสำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานอัยการสูงสุด สำนักงานอธิบดีผู้พิพากษาภาค 7 และโรงเรียนนายร้อยตำรวจ รวมทั้งองค์กรต่าง ๆ ที่เกี่ยวข้อง ที่ได้กรุณาสนับสนุนให้ข้อมูลและมุมมองข้อเสนอแนะ ซึ่งทั้งหมดต่างก็มีพื้นฐานอยู่บนหลักการเดียวกันเพื่อพัฒนางานด้านการป้องกัน ปราบปรามสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์ให้เกิดประสิทธิภาพสูงสุด อันเป็นประโยชน์อย่างยิ่งในการจัดทำรายงานเล่มนี้

คณะผู้ศึกษาวิจัยขอขอบพระคุณทุกท่านที่ให้การสนับสนุนกระบวนการศึกษา และหวังว่าคู่มือฉบับนี้จะเป็นประโยชน์ต่อการปฏิบัติงานตามเจตนารมณ์ และวัตถุประสงค์ของการวิจัยในการป้องกันและปราบปรามอาชญากรรมเทคโนโลยี

คณะผู้ศึกษาวิจัย
กันยายน 2562

บทคัดย่อ

การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี รวมทั้งการสืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์โดยเฉพาะ บังคับใช้กฎหมายโดยมุ่งเน้นการอำนวยความยุติธรรมป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีและบริการประชาชน อย่างมีมาตรฐานสากล เพื่อทำให้เกิดความสงบเรียบร้อย มั่นคง แก่สังคมและประเทศชาติ โดยมีวัตถุประสงค์เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กำหนดรูปแบบการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และสร้างองค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยการวิจัยเชิงคุณภาพ ศึกษาแนวคิดทฤษฎีที่เกี่ยวข้องจากเอกสาร และงานวิจัยที่เกี่ยวข้อง ประชากรเป้าหมาย คือ ผู้มีประสบการณ์เกี่ยวกับการทำสำนวนการสอบสวนรายงานการสืบสวนในกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี รวมทั้ง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จัดการสนทนากลุ่มย่อย และสัมภาษณ์เชิงลึกจากตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจทั่วประเทศ รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) เจ้าหน้าที่ตำรวจกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจ เจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) เจ้าหน้าที่ตำรวจสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) และนักวิชาการทางด้านเทคโนโลยีสารสนเทศจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) เพื่อถอดบทเรียนและสกัดความรู้ที่ได้จากการจัดประชุมกลุ่มย่อย และการสัมภาษณ์ ผลการวิจัยพบว่า 1) การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ต้องมีการพัฒนาหน่วยงานตำรวจทั้งทางด้านบุคลกร การฝึกอบรม งบประมาณ อุปกรณ์เครื่องมือ เทคโนโลยี การบริหารจัดการนโยบายและยุทธศาสตร์ รวมทั้งการบูรณาการร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องเพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน 2) รูปแบบการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ควรมีการจัดแบ่งคดีอาชญากรรมทางเทคโนโลยีออกเป็นประเภทต่าง ๆ โดยจัดแบ่งเจ้าหน้าที่ออกเป็นระดับ ลดกระบวนการที่ไม่สามารถทำได้ และมีรูปแบบการทำงานโดยการปรับโครงสร้างของงานออกเป็น 3 ระดับ คือ (1) ระดับสถานีตำรวจเพิ่มงานสอบสวนทางด้านอาชญากรรมทางเทคโนโลยี (2) ระดับกองบังคับการอาชญากรรมทางเทคโนโลยีและกองบังคับการอาชญากรรมทางเศรษฐกิจปรับโครงสร้างเป็นกองบัญชาการอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ โดยขยายออกไป 10 ศูนย์ในส่วนภูมิภาค รวมทั้ง (3) พัฒนาระดับศูนย์พิสูจน์หลักฐานอีก 8 ศูนย์ให้สามารถตรวจพิสูจน์อาชญากรรมทางเทคโนโลยีได้ และ 3) องค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ประกอบด้วยขั้นตอนการปฏิบัติงานทั้งทางด้านการสอบสวน ประเภทของคดี การตรวจสถานที่เกิดเหตุ การเก็บพยานหลักฐาน การตั้งประเด็นคำถามทั้งในการ

สอบสวน และการตรวจพิสูจน์หลักฐาน โดยการนำผลการวิจัยไปใช้ประโยชน์ เพื่อจัดทำแผนยุทธศาสตร์พัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และจัดทำคู่มือ การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเพื่อเป็นแนวทางปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้ความคุ้มครองทางกฎหมาย สิทธิและเสรีภาพอย่างรวดเร็ว เที่ยงตรง และเสมอภาค เป็นที่ยอมรับ ศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

Abstract

The development of police departments that operate in the prevention and suppression of technology criminals with duties and responsibilities in maintaining public order, preventing and suppressing criminals related to specific technology, including investigations and operations in accordance with the Criminal Procedure Law and other laws that especially related to computer systems. Enforcing the law with a focus on facilitating justice prevent and suppress crime in technology and public services with international standards. In order to create peace and stability for society and the nation the purpose of the research is to study the development of police departments that work in the prevention and suppression of technological crimes. Determine the operational model for the prevention and suppression of technological crimes and create knowledge and a guide for police development that works in the prevention and suppression of technological crimes by qualitative research. Study relevant theoretical concepts from documents and related research. The target population is people with experience in conducting investigations, investigative report on laws relating to technology crimes, including the development of police departments working in the prevention and suppression of technological crimes. Focus group discussions and in-depth interviews from representatives of the police department executives of the Metropolitan Police Station and the police station including the Crime Suppression Division on Technology Crimes Suppression Division (TCSD), Police officers of Computer forensic Sub-Division, office of Forensic Science , Police officers of Technology Crime Suppression Division, Police officer of Office of Information and Communication Technology (ICT) and academic in information technology from the Ministry of Digital Economy and Society (MDES) to extract lessons and extract knowledge from the meeting of focus group and in-depth interviews. The results of the research are as follows: 1) the development of police departments working in the prevention and suppression of technological crimes must develop police departments in terms of personnel, training, budget, equipment, technology, management policies and strategies including joint integration among relevant agencies to increase operational efficiency 2) forms of operation for prevention and suppression of technological crimes should be divided into different types, with officials divided into levels, reduce processes that cannot be done and there is a work pattern by adjusting the structure of the work into 3 levels as the police station level, increase the criminal investigation in technology of Technology Crime Division and the Economic Crime Division, restructured to be Technology and Economic Crime Headquarters, expanding to 10 regional centers and development for scientific crime detection center 8 regional center Can detection of technology criminals 3) the police knowledge and development manual that works in the prevention and suppression of technological crimes consists of operational procedures including investigations, case types, crime scene investigations, evidence collection, and questioning in the investigation and forensics by making use of the research results to formulate a strategic plan, develop a police department operating in the Prevention and Suppression Technology Crime Suppression and guide the development of police agencies that operate in preventing and combating crime technology. To be a guideline for the prevention and suppression of technology crimes, providing legal protection, rights and freedoms quickly, honestly and equitably, to continue to accept the faith and confidence of people and society.

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญภาพ

สารบัญภาพ (ต่อ)

สารบัญภาพ (ต่อ)

หน้า

ภาพที่

บทที่ 1
บทนำ

การศึกษาวิจัย เรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ผู้วิจัยได้นำเสนอประเด็นต่าง ๆ ในบทนำ โดยมีรายละเอียดดังต่อไปนี้

1. ความสำคัญของปัญหา
2. คำถามในการวิจัย
3. วัตถุประสงค์ของการวิจัย
4. ขอบเขตของการวิจัย
5. ผลที่คาดว่าจะได้รับ
6. ผลที่คาดว่าจะได้รับเมื่อสิ้นสุดการวิจัย
7. กรอบแนวคิดของการวิจัย
8. กรอบวิเคราะห์ของการวิจัย

1. ความสำคัญของปัญหา

จากการเจริญเติบโตอย่างรวดเร็วของเทคโนโลยีในปัจจุบัน ได้นำมาซึ่งความสะดวกสบายความรวดเร็วฉับไว ส่งผลให้ชีวิตประจำวันของผู้คนในยุคเทคโนโลยีสารสนเทศง่ายขึ้น นอกจากประโยชน์มหาศาลที่ได้รับจากเทคโนโลยีอันทันสมัยนี้ สิ่งที่แฝงมาด้วย คือ ภัยร้ายที่อาจคุกคามชีวิต และทำให้สูญเสียทรัพย์สินได้อย่างง่ายดายอีกด้วย ดังนั้น หลายหน่วยงานทั่วโลกรวมทั้งประเทศไทย จึงได้มีการทำการสำรวจสถิติความเสียหายที่เกิดขึ้น จากอาชญากรรมทางเทคโนโลยีเพื่อเป็นบันทึกข้อมูลที่เป็นประโยชน์ในการป้องกันและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีต่อไป ปัจจุบันมีหน่วยงานของต่างประเทศหลายหน่วยงานที่ทำการสำรวจข้อมูลสถิติเกี่ยวกับความเสียหายที่เกิดขึ้นจากอาชญากรรมทางเทคโนโลยี เช่น Crime Scene Investigation (CSI) และ International Prevention Research Institute (IPRI) ซึ่งจากรายงานการสำรวจความเสียหายที่เกิดขึ้นของ CSI ประเทศสหรัฐอเมริกา พบว่า ความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมา คือ การฉ้อโกงทางคอมพิวเตอร์ และการปล่อยไวรัส ตามลำดับ ในขณะที่ AusCert ซึ่งเป็นหน่วยงานที่ช่วยเหลือฉุกเฉิน (CERT) ในประเทศออสเตรเลีย และประเทศชั้นนำในภูมิภาคเอเชีย/แปซิฟิก ได้ทำการสำรวจความเสียหายที่เกิดจากการก่ออาชญากรรมทางเทคโนโลยี พบว่า ความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมาคือ การปล่อยไวรัสและการเข้าถึงอินเทอร์เน็ตหรือเมล์โดยไม่ได้รับอนุญาตจากคนในองค์กรตามลำดับเว็บไซต์ที่มีชื่อเสียงหลายเว็บไซต์ก็ได้ทำการสำรวจข้อมูลและผลกระทบของการก่ออาชญากรรมทางเทคโนโลยีเช่นเดียวกัน

จากการที่คอมพิวเตอร์มีคุณประโยชน์นานับปการ จึงมีผู้นำเทคโนโลยีเหล่านั้น มาเป็นช่องทางหรือเป็นเครื่องมือที่ใช้ในการกระทำความผิด ซึ่งลักษณะหรือรูปแบบของความสัมพันธ์ระหว่างคอมพิวเตอร์กับอาชญากรรมทางเทคโนโลยี พอสรุปได้ดังนี้

1. Computer as “Targets” Crimes คือ คอมพิวเตอร์เป็นเป้าหมายในการก่ออาชญากรรม เช่น การลักทรัพย์เครื่องคอมพิวเตอร์ หรือชิ้นส่วนของเครื่องคอมพิวเตอร์ โดยเฉพาะที่มีขนาดเล็กแต่มีราคาแพง

2. Facilitation of “Traditional” Crimes คือ คอมพิวเตอร์เป็นเครื่องอำนวยความสะดวกในการก่ออาชญากรรมในรูปแบบ “ดั้งเดิม” เช่น ใช้เครื่องคอมพิวเตอร์ในการเก็บข้อมูลลูกค้ายาเสพติด หรือในกรณี UNABOMBER ซึ่งอาชญากรใช้คอมพิวเตอร์ในการกำหนดตัวเหยื่อจาก on-line address แล้วส่งระเบิดแสวงเครื่องไปทางไปรษณีย์ โดยวัตถุประสงค์เพื่อสังหารบุคคลที่ชอบเทคโนโลยีชั้นสูง

3. Computer-unique Crime คือ อาชญากรรมที่เกิดกับคอมพิวเตอร์โดยเฉพาะ เช่น การสร้างให้ไวรัสคอมพิวเตอร์ (computer virus) แพร่ระบาดไปในระบบเครือข่ายคอมพิวเตอร์โดยมีเจตนาที่จะสร้างความเสียหาย Nuke การลักลอบเข้าไปในระบบคอมพิวเตอร์ (hacking /cracking) การละเมิดทรัพย์สินทางปัญญาที่เกี่ยวกับคอมพิวเตอร์ (violation of computer intellectual properties)

4. Computer as “Instrumentality” of Crimes คอมพิวเตอร์เป็นเครื่องมือในการประกอบอาชญากรรม เช่น การใช้เครื่องคอมพิวเตอร์ในการโอนเงินจากบัญชีธนาคารจากบัญชีหนึ่งไปเข้าอีกบัญชีหนึ่งโดยมีเจตนาทุจริต ใช้เครื่องคอมพิวเตอร์ในการเป็นเจ้ามือรับพนันเอาทรัพย์สิน หรือ ใช้คอมพิวเตอร์ในการเผยแพร่เอกสาร สิ่งพิมพ์ รูปภาพ หรือ โฆษณาวัตถุ ลามก อนาจาร ผิดกฎหมาย

โดยปัญหาของอาชญากรรมทางเทคโนโลยีนั้น สาเหตุส่วนใหญ่ที่ทำให้เป็นปัญหา และไม่ได้รับความสนใจ เช่น

1) อาชญากรรมทางเทคโนโลยีโดยธรรมชาติจะมีความไม่เป็นส่วนตัว (Impersonal) จึงไม่มีผลกระทบต่อจิตใจและความรู้สึก (emotion) ของประชาชนโดยทั่วไปและถูกมองข้ามไป

2) อาชญากรรมทางเทคโนโลยีเช่น การละเมิดทรัพย์สินทางปัญญา (Theft of Intellectual Property), การโอนเงินโดยผิดกฎหมาย (Unlawful Transfer of Money) การฉ้อโกงด้านการสื่อสาร (Telecommunication Fraud) มีความแตกต่างกับอาชญากรรมแบบดั้งเดิมที่เจ้าหน้าที่ตำรวจมีความคุ้นเคยและเข้าใจเป็นอย่างดี เช่น การลักทรัพย์ ทำร้ายร่างกาย

3) เจ้าหน้าที่ตำรวจมักจะมองไม่เห็นว่าอาชญากรรมทางเทคโนโลยีนี้ เป็นปัญหาที่กระทบต่อประสิทธิภาพการปฏิบัติงานของตนจึงไม่ให้ความสนใจ

4) อาชญากรรมทางเทคโนโลยีแตกต่างจากอาชญากรรมรุนแรง (Violent crime) จึงทำให้เจ้าหน้าที่ผู้รับผิดชอบมีความจำเป็นที่จะต้องทุ่มเท สรรพกำลังไปในการแก้ไขปัญหาอาชญากรรมในรูปแบบทั่วไป

5) อาชญากรรมทางเทคโนโลยีมีความเกี่ยวพันอย่างยิ่งกับเทคโนโลยีสมัยใหม่ ซึ่งจะทำให้บุคคลที่ไม่มีความรู้เกี่ยวกับเทคโนโลยีที่เกี่ยวข้องเกิดความไม่กล้า (Intimidated) ในการที่จะเข้าไปยุ่งเกี่ยวข้องด้วย

6) บุคคลโดยส่วนมากจะมองอาชญากรรมทางเทคโนโลยีในลักษณะมิติเดี่ยว (Unidimensionally) ในลักษณะสภาวะของเหตุการณ์ที่เกิดขึ้นเป็นครั้ง ๆ ไป โดยอาจไม่นึกถึงผลกระทบความรุนแรงการแพร่กระจาย และปริมาณของความเสียหายที่เกิดขึ้น ในการก่ออาชญากรรมแต่ละครั้งนั้น

7) เทคโนโลยีที่เกี่ยวข้อง และประสิทธิภาพในการใช้เทคโนโลยีของอาชญากรมีการพัฒนาที่รวดเร็ว ทำให้ยากต่อการเรียนรู้ถึงความเปลี่ยนแปลงในวงการของอาชญากรรมประเภทนี้

8) ผู้เสียหายกลับจะตกเป็นผู้ที่ถูกประณามว่า เป็นผู้เปิดช่องโอกาสให้กับอาชญากรในการกระทำผิดกฎหมาย เช่น ผู้เสียหายมักถูกตำหนิว่าไม่มีการวางระบบการรักษาความปลอดภัยที่เหมาะสมกับโครงข่ายงานคอมพิวเตอร์ บางครั้งจึงมักไม่กล้าเปิดเผยว่า ระบบของตนถูกบุกรุกทำลาย

9) ทรัพย์สินทางปัญญาโดยทั่วไปจะไม่สามารถประเมินราคาความเสียหายได้อย่างแน่ชัด จึงทำให้คนทั่วไปไม่รู้สึกถึงความรุนแรงของอาชญากรรมประเภทนี้

10) พนักงานเจ้าหน้าที่ที่เกี่ยวข้องอาจไม่มีความรู้ ความชำนาญ หรือความสามารถพอเพียงที่จะสอบสวนดำเนินคดีกับอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ

11) บุคคลทั่วไปมักมองเห็นว่า อาชญากรรมทางเทคโนโลยีนี้ไม่ได้เกิดขึ้นบ่อยครั้ง จึงไม่ควรค่าต่อการให้ความสนใจ

12) เจ้าหน้าที่ตำรวจมักใช้ความรู้ความเข้าใจในอาชญากรรมแบบดั้งเดิมนำมาใช้ในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี ซึ่งเป็นเหตุให้อาชญากรรมประเภทนี้ไม่ครบองค์ประกอบความผิดตามอาชญากรรมแบบดั้งเดิม และถูกมองข้ามไปโดยไม่พบการกระทำผิด

13) เจ้าหน้าที่ตำรวจโดยทั่วไปไม่มีการเตรียมการเพื่อรองรับอาชญากรรมทางเทคโนโลยีอย่างจริงจัง

14) ในปัจจุบันนี้อาชญากรรมทางเทคโนโลยีไม่ใช่อาชญากรรมที่มีผลกระทบต่อความมั่นคงทางการเมือง เมื่อเทียบกับอาชญากรรมที่เกี่ยวกับทรัพย์ หรือ ชีวิตร่างกาย ซึ่งทำให้ประชาชนเกิดความรู้สึกไม่ปลอดภัยในชีวิตและทรัพย์สิน (ญาณพล ยั่งยืน, 2555)

ด้วยปัญหาทางด้านอาชญากรรมทางเทคโนโลยีมีปัญหาอยู่หลายประการที่กล่าวมาข้างต้นนั้น ประเด็นปัญหาที่สำคัญโครงสร้างทางกฎหมายทำให้เกิดปัญหาด้านการสืบสวนสอบสวนทางด้านอาชญากรรมทางเทคโนโลยีกฎหมาย และความรู้ของพนักงานสอบสวน ตลอดจนการรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล ยังก้าวไปไม่ทันต่อการกระทำผิดทางด้านอาชญากรรมทางเทคโนโลยี เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจาก ความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน (Globalization) ความรู้ทางด้านอาชญากรรมทางเทคโนโลยีของเจ้าหน้าที่รัฐยังไม่เพียงพอ การศึกษา การค้นหา การเก็บรวบรวมพยานหลักฐาน และการพิสูจน์หลักฐาน

ดิจิตอล เป็นอีกเรื่องหนึ่งที่เจ้าหน้าที่รัฐยังไม่มีความรู้เพียงพอ การหาแนวทางและวิธีการตรวจพิสูจน์ให้มีวิธีการที่ทันสมัยมากยิ่งขึ้น เป็นเรื่องที่ต้องดำเนินการ (ณรงค์ กุลนิเทศ, 2557)

ในปัจจุบันมีหน่วยงานหลักหลายหน่วยงานที่มีภารกิจที่บังคับใช้กฎหมาย อำนวยความยุติธรรม ป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงการตรวจพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ที่มีภารกิจป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี รับแจ้งแบะแสจากประชาชน ตลอดจนให้คำปรึกษาแนะนำ ตลอดจนรวบรวมสภาพปัญหา เพื่อเสนอแนะแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยี และสนับสนุนการปฏิบัติงานของหน่วยงานอื่น ตลอดจนประสานความร่วมมือระหว่างหน่วยงานภายในประเทศและต่างประเทศในการป้องกันอาชญากรรมทางเทคโนโลยี เป็นต้น และหน่วยงานที่สำคัญ คือ กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจที่มีหน้าที่และความรับผิดชอบเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐานและของกลางในคดีที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยี และสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.) สำนักงานตำรวจแห่งชาติ ที่มีหน้าที่ศึกษา วิเคราะห์ วิจัย และพัฒนาระบบงานเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนฝึกอบรมเทคโนโลยีสารสนเทศและการสื่อสารให้แก่ข้าราชการตำรวจ ซึ่งภารกิจ และหน้าที่ความรับผิดชอบของแต่ละหน่วยงานมีการทำงานที่คล้ายคลึงกัน ทำให้เกิดปัญหาในด้านต่าง ๆ เช่น อำนาจหน้าที่รับผิดชอบหรือการครอบครองวัตถุพยานที่อาจจะมีปัญหาในการตรวจพิสูจน์

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 (พ.ศ. 2560-2564) มุ่งเสริมสร้างกลไกการพัฒนาให้มีประสิทธิภาพและสอดคล้องกับสถานการณ์ที่เป็นปัจจุบันมากขึ้นทั้งกลไกที่เป็นกฎหมายและกฎระเบียบต่างๆ และกลไกการทำงานในรูปแบบของคณะกรรมการ หรือหน่วยงานที่รับผิดชอบการขับเคลื่อนยุทธศาสตร์ในทุกระดับให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ ลดความซ้ำซ้อนทั้งในระดับประเทศและระดับพื้นที่ให้ดำเนินงานได้อย่างมีประสิทธิภาพ และในขณะเดียวกันก็เพิ่มบทบาทของกลไกภาคองค์ความรู้ เทคโนโลยี นวัตกรรม และความคิดสร้างสรรค์ให้เป็นเครื่องมือหลักในการขับเคลื่อนการพัฒนาในทุกภาคส่วน โดย ข้อ 1.3 (สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักนายกรัฐมนตรี, 2558, หน้า 3) ระบุว่าประเทศไทยต้องเผชิญกับแรงกดดันและความเสี่ยงมากขึ้นภายใต้สถานการณ์ที่ กระแสโลกาภิวัตน์เข้มข้นมากขึ้น เป็นโลกไร้พรมแดน โดยมีการเคลื่อนย้ายคน เงินทุน องค์ความรู้ เทคโนโลยี ข่าวสาร สินค้าและบริการอย่างเสรีทำให้การแข่งขันในตลาดโลกรุนแรงขึ้น ส่งผลให้มีการรวมตัวด้านเศรษฐกิจ ของกลุ่มต่างๆ ในโลกมีความเข้มข้นขึ้น ประเทศเศรษฐกิจใหม่มีขีดความสามารถในการแข่งขันมากขึ้น เช่น จีน อินเดีย ละตินอเมริกา และเวียดนาม ซึ่งมีแรงงานราคาถูกและมีมาตรการอื่นๆประกอบในการดึงดูดการลงทุน จากต่างประเทศได้เพิ่มขึ้น นอกจากนั้นการพัฒนาการสื่อสารด้วยเทคโนโลยีสมัยใหม่ทำให้สังคมโลกมีความเชื่อมโยงกันอย่างใกล้ชิดมากขึ้น เกิดภัยคุกคามและความเสี่ยง เช่น การก่อการร้าย โรคระบาด อาชญากรรมข้ามชาติ เป็นต้น

จากความเป็นมาดังกล่าวข้างต้น ผู้วิจัยมีความสนใจที่จะการศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยศึกษาจากเอกสารงานวิจัยที่เกี่ยวข้องทั้งภายในประเทศ และต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีในแต่ละหน่วยงาน เพื่อรวบรวมข้อมูลเกี่ยวกับการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำมาพัฒนางาน รวมทั้งการสัมภาษณ์ผู้ที่ปฏิบัติงานที่เกี่ยวข้องกับ งานทางด้านดังกล่าว เพื่อให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้ง คุ้มครองสิทธิและเสรีภาพด้วย ความรวดเร็ว เที่ยงตรง และเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้เป็นที่ยอมรับศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

2. คำถามในการวิจัย

1) การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีจะสามารถแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีได้เป็นอย่างไร

2) องค์ความรู้ในการจัดทำคู่มือการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จะสามารถนำมาใช้ประโยชน์ได้เป็นอย่างไร

3. วัตถุประสงค์ของการวิจัย

1) เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) เพื่อกำหนดรูปแบบการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

3) เพื่อสร้างองค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

4. ขอบเขตของการวิจัย

1) ขอบเขตเนื้อหาของการวิจัย

การวิจัยครั้งนี้ เป็นการศึกษาเกี่ยวกับการวิจัยเชิงคุณภาพมาดำเนินการ เพื่อนำข้อค้นพบที่ได้รับมาถอดบทเรียน โดยนำแนวคิดทฤษฎีที่เกี่ยวข้องที่ได้จากการศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้องกับการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และข้อมูลสำคัญและนำมาถอดบทเรียน โดยมีประเด็นหลัก ๆ ดังนี้

ประเด็นที่ 1 หน่วยงานตำรวจที่ปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 2 การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 3 การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 4 องค์ความรู้ และความชำนาญงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 5 การพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 6 การสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยี

2) ขอบเขตด้านกลุ่มเป้าหมาย/พื้นที่

กลุ่มเป้าหมายในการวิจัยครั้งนี้ คือ ผู้แทนจากหน่วยงานที่ทำหน้าที่เกี่ยวข้องกับ ตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยศึกษาเฉพาะกลุ่มเป้าหมายที่ได้ปฏิบัติงานโดยตรง โดยทำการคัดเลือกเข้าร่วม ซึ่งประกอบด้วย

2.1) การประชุมกลุ่มย่อย (focus group)

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) เจ้าหน้าที่ตำรวจกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจ

(3) เจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(4) เจ้าหน้าที่ตำรวจสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.)

(5) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES)

2.2) การสัมภาษณ์แบบเจาะลึก (in-depth interview)

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) พนักงานสอบสวน ฝ่ายสืบสวน และฝ่ายป้องกันและปราบปรามของสถานีตำรวจนครบาล และสถานีตำรวจภูธร

(3) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

(4) อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมทางเทคโนโลยี

3) ขอบเขตด้านระยะเวลา

การวิจัยครั้งนี้มีระยะเวลาดำเนินการ วันที่ 3 เดือนกันยายน พ.ศ. 2561 ถึงวันที่ 31 สิงหาคม พ.ศ. 2562

5. ผลที่คาดว่าจะได้รับ

1) ได้ทราบถึงแนวทางในการพัฒนานโยบายการบริหาร การจัดการ รวมทั้งปัญหาอุปสรรคในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การบูรณาการการทำงานของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และข้อกฎหมายและระเบียบที่เหมาะสมต่อการนำไปใช้ในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) สรุปผลการศึกษาวิจัย จัดพิมพ์รายงานวิจัยฉบับสมบูรณ์

3) ได้คู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ใช้ในการปฏิบัติงานของหน่วยงานตำรวจ

6. ผลที่คาดว่าจะได้รับเมื่อสิ้นสุดการวิจัย

1) Output

1.1) ทำให้เกิดองค์ความรู้และความเข้าใจที่จัดทำในรูปแบบคู่มือการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

1.2) ทำให้เกิดการพัฒนาประสิทธิภาพงานของหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) Outcome

2.1) ทำให้เกิดการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

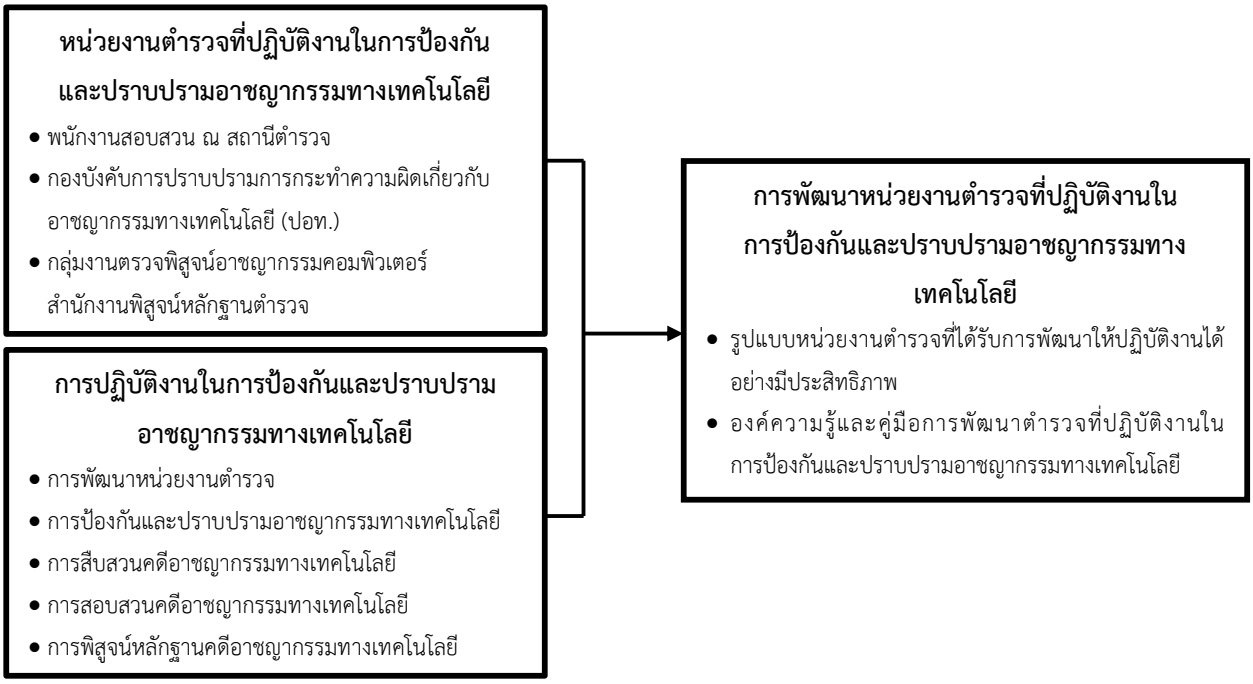
3) Impact

3.1) ทำให้เกิดแนวความคิดขององค์ความรู้และความเข้าใจที่ในการปฏิบัติงานสำหรับหน่วยงานตำรวจที่ปฏิบัติงานหน้าที่เกี่ยวข้องในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

3.2) ทำให้การเกิดอาชญากรรมทางเทคโนโลยีของประเทศไทยมีปริมาณลดลง และหน่วยงานตำรวจที่ปฏิบัติงานสามารถปฏิบัติหน้าที่ในด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากขึ้น

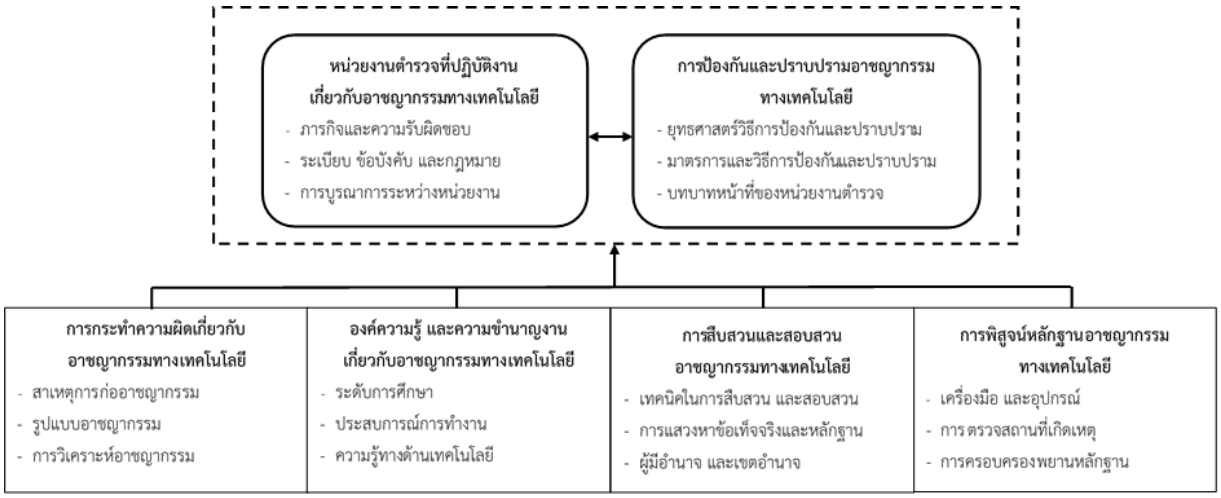
7. กรอบแนวคิดในการวิจัย (Conceptual Framework)

คณะผู้วิจัยได้นำที่มาและความสำคัญ และการทบทวนเอกสารเชิงสังเคราะห์ในการวิจัย แนวคิดต่าง ๆ รวมถึงงานวิจัยที่เกี่ยวข้องเรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้มาสังเคราะห์ และนำมารวบรวมให้เกิดกรอบแนวคิดของการวิจัย และกรอบวิเคราะห์ในการวิจัย ได้ดังนี้



ภาพที่ 1-1 กรอบแนวคิดในการวิจัย (Conceptual Framework)

8. กรอบวิเคราะห์ในการวิจัย (Analysis Framework)



ภาพที่ 1-2 กรอบวิเคราะห์ของการวิจัย (Analysis Framework)

บทที่ 2

ทบทวนวรรณกรรม

การศึกษาวิจัยเรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งผู้วิจัยได้ทำการทบทวนวรรณกรรมโดยมีรายละเอียดดังต่อไปนี้

1. แนวความคิดและทฤษฎีเกี่ยวกับอาชญากรรม
2. แนวความคิดและทฤษฎีเกี่ยวกับเทคโนโลยีสารสนเทศ
3. แนวความคิดและทฤษฎีเกี่ยวกับอาชญากรรมทางเทคโนโลยี
4. แนวความคิดและทฤษฎีเกี่ยวกับการป้องกันปราบปรามอาชญากรรม
5. แนวความคิดและทฤษฎีเกี่ยวกับการบริหารจัดการ
6. แนวความคิดและทฤษฎีเกี่ยวกับประสิทธิภาพการปฏิบัติงาน
7. หน่วยงานหลักและสนับสนุนที่ปฏิบัติงานเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีของประเทศไทย
8. หน่วยงานงานป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของต่างประเทศ
9. งานวิจัยที่เกี่ยวข้อง

1. แนวความคิดและทฤษฎีเกี่ยวกับอาชญากรรม

แนวความคิดอาชญากรรม

อาชญากรรม (Crime) เป็นปรากฏการณ์ (Phenomenon) ปกติทางสังคมอย่างหนึ่ง การเกิดอาชญากรรมก่อให้เกิดความเสียหาย รวมทั้งความไม่สงบเรียบร้อยในสังคม การเกิดอาชญากรรม เป็นการกระทำของมนุษย์ที่เป็นสัตว์สังคม ที่มีความขัดแย้งจากการอยู่ร่วมกัน ดังนั้นทุกสังคมจึงมีการก่ออาชญากรรมอย่างไม่อาจหลีกเลี่ยงได้ ในแต่ละสังคมจึงมีการกำหนดกฎ ระเบียบ วิธีปฏิบัติขึ้น เพื่อควบคุมพฤติกรรมของบุคคลในสังคม และเพื่อให้คนในสังคมยอมรับและอยู่ร่วมกันได้อย่างปกติสุข ในปัจจุบันการก่ออาชญากรรมได้กลายเป็นปัญหาระดับชาติ เนื่องจากการแพร่กระจาย และระดับความรุนแรงของอาชญากรรมที่มีผลกระทบอย่างกว้างขวาง ในยุคโลกาภิวัน์ อาชญากรรมถือว่าเป็นภัยคุกคามต่อคนทั่วโลก เนื่องจากมีการเกิดอาชญากรรมขององค์กรข้ามชาติที่มีการขยายตัวอย่างรวดเร็ว และได้รับความสนใจอย่างมากในช่วงไม่กี่ปีที่ผ่านมา อนุสัญญาสหประชาชาติว่าด้วยองค์กรอาชญากรรมข้ามชาติ เริ่มมีผลบังคับใช้ในปี 2546 ระบุอาชญากรรมข้ามชาติถูกจัดเป็นหนึ่งในหกกลุ่มของภัยคุกคามที่โลกต้องกังวลทั้งในปัจจุบันและในทศวรรษข้างหน้า มีความพยายามในการจัดการปัญหาอาชญากรรมที่เกิดขึ้น แต่สิ่งสำคัญคือการจัดการกับกลุ่มคนที่

ก่ออาชญากรรม หรือผู้ที่มีส่วนร่วมในการกระทำความผิด อาชญากรรมที่เกิดขึ้นมีหลากหลายรูปแบบ ดังนั้นการจัดการปัญหาอาชญากรรมจึงมีความแตกต่างกันออกไป

ความหมาย

มีนักวิชาการให้ความหมาย อาชญากรรม หมายถึง บุคคลหรือกลุ่มบุคคลในองค์กรกระทำความผิดตามที่กฎหมายกำหนดไว้อย่างเป็นทางการ หรือ ละเลยไม่ปฏิบัติตามกฎหมายที่กำหนด มีผลกระทบทางกายภาพหรือทางเศรษฐกิจอย่างร้ายแรงต่อพนักงาน ผู้บริโภคหรือประชาชนทั่วไป (Burke, 2009) อาชญากรรม หมายถึง การกระทำใดๆ ที่ถูกบัญญัติไว้ว่าเป็นความผิดตามประมวลกฎหมายอาญา และกฎหมายอื่นที่มีโทษทางอาญา อาชญากรรม หมายถึง ปรากฏการณ์อย่างหนึ่งของสังคมที่เกิดขึ้นโดยการกระทำของบุคคล ซึ่งการกระทำนั้น ๆ กฎหมายได้บัญญัติเป็นข้อห้ามและถือว่าเป็นความผิด ซึ่งผู้กระทำผิดจะต้องได้รับการลงโทษ (ประเทือง ธนิยผล, 2548) หมายถึง การกระทำที่มีลักษณะความรุนแรง หรือการกระทำโดยมีเจตนาฝ่าฝืนหรือขัดต่อกฎหมายที่วางไว้และเป็นอันตรายต่อสังคม ผู้กระทำความผิดจะต้องได้รับโทษตามกฎ และข้อบังคับของสังคมนั้น (ธเนศ เกษศิลป์, 2560) อาชญากรรม หมายถึง การจัดประเภทตามกฎหมายของพฤติกรรมโดยองค์การที่มีอำนาจหน้าที่ในทางการเมืองของสังคม โดยเป็นพฤติกรรมต่อต้านสังคม (สุดสงวน สุธีสร, 2545) หมายถึง พฤติกรรมการกระทำความผิด โดยอาศัยกฎหมายอาญาเป็นเกณฑ์ในการตัดสินว่าพฤติกรรมการกระทำความผิด โดยอาศัยกฎหมายอาญาเป็นเกณฑ์ในการตัดสินว่าพฤติกรรมการกระทำใดเป็นความผิดและจะต้องได้รับการลงโทษ พฤติกรรมการกระทำที่เป็นอาชญากรรมสามารถแยกได้ 2 ประการคือ (ศิริประภา รัตตัญญู, 2550)

1) การกระทำที่เป็นความผิดในตัวเอง (Mala in Se) หมายถึง การกระทำผิดที่มองเห็นได้ด้วยตัวเองว่าเป็นสิ่งไม่ดี เป็นการกระทำที่ขัดต่อหลักศีลธรรมของสังคมอย่าง ร้ายแรง

2) การกระทำผิดที่กฎหมายบัญญัติว่าเป็นความผิด (Mala Prohibita) หมายถึง การกระทำที่ไม่ขัดต่อหลักศีลธรรม เช่น การลักลอบเข้าเมือง การฝ่าฝืนกฎจราจร เป็นต้น ณรงค์ ทรัพย์เย็น และ ธงชาติ รอดคลอง (2551) ระบุความหมายของอาชญากรรมจะมีนัยแตกต่างกันตามมุมมองของแต่ละวิชาชีพ ดังนี้

1. อาชญากรรมในความหมายของนักกฎหมาย เห็นว่าอาชญากรรมเป็นความประพฤติที่กฎหมายอาญาห้ามและมีบทกำหนดโทษไว้ คือการกระทำหรือการงดเว้นการกระทำใดๆที่กฎหมายบัญญัติไว้ว่าเป็นความผิดและกำหนดโทษไว้ชัดเจน เช่น ความผิดฐานฆ่าคนตาย ฐานลักทรัพย์ วิ่งราวทรัพย์ ชิงทรัพย์ เป็นต้น

2. อาชญากรรมในความหมายของนักอาชญาวิทยา จะมองกันในแง่ของความร้ายแรงของการกระทำและความชั่วที่มีอยู่ในตัวของผู้กระทำมากกว่า กล่าวคือ จะมองความหมายของอาชญากรรมตามความหมายอย่างแคบ ซึ่งหมายถึงการกระทำที่มีลักษณะชั่วร้าย และเป็นอันตรายต่อสังคมอย่างมาก

3. อาชญากรรมในความหมายของนักสังคมวิทยา เห็นว่าความประพฤติผิดขัดแย้งหรือละเมิดต่อระเบียบของสังคมนั้น มิได้หมายความว่าการขัดแย้งจะเป็นอาชญากรรมเสมอไป แต่มีความหมายเพียงว่าผู้นั้นประพฤติและปฏิบัติไม่ถูกต้องตามระเบียบที่สังคมกำหนดไว้เท่านั้น การขัดแย้งหรือละเมิดต่อสังคมที่ตราไว้เป็นกฎหมายนั้น จึงเรียกว่าเป็นการกระทำผิดกฎหมาย หรือเป็นการก่ออาชญากรรม ยกเว้นความผิดลหุโทษไม่ถือว่าเป็นการก่ออาชญากรรม

หลักการสำคัญอาชญากรรม

สุดสงวน สุธีสร (2545) ระบุ อาชญากรรม เป็นพฤติกรรมต่อต้านสังคม มีหลักสำคัญ 5 ประการ คือ

1. การกระทำนั้นจะต้องกระทำในขณะที่ผู้กระทำมีสติสัมปชัญญะ มีเจตนาร้ายและมีผลร้ายที่เกิดจากการกระทำนั้น

2. การกระทำนั้นจะต้องเป็นการกระทำ ที่ต้องห้ามตามกฎหมาย ในขณะที่ใช้บังคับอยู่ในขณะที่การกระทำนั้นได้เกิดขึ้น อีกนัยหนึ่งกฎหมายย่อมไม่มีผลย้อนหลังไปใช้บังคับการกระทำที่ได้เกิดขึ้นก่อนที่จะมีกฎหมายกำหนดว่าด้วยการกระทำนั้นเป็นความผิด

3. ผู้กระทำผิดจะต้องมีเจตนาร้ายในการประกอบการกระทำนั้น

4. จะต้องมีความสัมพันธ์กันระหว่างการกระทำกับผลร้ายที่เกิดขึ้น

5. การกระทำนั้นจะต้องมีกฎหมายกำหนดโทษไว้อย่างชัดเจน

พฤติกรรมอาชญากร

อาชญากรรมเป็นพฤติกรรมที่เกิดจากการกระทำของอาชญากร สามารถแบ่งประเภทของอาชญากรรมตามพฤติกรรมอาชญากรได้ 9 ประเภท ดังนี้

1. พฤติกรรมอาชญากรที่กระทำผิดต่อบุคคลด้วยความรุนแรง (Violent Personal Criminal Behavior) เช่น การประทุษร้ายต่อบุคคล การใช้อาวุธทำร้ายร่างกายบุคคลอื่น

2. พฤติกรรมอาชญากร ที่กระทำต่อทรัพย์สินตามแต่โอกาสจะอำนวย (Occasional Property Criminal behavior)

3. พฤติกรรมอาชญากรที่ขัดต่อความเป็นระเบียบเรียบร้อยของสังคม (Public Order Criminal Behavior)

4. พฤติกรรมอาชญากรทางการเมือง (Political Criminal Behavior)

5. พฤติกรรมอาชญากรพื้นฐาน (Conventional Criminal Behavior) หมายถึง อาชญากรรมที่เกิดขึ้นและเห็นอยู่ประจำ เช่น การฉกชิงวิ่งราว การทำร้ายร่างกาย

6. พฤติกรรมอาชญากรในการประกอบอาชีพ (occupational criminal Behavior) อาชญากรรมเกิดจากอาชีพของบุคคลนั้น เช่น เรื่องการทุจริตในหน่วยงาน หรือบริษัทของตนเอง โดยใช้อาชีพของตนเองแล้วแสวงหาช่องทาง และช่องโอกาสในการประกอบอาชญากรรม

7. พฤติกรรมอาชญากรนิติบุคคล (Corporate Criminal Behavior) เป็นลักษณะการกระทำโดยกลุ่มบุคคล ของบริษัท ห้างร้าน เป็นต้น

8. พฤติกรรมอาชญากรองค์การ (Organizational Criminal Behavior) เป็นอาชญากรรมที่อยู่ในลักษณะองค์การ เช่น แก๊งมาเฟีย ซึ่งมีหัวหน้าแก๊ง และมีสาขาย่อย ส่วนมากจะประกอบการค้าผิดกฎหมาย โดยมีธุรกิจบังหน้า มักมีอิทธิพล มีอำนาจ และส่วนใหญ่มักอยู่เบื้องหลังนักการเมือง จึงเป็นอาชญากรที่ยากแก่การทำลาย

9. พฤติกรรมอาชญากรอาชีพ (Professional Criminal Behavior) คนกลุ่มนี้จะเกิดมาเพื่อเป็นมืออาชีพจะประกอบอาชีพที่ผิดกฎหมาย ในขณะที่ผู้อื่นประกอบอาชีพโดยสุจริต แต่คนกลุ่มนี้จะยึดอาชีพการเป็นอาชญากร

ประเภทของอาชญากรรม

ปุระชัย เปี่ยมสมบูรณ์ และคณะ (2531) ได้แบ่งอาชญากรรมออกเป็น 5 ประเภท ดังนี้

1. อาชญากรรมปราศจากผู้เสียหาย หมายถึง อาชญากรรมที่เกี่ยวข้องกับการละเมิดศีลธรรมจรรยาบุคคล การที่เรียกว่าอาชญากรรมปราศจากผู้เสียหาย ก็เพราะผู้เสียหายและผู้กระทำความผิดเป็นคนเดียวกัน เช่น ความผิดเกี่ยวกับการพนัน การค้าประเวณี การทำแท้ง การจำหน่ายสิ่งสามกอนาจาร เป็นต้น

2. อาชญากรรมพื้นฐาน หมายถึง อาชญากรรมซึ่งเกี่ยวกับการประทุษร้ายต่อทรัพย์ ร่างกายหรือชีวิตของบุคคลอื่น เช่นความผิดฐานลักทรัพย์ วิ่งราวทรัพย์สิน ชิงทรัพย์ ปล้นทรัพย์ ทำร้ายร่างกายและฆ่าผู้อื่น เป็นต้น นอกจากนี้อาชญากรรมพื้นฐาน ยังแยกพิจารณาได้เป็น 2 ชนิด คืออาชญากรรมพื้นฐานที่ไม่ใช้กำลังรุนแรง และอาชญากรรมพื้นฐานที่ใช้ความรุนแรง

3. อาชญากรรมองค์การ หมายถึง อาชญากรรมที่อาชญากรได้รวมตัวเข้าด้วยกันตามสายการบังคับบัญชาในรูปขององค์การ โดยจัดการวางแผนและดำเนินงานเพื่อไปประกอบธุรกิจผิดกฎหมายต่าง ๆ เช่น การค้าหญิงโดยบังคับค้าประเวณี การค้าสินค้าหนีภาษี การค้าแร่เถื่อน และการค้าไม้เถื่อน เป็นต้น

4. อาชญากรรมคอปกขาว หมายถึง อาชญากรรมที่ผู้กระทำผิดเป็นบุคคลที่อยู่ในตำแหน่งหน้าที่การงานไม่ว่าในราชการ รัฐวิสาหกิจหรือเอกชน และได้ใช้ตำแหน่งหน้าที่ดังกล่าวในทางไม่ชอบ เพื่อแสวงหาผลประโยชน์ส่วนตัว เช่น สมุห์บัญชีทำการยักยอกเงินในความรับผิดชอบของตนเอง ข้าราชการรับเงินค่าคอมมิชชั่นจากการประมูลก่อสร้างสถานที่ของทางราชการ คณะกรรมการคัดเลือกเพื่อแต่งตั้งเข้ารับราชการรับเงินโดยมิชอบจากบุคคลผู้สมัครสอบ เป็นต้น

5. อาชญากรรมพิเศษ หมายถึง อาชญากรรมที่มีลักษณะแตกต่างไปจากประเภทอาชญากรรมทั้ง 4 ประเภท ที่กล่าวมาแล้ว เช่น อาชญากรรมทางเศรษฐกิจและพาณิชย์ การก่อการร้าย และอาชญากรรมทางคอมพิวเตอร์ เป็นต้น

สาเหตุของอาชญากรรม

กฤษฎา แสงเจริญทรัพย์ (2559) ระบุถึงการศึกษาเพื่อหาสาเหตุของการเกิดอาชญากรรม ในทางอาชญาวิทยาได้แบ่งมุมมองของการศึกษาในเรื่องดังกล่าวออกเป็น 3 มุมมองที่สำคัญด้วยกัน กล่าวคือ มุมมองทางด้านชีววิทยา (Biology) มุมมองทางด้านจิตวิทยา (Psychology) และมุมมองทางด้านสังคมวิทยา (Sociology) ซึ่งในแต่ละมุมมองก็มีข้ออธิบายถึงสาเหตุของการเกิดอาชญากรรมที่แตกต่างกันออกไป พอที่จะสรุปได้ดังต่อไปนี้

1. มุมมองทางด้านชีววิทยา (Biology) เป็นการศึกษาถึงสาเหตุการเกิดของอาชญากรรม โดยใช้มุมมองทางด้านชีววิทยา อันได้แก่ การถ่ายทอดพฤติกรรมอาชญากรรมผ่านทางรหัสพันธุกรรม การศึกษาเกี่ยวกับสารเคมีในร่างกายที่ส่งผลต่อการเปลี่ยนแปลงของระบบประสาท หรือการทำงานในร่างกาย ตลอดจนลักษณะของโครโมโซม เป็นต้น ซึ่งสาเหตุต่างๆเหล่านี้ สามารถส่งผลกระทบที่สำคัญต่อพฤติกรรมอาชญากรรมของบุคคลได้มากกว่าองค์ประกอบทางด้านสังคม หรือองค์ประกอบทางด้านสิ่งแวดล้อม

2. มุมมองทางด้านจิตวิทยา (Psychology) เป็นการศึกษาถึงสาเหตุการเกิดของอาชญากรรมโดยอาศัยหลักเกณฑ์ในการวิเคราะห์พฤติกรรมของมนุษย์ทางด้านจิตวิทยา อันได้แก่ การศึกษาถึงพัฒนาการของ

บุคคลตั้งแต่วัยเด็ก รวมถึงปัญหาที่อาจเกิดขึ้นในแต่ละช่วงวัยที่ส่งผลกระทบต่อการถูกกำหนดรูปแบบ (shape) บุคลิกภาพของบุคคลนั้นในวัยผู้ใหญ่ รวมถึงเป็นกระบวนการศึกษาถึงสภาพปัญหาที่เกิดขึ้นกับจิตใจ (mental) ของบุคคลที่อาจนำไปสู่การก่ออาชญากรรม

3. มุมมองทางด้านสังคมวิทยา (Sociology) ในขณะที่มุมมองทางด้านชีววิทยา และมุมมองทางด้านจิตวิทยา มองว่าการก่ออาชญากรรมเป็นเงื่อนไขที่เกิดจากตัวบุคคลนั้นเอง ในช่วงศตวรรษที่ 20 นักสังคมวิทยาได้ท้าทายความเชื่อดังกล่าวโดยเริ่มหาสาเหตุในการเกิดอาชญากรรม โดยพิจารณาจากองค์ประกอบภายนอกของตัวผู้กระทำความผิด อันได้แก่องค์ประกอบทางด้านสังคม เช่น การเบี่ยงเบนทางวัฒนธรรม (cultural deviance) ความตึงเครียดทางสังคม (strain theories) การเรียนรู้ที่แตกต่าง (differential association) เป็นต้น

ทฤษฎีอาชญากรรมและความยุติธรรม (Theories of Crime and Justice)

ณัฐฐ์วัฒน์ สุทธิโยธิน (2554) ระบุ ทฤษฎีอาชญาวิทยา สามารถจัดแบ่งเป็น 4 กลุ่มหลัก ดังนี้

1. ทฤษฎีอาชญาวิทยาของสำนักอาชญาวิทยาคลาสสิค (Classical School) ประกอบด้วยทฤษฎี 3 กลุ่มหลัก คือ

1.1 ทฤษฎีอาชญาวิทยาสำนักคลาสสิค : โดย ซีซาร์ เบ็คคาเรีย (Cesare Beccaria) เขาเห็นว่าบุคคลทุกคนควรมีความเท่าเทียมกันในกฎหมาย มีหลัก 3 ประการ คือ

(1) การลงโทษต้องกระทำด้วยความรวดเร็ว (Swiftness)

(2) การลงโทษต้องมีความแน่นอน (Certainty) และ

(3) การลงโทษต้องมีความเคร่งครัด (Severity)

และวางหลักการสำคัญของกฎหมายอาญา 2 ประการคือ

(1) “ไม่มีอาชญากรรม ถ้าไม่มีกฎหมาย” (nullum criemen sig lego)

(2) ศาลเป็นเพียงผู้พิจารณาพิพากษาคดี ไม่ควรมีอำนาจในการกำหนดอัตราโทษ การกำหนดอัตราโทษทางอาญาเป็นอำนาจของสภานิติบัญญัติ ซึ่งเป็นไปตามทฤษฎีสัญญาประชาคม

1.2 ทฤษฎีอาชญาวิทยาสำนักคลาสสิค : โดย เจเรมี เบ็นธัม (Jeremy Bentham), วิลเลียม แบล็คสโตน (William Blackstone) และ โรเบิร์ต พีล (Robert Peel) โดยเจเรมี เบ็นธัม มีความเชื่อว่า “...การลงโทษอาชญากรรมแต่ละประเภท จะต้องก่อให้เกิดความเจ็บปวดจากความทุกข์ทรมานที่ได้รับจากการลงโทษ มากกว่าความเพลิดเพลินที่จะได้รับจากการประกอบอาชญากรรม...” เพื่อให้ผู้กระทำผิดเกิดความหลาบจำ มีการจำแนกเพศ อายุ และประเภทความผิดของผู้ต้องขัง และประณามความไร้มาตรฐานของกฎหมายอาญา ความไม่คงเส้นคงวาของกฎหมายอาญาและกระบวนการยุติธรรมของศาล

1.3 ทฤษฎีอาชญาวิทยาสำนักนีโอคลาสสิค: โดย รอสซี่ การ์ราด และจอลี่ (Rossi, Garraud and joly) มีข้อเสนอ คือ

(1) ให้นำพฤติการณ์แห่งคดีมาใช้เพื่อประกอบการพิจารณาคดีเพื่อพิพากษาลงโทษอย่างเหมาะสม

(2) ให้ศาลตระหนักถึงความจำเป็นในการพิจารณาถึงภูมิหลังของผู้กระทำผิด ไม่จำกัดการพิจารณาอยู่เพียงแค่เฉพาะพฤติกรรมในขณะที่กระทำผิด

(3) ให้กระบวนการยุติธรรมโดยเฉพาะศาล รับฟังคำให้การของผู้เชี่ยวชาญหรือผู้ชำนาญการในบางสาขาวิชา เพื่อประโยชน์ในการพิจารณาคดีได้อย่างถ่องแท้ยิ่งขึ้น โดยถือว่าผู้เชี่ยวชาญหรือผู้ชำนาญการเหล่านั้นเป็นพยานบุคคล และ

(4) ขอให้กระบวนการยุติธรรมให้ความสนใจกับกลุ่มบุคคลที่อาจมีความรับผิดทางอาญาแตกต่างไปจากบุคคลโดยทั่วไป เนื่องจากกลุ่มบุคคลนี้ ไม่สามารถกำหนดเจตจำนงอิสระได้ทัดเทียมกับบุคคลอื่น และสมควรที่กฎหมายจะให้ความปรานีและผ่อนปรนการลงโทษ อาทิ กลุ่มบุคคลวิกลจริต บุคคลปัญญาอ่อน คนชรา บุคคลผู้มีความพิการ

2. ทฤษฎีอาชญาวิทยาสำนักปฏิฐานนิยม (Postivism School) มีสาระสำคัญ ดังนี้

2.1 กำเนิดสำนักปฏิฐานนิยาม การนำวิธีการทางวิทยาศาสตร์มาประยุกต์ใช้ในการศึกษาสังคม โดยแบ่งการศึกษาสังคม 3 ระยะ คือ ระยะสังคมแบบดั้งเดิม (Primitive society) มนุษย์มีหลักการคิดที่อิงอยู่กับความเชื่อในธรรมชาติตามความรู้สึกนึกคิดของตน ระยะสังคมใช้ “หลักเหตุผล” (Rational) และ ระยะที่มนุษย์ใช้ “วิธีการทางวิทยาศาสตร์” (Scientific Method) ในการพิจารณาธรรมชาติและชีวิต โดยออกุสท์ ก็องต์เรียกระยะสุดท้ายนี้ว่า Positive stage หรือ “แนวคิดแบบปฏิฐานนิยม” อันเป็นต้นกำเนิดของ “สำนักปฏิฐานนิยม”

2.2 ทฤษฎีอาชญาวิทยาภูมิศาสตร์อาชญากรรม แนวคิด สภาพแวดล้อมของปรากฏการณ์อาชญากรรม เช่น อาชญากรรมประเภทประทุษร้ายต่อชีวิตและร่างกาย มักปรากฏในเขตพื้นที่ภูมิอากาศร้อนมากกว่าเขตพื้นที่ภูมิอากาศหนาว ในทางกลับกันอาชญากรรมเกี่ยวกับทรัพย์สิน จะเพิ่มขึ้นเมื่อเข้าใกล้เขตพื้นที่อากาศหนาวหรือเมื่อใกล้ขั้วโลก

3. ทฤษฎีอาชญาวิทยาสำนักอิตาเลียน มีฐานคติซึ่งสรุปได้ดังนี้

1) บุคคลกระทำความผิด เพราะอิทธิพลของสิ่งแวดล้อม ด้วยเหตุนี้จึงไม่ถือว่าเป็นปมด้อยทางศีลธรรม

2) กฎหมายป้องกันสิทธิเสรีภาพจัดเป็นสิ่งที่ไม่จำเป็น

3) อาชญากรรมต้องมีการกำหนดนิยามตามหลักวิทยาศาสตร์สังคม

4) ระเบียบวิธีวิจัยทางวิทยาศาสตร์เป็นเครื่องมือที่ได้รับการยอมรับเพื่อการค้นหาองค์ความรู้

5) กฎหมายอาญาอยู่ภายนอกขอบเขตของอาชญาวิทยา

6) เป้าหมายของสำนักปฏิฐานนิยม คือ การฟื้นฟูบุคลิกภาพและการบำบัดรักษาผู้กระทำความผิด

4. ทฤษฎีอาชญาวิทยาของสำนักอาชญาวิทยาชิคาโก สำนักนี้เกิดขึ้นในสหรัฐอเมริกาตอนปลายศตวรรษที่ 19 จนถึงต้นศตวรรษที่ 20 ที่เมืองใหญ่ ๆ ประสบปัญหามากการกระทำผิดกฎหมายของเด็ก เยาวชน และปัญหาอาชญากรรมเกิดสูงขึ้น ปรากฏแก๊งต่าง ๆ เข้าควบคุมท้องถนนหลายแก๊ง คนส่วนใหญ่ให้ความสนใจ

เนื่องจากเกิดความโกลาหลขึ้นในมหานครชิคาโก สังคมต้องการคำตอบว่าเพราะอะไรจึงเกิดปัญหานี้มากขึ้นอย่างผิดปกติและจะจัดการอย่างไร

1) ทฤษฎีการส่งผ่านค่านิยมทางวัฒนธรรม (The Transmission of Cultural Value) แนวคิดของสำนักอาชญาวิทยาชิคาโกมุ่งศึกษาในมิติเกี่ยวกับ “ทฤษฎีการส่งผ่านค่านิยมทางวัฒนธรรม” จากคนกลุ่มหนึ่งไปยังกลุ่มอื่น ๆ รวมทั้งการส่งผ่านข้ามรุ่น จากรุ่นหนึ่งไปยังอีกรุ่นหนึ่ง โดยเฉพาะประเด็นเรื่องเด็กและเยาวชนรุ่นใหญ่ได้ส่งผ่านค่านิยมต่อต้านสังคม เทคนิคการทำผิด และการประกอบอาชญากรรมของรุ่นตนเอง ไปยังเด็กและเยาวชนรุ่นเล็ก เกิดปัญหา “ความโกลาหลและความไร้ระเบียบ” (Chaos) และ “สภาพไร้ปทัสสถาน” (Normlessnes) เกิดขึ้น

2) ทฤษฎีนิเวศน์วิทยาอาชญากรรม โรเบิร์ต อี พาร์ก (Robert E. Park) นักสังคมวิทยาแห่งมหาวิทยาลัยชิคาโก ได้นำเสนอโมเดลในการศึกษาปัญหาอาชญากรรมของนครชิคาโก โดยใช้กรอบแนวคิดเกี่ยวกับระบบนิเวศน์มาเป็นแนวทางในการศึกษาปัญหา เสนอว่าพฤติกรรมมนุษย์ส่วนใหญ่โดยเฉพาะวิถีทางการเจริญเติบโตของเมือง มีลักษณะสอดคล้องกับหลักการเรื่องนิเวศวิทยา ประกอบด้วยหน่วยย่อยในการรับรู้ความรู้สึก โดยผ่านทางการปฏิสัมพันธ์ระหว่างกันของประชาชนและกลุ่มประชาชนที่อยู่ในเมืองนั้น มีการพึ่งพากันระหว่างพลเมืองที่หลากกลาย และหน่วยย่อยทางสังคมและเมืองนั้น พลเมืองทุก ๆ คนต่างก็มีบทบาทหน้าที่ มีส่วนที่เอื้อประโยชน์แก่บุคคลอื่นของสังคม การดำเนินชีวิตจึงบ่งบอกคุณลักษณะเฉพาะของเมืองได้

3) ทฤษฎีการขยายตัวจากศูนย์กลางเดียวกัน (Theory of Concentric Circle) โดยเออร์เนส เบอร์เกส (Ernest Burgess) ได้นำแนวคิดของ พาร์ก มาพัฒนา และนำเสนอทฤษฎีเกี่ยวกับการเจริญเติบโตของเมือง ที่เป็นการเจริญเติบโตแบบขยายวงกว้างออกไป เป็นการขยายจากข้างในออกไปข้างนอก เบอร์เกส กล่าวว่า แหล่งที่มาของการเจริญเติบโตเกิดขึ้นมาจากใจกลางของตัวเมือง การเจริญเติบโตของภายในตัวเมืองเป็นแรงผลักดันส่งไปยังพื้นที่หรือโซนที่อยู่ติดต่อกัน ซึ่งโซนนี้ก็กำลังเริ่มเจริญเติบโตอยู่และก็กำลังจะส่งแรงผลักดันไปยังโซนถัดไป

สามารถอธิบายได้ว่าการที่ผู้กระทำผิดได้เรียนรู้พฤติกรรมอาชญากร จากเยาวชนที่สูงวัยกว่าที่อยู่ในชุมชนนั้น ผลสุดท้ายความล้มเหลวของชุมชนถิ่นที่อยู่ในการจัดระเบียบตัวเอง ก็จะทำให้เด็กและเยาวชนผู้กระทำผิดที่แก่กว่าจะถ่ายทอดพฤติกรรมอาชญากรให้แก่เด็กและเยาวชนที่อ่อนกว่า กล่าวอีกนัยหนึ่ง เด็กและเยาวชนผู้กระทำผิดที่อยู่ในถิ่นฐานชุมชนนั้น จะกลายเป็นผู้ทำหน้าที่จัดระเบียบทางสังคมแทนชุมชนถิ่นที่อยู่ที่ไม่สามารถทำได้สำเร็จ และในที่สุดเด็กและเยาวชนที่อ่อนวัยกว่า ก็จะเดินตามรอยของรุ่นพี่

ทฤษฎีอาชญาวิทยาในมิติสังคมวิทยาเชิงโครงสร้างหน้าที่ ประกอบด้วย

1. ทฤษฎีโครงสร้างหน้าที่ (Functionalism) โดย ก็องต์ (Comte) อธิบายว่า สังคมเปรียบเสมือนร่างกายมนุษย์ ประกอบด้วยระบบย่อยต่าง ๆ ที่มีหน้าที่ และทำหน้าที่ประสานสัมพันธ์กัน มีความสำคัญต่อกัน สังคมมนุษย์ก็มีระบบย่อยที่มีบทบาทหน้าที่แตกต่างกัน มีความเกี่ยวข้องเชื่อมโยงกันในลักษณะการประสานสัมพันธ์ หากระบบใดระบบหนึ่งบกพร่องจะส่งผลกระทบไปยังระบบอื่นๆ พลังของระเบียบสังคม (social order) เป็นสิ่งที่มีอิทธิพลควบคุมพฤติกรรมของคนในสังคม

2. ทฤษฎีอโนมี (Anomie Theory) โดย เอมิล เดอร์ไคม์ (Emile Durkheim (1858-1917) โดยเดอร์ไคม์ กล่าวว่า การเปลี่ยนแปลงทางสังคมอย่างรวดเร็วจากสังคมเกษตรกรรมไปเป็นสังคมอุตสาหกรรม ทำให้สังคมล้มเหลวในบทบาทการทำหน้าที่จัดการความปรารถนา และความคาดหวังของคนในสังคม การเปลี่ยนแปลงทางสังคมอย่างรวดเร็วนำไปสู่การเกิดปัจจัยอื่นตามมาอย่างเช่น สงคราม การแย่งชิง การเคลื่อนย้ายอพยพแรงงาน การเคลื่อนไหวทางสังคม เมื่อความสามารถของสังคมในการจัดการกลไกต่างๆ ล้มเหลว ความเห็นแก่ตัวและความโลภของคนในสังคมมีมากเกินกว่าที่สังคมจะสามารถควบคุมได้ จะทำให้เกิดสภาวะที่ “อโนมี” หมายถึงสภาวะที่ไร้ปทัสฐาน หรือ สภาวะไร้บรรทัดฐาน (normlessness) ซึ่งจะก่อให้เกิดปัญหาสังคม รวมทั้งปัญหาอาชญากรรมตามมา

3. ทฤษฎีความตึงเครียด (Strain Theory) โรเบิร์ต เค เมอร์ตัน (Robert K. Merton) ระบุสังคมให้ความสำคัญและตระหนักต่อเป้าหมายและวิธีการไปสู่เป้าหมายแตกต่างกัน บางสังคมให้ความสำคัญต่อเรื่องหนึ่งมากกว่าอีกเรื่องหนึ่ง ตัวอย่างที่เห็นได้ชัดเจนในสังคมอเมริกันคือ การให้ความสำคัญต่อเป้าหมายมากกว่าวิธีการไปสู่เป้าหมาย ทำให้เกิดความไม่ได้ดุลยภาพระหว่างเป้าหมายและวิธีการไปสู่เป้าหมาย เช่น สังคมอเมริกันให้เป้าหมายความร่ำรวยมั่งคั่งมากเกินไป จนเกินกำลังที่จะหาวิธีการไปสู่เป้าหมายได้ ทำให้ประชาชนจะเกิดความตึงเครียด (Strain) และเกิด ความคับข้องใจ (Frustration) และนำไปสู่ปัญหาอาชญากรรมในที่สุด

ทฤษฎีอาชญาวิทยาในมิติสังคมวิทยาเชิงความสัมพันธ์ ประกอบด้วย

1. ทฤษฎีความสัมพันธ์ที่แตกต่าง (Differential Association) เป็นทฤษฎีที่ตั้งอยู่บนพื้นฐานแนวคิดเรื่องการเรียนรู้ทางสังคม โดยมุ่งศึกษากระบวนการเรียนรู้เกี่ยวกับอาชญากรรม เพื่ออธิบายว่า ทำไมบุคคลบางคนจึงถูกชักนำเข้าสู่การเป็นอาชญากร ในขณะที่ทฤษฎีโครงสร้างหน้าที่จะอธิบายถึงความแตกต่างในการจัดระเบียบทางสังคมว่า ทำไมอัตราการเกิดอาชญากรรมจึงสูงขึ้นในกลุ่มใดกลุ่มหนึ่งของสังคมอเมริกัน ซึ่งกลุ่มบุคคลเหล่านี้ประกอบอาชญากรรม เช่นในพื้นที่สลัม

2. ทฤษฎีอาชญาวิทยาว่าด้วยการกระทำผิดของเด็กและเยาวชน แนวคิดทฤษฎี กล่าวถึงวัฒนธรรมหลักที่แสดงให้เห็นถึงบรรทัดฐานและค่านิยมที่เด่นชัด บ่งชี้วิถีชีวิตของกลุ่มคนในสังคม ซึ่งวัฒนธรรมนั้นจะต้องมีความเด่นชัดและแตกต่างจากวัฒนธรรมอื่น และวัฒนธรรมย่อยที่ทำให้เกิดการเรียนรู้และถ่ายทอดการประกอบอาชญากรรมจากคนรุ่นหนึ่งไปยังคนอีกรุ่นหนึ่ง แนวคิดนี้เชื่อว่า อาชญากรสามารถถ่ายทอดไปยังเด็กรุ่นต่อไปที่อยู่ในถิ่นพำนักของพวกเขา เด็กและเยาวชนผู้ซึ่งไม่พอใจต่อสถานภาพของตนซึ่งเป็นสภาวะที่

ขาดแคลนในตนเองที่กระตุ้นการกระทำผิดจะยิ่งสามารถถูกดึงดูดโดยโดยสิ่งล่อใจจากกลุ่มแก๊งซึ่งสามารถหยิบยื่นมิตรภาพ ความตื่นเต้น และการปกป้องเด็กเหล่านี้ได้

3. ทฤษฎีการตีตรา สาระสำคัญของทฤษฎีการตีตรา คือ 1) การระบายสีให้กับความชั่วร้ายคือจะต้องปฏิเสธการระบายสีให้แก่ความชั่วเหมือนที่เคยทำมา พยายามรณรงค์เรื่องการเลิกระบายสีความชั่ว โดยการใช้โปรแกรมการปรับเปลี่ยนแบบต่างๆ เพราะแม้อาชญากรรมจะเป็นสิ่งที่ชั่วร้าย แต่หากสังคมผลักดันให้อาชญากรถลำลึกลงไปอีกจะกลายเป็นภัยต่อส่วนร่วมมากขึ้น จนไม่อาจจะยอมให้ผู้กระทำผิดกลับตัวเป็นคนดีได้ 2) การเบี่ยงเบนก่อนที่จะถูกตีตรา เช่น การใช้ยาเสพติ และการถูกสังคมตีตราทำให้อาชญากรกลายเป็นอาชญากรร้ายแรง และเมื่อใดก็ตามที่บุคคลถูกตราหน้าจากสังคมว่าเป็นผู้เบี่ยงเบน บุคคลนั้นจะตกอยู่ในภาวะที่ไม่สามารถกอบกู้ภาพพจน์ของตนในฐานะพลเมืองดีกลับคืนมา

4. ทฤษฎีอาชญาวิทยาแบบบูรณาการ (Integrated Theories of Criminology) แนวคิดทฤษฎีมี 3 รูปแบบ คือ

4.1 การบูรณาการทางทฤษฎีแบบผลสืบเนื่อง (End-to-End theoretical Integration) รูปแบบการบูรณาการทางทฤษฎีแบบนี้ ในลักษณะของการเป็นเหตุและผลตามการจัดลำดับปัจจัยเชิงเหตุ-ผล (casual factors) เราสามารถจัดเรียงลำดับองค์ประกอบทางทฤษฎีที่นำมาหลอมรวมกันได้ สามารถอธิบายเรื่องอาชญากรรมได้ว่า เส้นทางที่นำไปสู่การเกิดอาชญากรรม และการกระทำผิดของเด็กและเยาวชน ตอนแรกมีสาเหตุมาจากความล้มเหลวของการจัดการและการควบคุมทางสังคม (ตามแนวทฤษฎีการยึดโยงสังคม) แต่ช่วงต่อมาอิทธิพลของกลุ่มที่มีพฤติกรรมไม่ดี (ตามแนวทฤษฎีความสัมพันธ์ที่แตกต่าง) กลายมาเป็นปัจจัยสำคัญยิ่งกว่าสาเหตุที่เกิดขึ้นในตอนแรก

4.2 การบูรณาการทางทฤษฎีแบบคู่ตรงข้าม(Side-by-Side theoretical Integration) รูปแบบการบูรณาการทางทฤษฎี มีการจัดประเภทคดีโดยใช้เกณฑ์ที่แน่นอน เช่น อาชญากรรมที่เกิดขึ้นแบบทันที กับ อาชญากรรมที่มีการตระเตรียมวางแผน มีการนำทฤษฎีตั้งแต่สองทฤษฎีมาใช้อธิบายในลักษณะคู่ขนานกัน ขึ้นอยู่กับคดีที่นำมาวิเคราะห์ โดยทฤษฎีที่นำมาวิเคราะห์นั้นจะมีความแตกต่างกันหรือมีลักษณะตรงข้ามกัน เช่น low self-control theory ใช้อธิบายอาชญากรรมที่ถูกกระตุ้นให้เกิดทันที เช่น อาชญากรรมข้างถนน ในขณะที่ rational choice theory อธิบายอาชญากรรมที่มีการวางแผน

4.3 การบูรณาการทางทฤษฎีแบบต่อยอด (Up-and-Down theoretical Integration) เป็นรูปแบบการบูรณาการแบบคลาสสิค เพราะเป็นรูปแบที่สัมพันธ์กับประวัติพัฒนาการของทฤษฎีอาชญาวิทยา ทฤษฎีการบูรณาการแบบนี้เป็นการพัฒนาต่อยอดระดับที่สูงขึ้นของทฤษฎีใดทฤษฎีหนึ่ง มีการพัฒนาสูงขึ้นในเชิงนามธรรม จนกระทั่งความเชื่อว่าสิ่งนั้นเป็นความจริงโดยที่ยังไม่ได้มีการพิสูจน์

ทฤษฎีอาชญาวิทยาเป็นแนวทางที่ทำให้ผู้ที่เกี่ยวข้องกับการเกิดอาชญากรรม และอาชญากรได้ตระหนักถึงสาเหตุ หรือปัจจัยต่าง ๆ ที่ทำให้เกิดอาชญากรรม โดยเฉพาะอาชญากรรมที่เกิดจากการกระทำของเด็กและเยาวชน ซึ่งการลงโทษจำเป็นที่จะต้องกระทำด้วยการพิจารณาอย่างรอบคอบ เพื่อป้องกันไม่ให้เกิดการตีตรา และเด็กหรือเยาวชนไม่สามารถกลับมาเป็นคนดีของสังคมได้

2. แนวความคิดและทฤษฎีเกี่ยวกับเทคโนโลยีสารสนเทศ

ปัจจุบันการเปลี่ยนแปลงและความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้ผู้บริหารองค์กรต่าง ๆ ปรับตัวโดยการนำเทคโนโลยีสารสนเทศมาประยุกต์ในการปฏิบัติงานเพื่อเพิ่มประสิทธิภาพการดำเนินงานขององค์กร ความก้าวหน้าของเทคโนโลยีถูกนำมาใช้ในระดับบุคคล สังคม องค์กรธุรกิจ เทคโนโลยีสารสนเทศกระตุ้นให้ทุกภาคส่วนมีการปรับรูปแบบภายในสังคม องค์กร และระดับบุคคลด้วยเชิงกัน ปฏิเสธไม่ได้ว่าในปัจจุบันการดำเนินชีวิตของบุคคล มีเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้องอย่างไม่อาจหลีกเลี่ยงได้

ความหมาย

เทคโนโลยีสารสนเทศมีกำเนิดจากสองคำ คือ เทคโนโลยีและคำว่าสารสนเทศ จึงเรียกกันว่าเทคโนโลยีสารสนเทศ ซึ่งหมายถึง เทคโนโลยีสองสาขาหลักที่ประกอบด้วยเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีสื่อสารโทรคมนาคมที่ผนวกเข้าด้วยกัน เพื่อใช้ในกระบวนการสร้างสรรค์ จัดหา จัดเก็บ ค้นคืน จัดการ ถ่ายทอดและเผยแพร่ข้อมูลในรูปดิจิทัล (digital data) ไม่ว่าจะเป็นเสียง ภาพ ภาพเคลื่อนไหว ข้อความหรือตัวอักษร และตัวเลข เพื่อเพิ่มประสิทธิภาพ ความถูกต้อง ความแม่นยำ และความรวดเร็วให้ทันต่อการนำไปใช้ประโยชน์ (สุพรรษา ยวงทอง และคณะ, 2555, หน้า 2)

เทคโนโลยีสารสนเทศ คือ เทคโนโลยีของการจัดการข้อมูล และประมวลผลข้อมูล (ฝ่ายตำราวิชาการคอมพิวเตอร์, 2557, หน้า 180) เทคโนโลยีสารสนเทศ คือ ความก้าวหน้าทางเทคโนโลยีด้านต่างๆ ที่ทำให้เกิดวิธีการใหม่ๆ ในการจัดเก็บความรู้ การส่งผ่าน และการสื่อสารสารสนเทศ การเข้าถึงข้อมูลสารสนเทศ รวมไปถึงการสร้างอุตสาหกรรมสารสนเทศ ความต้องการสารสนเทศ และการจัดการสารสนเทศให้มีประสิทธิภาพ (เศรษฐชัย ชัยสนิท, 2558, หน้า 4) เทคโนโลยีสารสนเทศ คือ การประยุกต์เอาความรู้ทางด้านวิทยาศาสตร์มาจัดการสารสนเทศที่ต้องการ โดยอาศัยเครื่องมือทางเทคโนโลยีใหม่ๆ เช่น เทคโนโลยีด้านคอมพิวเตอร์ เทคโนโลยีด้านเครือข่ายโทรคมนาคม และการสื่อสาร ตลอดจนอาศัยความรู้ในกระบวนการดำเนินงานสารสนเทศในขั้นตอนต่างๆ ตั้งแต่การแสวงหา การวิเคราะห์ การจัดเก็บ รวมถึงการจัดการเผยแพร่และแลกเปลี่ยนสารสนเทศด้วยเพื่อเพิ่มประสิทธิภาพ ความถูกต้อง แม่นยา และความรวดเร็วทันต่อการนำมาใช้ประโยชน์ (สุพรรษา ยวงทอง, 2558, หน้า 218) และ เทคโนโลยีสารสนเทศ คือ เทคโนโลยีที่นำมาใช้เพื่อการผลิต การจัดการ การจัดเก็บ การสื่อสาร และการเผยแพร่ข้อมูล รวมถึงคอมพิวเตอร์ที่มีการเชื่อมโยงเข้ากับระบบสื่อสารความเร็วสูงเพื่อนำส่งข้อมูล เสียง และวิดีโอ (โอภาส เอี่ยมสิริวงษ์, 2557, หน้า14)

จากความหมายดังกล่าวข้างต้น สรุปได้ว่า เทคโนโลยีสารสนเทศ คือ การประยุกต์เอาความรู้ทางด้านวิทยาศาสตร์ โดยอาศัยเครื่องมือคือคอมพิวเตอร์และอุปกรณ์โทรคมนาคม เพื่อนำมาจัดการสารสนเทศตั้งแต่การผลิต การจัดเก็บ การสืบค้น การจัดการ การสื่อสาร และการเผยแพร่ข้อมูล เพื่อเพิ่มประสิทธิภาพ ความถูกต้อง แม่นยำ รวดเร็วทันต่อการนำไปใช้ประโยชน์

ความสำคัญของเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศจัดเป็นเทคโนโลยียุทธศาสตร์สำคัญของยุคปัจจุบันและอนาคตเนื่องจากมีความสามารถในการเพิ่มประสิทธิภาพและสมรรถภาพในเกือบทุกๆ กิจกรรม โดยก่อให้เกิดการลดต้นทุนหรือค่าใช้จ่าย ช่วยเพิ่มคุณภาพงาน การสร้างกระบวนการหรือกรรมวิธีใหม่ ๆ แก่ผู้ใช้ ได้รับสารสนเทศตามต้องการ สามารถสรุปประโยชน์ของสารสนเทศต่อผู้ใช้ได้ ดังนี้ (สุขุม เฉลยทรัพย์ และคณะ, 2555)

1. เทคโนโลยีสารสนเทศช่วยเพิ่มผลผลิต ลดต้นทุน และเพิ่มประสิทธิภาพในการทำงานในการประกอบธุรกิจ และการอุตสาหกรรม จึงได้มีการนำคอมพิวเตอร์ และระบบสื่อสารโทรคมนาคมเข้ามาช่วยในการทำงาน เช่น ระบบสำนักงานอัตโนมัติ การบริการในระบบออนไลน์ที่สามารถดำเนินกิจกรรมทางการเงินได้สะดวก รวดเร็วโดยไม่จำกัดสถานที่และเวลา เป็นต้น

2. เทคโนโลยีสารสนเทศเปลี่ยนรูปแบบการบริการเป็นแบบกระจาย โดยการพัฒนาระบบข้อมูลและรูปแบบการบริการให้ผู้ใช้บริการสามารถเลือกรูปแบบการบริการได้ตามความต้องการและสามารถเลือกเวลาและสถานที่บริการได้ตามสะดวก เช่น สามารถสั่งซื้อสินค้าได้ทุกที่ ทุกเวลา สามารถสอบถามข้อมูลผ่านทางโทรศัพท์ นักศึกษาทำการลงทะเบียน และตรวจผลการเรียนได้โดยไม่จำกัดสถานที่ เป็นต้น

3. เทคโนโลยีสารสนเทศเป็นสิ่งที่จำเป็นสำหรับการดำเนินการจัดเก็บรวบรวมข้อมูลในหน่วยงานต่าง ๆ ในปัจจุบันทุกหน่วยงานไม่ว่าจะเป็นของรัฐหรือเอกชนต่างก็พัฒนาระบบรวบรวมจัดเก็บข้อมูลเพื่อใช้ในองค์กรเนื่องจากสามารถเก็บข้อมูลได้เป็นจำนวนมาก ใช้พื้นที่ในการจัดเก็บน้อย อำนวยความสะดวกในการค้นหา และปรับปรุงข้อมูลให้ทันสมัยได้โดยง่าย ตัวอย่างของงาน เช่น ระบบทะเบียนราษฎร์ ระบบการจัดเก็บภาษี ระบบเวชระเบียนในโรงพยาบาล เป็นต้น

4. เทคโนโลยีสารสนเทศช่วยการเสริมสร้างคุณภาพชีวิตให้ดีขึ้น สภาพความเป็นอยู่ของสังคมเมืองมีการพัฒนาระบบประมวลผลด้วยคอมพิวเตอร์ มีการพัฒนาระบบสื่อสารโทรคมนาคม เพื่อติดต่อสื่อสารให้สะดวกขึ้น ดังนั้นในการดำเนินชีวิตประจำวันจึงสะดวกสบายมากยิ่งขึ้นจากการประยุกต์ใช้เทคโนโลยีสารสนเทศกับเครื่องอำนวยความสะดวกภายในบ้าน เช่น บ้านอัจฉริยะที่มีการควบคุมการทำงานด้วยระบบคอมพิวเตอร์ ตู้เย็นอัจฉริยะที่สามารถยืดอายุอาหารที่แช่ในตู้เย็นและมีระบบเตือนเมื่ออาหารใกล้หมดอายุ เป็นต้น

5. เทคโนโลยีสารสนเทศเพื่อการพัฒนาการเรียนการสอน ปัจจุบันระบบการเรียนการสอนมีความยืดหยุ่นมากยิ่งขึ้นเมื่อมีการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการเรียนการสอนที่เอื้อให้ผู้เรียนเรียนได้ตามอัธยาศัยโดยไม่จำกัดเวลา และสถานที่ เช่น บทเรียนออนไลน์ที่สามารถเรียนผ่านเว็บ ที่ผู้เรียนสามารถเลือกเรียนได้ทุกที่ ทุกเวลา ตามความต้องการของตน วีดีทัศน์ตามอัธยาศัยที่ผู้เรียนสามารถควบคุมบทเรียนได้เหมือนเปิดวีดิทัศน์ นอกจากนี้เทคโนโลยีสารสนเทศยังนำมาช่วยในด้านการจัดการ เช่น การจัดตารางสอน การคำนวณระดับคะแนน การเก็บข้อมูลต่าง ๆ ของผู้เรียน เป็นต้น

6. เทคโนโลยีสารสนเทศเพื่อการจัดการสภาพแวดล้อม ในการจัดการทรัพยากรธรรมชาติได้มีการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อช่วยในการจัดการ อาทิ การใช้ภาพถ่ายดาวเทียม การใช้ระบบ

สารสนเทศภูมิศาสตร์ (Geographic Information System: GIS) การจำลองรูปแบบสภาวะแวดล้อม การติดตามข้อมูลสภาพอากาศ การตรวจวัดมลภาวะ การจัดการน้ำและการเฝ้าระวังอุทกภัยด้วยระบบสารสนเทศภูมิศาสตร์ เป็นต้น

7. การป้องกันประเทศและความมั่นคงโดยเทคโนโลยีสารสนเทศ ในด้านกิจการทหาร และตำรวจเพื่อการรักษาความมั่นคงปลอดภัย และการป้องกันประเทศ มีการใช้เทคโนโลยีสารสนเทศมาช่วยในการดำเนินการ อาทิ การใช้คอมพิวเตอร์ทำประวัติผู้ก่อการร้าย ผู้ก่ออาชญากรรม ระบบเฝ้าระวังโดยใช้คอมพิวเตอร์เป็นตัวควบคุมการทำงาน อาวุธยุทธโธปกรณ์ และขีปนาวุธสมัยใหม่ เป็นต้น

8. การผลิตในอุตสาหกรรม และการพาณิชยกรรม ในการแข่งขันด้านการผลิตสินค้า อุตสาหกรรมจำเป็นต้องมองหาวิธีในการเพิ่มผลผลิต ควบคุมการผลิตให้ได้มาตรฐาน ดำเนินการได้รวดเร็ว และลดต้นทุนการผลิต เช่น การใช้ระบบคอมพิวเตอร์ควบคุมการผลิต และการบริการ การใช้หุ่นยนต์มาช่วยในด้านแรงงานและการทดสอบคุณภาพแทนแรงงานของมนุษย์ เป็นต้น

9. เทคโนโลยีสารสนเทศในด้านการแพทย์ จะนำมาใช้ในระบบแพทย์ทางไกล (Telemedicine) สามารถปรึกษาแพทย์ผู้เชี่ยวชาญทางไกลได้ อุปกรณ์ทางการแพทย์ที่นำระบบคอมพิวเตอร์มาช่วยในการคุณภาพและการตรวจรักษาโรค การใช้ระบบแพทย์ผู้เชี่ยวชาญ (Expert System) เพื่อการวินิจฉัยโรค

10. ความบันเทิงโดยอาศัยระบบเทคโนโลยีสารสนเทศ ปัจจุบันความบันเทิงรูปแบบต่าง ๆ ได้นำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อเพิ่มขีดความบันเทิง ให้ผู้ใช้บริการได้รับความสะดวกสบายมากยิ่งขึ้น เช่น การจองตั๋วหนังทางออนไลน์ การใช้คาราโอเกะออนดีมานด์ และระบบโฮมเธียร์เตอร์ที่ควบคุมด้วยระบบคอมพิวเตอร์ เป็นต้น

ปัจจุบันเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงอย่างมาก และกลายเป็นส่วนหนึ่งในชีวิตประจำวันของมนุษย์ มีความสำคัญ และเกี่ยวข้องกับคน ทุกระดับ ทั้งในระดับประเทศ ระดับองค์กร หรือระดับบุคคล ดังนี้

ระดับประเทศ ตามนโยบายเศรษฐกิจและสังคมดิจิตอลของรัฐบาลให้มีการนำเทคโนโลยีสารสนเทศที่ทันสมัย และหลากหลายมาเปลี่ยนแปลงวิธีการดำเนินชีวิตของประชาชน การดำเนินธุรกิจ การดำเนินงานของภาครัฐ ซึ่งจะส่งผลให้ประชาชนมีความรอบรู้ สามารถพัฒนา และใช้ประโยชน์จากเทคโนโลยีสารสนเทศได้อย่างรู้เท่าทัน มีโอกาสในการสร้างรายได้ และมีคุณภาพชีวิตที่ดีขึ้น เกิดความมั่งคั่งทางเศรษฐกิจที่แข่งขันได้ในเวทีโลก และความมั่นคงทางสังคมของประเทศต่อไป

ระดับองค์กร ในยุคของสังคมดิจิตอลที่ทำให้สามารถทำงานได้ทุกสถานที่ และทุกเวลาตลอด 24 ชั่วโมง ทั้งองค์กรภาครัฐ และเอกชนต้องพบกับข้อมูลจำนวนมหาศาลอย่างหลีกเลี่ยงไม่ได้ ดังนั้นความสามารถในการทำงานผ่านเครือข่ายอินเตอร์เน็ต ความเข้าใจเครือข่ายสังคมออนไลน์ การซื้อสินค้าและบริการทางอินเตอร์เน็ต และการวิเคราะห์ข้อมูลอย่างชาญฉลาด จึงเป็นสิ่งจำเป็นเพื่อความอยู่รอดขององค์กร การดำเนินงานในองค์กรจึงต้องมีเทคโนโลยีสารสนเทศเพื่อเป็นเครื่องมือช่วยในการปฏิบัติงานที่รวดเร็ว

ช่วยเพิ่มผลผลิต ลดต้นทุน ใช้เป็นกลยุทธ์เพื่อความได้เปรียบในการแข่งขัน สร้างความพึงพอใจกับลูกค้าหรือกลุ่มเป้าหมาย และเกิดประสิทธิภาพในการดำเนินงาน

ระดับบุคคล สำหรับคนทั่วไปเทคโนโลยีสารสนเทศช่วยให้เข้าถึงข้อมูลข่าวสาร สามารถพัฒนาตนเองให้เป็นคนที่ฉลาด รู้เท่าทันสื่อ เท่าทันโลก และยังเป็นเครื่องมือในการสร้างศักยภาพของบุคคล ช่วยยกระดับคนไปสู่สังคมแห่งการเรียนรู้ และสามารถนำไปใช้ในการประกอบอาชีพได้อย่างมีคุณภาพ นอกจากนี้เทคโนโลยีสารสนเทศยังเป็นส่วนหนึ่งในดำเนินชีวิตประจำวันของคนปัจจุบัน เช่น ดูรายการโทรทัศน์ผ่านเครือข่ายสังคมออนไลน์ ซื้อสินค้าผ่านทางอินเตอร์เน็ต จองตั๋วเดินทางแบบออนไลน์ การลงทะเบียนหรือดูผลการเรียนทางเว็บไซต์ เป็นต้น

ดังนั้น จะเห็นว่าเทคโนโลยีสารสนเทศมีความสำคัญและมีประโยชน์ทั้งในระดับประเทศ ระดับองค์กรและระดับบุคคล การเรียนรู้ และสามารถนำเทคโนโลยีสารสนเทศมาใช้ให้เกิดประโยชน์สูงสุดจึงมีความสำคัญและมีความจำเป็นอย่างไม่อาจจะหลีกเลี่ยงได้

ผลกระทบของเทคโนโลยีสารสนเทศ

ผลกระทบในเชิงบวก

การกำเนิดของคอมพิวเตอร์เป็นก้าวสำคัญที่นำไปสู่ยุคสารสนเทศ ในช่วงแรกมีการนำคอมพิวเตอร์มาใช้เป็นเครื่องคำนวณ แต่ต่อมาได้มีความพยายามพัฒนาให้คอมพิวเตอร์เป็นอุปกรณ์สำคัญสำหรับการจัดการข้อมูล เมื่อเทคโนโลยีอิเล็กทรอนิกส์ได้ก้าวหน้ามากขึ้นทำให้สามารถสร้างคอมพิวเตอร์ที่มีขนาดเล็กลงแต่ประสิทธิภาพสูง สภาพการใช้งานจึงใช้กันอย่างแพร่หลาย ผลของเทคโนโลยีสารสนเทศที่มีต่อชีวิตความเป็นอยู่และสังคมจึงมีมาก มีการเรียนรู้และใช้สารสนเทศกันอย่างกว้างขวาง ผลของเทคโนโลยีสารสนเทศโดยรวมทางบวก (สุขุม เฉลยทรัพย์ และคณะ, 2555) ดังนี้

1. การสร้างเสริมคุณภาพชีวิตที่ดีขึ้น สภาพความเป็นอยู่ของสังคมเมือง มีการพัฒนาใช้ระบบสื่อสารโทรคมนาคมเพื่อติดต่อสื่อสารให้สะดวกขึ้น มีการประยุกต์มาใช้กับเครื่องอำนวยความสะดวกภายในบ้าน เช่น ใช้เครื่องควบคุมเครื่องปรับอากาศและใช้ควบคุมระบบไฟฟ้าภายในบ้าน เป็นต้น

2. เสริมสร้างความเท่าเทียมในสังคมและการกระจายโอกาส เทคโนโลยีสารสนเทศทำให้เกิดการกระจายไปทั่วทุกหนทุกแห่ง แม้แต่ถิ่นทุรกันดาร ทำให้มีการกระจายโอกาสการเรียนรู้ มีการใช้ระบบการเรียนการสอนทางไกล การกระจายการเรียนรู้ไปยังถิ่นห่างไกล นอกจากนี้ในปัจจุบันมีความพยายามที่ใช้ระบบการรักษาพยาบาลผ่านเครือข่ายสื่อสาร

3. สารสนเทศกับการเรียนการสอนในสถาบันการศึกษา การเรียนการสอนในโรงเรียนมีการนำคอมพิวเตอร์และเครื่องมือประกอบช่วยในการเรียนรู้ เช่น วีดิทัศน์ เครื่องฉายภาพ คอมพิวเตอร์ช่วยสอน คอมพิวเตอร์ช่วยจัดการศึกษา จัดตารางสอน คำนวณระดับคะแนน จัดชั้นเรียน ทำรายงานเพื่อให้ผู้บริหารได้ทราบถึงปัญหาและการแก้ปัญหาที่อาจเกิดขึ้นในสถานศึกษา ปัจจุบันมีการเรียนการสอนทางด้านเทคโนโลยีสารสนเทศในสถานศึกษาทุกระดับมากยิ่งขึ้น

4. เทคโนโลยีสารสนเทศกับสิ่งแวดล้อม การจัดการทรัพยากรธรรมชาติหลายอย่างจำเป็นต้องใช้สารสนเทศ เช่น การดูแลรักษาป่าจำเป็นต้องใช้ข้อมูล มีการใช้ภาพถ่ายดาวเทียม การติดตามข้อมูลภาพถ่ายทางอากาศการพยากรณ์อากาศ การจำลองรูปแบบสภาวะสิ่งแวดล้อมเพื่อปรับปรุงแก้ไข การเก็บรวมรวมข้อมูลคุณภาพน้ำในแม่น้ำลำคลองต่าง ๆ การตรวจวัดมลภาวะ ตลอดจนการใช้ข้อมูลระบบการตรวจวัดระยะไกลมาช่วยที่เรียกว่าโทรมาตร เป็นต้น

5. เทคโนโลยีสารสนเทศกับการป้องกันประเทศ กิจการทางด้านการทหารมีการใช้เทคโนโลยี อาวุธยุทโธปกรณ์สมัยใหม่ล้วนแต่เกี่ยวข้องกับคอมพิวเตอร์และระบบควบคุม มีการใช้ระบบป้องกันภัย ระบบเฝ้าระวังที่มีคอมพิวเตอร์ควบคุมการทำงาน

6. เทคโนโลยีสารสนเทศกับการป้องกันประเทศ กิจการทางด้านการทหารมีการใช้เทคโนโลยี อาวุธยุทโธปกรณ์สมัยใหม่ล้วนแต่เกี่ยวข้องกับคอมพิวเตอร์และระบบควบคุม มีการใช้ระบบป้องกันภัย ระบบเฝ้าระวังที่มีคอมพิวเตอร์ควบคุมการทำงาน

ผลกระทบในเชิงลบ

1. ผลกระทบของเทคโนโลยีสารสนเทศต่อการศึกษาการใช้เทคโนโลยีสารสนเทศ มาผลิตสื่อการเรียนการสอนอาทิ บทเรียนคอมพิวเตอร์ช่วยสอนบทเรียนผ่านเว็บ หรือบทเรียนออนไลน์ (e-Learning) อาจทำให้เกิดปัญหาที่เห็นได้ชัดเจน เช่น

1.1 ผู้สอนกับผู้เรียนจะขาดความสัมพันธ์และความใกล้ชิดกัน เพราะผู้เรียนสามารถที่จะเรียนได้ในโปรแกรมสำเร็จรูป ทำให้ความสำคัญของสถานศึกษาและผู้สอนลดน้อยลง

1.2 ผู้เรียนที่มีฐานะยากจนไม่สามารถที่จะใช้สื่อประเภทนี้ได้ทำให้เกิดข้อได้เปรียบเสียเปรียบกันระหว่างนักเรียนที่มีฐานะดีและยากจน ทำให้เห็นว่าผู้ที่มีฐานะทางเศรษฐกิจก็ย่อมที่จะมีโอกาสทางการศึกษาและทางสังคมดีกว่าด้วย ผลกระทบในการนำเทคโนโลยีสารสนเทศมาใช้ในด้านการเรียนการสอนควรนำมาใช้เป็นสื่อเสริมอย่างเหมาะสมต้องยึดผู้เรียนเป็นสำคัญให้ผู้เรียนเกิดกระบวนการคิด ส่วนบทบาทของสถาบันการศึกษาควรจัดสรรสื่อให้เพียงพอและเหมาะสมกับผู้เรียนและสภาวะแวดล้อมจะให้เกิดการใช้เทคโนโลยีได้อย่างคุ้มค่า

2. ผลกระทบของเทคโนโลยีสารสนเทศต่อสิ่งแวดล้อม อาจเกิดปัญหามลพิษต่อสิ่งแวดล้อม ทั้งนี้ก็เพราะมนุษย์นำเทคโนโลยีทางด้านเทคโนโลยีสารสนเทศ ไปพัฒนาอย่างผิดวิธีและนำไปใช้ในทางที่ผิด เพราะมุ่งเพียงแต่จะก่อประโยชน์ให้แก่ตนเองเท่านั้น ดังนั้นผู้นำมาใช้จึงควรพิจารณาให้รอบคอบ ความเหมาะสม มีการประเมินความจำเป็น วิเคราะห์ผลกระทบต่อสิ่งแวดล้อมก่อนที่จะนำมาใช้

3. ผลกระทบของเทคโนโลยีสารสนเทศต่อสังคม

3.1 การนำเทคโนโลยีมาใช้อาจทำให้เกิดปัญหาการว่างงานจากการใช้แรงงานมนุษย์ เพราะภาคอุตสาหกรรมหรือภาคการเกษตรมีความต้องการใช้แรงงานมนุษย์ลดลงในการเพิ่มผลผลิต

3.2 การปรับตัวเพื่อให้ทันกับเทคโนโลยีสมัยใหม่ของพนักงานที่มีอายุมากหรือมีความรู้น้อยก็จะทำให้ไม่สามารถปรับตัวเข้ากับเทคโนโลยีเหล่านี้ได้ และรู้สึกว่าเทคโนโลยีสมัยใหม่เป็นสิ่งที่ทำได้ยากต้องมีความรู้จึงจะเข้าใจได้

3.3 สมาชิกในสังคมมีการดำเนินชีวิตที่ต่างคนต่างอยู่ ไม่มีความสัมพันธ์กันภายในสังคม เพราะต่างมีชีวิตที่ต้องรีบเร่งและดิ้นรน

4. ผลกระทบของเทคโนโลยีสารสนเทศต่อเศรษฐกิจ

4.1 มนุษย์สามารถจับจ่ายใช้สอยได้ง่ายมากขึ้น เพราะมีบัตรเครดิตทำให้ไม่ต้องพกเงินสด หากต้องซื้ออะไรที่ไม่ได้เตรียมการไว้ล่วงหน้าก็สามารถซื้อได้ทันทีเพียงแต่มีบัตรเครดิตเท่านั้น ทำให้อัตราการเป็นหนี้สูงขึ้น

4.2 การแข่งขันกันทางธุรกิจมีมากขึ้นเพราะต่างก็มุ่งหวังผลกำไรซึ่งก็เกิดผลดี คืออัตราการขยายตัวทางธุรกิจสูงขึ้นแต่ผลกระทบก็เกิดตามมา ซึ่งบางครั้งก็มุ่งแต่แข่งขันจนลืมความมีมนุษยธรรมหรือความมีน้ำใจไป

5. ผลกระทบของเทคโนโลยีสารสนเทศต่อสุขภาพจิต

5.1 เมื่อดำเนินการชีวิตแบบเดิมที่เป็นแบบเรียบง่าย ต้องเปลี่ยนมาปรับตัวให้ทันกับเหตุการณ์ปัจจุบันตลอดเวลาก็อาจจะทำให้เกิดความเครียด ความวิตกกังวลไม่ว่าจะในหน้าที่การงานหรือการดำเนินชีวิตประจำวัน

5.2 พฤติกรรมของเยาวชน โดยเฉพาะเกมคอมพิวเตอร์ทำให้เยาวชนมีพฤติกรรมการชอบการต่อสู้และการใช้กำลัง เป็นต้น

5.3 นักธุรกิจต้องทำงานแข่งกับเวลา ไม่มีเวลาได้พักผ่อนก็ก่อให้เกิดวามเครียด สุขภาพจิตก็เสียตามมาด้วย

การใช้เทคโนโลยีสารสนเทศมีทั้งด้านบวกและด้านลบ หากนำมาใช้ให้เหมาะสมก็จะส่งผลต่อคุณภาพชีวิตให้ดีขึ้น และเพิ่มศักยภาพการทำงานในหลายสาขาอาชีพ แต่หากใช้เทคโนโลยีสารสนเทศโดยไม่ระมัดระวังและขาดจิตสำนึก คุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศ ก็จะส่งผลกระทบหลายด้านเช่นกัน ดังนั้นผู้ใช้เทคโนโลยีสารสนเทศจึงควรมีความรู้ความเข้าใจในเรื่องของกฎหมายเทคโนโลยีสารสนเทศ จริยธรรมในการใช้เทคโนโลยีสารสนเทศ รวมถึงความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

3. แนวความคิดและทฤษฎีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

เทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว และเป็นส่วนหนึ่งของชีวิตประจำวันของบุคคลและการดำเนินธุรกิจขององค์กรต่าง ๆ อีกทั้งยังเป็นส่วนหนึ่งของความเป็นอยู่ในการดำรงชีวิตประจำวันของมนุษย์ในยุคสังคมสารสนเทศ แต่บางครั้งยังมีผู้ใช้เทคโนโลยีสารสนเทศไปในทางที่ก่อให้เกิดอันตราย หรือความเสียหายกับผู้อื่น ความเสียหายดังกล่าวนับตั้งแต่การสร้างความรำคาญไปจนถึงสร้างความเสียหายที่มีมูลค่ามหาศาล เนื่องจากการใช้คอมพิวเตอร์เพื่อทำความผิดนั้นเป็นการที่ใช้เทคโนโลยีที่ซับซ้อนยากต่อ การตรวจพบ หรือค้นหาร่องรอยในการก่อความผิด ดังนั้นองค์กรจึงต้องให้ความสำคัญกับระบบเทคโนโลยีสารสนเทศ เพราะหากระบบผิดพลาดไม่ว่าจะด้วยสาเหตุของตัวระบบเอง หรือมีบุคคลมาทำให้ระบบผิดพลาดหรือเกิดความเสี่ยง (Information system risk) จะก่อให้เกิดความสูญเสีย เสียหายอย่างมาก

ความเสี่ยงหรือภยันตรายที่สามารถเกิดขึ้นได้กับระบบคอมพิวเตอร์และสารสนเทศมีเป็นจำนวนมาก จากรายงานของ Kaspersky Security Bulletin ในปี ค.ศ. 2013 (วอนชนก ไชยสุนทร, 2561) พบว่าความเสี่ยงทีเกิดจากการจู่โจมหรือบุกรุกระบบงานดิจิทัลและคอมพิวเตอร์ทั้งในระดับบุคคลและระดับองค์การอันดับแรกเกิดจากไวรัสคอมพิวเตอร์ เวิร์ม สปายแวร์ และมัลแวร์ชนิดต่าง ๆ รองลงมาคือ สแปม ฟิชชิ่ง การโจรกรรมข้อมูล และการโจรกรรมอุปกรณ์คอมพิวเตอร์ โดยเฉพาะอย่างยิ่งการโจรกรรมอุปกรณ์เคลื่อนที่ต่าง ๆ ตามลำดับ จากข้อมูลดังกล่าวแสดงให้เห็นถึงภยันตรายและความเสี่ยงที่สามารถเกิดขึ้นได้กับระบบสารสนเทศขององค์การ ซึ่งมีการเปลี่ยนแปลงรูปแบบอยู่ตลอดเวลา องค์การจึงจำเป็นที่จะต้องมีการระมัดระวัง จัดหาวิธีการรักษาความปลอดภัย รวมทั้งเตรียมความพร้อมเพื่อรับมือกับภัยอันตรายจากการใช้งานระบบเทคโนโลยีสารสนเทศ

วอนชนก ไชยสุนทร (2561) ระบุข้อสรุปจากการประชุมสหประชาชาติถึงประเภทอาชญากรรมทางคอมพิวเตอร์ว่าสามารถจัดแบ่งได้ 5 ประเภท ได้แก่

1. การเข้าถึงข้อมูลและระบบสารสนเทศของผู้อื่นโดยไม่ได้รับอนุญาต
2. การสร้างความเสียหายแก่ข้อมูลหรือโปรแกรมคอมพิวเตอร์ของบุคคลหรือของหน่วยงานอื่น
3. การก่อกวนการทำงานของระบบคอมพิวเตอร์หรือเครือข่ายให้ไม่สามารถทำงานได้ตามปกติ
4. การยับยั้งหรือก่อกวนการสื่อสารของระบบการสื่อสารและเครือข่ายโดยไม่ได้รับอนุญาต
5. การโจรกรรมข้อมูลบนคอมพิวเตอร์ รวมถึงการขโมยหรือลักลอบ ดักจับ ข้อมูลและสารสนเทศของผู้อื่น

นอกจากนั้นคณะกรรมการเฉพาะกิจร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์ ระบุเพิ่มเติมว่าประเภทของอาชญากรรมทางคอมพิวเตอร์ในปัจจุบัน มีเพิ่มขึ้นอีกเป็นจำนวนมาก (วอนชนก ไชยสุนทร, 2561) ได้แก่

1. การขโมยข้อมูลทางอินเทอร์เน็ต รวมถึงการลักลอบใช้ประโยชน์จากระบบคอมพิวเตอร์และระบบสารสนเทศของผู้อื่น

2. การละเมิดทรัพย์สินทางปัญญา จำพวกลิขสิทธิ์ สิทธิบัตร รวมทั้งการใช้ซอฟต์แวร์ผิดกฎหมาย

3. การเผยแพร่ข้อมูลที่ไม่เป็นความจริง ไม่เหมาะสม ก่อให้เกิดความเสียหายกับทั้งและองค์การธุรกิจ

4. การใช้คอมพิวเตอร์และระบบสารสนเทศในการโจรกรรม เช่น การยักยอกเงินจากระบบธนาคาร เป็นต้น

5. การก่อกวนระบบงานทั้งระบบงานส่วนบุคคลขององค์การต่าง ๆ และระบบงานของทางราชการทำให้ไม่สามารถทำงานได้ตามปกติ

6. การสร้างข้อมูลเท็จเพื่อการปกปิดความผิดของตนเอง โดยใช้ระบบการสื่อสารและเทคโนโลยีมาเป็นเครื่องมือ

รูปแบบการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

สุขุม เฉลยทรัพย์ และคณะ (2555) ระบุถึงรูปแบบการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีลักษณะดังต่อไปนี้

1. การเข้าถึงระบบและข้อมูลคอมพิวเตอร์

สำหรับมาตราที่เกี่ยวข้องกับการเข้าถึงระบบและข้อมูลคอมพิวเตอร์ โดยการเข้าถึงโดยมิชอบหมายถึง การบุกรุก และการล่วงรู้มาตรการป้องกันระบบคอมพิวเตอร์ โดยรูปแบบการกระทำผิดมีรายละเอียดดังนี้

1.1 สปายแวร์ เป็นโปรแกรมที่อาศัยช่องทางการเชื่อมต่อกับอินเทอร์เน็ตขณะที่เราที่ท่องเว็บไซต์บางเว็บหรือทำการดาวน์โหลดข้อมูล แอบเข้ามาติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ โดยผู้ใช้อาจไม่ได้เจตนา และอาจทำการติดตามหรือสะกดรอยข้อมูลของผู้ใช้ซึ่งอาจส่งผลในลักษณะต่างๆ ต่อเครื่องคอมพิวเตอร์เช่น ปรากฏป๊อบอัพโฆษณาเล็กๆ ขณะใช้เครื่องคอมพิวเตอร์โดยไม่ได้เรียกขึ้นมา เครื่องคอมพิวเตอร์ทำงานช้าลงหรืออาจเข้าสู่เว็บไซต์ต่างๆ ได้ช้าหรือเมื่อเปิดเว็บบราวเซอร์ก็จะลิงค์ไปยังเว็บไซต์หลักของตัวสปายแวร์ที่ถูกตั้งค่าไว้ หากเกิดอาการรุนแรงสปายแวร์บางเวอร์ชั่น อาจทำการติดตามค้นหารหัสผ่านที่พิมพ์ลงไปเพื่อทำการล็อกอินเข้าแอคเคาน์เตอร์ต่างๆ

1.2 สนิฟเฟอร์ คือโปรแกรมที่คอยดักฟังการสนทนาบนเครือข่าย รวมถึงการดักจับแพ็กเก็ตในเครือข่าย โปรแกรมสนิฟเฟอร์จะถอดรหัสข้อมูลในแพ็กเก็ตและเก็บบันทึกไว้ให้ผู้ติดตั้งนำไปใช้งาน ซึ่งแฮกเกอร์นิยมนำมาใช้เพื่อเจาะเข้าไปในเครื่องคอมพิวเตอร์ปลายทางสำหรับดักจับข้อมูล เช่น ชื่อบัญชี หรือชื่อผู้ใช้และรหัสผ่าน เพื่อนำไปใช้เจาะระบบอื่นต่อไป

1.3 ฟิชชิ่ง เป็นการหลอกลวงเหยื่อเพื่อลวงเอาข้อมูลส่วนตัว โดยการส่งอีเมลหลอกลวง (Spoofing) เพื่อขอข้อมูลส่วนตัว หรืออาจสร้างเว็บไซต์ปลอม เพื่อหลอกลวงให้เหยื่อ หรือผู้รับอีเมลเปิดเผยข้อมูลส่วนบุคคล หรือข้อมูลด้านการเงิน เพื่อนำไปใช้ประโยชน์ในทางที่ผิดต่อไป

2. การรบกวนระบบและข้อมูลคอมพิวเตอร์

การกระทำผิดเกี่ยวกับการรบกวนระบบและข้อมูลคอมพิวเตอร์ จะเกี่ยวข้องกับมาตรา 9 และมาตรา 10 ลักษณะความผิดจะทำการรบกวนหรือทำลายระบบ และข้อมูลคอมพิวเตอร์ โดยใช้เครื่องมือที่ผู้กระทำผิดกระทำการเรียกว่า มะลิซเชิส โค๊ด (Malicious Code) ซึ่งจะอยู่ในรูปแบบต่างๆ เช่น ไวรัส เวิร์ม หรือหนอนอินเทอร์เน็ต และโทรจัน อันส่งผลในการรบกวน และสร้างความเสียหายให้กับระบบคอมพิวเตอร์ อาทิ การตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ การทำให้คอมพิวเตอร์ทำงานผิดปกติหรือหยุดการทำงาน เป็นต้น นอกจากนี้ยังมีการโจมตีอีกรูปแบบหนึ่งคือ ดิไนออล อ๊อฟ เซอร์วิส (Denial of Service) ที่เป็นการโจมตีเพื่อให้ไม่สามารถบริการระบบเครือข่ายได้อีกต่อไป สำหรับรายละเอียดการโจมตีระบบและข้อมูลคอมพิวเตอร์มีดังนี้

2.1 ไวรัสคอมพิวเตอร์ เป็นโปรแกรมชนิดหนึ่งที่พัฒนาขึ้นเพื่อก่อให้เกิดความเสียหายต่อข้อมูล หรือระบบคอมพิวเตอร์ ซึ่งในปัจจุบันไวรัสคอมพิวเตอร์ได้พัฒนารูปแบบ เทคนิคการแพร่กระจาย และความสามารถ รวมทั้งความรุนแรง ในการก่อความเสียหายแก่ระบบแตกต่างไปจากเดิมมาก ซึ่งมีรูปแบบ ดังนี้

2.1.1 หนอนอินเทอร์เน็ต (Internet Worm) หมายถึง โปรแกรมที่ออกแบบมาให้สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นได้ด้วยตัวเอง โดยอาศัยระบบเครือข่ายคอมพิวเตอร์ เช่น อีเมล หรือการแชร์ไฟล์ ทำให้การแพร่กระจายเป็นไปอย่างรวดเร็วและเป็นวงกว้าง

2.1.2 โทรจัน (Trojan) หมายถึง โปรแกรมที่ออกแบบมาให้แฝงเข้าไปสู่ระบบคอมพิวเตอร์ของผู้ใช้อื่นในหลากหลายรูปแบบ เช่น โปรแกรม หรือการ์ดอวยพร เป็นต้น เพื่อดักจับ ติดตาม หรือควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ถูกคุกคาม

2.1.3 โค๊ด (Exploit) หมายถึง โปรแกรมที่ออกแบบมาให้สามารถเจาะระบบโดยอาศัยช่องโหว่ของระบบปฏิบัติการ หรือแอพพลิเคชั่นที่ทำงานอยู่บนระบบ เพื่อให้ไวรัสหรือผู้บุกรุกสามารถครอบครอง ควบคุม หรือกระทำการอย่างหนึ่งอย่างใดบนระบบได้

2.1.4 ข่าวไวรัสหลอกลวง (Hoax) มักจะอยู่ในรูปแบบของการส่งข้อความต่อๆ กันไป เหมือนกับการส่งจดหมายลูกโซ่ โดยข้อความประเภทนี้จะใช้หลักจิตวิทยา ทำให้ข่าวสารนั้นน่าเชื่อถือ ถ้าผู้ที่ได้รับข้อความปฏิบัติตามอาจจะทำให้เกิดความเสียหายต่อระบบคอมพิวเตอร์ เช่น การให้ลบไฟล์ข้อมูลที่จำเป็นของระบบปฏิบัติการโดยหลอกว่าเป็นไวรัสคอมพิวเตอร์ ทำให้ระบบปฏิบัติการทำงานผิดปกติ เป็นต้น

2.2 ดิไนออล อ๊อฟ เซอร์วิส (Denial of Service: DoS) หรือ ดิสตริบิวต์ ดิไนออล อ๊อฟ เซอร์วิส (Distributed Denial of Service: DDoS) เป็นการโจมตีจากผู้บุกรุกที่ต้องการทำให้เกิดภาวะที่ระบบคอมพิวเตอร์ไม่สามารถให้บริการได้ หรือผู้ใช้งานไม่สามารถเข้าใช้บริการรวมถึงทรัพยากรในระบบได้นอกจากนี้การโจมตีรูปแบบนี้ยังสามารถทำให้เครื่องคอมพิวเตอร์หรือเครือข่ายไม่สามารถใช้งานได้ รูปแบบโจมตีของ DoS หรือ DDoS มีหลากหลายรูปแบบดังนี้

2.2.1 การแพร่กระจายของไวรัสปริมาณมากในเครือข่าย ก่อให้เกิดการติดขัดของการจราจรในระบบเครือข่าย ทำให้การสื่อสารในเครือข่ายตามปกติช้าลง หรือใช้ไม่ได้

2.2.2 การส่งแพ็กเก็ตจำนวนมากเข้าไปในเครือข่ายหรือ ฟลัดดิ้ง (flooding) เพื่อให้เกิดการติดขัดของการจราจรในเครือข่ายมีสูงขึ้น ส่งผลให้การติดต่อสื่อสารภายในเครือข่ายช้าลง

2.2.3 การโจมตีข้อบกพร่องของซอฟต์แวร์ระบบ เพื่อจุดประสงค์ในการเข้าถึงสิทธิ์การใช้สูงขึ้น จนไม่สามารถเข้าไปใช้บริการได้

2.2.4 การขัดขวางการเชื่อมต่อใดๆ ในเครือข่ายทำให้คอมพิวเตอร์หรืออุปกรณ์เครือข่ายไม่สามารถสื่อสารกันได้

2.2.5 การโจมตีที่ทำให้ซอฟต์แวร์ในระบบปิดตัวเองลงโดยอัตโนมัติ หรือไม่สามารถทำงานต่อได้จนไม่สามารถให้บริการใดๆ ได้อีก

2.2.6 การกระทำใดๆ ก็ตามเพื่อขัดขวางผู้ใช้ระบบในการเข้าใช้บริการในระบบได้ เช่น การปิดบริการเว็บเซิร์ฟเวอร์ลง

2.2.7 การทำลายระบบข้อมูล หรือบริการในระบบ เช่น การลบชื่อ และข้อมูลผู้ใช้ออกจากระบบ ทำให้ไม่สามารถเข้าสู่ระบบได้

3. การสแปมเมล (จดหมายบุกรุก)

ความผิดฐานการสแปมอีเมล จะเกี่ยวข้องกับมาตรา 11 ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ลักษณะการกระทำ เป็นการส่งจดหมายอิเล็กทรอนิกส์หรืออีเมลไปให้บุคคลอื่น โดยการซ่อนหรือปลอมชื่อ อีเมล และหากการส่งอีเมลไปให้ผู้รับคนใดคนหนึ่งมากเกินปกติ ก็ถือว่าเป็นการส่งอีเมลสแปมเช่นกัน บางครั้งการส่งอีเมลในลักษณะที่ผู้รับไม่ต้องการก็อาจเรียกว่า อีเมลขยะ (Junk Email)

4. การใช้โปรแกรมเจาะระบบ (Hacking Tool)

การกระทำผิดฐานเจาะระบบโดยใช้โปรแกรม จะเกี่ยวข้องกับมาตรา 13 ซึ่งการเจาะระบบนิยมเรียกว่าการแฮกระบบ (Hack) เป็นการเข้าสู่ระบบคอมพิวเตอร์ที่ได้มีการรักษาความปลอดภัยไว้ ให้สามารถเข้าใช้ได้สำหรับผู้ที่อนุญาตเท่านั้น ส่วนผู้ที่เข้าสู่ระบบโดยไม่ได้รับอนุญาตจะเรียกว่า แฮกเกอร์ ซึ่งวิธีการที่แฮกเกอร์ใช้ในการเจาะระบบมีหลายวิธี เช่น การอาศัยช่องโหว่ของระบบปฏิบัติการ (โอเอส) เมื่อเจาะเข้ามาในระบบได้ ก็อาจมีการนำโปรแกรมบางส่วนมาใช้งานเพื่อเจาะระบบเข้าสู่ส่วนที่สำคัญอื่นๆ ต่อไป บางครั้งแฮกเกอร์วางโปรแกรมโทรจันเอาไว้หรือสิ่งที่แฮกเกอร์นำมาแอบซ่อนไว้ในระบบ เพื่อเป็นตัวคอยเปิดช่องทางให้เข้ามาใหม่ในภายหลัง หรือเป็นตัวเก็บรวบรวมข้อมูลบางอย่างเอาไว้ เพื่อจะได้นำมาใช้ประโยชน์ในภายหลัง

5. การโพสต์ข้อมูลเท็จ

สำหรับการโพสต์ข้อมูลเท็จ หรือการใส่ร้าย กล่าวหาผู้อื่น การหลอกลวงผู้อื่นให้หลงเชื่อ หรือการโฆษณาชวนเชื่อใดๆ ที่จะส่งผลกระทบต่อระบบเศรษฐกิจ สังคม หรือก่อให้เกิดความเสื่อมเสียต่อสถาบันพระมหากษัตริย์เหล่านี้ เป็นการกระทำตามมาตรา 14 และ มาตรา 15 ของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นอกจากนี้การฟอร์เวิร์ดอีเมล หรือการส่งต่ออีเมลก็ถือเป็นความผิดด้วย เพราะมีส่วนในการเป็นผู้เผยแพร่ข้อมูลดังกล่าวด้วย

6. การตัดต่อภาพ

ความผิดฐานการตัดต่อภายให้ผู้อื่นได้รับความเสียหาย เป็นความผิดในมาตรา 16 ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งการกระทำผิดรวมถึงการแต่งเติม หรือดัดแปลงรูปภาพด้วยวิธีใดๆ จนเป็นเหตุให้ผู้ถูกกระทำได้รับความเสื่อมเสียชื่อเสียง ถูกเกลียดชังหรือได้รับความอับอาย แต่ถ้าหากผู้กระทำความผิดเป็นผู้ตัดต่อภาพ และเผยแพร่เองด้วย ก็อาจได้รับโทษทั้งมาตรา 14 มาตรา 15 และมาตรา 16 พร้อมกันด้วย

รูปแบบในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้มีหลากหลายรูปแบบอาทิ การเข้าถึงระบบและข้อมูลคอมพิวเตอร์ การรบกวนระบบและข้อมูลคอมพิวเตอร์ การใช้จดหมายบุกรุก การใช้โปรแกรมเจาะระบบ การโพสต์ข้อมูลเท็จ และการตัดต่อภาพ ดังนั้นผู้ใช้จึงต้องมีความรู้เท่าทันเทคโนโลยีสารสนเทศเพื่อความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

การรักษาความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ

การใช้งานด้านเทคโนโลยีสารสนเทศมีความเสี่ยงต่อการถูกบุกรุก โจมตี จากรูปแบบการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เสนอแนวทางป้องกันเพื่อการใช้งานระบบคอมพิวเตอร์ได้อย่างปลอดภัย ดังมีรายละเอียดดังนี้

1. แนวทางป้องกันภัยจากสปายแวร์

สปายแวร์เป็นโปรแกรมที่ไม่พึงประสงค์ที่แอบเข้ามาในระบบการใช้งานของเราและอาจติดตามการทำงานข้อมูลของเราได้ ดังนั้นการป้องกันสปายแวร์สามารถทำได้ ดังนี้

1.1 ไม่คลิกลิงก์บนหน้าต่างเล็กของป๊อบอัพโฆษณา ให้รีบปิดหน้าต่างโดยคลิกที่ปุ่ม “X”

1.2 ระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี โดยเฉพาะเว็บไซต์ที่ไม่น่าเชื่อถือ เพราะสปายแวร์จะแฝงตัวอยู่ในโปรแกรมดาวน์โหลดมา

1.3 ไม่ควรติดตามอีเมลลิงก์ที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ เพราะอาจให้ผลตรงกันข้าม

2. แนวทางป้องกันภัยจากสนิฟเฟอร์

สำหรับการป้องกันสนิฟเฟอร์วิธีที่ดีที่สุดที่สามารถป้องกันการดักฟัง หรือการดักจับแพ็กเก็ตทางออนไลน์ ก็คือ การเข้ารหัสข้อมูล โดยทำได้ ดังนี้

2.1 SSL (Secure Socket Layer) ใช้ในการเข้ารหัสข้อมูลผ่านเว็บ ส่วนใหญ่จะใช้ในธุรกรรมอิเล็กทรอนิกส์

2.2 SSH (Secure Shell) ใช้ในการเข้ารหัสเพื่อเข้าไปใช้งานบนระบบยูนิกซ์ เพื่อป้องกันการดักจับ

2.3 VPN (Virtual Private Network) เป็นการเข้ารหัสข้อมูลที่ส่งผ่านทางอินเทอร์เน็ต

2.4 PGP (Pretty Good Privacy) เป็นวิธีการเข้ารหัสของอีเมล แต่ที่นิยมอีกวิธีหนึ่งคือ S/MIME

3. แนวทางป้องกันภัยจากฟิชชิ่ง

ลักษณะของฟิชชิ่งส่วนใหญ่เป็นการส่งอีเมลหลอกลวง เพื่อขอข้อมูลส่วนตัว ดังนั้นแนวทางป้องกันสามารถทำได้ง่ายๆ ดังนี้

3.1 หากอีเมลส่งมาในลักษณะของข้อมูล อาทิ จากธนาคาร บริษัทประกันชีวิต ฯลฯ ควรติดต่อกับธนาคารหรือบริษัท และสอบถามด้วยตนเอง เพื่อป้องกันไม่ให้ถูกหลอกเอาข้อมูลไป

3.2 ไม่คลิกลิงก์ที่แฝงมากับอีเมลไปยังเว็บไซต์ที่ไม่น่าเชื่อถือ เพราะอาจเป็นเว็บไซต์ปลอมที่มีหน้าตาคล้ายธนาคารหรือบริษัททางด้านการเงิน ให้กรอกข้อมูลส่วนตัว และข้อมูลบัตรเครดิต

4. แนวทางป้องกันภัยจากไวรัสคอมพิวเตอร์

ติดตั้งซอฟต์แวร์ป้องกันไวรัสบนระบบคอมพิวเตอร์ และทำการอัพเดทฐานข้อมูลไวรัสของโปรแกรมอยู่เสมอ

4.1 ตรวจสอบและอุดช่องโหว่ของระบบปฏิบัติการอย่างสม่ำเสมอ

4.2 ปรับแต่งการทำงานของระบบปฏิบัติการ และซอฟต์แวร์บนระบบให้มีความปลอดภัยสูงเช่น ไม่ควรอนุญาตให้โปรแกรมไมโครซอฟต์ออฟฟิสเรียกใช้มาโคร เปิดใช้งานระบบไฟร์วอลที่ติดตั้งมาพร้อมกับระบบปฏิบัติการ Windows XP หรือระบบปฏิบัติการอื่นๆ ปิดการแชร์ไฟล์ผ่านเครือข่ายหากไม่มีความจำเป็น

4.3 ใช้ความระมัดระวังในการเปิดอ่านอีเมล และการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ เช่น หลีกเลี่ยงการเปิดอ่านอีเมลและไฟล์ที่แนบมาจนกว่าจะรู้แหล่งที่มา ตรวจหาไวรัสบนสื่อบันทึกข้อมูลทุกครั้งก่อนเปิดเรียกใช้ไฟล์บนสื่อนั้นๆ และไม่ควรเปิดไฟล์ที่มีนามสกุลแปลก ๆ เป็นต้น

5. แนวทางป้องกันภัยการโจมตีแบบ DoS (Denial of Service)

รูปแบบการโจมตีในลักษณะนี้จะส่งผลให้ระบบคอมพิวเตอร์ไม่สามารถให้บริการแก่ผู้เข้าใช้บริการได้ ซึ่งส่งผลกระทบถึงความสูญเสียทั้งในแง่ของเวลาและทรัพย์สินสำหรับองค์กร ดังนั้นมาตรการในการลดผลกระทบหรือความเสี่ยงต่อการถูกโจมตี มีดังนี้ (ซีเอส ล็อกซอินโฟ, 2551, หน้า 28-29)

5.1 ใช้กฎการฟิลเตอร์แพ็กเก็ตบนเราเตอร์สำหรับกรองข้อมูล เพื่อลดผลกระทบต่อปัญหาการเกิด DoS รวมถึงความเสี่ยงที่อาจจะเกิดจากบุคคลภายในองค์กรเป็นต้นกำเนิดการโจมตีแบบ DoS ไปยังเครือข่ายเป้าหมายอื่นด้วย

5.2 ติดตั้งซอฟต์แวร์เพิ่มเติมในการแก้ไขปัญหาของการโจมตีโดยใช้ TCP SYN Flooding ซึ่งจะช่วยให้ระบบยังสามารถทำงานได้ในสภาวะที่ถูกโจมตีได้ยาวนานขึ้น

5.3 ปิดบริการบนระบบที่ไม่มีการใช้งานหรือบริการที่เปิดโดยดีฟอลต์ เช่น บนเว็บเซิร์ฟเวอร์ไม่ควรเปิดพอร์ตให้บริการโอนย้ายไฟล์ผ่านโปรโตคอล FTP

5.4 นำระบบการกำหนดโควตามาใช้ โดยการกำหนดโควตาเนื้อที่ดิสก์สำหรับผู้ใช้ระบบหรือสำหรับบริการในระบบ และควรพิจารณาการแบ่งพาร์ทิชั่นออกเป็นส่วนเพื่อลดความเสี่ยงหรือผลกระทบที่เนื้อที่บนพาร์ทิชั่นใดๆ เต็ม จะได้ไม่ส่งผลกระทบต่อข้อมูลหรือการทำงานของระบบพาร์ทิชั่นอื่นไปด้วย รวมทั้งการกำหนดโควตาของการสร้างโพรเซสในระบบ หรือโควตาในเรื่องอื่นที่มีผลต่อการใช้งานทรัพยากรในระบบล้วนเป็นสิ่งที่ควร

นำมาใช้ และควรศึกษาคู่มือระบบเพื่อหลีกเลี่ยงปัญหาที่อาจจะเกิดจากความเลินเล่อของผู้ดูแลระบบหรือการแก้ไขปัญหาเมื่อเกิดเหตุฉุกเฉินขึ้น

5.5 สังเกตและเฝ้ามองพฤติกรรมและประสิทธิภาพการทำงานของระบบ นำตัวเลขตามปกติของระบบมากำหนดเป็นบรรทัดฐานในการเฝ้าระวังในครั้งถัดไป เช่น ปริมาณการใช้งานฮาร์ดดิสก์ ประสิทธิภาพการใช้งานหน่วยประมวลผลกลางหรือซีพียู ปริมาณการจราจรในเครือข่ายที่เกิดขึ้นในช่วงเวลาหนึ่ง เป็นต้น

5.6 ตรวจตราระบบการจัดการทรัพยากรระบบตามกายภาพอย่างสม่ำเสมอ แน่ใจว่าไม่มีผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้ มีการกำหนดตัวบุคคลที่ทำหน้าที่ในส่วนต่างๆ ของระบบอย่างชัดเจน รวมถึงการกำหนดสิทธิในการเข้าถึงระบบอย่างรัดกุมด้วย เช่น เทอร์มินอลที่ไม่ได้เปิดให้ใช้งานมีการเปิดขึ้นหรือไม่ จุดเข้าถึงการเชื่อมต่อเข้าเครือข่าย อุปกรณ์ สวิตช์ อุปกรณ์เราเตอร์ ห้องเซิร์ฟเวอร์ ระบบควบคุมการเข้าใช้ห้องเครือข่ายสายสำหรับการเชื่อมต่อมีสภาพชำรุด หรือสภาพอันบางชี้ถึงสาเหตุที่ไม่ปกติหรือไม่ ระบบการถ่ายเทอากาศ ระบบไฟฟ้าสำรองทำงานเป็นปกติหรือไม่ เป็นต้น

5.7 ใช้โปรแกรมทริปไวร์ (Tripwire) หรือโปรแกรมใกล้เคียงตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์คอนฟิกหรือไฟล์ที่สำคัญต่อการทำงานในระบบ

5.8 ติดตั้งเครื่องเซิร์ฟเวอร์ฮ็อตสแปร์ (hot spares) ที่สามารถนำมาใช้แทนเครื่องเซิร์ฟเวอร์ได้ทันทีเมื่อเหตุฉุกเฉินขึ้น เพื่อลดช่วงเวลาดาวน์ไทม์ของระบบ หรือลดช่วงเวลาที่เกิด Denial of Service ของระบบลง ซึ่งการที่ไม่สามารถเข้าใช้งานระบบได้ ถือว่าเข้าสู่ภาวะของ Denial of Service เช่นเดียวกัน แม้ว่าจะเกิดจากสาเหตุของผู้บุกรุกหรือสาเหตุอื่นก็ตาม

5.9 ติดตั้งระบบสำรองเครือข่าย หรือระบบป้องกันความสูญเสียการทำงานของระบบเครือข่าย หรือระบบสำรองเพื่อให้ระบบเครือข่ายสามารถใช้ได้ตลอดเวลา

5.10 การสำรองข้อมูลบนระบบอย่างสม่ำเสมอ โดยเฉพาะคอนฟิกที่สำคัญต่อการทำงานของระบบ พิจารณาออกนโยบายสำหรับการสำรองข้อมูลที่สามารถบังคับใช้ได้จริง

5.11 วางแผนและปรับปรุงนโยบายการใช้งานรหัสผ่านที่เหมาะสม โดยเฉพาะผู้ที่มีสิทธิ์สูงสุดในการเข้าถึงระบบทั้ง root บนระบบ UNIX หรือ Administrator บนระบบ Microsoft Windows NT

6. แนวทางป้องกันสแปมเมลหรือจดหมายบุกรุก

การป้องกันอีเมลสแปมจริงๆ นั้นอาจทำไม่ได้ 100 % แต่ก็สามารถจะลดปัญหาจากอีเมลสแปมได้ดังนี้

6.1 แจ้งผู้ให้บริการอินเทอร์เน็ตบล็อกอีเมลที่มาจากชื่ออีเมลหรือโดเมนนั้นๆ

6.2 ตั้งค่าโปรแกรมอีเมลที่ใช้บริการอยู่โดยสามารถกำหนดได้ว่าให้ลบหรือย้ายอีเมลที่คาดว่าจะเป็น สแปมไปไว้ในโฟลเดอร์ขยะ (Junk) หรือกำหนดค่าที่จะใช้เป็น keyword ว่าหากมีคำนี้ในอีเมลให้ย้ายไปโฟลเดอร์ขยะ หรือกำหนดให้บล็อกอีเมลจากชื่ออีเมลที่ระบุไว้ได้

6.3 ไม่สมัคร (Subscribe) จดหมายข่าว (Newsletter) บนเว็บไซต์ หรือโพสต์อีเมลลงในเว็บบอร์ดต่างๆ มากเกินไป เพราะจะเป็นการเปิดเผยอีเมลของเราสู่โลกภายนอก ซึ่งอาจได้อีเมลของเราได้ด้วยวิธีการหนึ่ง เช่น การใช้ซอฟต์แวร์ดูดอีเมลจากเว็บไซต์ หรือเว็บไซต์ผู้ให้บริการดังกล่าวอาจนำข้อมูลอีเมลไปขายเพื่อหากำไร

6.4 การป้องกันอีเมลบอมบ์ ลักษณะของอีเมลบอมบ์จะเป็นการส่งอีเมลหลายๆ ฉบับไปหาคนเพียงคนเดียวหรือไม่กี่คนเพื่อหวังผลให้ไปรบกวนระบบอีเมลให้ล่มหรือทำงานผิดปกติ ในการป้องกันอีเมลบอมบ์สามารถทำได้ดังนี้

6.4.1 กำหนดขนาดของอีเมลบอกซ์แต่ละแอคเคาท์ว่าสามารถเก็บอีเมลได้สูงสุดเท่าใด

6.4.2 กำหนดจำนวนอีเมลที่มากที่สุดที่สามารถส่งได้ในแต่ละครั้ง

6.4.3 กำหนดขนาดของอีเมลที่ใหญ่ที่สุดที่สามารถรับได้

6.4.4 ไม่อนุญาตให้ส่งอีเมลจากแอคเคาน์ที่ไม่มีตัวตนจริงในระบบ

6.4.5 ตรวจสอบว่ามีอีเมลแอคเคาท์นี้จริงในระบบก่อนส่ง ถ้าเช็คไม่ผ่าน แสดงว่าอาจมีการปลอมชื่อมา

6.4.6 กำหนด keyword ให้ไม่รับอีเมลเข้ามาจาก subject ที่มีคำที่กำหนดไว้

6.4.7 หมั่นอัพเดทรายชื่อโดเมนที่ติด black list จากการส่งอีเมลสแปมหรือ อีเมลบอมบ์

7. การป้องกันภัยจากการเจาะระบบ

แนวทางป้องกันโดยใช้ไฟร์วอลล์ ซึ่งไฟร์วอลล์อาจจะอยู่ในรูปของฮาร์ดแวร์หรือซอฟต์แวร์ก็ได้ โดยเปรียบเสมือนยามเฝ้าประตูที่จะเข้าสู่ระบบ ตรวจค้นทุกคนที่เข้าสู่ระบบ มีการตรวจบัตรอนุญาต จดบันทึกข้อมูลการเข้าออก ติดตามพฤติกรรมการใช้งานในระบบ รวมทั้งสามารถกำหนดสิทธิ์ที่จะอนุญาตให้ใช้ระบบในระดับต่างๆ ได้

แนวโน้มด้านความปลอดภัยในอนาคต

เทคโนโลยีด้านการรักษาความปลอดภัยบนระบบเทคโนโลยีสารสนเทศได้พัฒนาไปอย่างรวดเร็วเพื่อรองรับรูปแบบการก่ออาชญากรรมทางคอมพิวเตอร์ ซึ่งเปรียบเสมือนการแข่งขันกับกลุ่มแฮกเกอร์ที่ได้พัฒนาเทคนิคการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ๆ จึงมีความพยายามในการรักษาความปลอดภัยที่ได้คาดการณ์แนวโน้มด้านความปลอดภัยที่อาจเกิดขึ้นในอนาคต เพื่อที่จะสามารถป้องกันหรือหาทางแก้ไขไม่ให้สิ่งที่เป็นอันตรายเหล่านี้เกิดขึ้นได้ มีรายละเอียด ดังนี้ (สุขุม เฉลยทรัพย์ และคณะ, 2555)

1. หลายหน่วยงานมีการใช้มาตรการ และข้อบังคับต่าง ๆ เพื่อให้พนักงานมีความระมัด ระวังในการใช้งานคอมพิวเตอร์ คอมพิวเตอร์แลปท็อปมากขึ้น เพื่อเป็นการช่วยปกป้องข้อมูลในกรณีที่แลปท็อปถูกคนร้ายขโมยไป ฉะนั้นมาตรการเพื่อการรักษาความปลอดภัยของข้อมูลในอนาคตจะต้องกำหนดให้เจ้าหน้าที่ผู้ถือครองแลปท็อปต้องทำการเข้ารหัสข้อมูลที่อยู่บนเครื่อง รวมทั้งการใช้งานการตรวจสอบตัวตนแบบ two-factor ในการล็อกอินเข้าเครื่องแลปท็อป ตลอดจนมีมาตรการให้บริษัทผู้ผลิตแลปท็อปพัฒนาผลิตภัณฑ์ที่สนับสนุนการเข้ารหัสข้อมูล โดยไม่จำเป็นต้องใช้ซอฟต์แวร์ภายนอกมาเสริม

2. ปัญหาความปลอดภัยของข้อมูลใน PDA สมาร์ทโฟน และ iPhone ปัจจุบันการพัฒนา PDA สมาร์ทโฟน และ iPhone เป็นไปยังรวดเร็วและมีความสามารถแทบจะทัดเทียมเครื่องคอมพิวเตอร์ทั้งในด้านการเก็บข้อมูล การเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต ดังนั้นผู้ใช้จึงนิยมเก็บข้อมูลส่วนตัวที่สำคัญไว้ใน PDA สมาร์ทโฟน

และ iPhone ดังนั้นหากอุปกรณ์ดังกล่าวสูญหายข้อมูลที่อยู่ในอุปกรณ์ก็อาจถูกนำไปใช้ประโยชน์ไปในทางที่ผิดได้โดยง่าย จึงจำเป็นอย่างยิ่งที่ต้องมีการเข้ารหัสข้อมูลที่อยู่ใน PDA สมารทโฟน และ iPhone เช่นเดียวกับแลปท็อป

3. การออกกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคล ประเทศไทยได้ออกกฎหมายที่เกี่ยวข้องกับการกระทำผิดหรือการก่ออาชญากรรมทางคอมพิวเตอร์และทางด้านเทคโนโลยีสารสนเทศหลายฉบับ ทำให้คาดการณ์กันว่าภายในอนาคตแนวโน้มการออกกฎหมายจะเน้นไปทางด้านการปกป้องข้อมูลส่วนบุคคลเป็นหลัก ไม่ว่าจะเป็นการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การบังคับให้บริษัทหรือหน่วยงานที่ทำงานเกี่ยวกับข้อมูลส่วนบุคคลต้องมีมาตรฐานการป้องกันข้อมูลที่ดีเพียงพอ โดยคาดว่าจะมีบทลงโทษที่รุนแรงมากขึ้นสำหรับการขโมยข้อมูลส่วนบุคคล นอกจากนี้กฎหมายอาจมีการกล่าวถึงบริษัทหรือหน่วยงานที่ทำงานเกี่ยวกับข้อมูลส่วนบุคคล ไม่ว่าจะเป็น ธนาคาร โรงพยาบาล หรือบริษัทประกันภัย จะต้องมีมาตรการป้องกันการเข้าถึงข้อมูลส่วนบุคคลที่ดีพอและได้มาตรฐาน กฎหมายดังกล่าวจะเปรียบเหมือนข้อมูลบังคับให้หน่วยงานและบริษัททั้งหลายให้ความสนใจในการป้องกันข้อมูลส่วนบุคคลให้มากขึ้น

4. หน่วยงานภาครัฐที่สำคัญเป็นเป้าหมายการโจมตีของแฮกเกอร์ เนื่องจากความปลอดภัยของระบบคอมพิวเตอร์ในหน่วยงานของรัฐมีน้อยกว่าเมื่อเทียบกับหน่วยงานเอกชนทำให้โอกาสที่จะบุกรุกสำเร็จมีมากกว่า นอกจากนี้ระบบโครงสร้างพื้นฐาน และระบบสาธารณูปโภคต่าง ๆ ก็กลายเป็นเป้าหมายหลักในการโจมตีด้วยเช่นกัน

5. หนอนอินเทอร์เน็ต (Worms) บนโทรศัพท์มือถือ ปัจจุบันโทรศัพท์มือถือจำนวนมากได้ถูกติดตั้งระบบปฏิบัติการเสมือนเป็นเครื่องคอมพิวเตอร์ เช่น ระบบปฏิบัติการ Mac OS X ระบบปฏิบัติการ Microsoft Windows Mobile หรือระบบปฏิบัติการบนโทรศัพท์มือถืออื่นๆ เป็นต้น ซึ่งลักษณะการทำงานก็จะคล้ายกับระบบเครือข่ายทั่วๆ ไปที่หนอนอินเทอร์เน็ตสามารถแพร่กระจายสู่เครื่องคอมพิเตอร์ผ่านทางเว็บบราวเซอร์ โดยที่หนอนอินเทอร์เน็ตบนโทรศัพท์มือถือก็ได้พัฒนาโปรแกรมบุกรุก (Exploit) ใช้สำหรับโจมตีช่องโหว่ของทิฟฟ์ ไลบาร์รี่ (TIFF Library) ซึ่งเป็นชุดคำสั่งที่ใช้สำหรับพัฒนาโปรแกรมรูปภาพแบบหนึ่ง ซึ่งช่องโหว่ดังกล่าวสามารถใช้โจมตีโทรศัพท์มือถือได้หลายรุ่น ผ่านทางโปรแกรมเว็บบราวเซอร์ หากผู้ใช้ทำการเรียกดูเว็บที่มีการฝังไฟล์รูปภาพแบบ TIFF ของแฮกเกอร์ไว้ แฮกเกอร์จะสามารถเข้าควบคุมโทรศัพท์มือถือของผู้ใช้ได้โดยง่าย

6. เป้าหมายการโจมตี VoIP (Voice over IP) มีมากขึ้น เนื่องจาก VoIP เป็นเทคโนโลยีทางเลือกที่องค์กรนำมาใช้งานโทรศัพท์ระหว่างประเทศที่มีค่าใช้จ่ายน้อย ลักษณะของ VoIP จะใช้เทคโนโลยีการส่งข้อมูลเสียงบน IP โปรโตคอล รูปแบบการโจมตีจะมีสองลักษณะคือ การทำให้ระบบ VoIP ไม่สามารถทำงานได้ เช่น การส่งข้อมูลจำนวนมากไปยังระบบเครือข่าย ทำให้ VoIP ในระบบเครือข่ายที่ถูกโจมตีไม่สามารถส่งข้อมูลได้ หรือแฮกเกอร์อาจส่งข้อมูลไปรบกวนข้อมูลเสียงบนระบบ VoIP ทำให้ผู้ใช้งานไม่สามารถฟังเสียงที่ถูกส่งมาได้ เป็นต้น และอีกรูปแบบหนึ่งคือ การขโมยข้อมูลเสียงที่ถูกส่งโดย VoIP หรือการเปลี่ยนแปลงข้อมูลเสียงที่ถูกส่งโดย VoIP ก่อนที่จะไปถึงผู้ใช้ เป็นต้น

7. ภัยจากช่องโหว่แบบซีโร-เดย์ (Zero-Day) ลักษณะของช่องโหวแบบ Zero-Day คือ ช่องโหว่ของระบบปฏิบัติการหรือซอฟต์แวร์ต่างๆ ที่ถูกแฮกเกอร์นำไปใช้ในการโจมตีระบบ แต่ยังไม่มีโปรแกรมซ่อมแซมช่อง

โหว่จากทางเจ้าของผลิตภัณฑ์ บางครั้งบริษัทบางแห่งผู้เป็นเจ้าของผลิตภัณฑ์ก็ทำธุรกิจเกี่ยวกับการรับซื้อช่องโหว่แบบ Zero-Day จากผู้ที่ค้นพบช่องโหว่ เมื่อมีผู้ที่ค้นพบช่องโหว่แล้วก็จะติดต่อไปยังเจ้าของผลิตภัณฑ์ที่มีช่องโหว่ช่วยกันแก้ไขปัญหาต่อไป ซึ่งรูปแบบธุรกิจดังกล่าวถือเป็นอีกทางเลือกหนึ่งสำหรับผู้ที่ต้องการขายข้อมูลของช่องโหว่ต่างๆ แทนที่การขายช่องโหว่กับกลุ่มอาชญากรรมเหมือนที่แล้วมา แต่อย่างไรก็ตามรูปแบบธุรกิจดังกล่าวช่วยลดความรุนแรงที่เกิดจากช่องโหว่แบบ Zero-Day ได้เพียงส่วนหนึ่งเท่านั้น ยังมีโอกาสที่ แฮกเกอร์เลือกที่จะไม่ขายข้อมูลเกี่ยวกับช่องโหว่ Zero-Day แล้วใช้ประโยชน์จากช่องโหว่ดังกล่าวด้วยวิธีการของแฮกเกอร์เอง ดังนั้นผู้ดูแลระบบยังคงต้องมีความพร้อมในการรับมือการโจมตีด้วยช่องโหว่แบบ Zero-Day ต่อไป

8. Network Access Control (NAC) มีบทบาทสำคัญมากขึ้นในองค์กร NAC เป็นเทคโนโลยีที่เข้ามาใช้มากขึ้นในองค์กรเพื่อจัดการปัญหาที่บุคลากรในองค์กรนำเครื่องคอมพิวเตอร์ที่ไม่ได้รับอนุญาต เช่น แลปท็อปคอมพิวเตอร์ส่วนบุคคล เข้ามาเชื่อมต่อกับระบบเครือข่ายภายในขององค์กร การกระทำดังกล่าวอาจทำให้ระบบเครือข่ายภายในองค์กรถูกบุกรุกผ่านทางเครื่องคอมพิวเตอร์ส่วนบุคคลของบุคลากรได้ หากเครื่องดังกล่าวไม่มีระบบความปลอดภัยที่เพียงพอ ซึ่ง NAC ก็คือ คอมพิวเตอร์หรืออุปกรณ์ทุกอย่างต้องถูกควบคุมให้ตรงตามนโยบายขององค์กรก่อนที่จะนำไปเชื่อมต่อเข้ากับระบบเครือข่ายขององค์กร หากไม่ตรงตามนโยบายแล้ว เครื่องคอมพิวเตอร์หรืออุปกรณ์นั้นจะไม่สามารถใช้งานระบบเครือข่ายได้ เทคโนโลยีต่างๆ ได้ถูกรวบรวมไว้ใน NAC เพื่อใช้ในการควบคุมอุปกรณ์ให้ตรงตามนโยบายเช่น ระบบ Anti-Virus ระบบป้องกันการบุกรุก (IPS) และไฟร์วอลล์ เป็นต้น นอกจากนี้ NAC ยังมีประโยชน์ในการสืบหาเครื่องคอมพิวเตอร์ที่ติดมัลแวร์หรือถูกบุกรุกได้ด้วย ตัวอย่างผลิตภัณฑ์ NAC เช่น Network Admission Control, Network Access Protection และ Infranet เป็นต้น ซึ่งการจะเลือกผลิตภัณฑ์ตัวใดนั้น ต้องพิจารณาการใช้งานที่สามารถนำมาติดตั้งและประยุกต์ใช้งานภายในองค์กรได้อย่างมีประสิทธิภาพ

การรักษาความปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ เป็นความจำเป็นที่ผู้ใช้เทคโนโลยีสารสนเทศต้องทราบ และรูปแนวทางที่จะป้องกันภัยจากการก่ออาชญากรรมคอมพิวเตอร์ที่มีรูปแบบการบุกรุก โจมตีหลากหลายวิธี นับตั้งแต่การเข้าถึงระบบและข้อมูลทางคอมพิวเตอร์ การรบกวนระบบคอมพิวเตอร์ การเข้าเจาะระบบของแฮกเกอร์ เป็นต้น และในอนาคตก็สามารถคาดการณ์รูปแบบการโจมตี และเตรียมรับมือกับรูปแบบการกระทำผิด อาทิ การออกกฎหมายควบคุมเพื่อปกป้องข้อมูลส่วนบุคคลให้เป็นรูปธรรมอย่างชัดเจน การออกข้อบังคับเพื่อการเข้าถึงระบบได้ยากขึ้นเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าสู่ระบบ รวมถึงหน่วยงานของรัฐที่ต้องเฝ้าระวังการเข้าโจมตีหรือบุกรุกจากแฮกเกอร์ ซึ่งจะมีการนำระบบ NAC (Network Access Control) เข้ามาใช้ในองค์กรมากขึ้น

อย่างไรก็ตามบางประเทศมีมาตรการกฎหมายและแนวทางการปฏิบัติในเรื่องความปลอดภัยของข้อมูล (Information security) และ การรั่วไหลของข้อมูล (Data leaking) เช่น ประเทศเนเธอร์แลนด์ มีกฎหมายบัญญัติและบ่งชี้ว่าเป็นอาชญากรรมทางไซเบอร์จะต้องมีการรายงานต่อเจ้าหน้าที่ตำรวจในทันที เพื่อเพิ่มความกดดันและความตระหนักต่อความปลอดภัยด้านไซเบอร์ในกลุ่มผู้ประกอบการมากยิ่งขึ้น โดยผู้ประกอบการนั้นจะต้องรายงานข้อมูลของบริษัท ลักษณะธุรกิจที่ดำเนินการและบริษัทคู่ค้าที่ทำการติดต่อด้วยทั้งหมดเพื่อเป็นประโยชน์

ต่อการจับกุม นอกจากนี้ทางสหภาพยุโรปยังมีกฎหมายที่เกี่ยวกับข้อมูลส่วนบุคคล (Privacy law) ซึ่งจะต้องนำมาพิจารณาหากต้องการทำธุรกิจที่นี่ ทั้งนี้ผู้บริโภคและบริษัทผู้ประกอบการในประเทศเนเธอร์แลนด์มีแนวทางปฏิบัติเพื่อความปลอดภัยทางไซเบอร์ (สำนักงานส่งเสริมการค้าในต่างประเทศ ณ กรุงเฮก ประเทศเนเธอร์แลนด์, 2017) ดังนี้

1. กลุ่มบุคคลทั่วไป มีการเตือนผู้บริโภคเกี่ยวกับภัยคุกคามทางไซเบอร์ผ่านสื่อโทรทัศน์เป็นครั้งคราว ซึ่งจัดทำโดยองค์กรภาครัฐและเอกชน เพื่อให้ประชาชนได้รับรู้และระมัดระวังถึงกลลวงต่าง ๆ ที่แฝงตัวจากการใช้งานอินเทอร์เนต เช่น การไม่เข้าลิงค์ในอีเมล์ที่ผิดปกติ การไม่เข้าเว็บไซต์ที่ไม่คุ้นเคยหรือไม่มีความน่าเชื่อถือ รวมถึงการไม่ให้ข้อมูลส่วนตัวของตนกับเว็บไซต์หรือบุคคลอื่น เป็นต้น

2. กลุ่มบริษัทและผู้ประกอบการ แนะนำให้เลือกใช้ระบบหรือเทคโนโลยีที่มีความก้าวหน้าและมีประสิทธิภาพสูง การเลือกใช้เทคโนโลยี Block chain เป็นตัวช่วยด้านการจัดเก็บฐานข้อมูลอย่างมีประสิทธิภาพและเชื่อถือได้ สามารถปรับใช้ได้กับทุกภาคอุตสาหกรรม โดยขณะนี้เทคโนโลยี Block chain กำลังถูกพัฒนาอย่างต่อเนื่องเพื่อลดความเสี่ยงและค่าใช้จ่ายในการบริหาร รวมทั้งเพิ่มประสิทธิภาพในการทำธุรกรรมที่ปลอดภัยและโปร่งใสมากขึ้น นอกจากนี้ภาคอุตสาหกรรมโลจิสติกส์ยังมีระบบบันทึกพิเศษเพื่อช่วยเพิ่มรักษาความปลอดภัยและลดปัญหาอาชญากรรมที่เรียกว่า 'Warning Register Logistics Sector หรือ WLS' ที่มุ่งเน้นด้านการตรวจสอบพนักงานและบันทึกข้อมูลทางอาญา โดยจะจัดเก็บรายชื่อผู้ต้องคดีความ (Black list) เป็นเวลาอย่างน้อย 4 ปี หรือจนกว่าจะพ้นคดีความ ทั้งนี้ระบบ WLS สามารถช่วยผู้ประกอบการคัดกรองพนักงานได้อย่างรวดเร็วและสามารถลดความเสี่ยงจากปัญหาอาชญากรรม (ไซเบอร์) ได้ระดับหนึ่ง การจัดสัมมนาหรืออบรมเกี่ยวกับเรื่องความปลอดภัยทางไซเบอร์ สำหรับพนักงานในองค์กรเพื่อให้รู้ถึงประเภทภัยคุกคามที่อาจจะเกิดขึ้นและวิธีปฏิบัติเมื่อประสบเหตุการณ์ และการทำประกันภัยความเสียหายด้านไซเบอร์สามารถช่วยชดเชยความเสียหายที่เกิดขึ้นจากอาชญากรรมไซเบอร์ได้บางส่วน

3. ภาครัฐ เหตุการณ์อาชญากรรมไซเบอร์ที่เกิดขึ้นบ่อยครั้งและสร้างความเสียหายอย่างมหาศาล ทำให้รัฐบาลเนเธอร์แลนด์ตระหนักและเห็นความสำคัญเรื่องความมั่นคงและปลอดภัยทางไซเบอร์(แห่งชาติ) มากขึ้น โดยในปีนี้ทางรัฐบาลได้ตั้งงบประมาณจัดสรรไว้ 26 ล้านยูโร และผลักดันกฎหมายใหม่ “Sleepwet” ที่มีจุดประสงค์เพื่อสร้างความมั่นคงและปลอดภัยของประเทศ โดยสามารถเข้าถึงเครือข่ายและข้อมูลทุกอย่างและมีหน่วยข่าวกรอง MIVD และ AIVD ของภาครัฐเป็นผู้ควบคุมดูแล ทั้งนี้เนื้อหาของกฎหมายใหม่ที่เปลี่ยนแปลงไปจากเดิมอย่างเห็นได้ชัด มี 4 ข้อหลักดังต่อไปนี้ 1) Sleepwet สามารถดักฟังการสนทนาออนไลน์ของบุคคลทั้งหมด ทั้งผู้ต้องสงสัยและบุคคลทั่วไป 2) อุปกรณ์และเครื่องมือสื่อสารทุกชนิดสามารถถูกแฮ็กได้ทั้งหมด 3) ประชาชนทุกคนสามารถเข้าดูฐานข้อมูลลับ DNA ได้ และ 4) การแบ่งปันข้อมูลให้กับหน่วยข่าวกรองต่างประเทศโดยไม่ต้องมีการวิเคราะห์ข้อมูลก่อน

ประเภทของอาชญากรรมทางเทคโนโลยี

การแบ่งประเภทของอาชญากรรมคอมพิวเตอร์ตามกระบวนการ ได้แก่

(1) การก่ออาชญากรรมคอมพิวเตอร์ในขั้นของกระบวนการนำเข้า (input process) นั้น คือ

(1.1) การสับเปลี่ยน Disk ในที่นี้หมายความรวม Disk ทุกชนิด ไม่ว่าจะเป็น Hard Disk, Floppy Disk รวมทั้ง Disk ชนิดอื่น ๆ ด้วย ในที่นี้น่าจะหมายถึง การกระทำในทางกายภาพ โดยการ Removable นั่นเอง ซึ่งเป็นความผิดชัดเจนในตัวของมันเองอยู่แล้ว

(1.2) การทำลายข้อมูลไม่ว่าจะใน Hard Disk หรือสื่อบันทึกข้อมูลชนิดอื่นที่ใช้ร่วมกับคอมพิวเตอร์โดยไม่ชอบกรณีการทำลายข้อมูลนั้น ไม่ว่าอย่างไรก็ถือเป็นความผิดทั้งสิ้น

(1.3) การป้อนข้อมูลเท็จในกรณีที่เป็นผู้มีอำนาจหน้าที่อันอาจเข้าถึงเครื่องคอมพิวเตอร์นั้น ๆ ได้หรือแม้แต่ผู้ที่ไม่มีอำนาจเข้าถึงก็ตามแต่ได้กระทำการอันมิชอบในขณะที่ตนเองอาจเข้าถึงได้

(1.4) การลักข้อมูลข่าวสาร (data / computer espionage) ไม่ว่าโดยการกระทำด้วยวิธีการอย่างใด ๆ ให้ได้ไป ซึ่งข้อมูลอันตนเองไม่มีอำนาจ หรือเข้าถึงโดยไม่ชอบกรณีการลักข้อมูลข่าวสารนั้นจะพบได้มากในปัจจุบันที่ข้อมูลข่าวสารถือเป็นทรัพย์อันมีค่ายิ่ง

(1.5) การลักใช้บริการหรือเข้าไปใช้โดยไม่มีอำนาจ (Unauthorized access) อาจกระทำโดยการเจาะระบบเข้าไป หรือใช้วิธีการอย่างใด ๆ เพื่อให้ได้มา ซึ่งรหัสผ่าน (Password) เพื่อให้ตนเองเข้าไปใช้บริการได้โดยไม่ต้องลงทะเบียนเสียค่าใช้จ่ายปัจจุบันพบได้มากตามเว็บบอร์ดทั่วไป ซึ่งมักจะมี Hacker ซึ่งได้ Hack เข้าไปใน server ของ ISP แล้วเอา account มาแจกฟรี ผู้ที่รับเอา account นั้นไปใช้จะมีความผิดตามกฎหมายอาญาฐานรับของโจรด้วย

(2) การก่ออาชญากรรมคอมพิวเตอร์ในส่วนกระบวนการ data processing นั้นอาจกระทำความผิดได้

(2.1) การทำลายข้อมูลและระบบโดยใช้ไวรัส (Computer sabotage) ซึ่งได้อธิบายการทำงานของ Virus ดังกล่าวไว้แล้วข้างต้น

(2.2) การทำลายข้อมูลและโปรแกรม (Damage to data and program) การทำลายข้อมูล โดยไม่ชอบย่อมจะต้องเป็นความผิด

(2.3) การเปลี่ยนแปลงข้อมูลและโปรแกรม (Alteration of data and program) เช่นกันการกระทำใดที่ก่อให้เกิดความเสียหาย โดยไม่มีอำนาจก็จะถือเป็นความผิด

(3) ส่วนกระบวนการนำออก (Output process) นั้น อาจกระทำความผิดได้โดย

(3.1) การขโมยขยะ (Swaging) หมายถึง ขยะหรือข้อมูลที่ไม่ใช้แล้วแต่ยังไม่ได้ทำลายนั่นเอง การขโมยขยะถือเป็นความผิดถ้าขยะที่ถูกขโมยไปนั้นอาจทำให้เจ้าของต้องเสียหายอย่างใด อีกทั้งเจ้าของอาจจะยังมิได้มีเจตนาสละการครอบครองก็ได้ต้องดูเป็นกรณีไป

(3.2) การขโมย print out คือ การขโมยงานหรือข้อมูลที่ print ออกมาแล้วนั่นเอง กรณีนี้อาจผิดฐานลักทรัพย์ด้วยเพราะเป็นการขโมยเอกสารอันมีค่า ถือได้ว่าผิดเหมือนกัน แต่ไม่ว่าอ ย่างไรก็ตาม แนวโน้มการก่ออาชญากรรมคอมพิวเตอร์ก็มีอัตราเพิ่มสูงขึ้นทุกปี

การกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์

การพัฒนากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ในเบื้องต้นนั้นพัฒนาขึ้นโดยคำนึงถึงลักษณะการกระทำความผิดต่อระบบคอมพิวเตอร์ ระบบข้อมูลและระบบเครือข่าย ซึ่งอาจสรุปความผิดสำคัญได้ 3 ฐานความผิด คือ

1) การเข้าถึงโดยไม่มีอำนาจ (unauthorized access)

2) การใช้คอมพิวเตอร์โดยไม่ชอบ (computer misuse)

3) ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (computer related crime)

ภัยคุกคามความปลอดภัยข้อมูลบนคอมพิวเตอร์

ปริญญา หอมเอนก (2547) ได้ชี้ทิศทางแนวโน้มภัยคุกคามความปลอดภัยข้อมูลบนคอมพิวเตอร์ไว้ 10 ข้อ ดังนี้

(1) ภัยสแปมเมล์ (SPAM Mail) มัลแวร์ หรือโปรแกรมมุ่งร้ายในรูปแบบต่าง ๆ ไม่ว่าจะมาทางกับไฟล์แนบหรือมาในรูปแบบของเนื้อหาล่อลวงในจากปี พ.ศ. 2540 ปริมาณสแปมเมล์เพิ่มขึ้นถึง 10 เท่า และมีแนวโน้มที่จะเพิ่มขึ้นเป็นทวีคูณในปีต่อ ๆ ไป เนื่องจากทุกวันนี้ สแปมเมอร์สามารถทำเงินได้จากการส่งสแปมเมล์กลายเป็นอาชีพด้านมืดที่ทำรายได้งามทางอินเทอร์เน็ต จนทางประเทศสหรัฐอเมริกาต้องออกกฎหมาย “CAN SPAM ACT” ขึ้นมาเพื่อต่อต้าน

(2) ภัยสปายแวร์ (Spy Ware) มีงานวิจัยเรื่องสปายแวร์ ระบุว่า 80% ของพีซีทั่วโลกติดสปายแวร์ และเครื่องพีซีเหล่านั้นล้วนมีโปรแกรมแอนตี้ไวรัส

ทั้งนี้เพราะโปรแกรมสปายแวร์ไม่ใช่โปรแกรมไวรัส ยกตัวอย่างเช่น โปรแกรมดักคีย์บอร์ด และเก็บหน้าจอการใช้งานคอมพิวเตอร์ของที่ในวงการเรียกว่า โปรแกรม KEY LOGGER เป็นโปรแกรมสปายแวร์ ที่ระบบแอนตี้ไวรัสส่วใหญ่มองไม่เห็น และไม่สามารถกำจัดสปายแวร์เหล่านี้ออกจากเครื่องคอมพิวเตอร์ได้

การติดสปายแวร์ จะมาจากการเข้าเว็บต่าง ๆ โดยไม่ระมัดระวังให้ดีพอ รวมทั้งการดาวน์โหลดไฟล์ที่มีสปายแวร์ติดมาด้วยตลอดจนการเปิดอีเมล์แนบไฟล์ (Attached file)

ล่าสุดมีโปรแกรมสปายแวร์ที่มาในรูปของ Cookies เวลาเข้าเว็บไซต์ที่ไม่เหมาะสม เช่น เว็บภาพลามก หรือเว็บที่ใช้ในการหาซีเรียล นัมเบอร์ของซอฟต์แวร์ผิดกฎหมาย เป็นต้น รวมถึงมากับโปรแกรม P2P

(3) ภัย Mal ware (Malicious Software) โปรแกรมมุ่งร้ายที่มาในรูปแบบต่าง ๆ ไม่ว่าจะเป็น ActiveX หรือ Java Applet ที่มากับการใช้งานบราวเซอร์ โดยไม่ได้รับการติดตั้งโปรแกรมอุดช่องโหว่

ระบบ หรือ Patch และอาจมาในรูปของไฟล์แนบที่อยู่ในอีเมล์ตลอดจนแฝงมากับโปรแกรม Shareware หรือโปรแกรม Utility หรือโปรแกรม P2P ที่นิยมใช้ในการดาวน์โหลดเพลงหรือภาพยนตร์ ผ่านทางอินเทอร์เน็ต

โปรแกรมมัลแวร์ อาจจะเป็นสปายแวร์ โทรจัน ไวรัส หรือหนอนคอมพิวเตอร์ที่รู้จักกันดีในช่วงหลัง ๆ ไวรัสคอมพิวเตอร์นี้ มักจะมากับ Email โดยมักจะมาในรูป Zip File และมีการปลอมแปลงชื่อผู้ส่ง ปลอมแปลงหัวเรื่องอีเมล์ เป็นส่วนเทคนิคการหลอกผู้ใช้ Email ให้หลงเชื่อที่เรียกว่า “Social Engineering” เป็นวิธีการเก่าแก่ที่ผู้ไม่หวังดีนิยมใช้

(4) ภัยจากการล่อลวงโดยวิธี Phishing และ Pharming การส่ง Email โดยมีการปลอมชื่อคนส่ง และชื่อเรื่อง (Email address & Email subject) ตลอดจนปลอมแปลงเนื้อหาในเมล์ให้ดูเหมือนจริงล่อให้ผู้ใช้คลิ๊ก เพื่อเข้าไปติดกับดักที่ฟิชเชอร์วางไว้ เพื่อดักจับยูสเซอร์เนม และรหัสผ่านเพื่อนำไปใช้ทำธุรกรรมอนนไลน์การชำระเงินผ่านเน็ต การซื้อสินค้าออนไลน์

(5) ภัยจากแฮคเกอร์ และใช้กูเกิลเป็นเครื่อง ปัจจุบันการเจาะระบบหรือแฮคไปยังเว็บแอพพลิเคชั่น ได้มีการเปลี่ยนแปลงรูปแบบไป โดยมีการอาศัย Google.com เป็นช่องทางค้นหาเว็บที่มีช่องโหว ซึ่งสามารถแฮคได้โดยง่าย จากนั้นจึงแฮคตามวีการปกติ และเนื่องจาก Google hacking นั้นจะเป็นการ hacking แบบไม่เลือกเหยื่อ ดังนั้นทุกเว็บที่มีช่องโหว่ที่ Google เห็นจึงมีโอกาสถูกแฮคได้เท่า ๆ กัน

(6) ภัยจากโปรแกรม Peer-to-Peer (P2P) เป็นภัยซึ่งเกิดจากผู้ใช้เป็นหลักเนื่องจากโปรแกรมประเภทนี้นั้นจะให้ประโยชน์กับเรื่องส่วนตัวของผู้ใช้ เช่น การใช้โปรแกรม KAZAA เพื่อดาวน์โหลดหนัง และเพลงแบบผิดกฎหมาย หรือใช้โปรแกรม SKYPE ในการพูดคุยสื่อสารแทนการใช้โทรศัพท์

การใช้โปรแกรมดังกล่าวนั้นจะนำภัยสองประเภทมาสู่องค์กร ทั้งการสิ้นเปลือง Bandwidth เครือข่ายขององค์กร และสร้างปัญหาด้านการรักษาความลับข้อมูล เคยพบว่ามีช่องโหว่บน KAZAA ซึ่งทำให้ Hacker สามารถเจาะมายังฮาร์ดดิสก์ของคนทั้งโลกที่ติดตั้งโปรแกรม KAZAA

(7) ภัยจากเครือข่ายไร้สาย การติดตั้งเครือข่ายไร้สายนั้นเป็นเรื่องที่ค่อนข้างอันตราย เนื่องมาจากโครงสร้างของเครือข่ายไร้สาย นั้นออกแบบมาอย่างไม่ปลอดภัยอีกทั้งเทคโนโลยีด้านนี้นั้นยังไร้พรมแดนสามารถขยายไปยังภายนอกองค์กรได้อีกด้วย อีกทั้งในปัจจุบันผู้ที่นำเทคโนโลยีด้านนี้มาใช้นั้นยังมีความรู้ในการใช้เทคโนโลยีนี้อย่างปลอดภัยน้อยมาก

(8) ภัย SPIM (SPAM Instant Messaging) โดยเป็นสแปมที่ใช้ช่องทางโปรแกรมข้อความทันใจ หรือ IM (Instant Messaging) ในการกระจาย Malicious Code โดยผู้ที่เป็นสปิมเมอร์จะใช้ BOT เพื่อค้นหาชื่อของคนที่ใช้โปรแกรมไอเอ็ม (IM: Instant Message) อยู่ จากนั้นจึงใช้ BOT แสดงคำพูดเพื่อให้เหยื่อเข้าใจว่าเป็นมนุษย์ จากนั้นจึงส่งโฆษณาข้อมูลหลอกลวงลิงค์เว็ปไซต์ หรือแม้แต่ Spyware และ Malware ต่าง ๆ ให้กับเหยื่อ

(9) ภัยไวรัสและหนอนคอมพิวเตอร์ เป็นการเจาะระบบโดยอาศัยช่องโหว่ของเครือข่าย ระบบปฏิบัติการ และแอพพลิเคชั่น และแนวโน้มของการเกิดช่องโหว่ระบบนั้นก็มีเพิ่มขึ้นเรื่อย ๆ อย่างต่อเนื่อง

จากการวิจัยพบว่าในปัจจุบันการกระจายของหนอนคอมพิวเตอร์ในปัจจุบันนั้นใช้เวลาในระดับนาที แต่มีการคาดการณ์ว่าในอนาคตจะมีระดับเป็นหน่วยวินาที

(10) ภัยพีดีเอ มัลแวร์ ข้อมูลใน พีดีเอ สามารถที่จะเป็นพาหะของไวรัส โทรจัน ฮอร์ส และ Malicious Mobile Code ต่าง ๆ ได้เหมือนกับข้อมูลที่อยู่ในเครื่องพีซี

จากการทบทวนแนวคิดและทฤษฎีอาชญากรรมทางเทคโนโลยี ผู้วิจัยนำมาทบทวนวรรณกรรมและใช้เป็นประเด็นในการดำเนินการวิจัยเพื่อให้เป็นแนวทางในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี

4. แนวความคิดและทฤษฎีเกี่ยวกับการป้องกันปราบปรามอาชญากรรม

ผลกระทบที่เกิดจากอาชญากรรมทางคอมพิวเตอร์ก่อให้เกิดความเสียหายให้กับหน่วยงานหรือองค์กรอย่างมาก จึงมีความพยายามในการที่จะป้องกันและปราบปรามอาชญากรรม คอมพิวเตอร์ ปุระชัย เปี่ยมสมบูรณ์ (2551, หน้า 190) กล่าวว่า การป้องกันและปราบปรามอาชญากรรมเป็นเป้าหมายของงานตำรวจ เซอร์ โรเบิร์ต พีล (Sir Robert Peel) บิดาของการตำรวจยุคใหม่ เน้นว่าการป้องกันและปราบปรามอาชญากรรม คืองานหลักของตำรวจ มีความสำคัญยิ่งกว่าการสืบสวนสอบสวน การจับกุม และการลงโทษผู้กระทำผิด โดยทฤษฎีและมาตรการป้องกันอาชญากรรมมีการพัฒนามาโดยตลอด การปฏิบัติงานในด้านนี้ภายใต้อิทธิพลของทฤษฎีสำคัญ 3 ทฤษฎี คือ

1. ทฤษฎีบังคับใช้กฎหมาย (Law Enforcement Approach) โดยไม่จำเป็นต้องร้องขอความช่วยเหลือจากประชาชนโดยตรง โดยให้ความมั่นใจได้ว่าตำรวจสามารถปฏิบัติงานด้านป้องกันอาชญากรรมได้โดยเอกเทศ ทฤษฎี ทฤษฎีนี้เกิดขึ้นกลาง ศตวรรษที่19 โดยมีความเชื่อว่าการปรากฏตัวของตำรวจบ่อย ๆ ย่อมมีผลในการยับยั้งผู้ที่มีแนวโน้มจะประกอบอาชญากรรมมิให้กระทำผิด เพราะเกรงกลัวต่อการถูกจับกุม จึงมุ่งกระจายกำลังเจ้าหน้าที่ตำรวจให้ครอบคลุมทั่วพื้นที่ มีสายตรวจแต่งเครื่องแบบให้เห็นเด่นชัดได้ง่าย และปฏิบัติงานตรวจทันทีโดยสม่ำเสมอ เพื่อเป็นการลดช่องโอกาสของผู้จะกระทำผิด และตามแนวความคิดนี้จึงให้ความสำคัญกับตำรวจสายตรวจเป็นอันมาก และกำหนดอัตราส่วนของตำรวจต่อประชาชนในจำนวนที่เชื่อว่าพอเพียงกับการรับผิดชอบปัญหาอาชญากรรม

2. ทฤษฎีชุมชนสัมพันธ์ (Community Relations Approach) ในราวทศวรรษที่1920 แนวทางปฏิบัติเกี่ยวกับ “ตำรวจชุมชนสัมพันธ์” ได้รับการพัฒนาขึ้นเกิดเป็นทฤษฎีชุมชนสัมพันธ์โดยมีรากฐานแนวความคิดและผลการวิจัยของนักอาชญาวิทยากลุ่มชิคาโก หรือสำนักนิเวศวิทยาอาชญากรรม ได้พยายามจูงใจให้นักอาชญาวิทยาทั้งหลายเห็นความสำคัญของปัจจัยต่างๆ ในสภาพแวดล้อมของเมืองที่มีผลกระทบต่อพฤติกรรมของอาชญากร ต่อมาความคิดเหล่านี้ได้แพร่หลาย ได้รับความสนใจและรวมตัวกันทำวิจัยในเรื่องนี้อย่างแพร่หลาย จากการศึกษาวิจัยสรุปได้ว่าอาชญากรรมเป็นปรากฏการณ์ถาวรตามลักษณะพื้นที่ บริเวณใดที่ขาดระเบียบในสังคมหรือเกิดมลภาวะแตกแยกของกลไกลทางสังคมที่มีหน้าที่ค้ำจุนระหว่างบุคคล หรือขาดความร่วมแรงร่วมใจตลอดจนกำลังใจของสมาชิกในสังคม ก็จะก่อให้เกิดอาชญากรรมได้ง่าย และมีสถิติสูงกว่าพื้นที่อื่น จากแนวความคิดนี้เอง

ต่อมาได้เกิดแนวความคิดที่เรียกว่า “หมู่บ้านในเมือง”(Urban Village) เพื่อสร้างความสัมพันธ์ในสังคมโดยจัดสภาพพื้นที่ในชุมชนให้มีลักษณะเอื้ออำนวยต่อการเพิ่มปฏิสัมพันธ์ทางสังคมของคนในชุมชนต่างๆ เพื่อลดปัญหาและป้องกัน อาชญากรรมได้มากขึ้น เป็นการจัดสภาพทั่วไปไม่ว่าจะในระดับเมือง ชุมชน หรือ ละแวกบ้านให้มีลักษณะเสริมสร้างความสัมพันธ์ระหว่างบุคคลให้ง่ายต่อการควบคุม และสังเกต ตรวจตราไม่ล่วงล้ำ สิทธิเสรีภาพส่วนบุคคล มุ่งสนับสนุน ส่งเสริมให้สมาชิกในชุมชนมีส่วนร่วมในการป้องกันชีวิต ร่างกายและทรัพย์สินของตนเอง และผู้อื่นให้ปลอดภัยจากอาชญากรรมและให้ปรับบทบาทตำรวจเสียใหม่โดยทำหน้าที่เป็นผู้วางแผน สนับสนุน และให้คำปรึกษาแก่ชุมชน นอกจากนี้ข้อเสนอที่ตามมาคือการยกเลิกตรวจสายตรวจที่ได้ปฏิบัติสืบทอดกันมาเป็นเวลานานโดยปริยาย ดังนั้นถ้ามีการประยุกต์ใช้มาตรการ และแนวคิดชุมชนสัมพันธ์ได้พยายามแสวงหาคำตอบสำหรับการป้องกันอาชญากรรมย่อมได้รับผลกระทบกระเทือนอย่างมาก อย่างไรก็ดีแนวคิดชุมชนสัมพันธ์ได้พยายามแสวงหาคำตอบสำหรับการป้องกันอาชญากรรมในปัจจุบันโดยมุ่งลดช่องว่างและโอกาสของการประกอบอาชญากรรมที่เกิดในชุมชน ซึ่งมีคุณค่าแม้ว่าแนวความคิดนี้จะไม่ช่วยสร้างความเข้าใจเกี่ยวกับสาเหตุของการเกิดอาชญากรรมในแง่ชีวภาคและจิตภาคเพิ่มขึ้นมากก็ตาม

3. ทฤษฎีควบคุมอาชญากรรมจากสภาพแวดล้อม (Theory of Crime Control Through Environmental Design) ทฤษฎีเป็นการผนวกเอาแนวทฤษฎีที่ 1 และทฤษฎีที่ 2 และเชื่อมโยงทฤษฎีว่าด้วย การป้องกันอาชญากรรมเข้ากับทางสังคมศาสตร์และพฤติกรรมศาสตร์ไว้ด้วยกัน อันเป็นการเชื่อมโยงองค์ความรู้สาขาอาชญาวิทยา ให้เข้ากับองค์ความรู้ สาขาพฤติกรรมศาสตร์ด้วย ทฤษฎีควบคุมอาชญากรรมจากสภาพแวดล้อม ได้ตระหนักถึงปัญหา ของอาชญากรรมที่เป็นปฏิสัมพันธ์ระหว่างบุคคลกับสภาพแวดล้อม เพื่อก่อให้เกิดพฤติกรรมต่างๆ พอสรุปได้คือ

1) มุ่งลดช่องโอกาสสำหรับประกอบอาชญากรรมในสภาพแวดล้อมแต่มิได้ละเลยความสำคัญของตัวบุคคลซึ่งมีแนวโน้ม หรือสำนึกที่จะละเมิดหรือไม่ละเมิดกฎหมาย

2) มีความเพียงพอในการควบคุมอาชญากรรมประเภทประทุษร้ายต่อทรัพย์ให้อยู่ ในขอบเขตที่เหมาะสม

3) มีคุณค่าทางปฏิบัติอยู่ในระดับสูงรวมทั้งส่งเสริมหลักของศีลธรรมและ มนุษยธรรม

4) มุ่งสนับสนุนการรวมตัวและสัมพันธภาพระหว่างสุจริตชนในสังคมเพื่อให้ เกิดแรงต้านทุจริตชน ซึ่งเป็นกลุ่มน้อยโดยอาศัยการที่อยู่ภายในกรอบของกฎหมาย

5) กำหนดนิยามของกฎหมายไว้เฉพาะกฎหมายที่ตราขึ้นเพื่อผลประโยชน์ของประชาชนจำนวนมากที่สุดได้รับประโยชน์สูงสุดจากการบัญญัติกฎหมายนั้น

ทฤษฎีให้ความสำคัญของสภาพแวดล้อมมาก เพราะถ้าหากจัดสภาพแวดล้อมให้แข็งแกร่ง สามารถที่จะขัดขวางการละเมิดกฎหมายได้โดยสมบูรณ์การกระทำก็ไม่สำเร็จ ในทางตรงข้ามหากจัดสภาพแวดล้อมไม่สมบูรณ์ก็อาจจะทำให้พฤติกรรมไม่ละเมิดกฎหมายเปลี่ยนไป เป็นพฤติกรรมละเมิดกฎหมายแฝงและนำไปสู่พฤติกรรมละเมิดกฎหมาย หรือการกระทำผิดอาญาได้ในที่สุด

การป้องกันปราบปรามอาชญากรรม โดยการใช้มาตรการและวิธีการต่าง ๆ ที่จะไม่ให้เกิดอาชญากรรมขึ้นโดยอาจจำแนกได้ดังนี้ คือ การกำจัด ต้นเหตุการณ์ ขจัดความปรารถนาที่จะกระทำผิด และการขจัดช่วง

โอกาสที่จะกระทำผิด ซึ่งทั้งหมดนี้ถือเป็นหน้าที่ของเจ้าหน้าที่รัฐบาล เอกชนและประชาชน ในการร่วมมือกัน ซึ่งถือว่าเป็นงานในหน้าที่ของตำรวจที่สำคัญที่สุดรวมตลอดจนถึง การใช้มาตรการต่าง ๆ ระงับเหตุการณ์การกระทำความผิด การจับกุมควบคุมอาชญากร เพื่อป้องกันอาชญากรรมย้อนกลับมากระทำความผิดอีก และการลงโทษอาชญากร เพื่อทำให้เกิดความเข็ดหลาบ ทั้งยังเป็นเครื่องเตือนใจแก่ผู้ที่คิดจะประกอบ อาชญากรรมอีกประการหนึ่งด้วย โดยอาจจะเป็นการป้องกันและระงับเหตุในการ เกิดอาชญากรรม และ/หรือเป็นการสืบสวนปราบปรามติดตามจับกุมภายหลังจาก การเกิดเหตุแล้ว การป้องกันปราบปรามอาชญากรรมด้วยการแสวงหาความร่วมมือ จากประชาชน งานตำรวจชุมชนสัมพันธ์ เป็นงานหนึ่งในแผนกรมตำรวจแม่บทที่เน้นให้ตำรวจสร้างความเข้าใจ ทัศนคติ ความศรัทธา ความเชื่อมั่นและความสัมพันธ์อันดี ระหว่างตำรวจกับประชาชน และให้ประชาชนได้มีส่วนสนับสนุนหรือมีส่วนร่วมในการปฏิบัติงานของตำรวจ ทั้งในด้านการป้องกันปราบปรามอาชญากรรม และรักษาความมั่นคงของชาติ รวมทั้ง การมีส่วนร่วมในการรักษาความปลอดภัยในชีวิตและทรัพย์สิน โดยให้ประชาชน และชุมชนได้เข้ามามีส่วนร่วมในการป้องกัน และแก้ไขปัญหาอาชญากรรม เน้นการขยายงานด้านชุมชนและมวลชนสัมพันธ์ มีการเผยแพร่อบรมให้ความรู้ด้านการป้องกันอาชญากรรมแก่ประชาชน องค์กรชุมชน รวมทั้งผู้นำท้องถิ่น ด้วยมาตรการป้องกันปราบปรามอาชญากรรมอาจแบ่งออกได้ 2 มาตรการ คือ

1) มาตรการป้องกัน อันได้แก่ มาตรการป้องกันพื้นฐาน มาตรการป้องกันตามปกติและมาตรการป้องกันในเชิงรุก ทั้ง 3 มาตรการนี้มีความคล้ายคลึงและแตกต่างกันคือ

1.1) มาตรการการป้องกันพื้นฐาน เป็นการปฏิบัติการใช้ แนวความคิดทสอดคล้องกับองค์ประกอบการเกิดอาชญากรรม ที่ประกอบด้วยสภาพแวดล้อมของสังคมสถานภาพของผู้ที่จะประกอบอาชญากรรม และโอกาสในการประกอบอาชญากรรม ซึ่งในด้านโอกาสในการประกอบอาชญากรรมนี้ถือว่าเป็นหน้าที่ของตำรวจที่จะต้องปฏิบัติโดยตรงเพื่อไม่ให้คนที่คิดจะประกอบอาชญากรรมมีโอกาสได้กระทำหรือให้มีโอกาสน้อยที่สุด โดยอาจจะทำในรูปของการตัดโอกาสโดยตรงหรือโดยอ้อมก็ได้ ก็คือการใช้กำลังของเจ้าหน้าที่ตำรวจในเครื่องแบบปรากฏในพื้นที่ และช่วงเวลาที่เหมาะสม ในเหตุการณ์ที่อาจจะเกิดอาชญากรรม เช่น ในช่วงเวลากลางคืนหรือในพื้นที่ล่อแหลมต่อการประกอบอาชญากรรมต่าง ๆ เป็นต้น

1.2) มาตรการป้องกันตามปกติ คือ การกำหนดแนวทางการปฏิบัติให้กับเจ้าหน้าที่ตำรวจที่มีหน้าที่เกี่ยวข้องให้ปฏิบัติงาน เพื่อผลการป้องกันการเกิดอาชญากรรมทั่วไปในทุกคดีและมีมาตรการติดตามตรวจสอบประเมินผลการปฏิบัติงานอย่างต่อเนื่องเป็นประจำ

1.3) มาตรการป้องกันเชิงรุก คือ การปฏิบัติหน้าที่ที่ใกล้เคียงกับการปราบปรามแต่ยังไม่ถึงขั้นของการจับกุม เป็นแต่การปฏิบัติที่เข้าไปใกล้กับคนร้ายมากขึ้นกว่ามาตรการป้องกันตามปกติ วิธีการนี้จะเน้นที่ความสม่ำเสมอ เพื่อป้องกันมากกว่าการหวังผลจับกุม

2) มาตรการปราบปราม แบ่งออกเป็นมาตรการปราบปรามตามปกติกับมาตรการปราบปรามเชิงรุก มาตรการปราบปรามตามปกติ ได้แก่ การสืบสวนหาข่าวปราบปรามอาวุธสงคราม อาวุธ

เถื่อน ยาเสพติด ของหนีภาษีและมือปืนรับจ้าง ส่วนมาตรการปราบปรามเชิงรุก ได้แก่ การจัดระดมพลเพื่อกวาดล้างให้สอดคล้องกับเหตุการณ์และสถานการณ์ที่เกิดอาชญากรรม

2.2) บทบาทหน้าที่ของตำรวจในการป้องกันอาชญากรรม

ปุระชัย เปี่ยมสมบูรณ์ ได้ให้ความหมายหรือคำจำกัดความของคำว่า “การป้องกันอาชญากรรมพื้นฐาน” โดยทั่วไปแล้วการป้องกันย่อมหมายถึง การดำเนินการใด เพื่อป้องกันมิให้ส่งผลที่จะเกิดขึ้นแต่ในเรื่องของการป้องกันอาชญากรรมพื้นฐาน มีปัญหาว่า การลงโทษผู้กระทำผิด หรือการสงเคราะห์ผู้พ้นโทษเช่นนี้เป็นการป้องกันอาชญากรรมพื้นฐานหรือไม่ ซึ่งการดำเนินการนี้ เกิดขึ้นภายหลังจากที่อาชญากรรมเกิดขึ้นแล้ว หรืออีก นัยหนึ่ง เป็นการป้องกันอาชญากรรมพื้นฐานโดยการข่มขวัญ ยับยั้งหรือการช่วยมิให้ผู้พ้นโทษ กลับไปกระทำความผิดขึ้นอีก ในบางกรณีเพื่อที่จะหลีกเลี่ยงความสับสนดังกล่าว จึงมีการหลีกเลี่ยงที่จะกล่าวถึงความหมายหรือคำจำกัดความโดยหันไป พิจารณาถึงระดับหรือขอบเขตของการป้องกันอาชญากรรม จึงได้ประยุกต์ระดับของการป้องกันของงานสาธารณสุขมาใช้กับการป้องกันอาชญากรรม โดยได้แบ่งระดับของการป้องกันออกเป็น 3 ระดับ คือ การป้องกันระดับแรก ระดับที่สอง ระดับที่สามในการป้องกันระดับแรกในทางสาธารณสุข หมายถึง การป้องกันโรคติดต่อโดยเน้นสุขภาพอนามัย การปลูกฝีฉีดยา การระวังเรื่องน้ำดื่มน้ำใช้สำหรับทางในทางอาชญาวิทยา หมายถึงการปรับปรุงสภาพแวดล้อมทางเศรษฐกิจและสังคมโดยเฉพาะของกลุ่มคนที่มีปัญหาการป้องกันในระดับที่สองเกี่ยวข้องกับการคัดเลือกผู้เริ่มมีอาการป่วยออกจากผู้อื่น ในทางอาชญาวิทยาเน้นที่การแยกเด็กหรือผู้ใหญ่ที่มีแนวโน้มที่จะกระทำผิดหรือมีพฤติกรรมเบี่ยงเบนที่ไม่ร้ายแรงเพื่อให้การเอาใจใส่โดยเฉพาะ การป้องกันระดับสาม งานสาธารณสุขเน้นในเรื่องการบำบัดรักษาผู้ป่วยในทางอาชญาวิทยา เน้นในเรื่องการปฏิบัติต่อผู้กระทำผิดเพื่อมิให้กระทำผิดซ้ำอีก

นอกจากนี้ ได้แบ่งการป้องกันอาชญากรรมพื้นฐาน ในแง่ของการป้องกันที่สภาพแวดล้อมหรือที่ตัวอาชญากร หรือในแง่ของการป้องกันก่อนที่จะเกิดอาชญากรรม และหลังจากเกิดอาชญากรรมแล้ว นอกจากนี้ ยังได้แบ่งในแง่การป้องกันทางตรงกับทางอ้อม ในด้านการฝึกอาชีพ การศึกษา การจับกุม ปราบปรามของตำรวจ การคุมประพฤติ และการจำคุก เป็นต้น ยังได้กล่าวถึงทฤษฎียังได้กล่าวถึงทฤษฎีว่าด้วยการป้องกันอาชญากรรมไว้ว่า ในกิจการตำรวจการป้องกันอาชญากรรมถือว่า เป็นเป้าหมายหลักที่กำหนดขึ้นเพื่อเป็นภารกิจของงานตำรวจ

แนวทฤษฎีที่ใช้ในการป้องกันอาชญากรรมแบบเก่า ได้แก่ ทฤษฎีบังคับใช้กฎหมาย และ “ทฤษฎีชุมชนสัมพันธ์” โดยแนวทางทฤษฎีบังคับใช้กฎหมายมียุทธวิธีที่ตำรวจใช้ คือการตรวจท้องที่ เนื่องจากการปรากฏตัวของตำรวจย่อมมีผลในการยับยั้งผู้ที่มีแนวโน้มจะประกอบอาชญากรรม เพราะความเกรงกลัวการจับกุม ฉะนั้นเจ้าหน้าที่ตำรวจสายตรวจจึงต้องแต่งเครื่องแบบ และรถวิทยุสายตรวจจึงควรมีลักษณะเด่นชัดเห็นได้ง่ายเพื่อเป็นการข่มขวัญยับยั้งอาชญากร หรือผู้ที่จะประกอบอาชญากรรมนอกจากนั้นการตรวจท้องที่สม่ำเสมอต่อเนื่อง จะทำให้สมาชิกในชุมชนเกิดความรู้สึกว่ามีตำรวจอยู่ทั่วไปทุกแห่ง ส่วนแนวทฤษฎีชุมชนสัมพันธ์ เพื่อป้องกันอาชญากรรมนั้น คือ การจัดสภาพทั่วไปไม่ว่าในระดับเมือง ชุมชน หรือละแวกบ้านในลักษณะเสริมสร้างความสัมพันธ์ระหว่างบุคคล ง่ายต่อการควบคุมสังเกตตรวจตรารวมทั้งมุ่ง

สนับสนุนส่งเสริมให้สมาชิกในชุมชน มีส่วนร่วมในการป้องกันชีวิต ร่างกายทรัพย์สินของตนเอง และผู้อื่นให้ปลอดภัยจากอาชญากรรม ทั้งนี้ควรได้รับความร่วมมือจากประชาชนด้วย ซึ่งสามารถดำเนินการได้ 3 แนวทาง ประกอบกัน คือ การประชาสัมพันธ์ การให้บริการแก่ชุมชน และการเข้ามีส่วนร่วมในกิจกรรมต่าง ๆ โดยเสริมสร้างความสัมพันธ์ในการทำงานร่วมกับประชาชน สโมสร สมาคม หรือองค์กรสาธารณกุศลต่าง ๆ

โดยแนวความคิดเกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่ได้ทำการศึกษาจะนำมาใช้ประโยชน์ในการหาแนวทางในการกำหนดประเด็นที่ใช้ในการวิจัยเพื่อการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

5. แนวความคิดและทฤษฎีเกี่ยวกับการบริหารจัดการ

ในอดีตที่ผ่านมาระบบการจัดการของการผลิต และกิจกรรมต่าง ๆ ก็ดี ทางเศรษฐกิจ ทางการตลาด มิได้มีความสลับซับซ้อนมากนัก และไม่ต้องอาศัยระบบของการจัดการเช่นในปัจจุบันนี้ กระทั่งเมื่อมีการปฏิวัติอุตสาหกรรมเกิดขึ้นในโลก (ประมาณ ปี ค.ศ. 1880 เป็นต้นมา) ซึ่งเป็นการเปลี่ยนแปลงอย่างมาก อันมีผลทำให้เศรษฐกิจ สังคม การเมือง มีการเปลี่ยนแปลงไปจากเดิมมาก ตลอดจนมีการเจริญเติบโตทางเศรษฐกิจอย่างรวดเร็ว และแนวคิดเกี่ยวกับการจัดการเริ่มเป็นที่ยอมรับและขยายตัวมากขึ้น มีการพัฒนามากขึ้นเป็นลำดับ

ขอบเขต และความหมายของการบริหารการจัดการ

บริบทที่สำคัญประการหนึ่งของนักบริหาร คือการจัดการ หรือการบริหารองค์กรให้สามารถอยู่ได้อย่างมีเสถียรภาพ ภายใต้สภาพแวดล้อมที่เปลี่ยนแปลง โดยรวบรวมเอากลุ่มกิจกรรมต่าง ๆ ขององค์กร นำไปสู่การปฏิบัติเพื่อความสาเร็จในเป้าหมาย โดยคำนึงถึงความมีประสิทธิภาพ ประสิทธิผล และความประหยัด

ความหมายขององค์กร

เชสเตอร์ ไอ บาร์นาร์ด (Chester I. Barnard) กล่าวว่า องค์กรคือ ระบบที่บุคคลสองคนหรือมากกว่าร่วมแรงร่วมใจกันทำงานอย่างมีจิตสำนึก

เฮอร์เบิร์ต จี ฮิกส์ (Herbert G. Hicks) กล่าวว่า องค์กรคือ กระบวนการจัดโครงสร้างให้บุคคลเกิดปฏิสัมพันธ์ ในการทำงานให้บรรลุวัตถุประสงค์ขององค์กรคือ กลุ่มบุคคลตั้งแต่ 2 คนขึ้นไป รวมกันขึ้นเพื่อที่จะดำเนินการให้บรรลุเป้าหมายที่กำหนดไว้

โดยที่บุคคลคนเดียวไม่สามารถดำเนินการให้สาเร็จได้โดยลำพัง ซึ่งพบว่าองค์กรจะเกิดขึ้นและมีอยู่ในสังคมมนุษย์ทุกหนทุกแห่ง และองค์กรก็เป็นเครื่องมือสำหรับการดำเนินการให้เป็นไปตามเป้าหมายและความสำเร็จ ดังนั้นการจัดการ (management) หรือการบริหาร (administration) สองคำนี้จึงเป็นคำที่คนส่วนใหญ่คุ้นเคยและใช้กันอยู่เสมออย่างกว้างขวาง จึงมีความหมายคล้ายคลึงกันและใช้ทดแทนกันอยู่เสมอ เพราะฉะนั้น การจัดการ (management) คือ การจัดการภารกิจภายในองค์กรให้บรรลุวัตถุประสงค์และเป็นไปตามนโยบายแผนงานที่ได้กำหนดไว้หรือการจัดการหมายถึง ภารกิจของบุคคลหนึ่งบุคคลใด หรือหลายคนที่เข้ามาทำหน้าที่ประสานให้การทำงานของแต่ละบุคคลที่ต่างฝ่ายต่างทำไม่สามารถบรรลุผลสาเร็จได้ ส่วน

การบริหาร (administration) หมายถึง การบริหารที่เกี่ยวข้องกับการดำเนินการในระดับและแผนงาน ซึ่งส่วนใหญ่ใช้กับการบริหารในภาครัฐหรือองค์กรขนาดใหญ่ จากความเห็นของนักวิชาการต่อคำดังกล่าว จะเห็นได้ว่ามีความแตกต่างกัน ขึ้นอยู่กับเจตนารมณ์ของผู้ใช้ว่าจะมีความเหมาะสมไปในทางใด ซึ่งอาจใช้คำทั้งสองแทนกันได้

องค์ประกอบขององค์กร (elements of organization) ที่สำคัญ 5 ประการ คือ

1) คน องค์กรจะประกอบด้วยคนตั้งแต่ 2 คนขึ้นไป ซึ่งส่วนใหญ่องค์กรจะมีคนเป็นจำนวนมากปฏิบัติงานร่วมกัน หรือแบ่งงานกันทำ เพื่อให้บรรลุเป้าหมายที่กำหนด โดยที่คนจะปฏิบัติงานร่วมกันได้จำเป็นต้องอาศัย “ความรู้ทางพฤติกรรมศาสตร์” เพื่อทำความเข้าใจซึ่งกันและกัน

2) เทคนิค การบริหารองค์กรต้องอาศัยเทคนิควิทยาการ หรือที่เรียกว่า เทคโนโลยี เพื่อการแก้ไขปัญหาหรือติดสินใจ หรืออาจกล่าวได้ว่าในปัจจุบันนี้องค์กรไม่สามารถจะบริหารงานได้โดยอาศัยแต่เฉพาะประสบการณ์ ความเฉลียวฉลาดของนักบริหารเท่านั้น ในหลายกรณีผู้บริหารต้องอาศัย เทคนิคทางการบริหารเพื่อการแก้ไขปัญหาหรือการตัดสินใจ และในขณะเดียวกันก็เป็นการลดความเสี่ยงอีกด้วย

3) ความรู้ ข้อมูล ข่าวสาร หรือที่เรียกว่า สารสนเทศ ในการปฏิบัติงานและการแก้ไขปัญหา การอาศัยเทคนิคทางการบริหาร ยังไม่เพียงพอสำหรับการบริหารองค์กร นักบริหารยังต้องอาศัยความรู้ข้อมูลข่าวสาร เพื่อความเข้าใจ เพื่อการวิเคราะห์ ตลอดจนการคาดคะเนแนวโน้มในอนาคตอีกด้วย ดังนั้นเทคนิคเพื่อการบริหารจึงควบคู่ไปกับ ความรู้ ข้อมูล ข่าวสาร

4) โครงสร้าง เป็นองค์ประกอบที่สำคัญไม่น้อยขององค์กร ซึ่งนักบริหารจะต้องจัดโครงสร้างให้สอดคล้องกับงาน เพื่อกำหนดอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม เพื่อให้งานขององค์กรบรรลุเป้าหมายได้อย่างมีประสิทธิภาพ

5) เป้าหมาย หรือวัตถุประสงค์ มนุษย์จัดตั้งองค์กรขึ้นมาก็เพื่อบรรลุเป้าหมายหรือวัตถุประสงค์ ดังนั้น องค์กรจึงต้องมีเป้าหมาย หรือวัตถุประสงค์ที่ชัดเจน

ความหมายของการบริหารจัดการ

มีนักวิชาการได้ให้ความหมายกันไว้มากมาย ตามแนวทาง เช่น

แมรี่ ปาร์คเกอร์ ฟอลเลต (Mary Parker Follett) “การบริหารการจัดการเป็นเทคนิคการทำงานให้สำเร็จโดยอาศัยผู้อื่น”

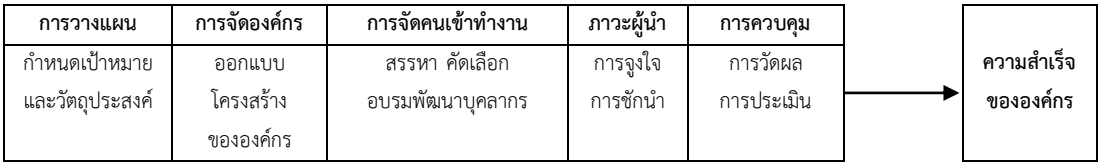
จอร์จ อา เทอร์รี่ (George R.Terry) “การบริหารการจัดการ เป็นกระบวนการของการวางแผนการจัดองค์กร การกระตุ้นและการควบคุมให้บรรลุจุดมุ่งหมายร่วมกัน โดยใช้ทรัพยากรบุคคลและอื่น ๆ”

เจมส์ เอ เอฟ สโตนเนอร์ (James A.F.Stoner) “การจัดการคือ กระบวนการ (Process) ของการวางแผน (Planning) การจัดองค์กร (Organization) การสั่งการ (Leading) และการควบคุม (Controlling) ความพยายามของสมาชิกในองค์กรและการใช้ทรัพย์กรต่าง ๆ เพื่อบรรลุวัตถุประสงค์ที่องค์กรกำหนดไว้”

หน้าที่ในการจัดการ (The Function of Management)

นักวิชาและนักบริหารได้มีการวิเคราะห์ว่า การจัดการเป็นความรู้ที่มีประโยชน์ ดังนั้นจึงได้จัดการศึกษาหน้าที่ของการจัดการ โดยแบ่งออกเป็น 5 ประเภท ดังนี้ คือ

1. การวางแผน (Planning)
2. การจัดองค์กร (Organization)
3. การจัดหาคนเข้าทำงาน (Staffing)
4. ภาวะผู้นำ (Leading) และ
5. การควบคุม (Controlling)



ภาพที่ 2-1 หน้าที่ของการจัดการ

สำหรับ Luther Gulick และ Lymdall Urwick ได้กำหนดหน้าที่ของผู้บริหารในการจัดการไว้ 7 ประการด้วยกันคือ

P = Planning การวางแผน
O = Organizing การจัดองค์กร
S = Staffing การจัดการคนเข้าทำงาน
D = Directing การอำนวยการ
CO = Co-ordinating การประสานงาน
R = Reporting การรายงาน
B = Budgeting งบประมาณ

หน้าที่ของการจัดการและทักษะในแต่ละระดับขององค์กร

ผู้บริหารคือ บุคคลที่ทำหน้าที่ประสานงานระหว่างกิจกรรมต่าง ๆ ขององค์กรเพื่อให้ดำเนินไปสู่วัตถุประสงค์ที่กำหนดไว้ ผู้บริหารขององค์กรจะสามารถจัดการตามกระบวนการจัดการอย่างมีประสิทธิภาพมากน้อย เพียงไรขึ้นอยู่ความสามารถทางการจัดการ 3 ชนิด คือ

1. ความสามารถด้านความคิด (Conceptual Skill) เป็นความสามารถในการมองภาพรวมทั่วทั้งองค์กร และความสามารถที่จะรวบรวมเอากิจกรรมและสถานการณ์ต่าง ๆ ตลอดจนเข้าใจในความสัมพันธ์ระหว่างองค์ประกอบต่าง ๆ ในองค์กร

2. ความสามารถด้านคน (Human Skill) ความสามารถในการทำงานร่วมกับผู้อื่น การทำงานเป็นทีมการสร้างบรรยากาศในการทำงาน และการยอมรับความคิดเห็นของผู้ร่วมงาน

3. ความสามารถด้านงานเทคนิค (Technical Skill) มีความรู้ ความชำนาญ กระบวนการวิธีการขั้นตอนต่าง ๆ ในการทำงาน และความสามารถในการประยุกต์ให้งานประสบความสำเร็จได้ดี

ระดับของผู้บริหารแบ่งออกเป็น 3 ระดับด้วยคือ

1. ผู้บริหารระดับสูง (Top Manager) ทำหน้าที่นำองค์กรไปสู่ความสำเร็จ โดยกำหนดนโยบายต่าง ๆ ขององค์กร เพภายใต้สภาพแวดล้อมที่เปลี่ยนแปลง ซึ่งมีทั้งปัจจัยภายในและปัจจัยภายนอก

2. ผู้บริหารระดับกลาง (Middle Manager) ทำหน้าที่ควบคุมประสานงานกับผู้บริหารระดับต้นให้ดำเนินงานตามนโยบายและแผนงานที่ได้กำหนดไว้ และนำผลสำเร็จรายงานต่อผู้บริหารระดับสูง

3. ผู้บริหารระดับต้น (first – line manager) เป็นผู้บริหารที่ใกล้ชิดกับผู้ปฏิบัติการและมีโอกาสรับรู้ปัญหาที่จริง

ทรัพยากรในการบริหารการจัดการ

ทรัพยากรหรือปัจจัยที่นักบริหารต้องให้ความสนใจ เพื่อให้การดำเนินการตามวัตถุประสงค์ขององค์กรประสบความสำเร็จ ซึ่งประกอบด้วยปัจจัยดังต่อไปนี้

คน (man) คือ ทรัพยากรบุคคลมีผลต่อความสำเร็จในการจัดการ

เงิน (money) คือ ปัจจัยสำคัญที่จะช่วยสนับสนุนให้กิจกรรมต่าง ๆ ขององค์กรดำเนินการต่อไปได้

วัสดุ (materials) คือ วัตถุดิบซึ่งเป็นปัจจัยที่สำคัญไม่แพ้ปัจจัยอื่น จำเป็นต้องมีคุณภาพและมีต้นทุนที่ต่ำเพราะมีผลกระทบต่อต้นทุนการผลิต

เครื่องจักร (machine) คือ เครื่องจักรอุปกรณ์ ที่มีศักยภาพที่ดีจะก่อให้เกิดประโยชน์สูงสุดต่อการผลิตเช่นกัน

วิธีการบริหารหรือวิธีการปฏิบัติ (managementor method) การจัดการหรือการบริหารในองค์กรธุรกิจประกอบด้วยระบบการผลิตหรือระบบการให้บริการต่าง ๆ หากมีระบบที่ชัดเจนตลอดจนมีระเบียบขั้นตอนวิธีการต่าง ๆ ในการทำงาน ย่อมส่งผลให้องค์กรประสบความสำเร็จได้ดี

เฮนรี่ เจ ฟาโยล (Henri J. Fayol) เป็นวิศวกรเหมืองแร่ชาวฝรั่งเศส ได้สร้างผลงานทางแนวความคิดเกี่ยวกับการบริหาร ซึ่งมุ่งที่ผู้บริหารระดับสูง โดยศึกษากฎเกณฑ์ที่เป็นสากล ได้เสนอแนวคิดและกำหนดหลักเกณฑ์ในการบริหารของผู้บริหาร ดังนี้

1) หน้าที่ของนักบริหาร (Management Functions) มีดังนี้

1.1) การวางแผน (planning) หมายถึง การที่ผู้บริหารจะต้องเตรียมการวางแผนการทำงานขององค์กรไว้ล่วงหน้า

1.2) การจัดองค์กร (organizing) หมายถึง การที่ผู้บริหารจะต้องเตรียมจัดโครงสร้างขององค์กรให้เหมาะสมกับทรัพยากรทางการบริหาร

1.3) การสั่งการ (directing) หมายถึง การที่ผู้บริหารจะต้องมีการวินิจฉัยสั่งการที่ดี เพื่อให้การดำเนินงานขององค์กรดำเนินการไปตามเป้าหมาย

1.4) การประสานงาน (co-ordinating) หมายถึง การที่มีผู้บริหารมีหน้าที่เชื่อมโยงต่าง ๆ ขององค์กรให้ดำนินไปอย่างสอดคล้องต้องกัน

1.5) การควบคุม (controlling) หมายถึง การที่ผู้บริหารคอยควบคุมและกำกับกิจกรรมต่าง ๆ ภายในองค์กรให้ดำเนินไปตามแผนที่วางไว้

2) หลักการบริหาร (management principle)

"General principles of management" (ทฤษฎีการจัดการของ Henri Fayol) ทฤษฎีการจัดการของ Henri Fayol มีความเชื่อว่าเป็นไปได้ที่เราจะหาทางศึกษาถึงศาสตร์ที่เกี่ยวข้องกับการจัดการ (management sciences) ซึ่งสามารถใช้ได้กับการบริหารทุกชนิด ไม่ว่าจะเป็นการบริหารงานอุตสาหกรรม หรืองานรัฐบาล ได้สรุปสาระสำคัญตามแนวความคิดของตนไว้ดังนี้ คือ

2.1) การแบ่งงานกันทำ (division of work) การแบ่งงานกันทำจะทำให้คนเกิดความชำนาญเฉพาะอย่าง (specialization) อันเป็นหลักการใช้ประโยชน์ของคนและกลุ่มคน ให้ทำงานเกิดประโยชน์สูงสุด

2.2) อำนาจหน้าที่ (authority) เป็นเครื่องมือที่จะทาให้ผู้บริหารมีสิทธิที่จะสั่งให้ผู้อื่นปฏิบัติงานที่ต้องการได้โดยจะมีความรับผิดชอบ (responsibility) เกิดขึ้นตามมาด้วย ซึ่งจะมีความสมดุลกันและกัน

2.3) ความมีระเบียบวินัย (discipline) บุคคลในองค์กรจะต้องเคารพเชื่อฟัง และปฏิบัติตามกฎเกณฑ์ กติกาและข้อบังคับต่าง ๆ ที่องค์กรกำหนดไว้ ความมีระเบียบวินัยจะมาจากความเป็นผู้นำที่ดี

2.4) เอกภาพในการบังคับบัญชา (unity of command) ในการทำงานใต้บังคับบัญชาควรได้รับคำสั่งจากผู้บังคับบัญชาเพียงคนเดียวเท่านั้น ไม่เช่นนั้นจะเกิดการโต้แย้งสับสน

2.5) เอกภาพในการสั่งการ (unity of direction) ควรอยู่ภายใต้การจัดการหรือการสั่งการโดยผู้บังคับบัญชาคนหนึ่งคนใด

2.6) ผลประโยชน์ขององค์กรมาก่อนผลประโยชน์ส่วนบุคคล (subordinatation of individual interest to the general interest) คำนึงถึงผลประโยชน์ขององค์กรเป็นอันดับแรก

2.7) ผลตอบแทนที่ได้รับ (remuneration of personnel) ต้องยุติธรรม และเกิดความพึงพอใจทั้ง 2 ฝ่าย

2.8) การรวมอำนาจ (centralization) ควรรวมอำนาจไว้ที่ศูนย์กลางเพื่อให้สามารถควบคุมได้

2.9) สายการบังคับบัญชา (scalar chain) การติดต่อสื่อสารควรเป็นไปตามสายงาน

2.10) ความมีระเบียบเรียบร้อย (order) ผู้บริหารต้องกำหนดลักษณะและขอบเขตของงานเพื่อประสิทธิภาพในการจัดระเบียบการทำงาน

2.11) ความเสมอภาค (equity) ยุติธรรม และความเป็นกันเอง เพื่อให้เกิดความจงรักภักดี

2.12) ความมั่นคงในการทำงาน (stability of tenture of personnel) การหมุนเวียนคนงานตลอดจนการเรียนรู้ และความมั่นคงในการจ้างงาน

2.13) ความคิดริเริ่ม (initiative) เปิดโอกาสให้แสดงความคิดเห็น ให้แสดงออกถึงความคิดริเริ่ม

2.14) ความสามัคคี (esprit de corps) หลีกเลี่ยงการแบ่งพรรคแบ่งพวกในองค์กร

6. แนวความคิดและทฤษฎีเกี่ยวกับประสิทธิภาพในการปฏิบัติงาน

ประสิทธิภาพ หมายถึง ความคล่องแคล่วในการปฏิบัติงานให้สำเร็จซึ่งไม่ได้กล่าว ถึงปัจจัยนำเข้าหรือความพึงพอใจ โดยประสิทธิภาพเป็นสิ่งที่วัดได้หลายมิติ ตามแต่วัตถุประสงค์ที่ต้องการพิจารณา คือ

1. ประสิทธิภาพในมิติของค่าใช้จ่ายหรือต้นทุนของการผลิต (input) ได้แก่ การใช้ทรัพยากรการบริหาร คือ คน เงิน วัสดุ เทคโนโลยี ที่มีอย่างประหยัด คุ้มค่า และเกิดการสูญเสียน้อยที่สุด

2. ประสิทธิภาพในมิติของกระบวนการการบริหาร (process) ได้แก่ การทำงานที่ถูกต้องได้มาตรฐาน รวดเร็ว และใช้เทคโนโลยีที่สะดวกกว่าเดิม

3. ประสิทธิภาพในมิติของผลผลิตและผลลัพธ์ ได้แก่ การทำงานที่มีคุณภาพเกิดประโยชน์ต่อสังคม เกิดผลกำไร ทันเวลา ผู้ปฏิบัติงานมีจิตสำนึกที่ดีต่อการทำงานและบริการเป็นที่พอใจของลูกค้า หรือผู้มารับบริการ

ทิพาวดี เมฆสวรรค์ (2538) ได้เสนอแนวคิดในการปรับปรุงประสิทธิภาพการบริหารงานภาครัฐโดยศึกษาการปรับปรุงระบบ ราชการของต่างประเทศที่ได้รับการยอมรับว่าประสบความสำเร็จได้ดังนี้

1) ต้องกำหนดแนวทางและเป้าหมายของการเปลี่ยนแปลงที่ชัดเจน หมายถึง การทำงานที่มีประสิทธิผลยึดถือผลสำเร็จ หรือผลสัมฤทธิ์ของงาน (results) เป็นหลักในการดำเนินงานโดยม่งที่ผลลัพธ์ (outcome) โดยมีการประเมินผล และวัดผลสำเร็จของงานอย่างเป็นรูปธรรมสามารถตอบสนองและสร้างความพึงพอใจแก่ลูกค้าผู้มารับบริการ ปรับปรุงโครงสร้าง และระบบงานเพื่อยุบเลิกงานที่ซ้ำซ้อน โดยสร้างสรรค์กระบวนการ ทำงานใหม่ ลดขนาดกำลังคน เพื่อลดค่าใช้จ่ายขององค์กรด้านบุคคลากร มีการกระจาย อำนาจการดัดสินใจจากระดับบนสู่ระดับเจ้าหน้าที่

2) ระบบการบริหารงานที่จะยึดผลสำเร็จของงาน และผลลัพธ์ขององค์กรเป็นหลักสำคัญในการดำเนินการรวมทั้งใช้มาตรการจูงใจและให้รางวัลตอบแทนแกองค์กรที่ ประสบความสำเร็จ

ธงชัย สันติวงษ์ (2526,หน้า 198) นิยามว่าประสิทธิภาพ หมายถึง กิจกรรมทางด้านการบริหารบุคคลที่ได้เกี่ยวข้องกับวิธีการ ซึ่งหน่วยงานพยายามกำหนดให้ทราบแน่ ชัดว่าพนักงานของตนสามารถปฏิบัติงานได้มีประสิทธิภาพมากน้อยเพียงใด

สมพงษ์ เกษมสิน (2550) ได้กล่าวถึง แนวคิดของ Harring Emerson ที่เสนอแนวความคิดเกี่ยวกับหลักการทำงานให้มี ประสิทธิภาพในหนังสือ "The Twelve Principles of Efficiency" ซึ่งได้รับการยกย่องและกล่าวขานกันมาก หลัก 12 ประการ มีดังนี้

- ทำความเข้าใจและกำหนดแนวคิดในการทำงานให้กระจ่าง
- ใช้หลักสามัญสำนึกในการพิจารณาความน่าจะเป็นไปได้ของงาน
- คำปรึกษาแนะนำต้องสมบูรณ์และถูกต้อง
- รักษาระเบียบวินัยในการทำงาน
- ปฏิบัติงานด้วยความยุติธรรม
- การทำงานต้องเชื่อถือได้มีความฉับพลัน มีสมรรถภาพและมีการลงทะเบียน ไว้เป็นหลักฐาน
- งานควรมีลักษณะแจ้งให้ทราบถึงการดำเนินงานอย่างทั่วถึง
- งานเสร็จทันเวลา
- ผลงานได้มาตรฐาน
- การดำเนินงานสามารถยึดเป็นมาตรฐานได้
- กำหนดมาตรฐานที่สามารถใช้เป็นเครื่องมือในการแก่สอนงานได้
- ให้บำเหน็จแก่งานที่ดี

นอกจากนี้ยังมีแนวความคิดที่เกี่ยวข้องกับปัจจัยในการปฏิบัติงานให้มีประสิทธิภาพ หรือปัจจัยที่มีผลต่อการปฏิบัติงานนั้น และมีนักทฤษฎีหลายท่านได้ศึกษาและสรุป เป็นปัจจัยสำคัญ ๆ ที่น่าสนใจดังต่อไปนี้

เบ็คเกอร์ และนิวเฮาเซอร์ (Becker and Neuhauser ,1975) ได้เสนอตัวแบบจำลองเกี่ยวกับประสิทธิภาพขององค์กร (model of organization efficiency) โดยกล่าวว่าประสิทธิภาพขององค์กร นอกจากจะพิจารณาถึง ทรัพยากร เช่น คน เงิน วัสดุ ที่เป็นปัจจัยนำเข้า และผลผลิตขององค์กร คือ การบรรลุเป้าหมายแล้วองค์กรในฐานะที่เป็นองค์กรในระบบเปิด (open system) ยังมีปัจจัย ประกอบอีกดังแบบจำลองในรูปสมมติฐานซึ่งสามารถสรุปได้ดังนี้

1) หากสภาพแวดล้อมในการทำงานขององค์กรนั้น มีความซ้ำซ้อนต่ำ (low task environment complexity) หรือมีความแน่นอน (certain) มีการกำหนดระเบียบ ปฏิบัติในการทำงานขององค์กรอย่างละเอียดถี่ถ้วนแล้ว แน่ชัดว่าจะนำไปสู่ความมีประสิทธิภาพขององค์กรมากกว่า องค์กรที่มีสภาพแวดล้อมในการทำงานยุ่งยาก และซับซ้อนสูง (high task environment complexity) หรือมีความไม่แน่นอน (uncertain)

2) การกำหนดระเบียบปฏิบัติชัดเจนเพื่อเพิ่มผลการทำงานที่มองเห็นได้มีผลทำ ให้ประสิทธิภาพมากขึ้นด้วย

3) ผลการทำงานที่มองเห็นได้สัมพันธ์ในทางบวกกับประสิทธิภาพ

4) หากพิจารณาควบคู่กันไปจะปรากฏว่าการกำหนดระเบียบปฏิบัติอย่างชัดเจน และผลการทำงานที่สามารถมองเห็นได้จะมีความสัมพันธ์มากขึ้นต่อประสิทธิภาพมากกว่าตัวแปรแต่ละตัวตามลำพัง

เบ็คเกอร์ และนิวเฮาเซอร์ ยังเชื่ออีกว่าการสามารถมองเห็นผลการทำงานขององค์กรได้ (visibility consequences) และมีความสัมพันธ์ของประสิทธิภาพขององค์กร เพราะองค์กรสามารถทดลองและเลือกระเบียบการปฏิบัติได้ซึ่งระเบียบการปฏิบัติและ ผลการปฏิบัติงานจะมีอิทธิพลต่อประสิทธิภาพในการปฏิบัติงาน ซึ่งเป็นนักทฤษฎีที่ศึกษา องค์กรระบบเปิด (open system) เช่นกันก็ได้ศึกษาในเรื่องปัจจัยที่สำคัญต่อประสิทธิภาพในการปฏิบัติงาน ซึ่งเขากล่าวว่าประสิทธิภาพ คือ ส่วนประกอบที่สำคัญของประสิทธิผลประสิทธิภาพขององค์กร ถ้าจะวัดจากปัจจัยนำเข้าเปรียบเทียบกับผลผลิตที่ได้ จะทำให้การวัดประสิทธิภาพคลาดเคล่อน จากความเป็นจริงขององค์กร หมายถึง การบรรลุเป้าหมาย (goal-attainment) ขององค์กรในการบรรลุเป้าหมายขององค์กรปัจจัยต่าง ๆ คือ การฝึกอบรม ประสบการณ์ความผูกพัน ยังมีความสำคัญต่อประสิทธิภาพในองค์กรด้วย การปฏิบัติงานของแต่ละคนจะถูกกำหนดโดย 3 ส่วน ดังนี้

1. คุณลักษณะเฉพาะส่วนบุคคล (individual attributes) แบ่งออกเป็น 3 กลุ่ม ดังนี้

1.1 demographic characteristics เป็นลักษณะที่เกี่ยวกับ เพศ อายุ เชื้อชาติเผ่าพันธุ์

1.2 competence characteristics เป็นลักษณะที่เกี่ยวกับความรู้ความสามารถ ความถนัดและความชำนาญของบุคคลซึ่งคุณลักษณะเหล่านี้จะได้มาจากการศึกษาอบรมและสั่งสมประสบการณ์

1.3 psychological characteristics เป็นคุณลักษณะทางด้านจิตวิทยา ซึ่งได้แก่ ทัศนคติ ค่านิยม การรับในเรื่องต่าง ๆ รวมทั้งบุคลิกภาพของแต่ละบุคคลด้วย

2. ระดับความพยายามในการทำงาน (work effort) จะเกิดขึ้นจากการมีแรงจูงใจในการทำงาน ได้แก่ ความต้องการ แรงผลักดันอารมณ์ความรู้สึก ความสนใจ ความ ตั้งใจ เพราะว่าคนที่มีแรงจูงใจในการทำงานสูงจะมีความพยายามที่จะอุทิศกำลังกายและ กำลังใจให้แก่การทำงาน มากกว่าผู้ที่แรงจูงใจในการทำงานต่ำ

3. แรงสนับสนุนจากองค์กรหรือหน่วยงาน (organization support) ซึ่งได้แก่ คำตอบแทน ความยุติธรรม การติดต่อสื่อสาร และวิธีการที่จะมอบหมายงานซึ่งมีผลต่อ กำลังใจผู้ปฏิบัติงาน

สรุปได้ว่า ประสิทธิภาพในการปฏิบัติงานของแต่ละบุคคลเกิดจากสภาพภูมิหลัง ของแต่ละคนที่ไม่เหมือนกัน สภาพร่างกายจิตใจ การศึกษา ความรู้ความสามารถ ความถนัดต่าง ๆ โดยมีปัจจัยสนับสนุนให้เกิดความแตกต่างจากการประเมินของผู้บังคับบัญชาแล้วให้คะแนนออกมาในระดับต่ำ ปานกลาง และระดับสูง ซึ่งมีผลต่อการปรับเปลี่ยนวิธีการทำงานให้ข้าราชการผู้นั้นมีประสิทธิภาพในการปฏิบัติงานที่มากขึ้นเรื่อย ๆ

ปัจจัยที่จะก่อให้เกิดประสิทธิภาพในการปฏิบัติงานว่า ประกอบด้วยปัจจัยหลัก 3 ปัจจัยด้วยกัน คือ

1. ปัจจัยส่วนบุคคล ได้แก่ เพศ จำนวนสมาชิกในครอบครัว อายุ ระยะเวลาในการทำงาน สติปัญญา ระดับการศึกษา บุคลิกภาพ เป็นต้น

2. ปัจจัยที่ได้รับมาจากงาน ได้แก่ ชนิดของงาน ทักษะความชำนาญ สถานภาพทางอาชีพ สถานภาพทางภูมิศาสตร์ ขนาดของธุรกิจ เป็นต้น

3. ปัจจัยที่ควบคุมได้โดยฝ่ายบริหาร เช่น ความมั่นคง รายได้ สวัสดิการ โอกาสก้าวหน้าในงาน สภาพการทำงาน ผู้ร่วมงาน ความรับผิดชอบ การจัดการ เป็นต้น

ปัจจัยที่มีอิทธิพลต่อบุคคลในการปฏิบัติงานว่า มีปัจจัยหลายประการที่มีอิทธิพลต่อพฤติกรรมในการปฏิบัติงานของแต่ละบุคคล ซึ่งได้แก่ กิจกรรมในงานและนอกงาน การรับสถานการณ์ ระดับความปรารถนา กลุ่มอ้างอิง เพศ ภูมิหลังทางวัฒนธรรม การศึกษา ประสบการณ์ และระยะเวลาในการปฏิบัติงาน

ปัจจัยในการปฏิบัติงานให้มีประสิทธิภาพ

ปัจจัยสำคัญในการปฏิบัติงานให้มีประสิทธิภาพนั้น มีปัจจัย 7 ประการที่มีอิทธิพลต่อประสิทธิภาพในการปฏิบัติงานในองค์กร คือ

1. กลยุทธ์ (strategy) คือ กลยุทธ์เกี่ยวกับการกำหนดภารกิจ การพิจารณาจุดอ่อน ชุดแข็งภายในองค์กร โอกาสและอุปสรรคภายนอก
2. โครงสร้าง (structures) โครงสร้างขององค์กรที่เหมาะสมจะช่วยในการปฏิบัติงาน
3. ระบบ (systems) ระบบขององค์กรที่จะบรรลุเป้าหมาย
4. แบบ (styles) แบบของการบริหารเพื่อบรรลุเป้าหมายขององค์กร
5. บุคลากร (staff) ผู้ร่วมองค์กร
6. ความสามารถ (skill)
7. ค่านิยม (shared values) ค่านิยมร่วมของคนในองค์กร

ทีมงานที่ประสิทธิภาพ

ทีมงานหรือกลุ่มทำงานที่มีประสิทธิภาพจะต้องมีความรู้สึกที่ดีต่อกันและกันใน หมู่สมาชิกและผู้ที่เป็นหัวหน้าต้องตระหนักว่าปัญหาส่วนใหญ่เกิดจากสภาพแวดล้อม และความสัมพันธ์ระหว่างบุคคล ดังนั้น ทีมงานที่มีประสิทธิภาพต้องมีเงื่อนไขที่สำคัญ คือ

1. ความรับผิดชอบและความผูกพัน โดยความผูกพันต่อองค์กรเป็นความผูกพัน ใน 3 ลักษณะ คือ
   1.1 ความปรารถนาอย่างแรงกล้าที่จะคงความเป็นสมาชิกในองค์กร
   1.2 มีความตั้งใจและความพร้อมที่จะใช้ความพยายามที่มีอยู่เพื่อองค์กร
   1.3 มีความเชื่อและยอมรับในคุณค่าและเป้าหมายขององค์กร
2. ความจำเป็นที่จะต้องพัฒนาความเข้าใจในความสัมพันธ์ระหว่างบุคคล เนื่องจากบุคคลเกิดความรู้สึกว่าตนเองมีความสำคัญ มีคุณค่าและมีการแลกเปลี่ยน ความคิดแบบริเริ่มสร้างสรรค์กับความก้าวหน้าให้องค์กร
3. ความจำเป็นต้องพัฒนาทักษะ ความสามารถของสมาชิกให้สมาชิกมีความรู้และความชำนาญงาน ตลอดจนเทคนิคการทำงานร่วมกับผู้อื่น
4. มีสิ่งอำนวยความสะดวกให้กับทีมงาน รวมทั้งการมีที่ปรึกษาเป็นบุคคลที่สาม ซึ่งทำหน้าที่เป็นผู้รวบรวมข้อมูล เพื่อพัฒนาการทำงาน ให้ข่าวสารย้อนกลับ แก้ไข ปัญหาความขัดแย้งและการไกล่เกลี่ย

ปัจจัยมีผลต่อประสิทธิภาพในการปฏิบัติงาน

สำหรับแนวคิดเรื่องปัจจัยที่สำคัญในการปฏิบัติงานให้มีประสิทธิภาพหรือปัจจัยที่มีผลต่อการปฏิบัติงาน นั้น มีนักทฤษฎีหลายท่านได้ทำการศึกษาและสรุปเป็นปัจจัยสำคัญ ๆ ที่น่าสนใจดังนี้

เบ็คเกอร์ และนิวเฮาเซอร์ ได้เสนอตัวแบบจำลองเกี่ยวกับประสิทธิภาพขององค์กร (model of organization efficiency) โดยกล่าวว่า ประสิทธิภาพขององค์กรนอกจากจะพิจารณาถึงทรัพยากร เช่น คน เงิน วัสดุ ที่เป็นปัจจัยนำเข้า และผลิตผลขององค์กร คือการบรรลุเป้าหมายแล้วองค์กรในฐานะที่ เป็นองค์กรในระบบเปิด (open system) ยังมีปัจจัยประกอบอีกดงแบบจำลองในรูป สมมติฐานซึ่งสามารถสรุปได้ดังนี้

1. หากสภาพแวดล้อมในการทำงานขององค์กรรความซับซ้อนต่ำ (low task environment complexity) หรือมีความแน่นอน (certainly) มีการกำหนดระเบียบปฏิบัติ ในการทำงานขององค์กรอย่างละเอียดถี่ถ้วนแน่ชัดจะนำไปสู่ความมีประสิทธิภาพของ องค์กรมากกว่าองค์กรที่มีสภาพแวดล้อมในการทำงานยุ่งยากซับซ้อนสูง (high- task environment complexity) หรือมีความไม่แน่นอน (uncertainly)

2. การกำหนดระเบียบปฏิบัติชัดเจนเพื่อเพิ่มผลการทำงานที่มองเห็นได้มีผลทำให้ประสิทธิภาพมากขึ้นด้วย

3. ผลการทำงานที่มองเห็นได้สัมพันธ์ในทางบวกกับประสิทธิภาพ

4. หากพิจารณาควบคู่กันจะปรากฏว่า การกำหนดระเบียบปฏิบัติอย่างชัดเจน และผลของการทำงานที่มองเห็นได้ มีความสัมพันธ์มากขึ้นต่อประสิทธิภาพมากกว่าตัวแปรแต่ละตัวตามลำพัง

Becker ยังเชื่ออีกว่า การสามารถมองเห็นผลการทำงานขององค์กรได้ (visibilitiy consequences) มีความสัมพันธ์ของประสิทธิภาพขององค์กร เพราะองค์กรสามารถทดลองและเลือกระเบียบปฏิบัติได้ ระเบียบปฏิบัติ และผลการปฏิบัติงานมีอิทธิพลต่อ ประสิทธิภาพในการปฏิบัติงาน

แคทซ์ และคาฮ์น ซึ่งเป็นนักทฤษฎีที่ศึกษาองค์กรระบบเปิด (open system) เช่นกันก็ได้ศึกษาในเรื่องปัจจัยที่สำคัญต่อประสิทธิภาพ ในการปฏิบัติงาน เขากล่าวว่า ประสิทธิภาพ คือส่วนประกอบที่สำคัญของประสิทธิผล ประสิทธิภาพ ขององค์กรนั้น ถ้าจะวัดจากปัจจัยนำเข้าเปรียบเทียบกับผลผลิตที่ได้นั้นจะทำให้การวัดประสิทธิภาพ คลาดเคลื่อนจากความเป็นจริงขององค์กร หมายถึง การบรรลุเป้าหมาย (goal attainment) ขององค์กรในการบรรลุเป้าหมายขององค์กรนั้น ปัจจัยต่าง ๆ คือ การฝึกอบรม ประสบการณ์ความผูกพัน ยังมีความสำคัญต่อประสิทธิภาพในองค์กรด้วย

Frederick Hertzberg ได้ศึกษาการบริหารงานในแบบวิทยาศาสตร์โดยได้นำเอาการบริหารงานแบบวิทยาศาสตร์ และความสัมพันธ์ระหว่างผู้ปฏิบัติงานมาศึกษาร่วมกันเพื่อให้ได้ปัจจัยสำคัญที่จะทำให้บุคคล ปฏิบัติงานได้อย่างมีประสิทธิภาพ ดังนั้นเขาจึงได้ศึกษาวิจัยถึงทัศคติของบุคคลที่พอใจ ในการทำงาน และไม่พอใจในการทำงานพบว่า บุคคลที่พอใจในการทำงานนั้นประกอบ ด้วยปัจจัยดังนี้

1. การที่สามารถทำงานได้บรรลุผลสำเร็จ

2. การที่ได้รับการยกย่องนับถือเมื่อทำงานสำเร็จ

3. ลักษณะเนื้อหาของงานเป็นสิ่งที่น่าสนใจ

4. การที่ได้มีความรับผิดชอบมากขึ้น

5. ความก้าวหน้าในการทำงาน

6. การที่ได้รับโอกาสพัฒนาความรู้และความสามารถในการทำงาน

ส่วนปัจจัยที่เกี่ยวกับสิ่งแวดล้อมของงานที่เป็นส่วนที่ทำให้เกิดความไม่พึงพอใจ ประกอบด้วยปัจจัย ดังนี้

1. นโยบายและการบริหารองค์กร (Policy and Administrion)

2. การควบคุมการบังคับบัญชา (Supervision)

3. สภาพการทำงาน (Work Conditions)

4. ความสัมพันธ์ระหว่างบุคคลทุกระดับในหน่วยงาน (Relation with Pee and Subordinate)

5. ค่าตอบแทน (Salary)

6. สถานภาพ (Status)

7. การกระทบกระเทือนต่อชีวิตส่วนตัว (Personal Life)

8. ความปลอดภัย (Security)

7. หน่วยงานหลักและสนับสนุนที่ปฏิบัติงานเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีของประเทศไทย

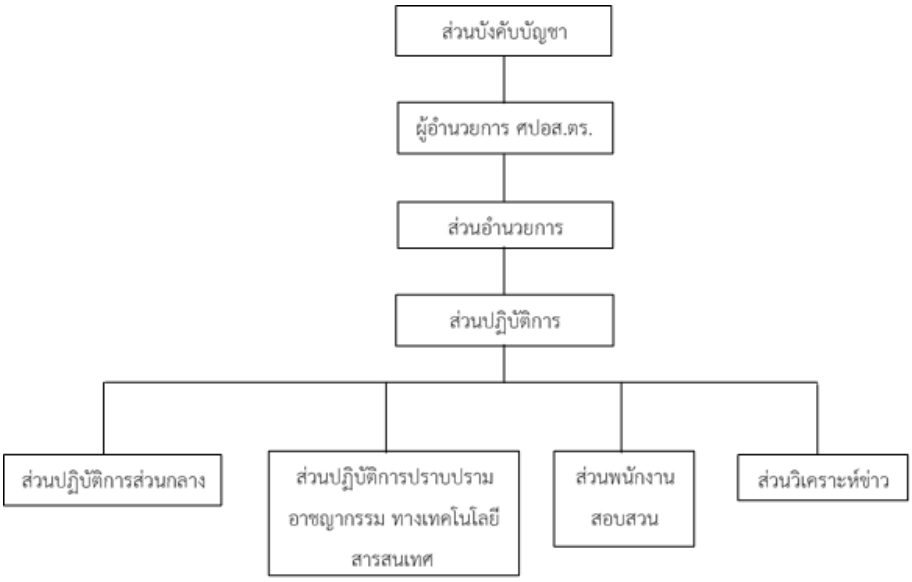
7.1 หน่วยงานหลัก

7.1.1 ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

ความเป็นมา

หน่วยงานที่รวบรวมข้าราชการตำรวจ ที่มีความรู้ความชำนาญมาปฏิบัติงานเพื่อแก้ไขปัญหาอาชญากรรมเทคโนโลยีสารสนเทศและการกระทำความผิดทางอาญา ตาม นโยบายสำนักงานตำรวจแห่งชาติ ปัจจุบันปัญหาอาชญากรรมได้เกิดขึ้นหลายรูปแบบ มีการขยายตัวเป็นวงกว้างและสลับซับซ้อน มีการนำเทคโนโลยีและการสื่อสารต่าง ๆ เข้ามาใช้เป็นเครื่องมือในการ กระทำความผิดรวมทั้งมีแนวโน้มที่บุคคลต่างชาติเข้ามา มีส่วนร่วมในการกระทำความผิดเพิ่มมากขึ้น ซึ่งส่งผลกระทบต่อความปลอดภัยในชีวิตและทรัพย์สินของประชาชน เป็นภัยต่อความมั่นคงและ ระบบเศรษฐกิจของประเทศ จึงจำเป็นต้องมีการบูรณาการระหว่างหน่วยงาน และมีบุคลากรที่มีความรู้ความชำนาญมาสนับสนุนการปฏิบัติงาน ดังนั้นเพื่อให้การบริหารราชการของสำนักงานตำรวจ แห่งชาติในด้านการปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยีสารสนเทศและการกระทำผิดทางอาญาที่เป็นนโยบายของสำนักงานตำรวจแห่งชาติ เป็นไปอย่างรวดเร็วและมีประสิทธิภาพจึงให้จัดตั้ง ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศสำนักงานตำรวจแห่งชาติ

โครงสร้างหน่วยงาน



ภาพที่ 2-2 โครงสร้างหน่วยงานศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.)

7.1.2 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (ปอศ.)

ความเป็นมา

ในปี พุทธศักราช 2496 เมื่อครั้ง พลตำรวจเอกเผ่า ศรียานนท์ ดำรงตำแหน่งอธิบดี กรมตำรวจ ได้มีการเร่งระดมปรับปรุงกรมตำรวจอย่างขนานใหญ่ในปีนั้นเอง ได้มีการจัดตั้งกองการต่างด้าวขึ้น เมื่อวันที่ 20 พฤษภาคม 2496 เพื่อทำหน้าที่ด้านการต่างด้าว และต่อมา ในปี 2498 กรมตำรวจได้มีการปรับเปลี่ยนโครงสร้างองค์กรอีกครั้งหนึ่ง โดยได้มีการปรับปรุงกองการต่างด้าว เป็น กองพิเศษ เพื่อทำหน้าที่ด้านการทะเบียนต่างด้าว และการสืบสวนสอบสวนคดีภาษีอากร จากนั้น ในปี 2503 เมื่อครั้ง จอมพลสฤษดิ์ ธนะรัชต์ ดำรงตำแหน่งอธิบดีกรมตำรวจได้มีการปรับเปลี่ยน กองพิเศษ เป็น กองทะเบียนคนต่างด้าวและภาษีอากร โดยทำหน้าที่ด้านการต่างด้าว และสืบสวนสอบสวนคดีภาษีอากร เหมือนเดิม ต่อมาในปี 2525 ได้เริ่มมีแนวความคิดในการก่อตั้ง กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ เพื่อรองรับการเติบโตและความรุนแรงของอาชญากรรมทางเศรษฐกิจ โดยฝ่ายบริหารและฝ่ายนิติบัญญัติได้มีการศึกษาหาแนวทางปรับปรุงกรมตำรวจเพื่อให้ตอบสนองนโยบายดังกล่าว จนกระทั่ง ในปี 2530 กรมตำรวจ ได้จัดตั้งหน่วยเฉพาะกิจป้องกันปราบปรามอาชญากรรมทางเศรษฐกิจและการเงินขึ้นมาเป็นการชั่วคราว ตามแนวความคิดดังกล่าว ในปี 2532 เมื่อครั้งพลตำรวจเอกเภา สารสิน ดำรงตำแหน่ง อธิบดีกรมตำรวจ คณะรัฐมนตรี ได้มีมติเมื่อวันที่ 30 ธันวาคม 2534 เห็นชอบให้ปรับปรุงกองทะเบียนคนต่างด้าวและภาษีอากร เป็นกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ขึ้นตรงต่อกองบัญชาการตำรวจสอบสวนกลาง กรมตำรวจ เสนอคณะรัฐมนตรีพิจารณา จนกระทั่ง ได้มีพระราชกฤษฎีกาแบ่งส่วนราชการกรมตำรวจ กระทรวงมหาดไทย (ฉบับที่ 20) พ.ศ. 2535

จัดตั้งกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ขึ้น ประกาศในราชกิจจานุเบกษา เล่มที่ 109 ตอนที่ 25 เมื่อวัน 19 มีนาคม 2535 และมีผลใช้บังคับตั้งแต่วันที่ 20 มีนาคม 2535 เป็นต้นไป หลังจากนั้น สำนักงานตำรวจแห่งชาติ ได้มีการปรับเปลี่ยนโครงสร้างครั้งใหญ่ เพื่อพัฒนาและเพิ่มพูนศักยภาพขององค์กร ให้รองรับการเปลี่ยนแปลงของสังคม จึงได้มีพระราชกฤษฎีกาแบ่งส่วนราชการ สำนักงานตำรวจแห่งชาติ พุทธศักราช 2548 และกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจแห่งชาติ พุทธศักราช 2548 ให้เลิกส่วนราชการเดิมตามพระราชกฤษฎีกาแบ่งส่วนราชการกรมตำรวจ กระทรวงมหาดไทย พ.ศ. 2539 แล้วให้จัดตั้งส่วนราชการใหม่นั้นมีผลให้ กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ถูกยกเลิกไปตามนัยดังกล่าว ทั้งนี้ตั้งวันที่ 30 มิถุนายน 2548 และให้จัดตั้งกองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี ขึ้นตั้งแต่วันที่ 30 มิถุนายน 2548 เป็นต้นไป ต่อมาวันที่ 7 กันยายน 2552 สำนักงานตำรวจแห่งชาติได้มีการปรับโครงสร้างอีกครั้งงานเทคโนโลยีถูกแยกออกไปเป็นกองบังคับปราบปรามอาชญากรรมทางเทคโนโลยี ตั้งอยู่ที่ศูนย์ราชการ ถนนแจ้งวัฒนะ ดังนั้น ลักษณะงานจึงคงเป็นคดีเศรษฐกิจเพียงอย่างเดียว โดยใช้หน่วยใหม่ ว่า กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ ชื่อย่อว่า บก.ปอศ.

โดยมีการแบ่งโครงสร้างภายในดังนี้

1. กองกำกับการ 1 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับภาษีทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมาย อื่นที่เกี่ยวข้องกับงานภาษีทุกประเภทและความผิดที่เกี่ยวเนื่องในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือ สนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

2. กองกำกับการ 2 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปราม อาชญากรรมที่เกี่ยวกับภาษีทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมาย อื่นที่เกี่ยวข้องกับงานภาษีทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร ยกเว้นในเขตพื้นที่กรุงเทพมหานคร รวมทั้ง ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

3. กองกำกับการ 3 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปราม อาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญา สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญาและความผิดที่เกี่ยวเนื่อง ในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

4. กองกำกับการ 4 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญาทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สิน

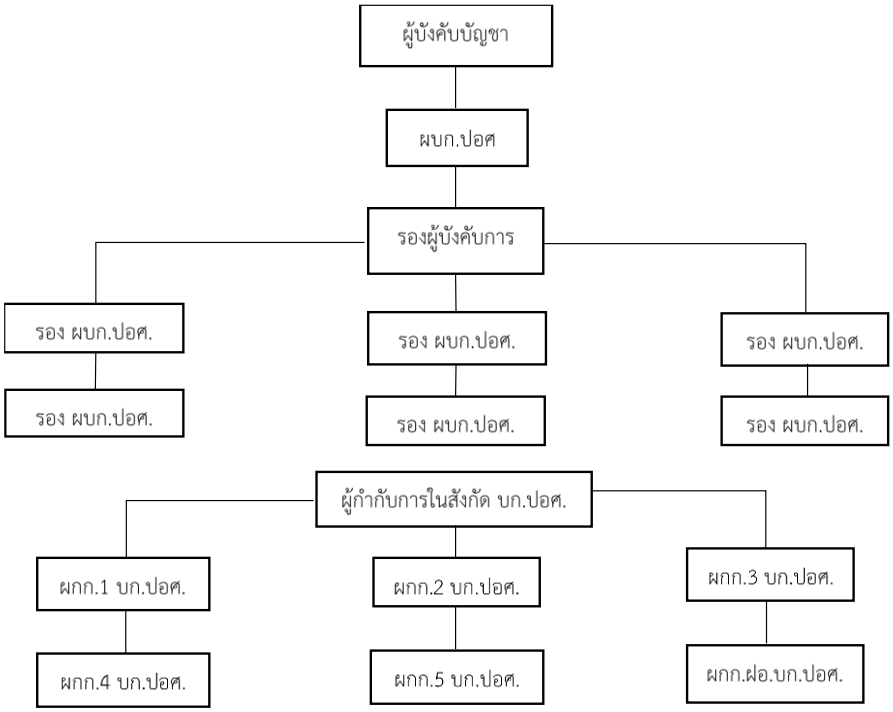
ทางปัญญาทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร ยกเว้นในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

5. กองกำกับการ 5 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับการเงินการธนาคารทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการงานการธนาคารทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

6. กลุ่มงานสอบสวน มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการปฏิบัติตามประมวลกฎหมายวิธีพิจารณาความอาญา สืบสวนสอบสวนการกระทำผิดที่มีโทษทางอาญาเกี่ยวกับอาชญากรรมทางเศรษฐกิจหรือการกระทำความผิดทางอาญาตามกฎหมายอื่นที่เกี่ยวเนื่องทั่วราชอาณาจักร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

7. ฝ่ายอำนวยการ รับผิดชอบงานอำนวยการ และงานธุรการรวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

โครงสร้างหน่วยงาน



ภาพที่ 2-3 โครงสร้างหน่วยงานกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

7.1.3 กองบังคับการการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

ความเป็นมา

ประวัติการจัดตั้งหน่วย เป็นหน่วยงานที่จัดตั้งขึ้นตามโครงสร้างใหม่ เมื่อวันที่ 7 กันยายน 2552 ตามพระราชกฤษฎีกา แบ่งส่วนราชการ สำนักงานตำรวจแห่งชาติ พ.ศ.2552 กฎกระทรวงแบ่งส่วนราชการเป็น กองบังคับการ หรือส่วนราชการอย่างอื่น ในสำนักงานตำรวจแห่ง ชาติ พ.ศ.2552 ระเบียบสำนักงานตำรวจแห่งชาติ ว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการ สำนักงานตำรวจแห่งชาติ พ.ศ. 2552

วัตถุประสงค์

พัฒนา บก.ปอท.ให้เป็นหน่วยงานป้องกันปราบปราม สืบสวนสอบสวนมืออาชีพ มีความทันสมัยเป็นสากล มีมาตรฐานทางจริยธรรมและจรรยาบรรณสูง จนเป็นที่ยอมรับของ ผู้บังคับบัญชา หน่วยงานภาครัฐและเอกชน ตลอดจนประชาชนโดยทั่วไป

นโยบาย

บก.ปอท. มีนโยบายมุ่งเน้น การพัฒนาบุคลากร ให้มีความรู้ความเชี่ยวชาญ ในการสืบสวนสอบสวน ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี มีความรับผิดชอบต่อหน้าที่ มีจิตใจที่เป็นธรรม พัฒนาระบบงานให้สามารถบริการ ประชาชนและหน่วยงานทั้งภาครัฐและเอกชนได้สะดวก รวดเร็ว พัฒนาหน่วยงาน ให้มีเครื่องมือที่ทันสมัยทันต่อเทคโนโลยีที่เปลี่ยนแปลงไป เพื่อให้สามารถสืบสวนสอบสวน ป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้อย่างมีประสิทธิภาพ

อำนาจหน้าที่

มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์

กองกำกับการ 1 : การกระทำผิดที่มุ่งต่อระบบคอมพิวเตอร์เป็นเป้าหมาย

กองกำกับการ 2 : การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด

กองกำกับการ 3 : การนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์ สู่ระบบคอมพิวเตอร์ที่เป็นความผิด

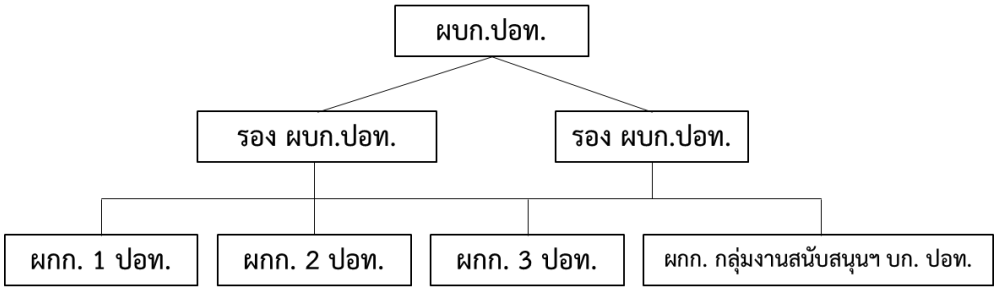
กลุ่มงานสนับสนุนคดีเทคโนโลยี : ปฏิบัติการโต้ตอบในเชิงรุกโดยฉับพลันทางอินเตอร์เน็ตและสนับสนุนคดีเทคโนโลยี

พันธกิจ

- ถวายการรักษาความปลอดภัยสำหรับองค์พระมหากษัตริย์ พระราชินี และพระบรมวงศานุวงศ์
- ป้องกันปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
- รับแจ้งเบาะแสจากประชาชน ตลอดจนให้คำปรึกษา แนะนำ ตลอดจนรวบรวมสภาพปัญหา เพื่อเสนอแนะแนวทางในการป้องกันอาชญากรรมทางเทคโนโลยี

- อำนวยความยุติธรรมโดยยึดหลักนิติธรรม
- รักษาความสงบเรียบร้อยและความมั่นคงภายใน
- หน่วยงานภายในประเทศและต่างประเทศ
- งานอื่นที่ได้รับมอบหมาย

โครงสร้างหน่วยงาน



ภาพที่ 2-4 โครงสร้างหน่วยงานกองบังคับการการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

7.1.4 กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

พันธกิจ

- เสนอนโยบาย แผนระดับชาติ และกฎหมาย ว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ด้านสถิติ ด้านอุตุนิยมวิทยา รวมทั้งด้านความมั่นคงปลอดภัยทางไซเบอร์
- พัฒนาและบริหารจัดการโครงข่ายสื่อสารโทรคมนาคม เพื่อการพัฒนาเศรษฐกิจและสังคมของประเทศ
- ส่งเสริม สนับสนุนการใช้เทคโนโลยีและนวัตกรรม การวิจัยและพัฒนา รวมทั้งการพัฒนากำลังคน ด้านดิจิทัล เพื่อเพิ่มขีดความสามารถในการแข่งขันของประเทศและยกระดับคุณภาพชีวิตของประชาชน
- ส่งเสริม สนับสนุนการนำเทคโนโลยีดิจิทัลมาใช้ในการยกระดับการทำงานของหน่วยงานภาครัฐสู่การเป็นรัฐบาลดิจิทัล
- บริหารจัดการระบบสถิติของประเทศเพื่อสนับสนุนการตัดสินใจ รวมทั้งส่งเสริมและพัฒนาการอุตุนิยมวิทยา ให้มีประสิทธิภาพ ทันต่อเหตุการณ์
- กำกับดูแลและติดตาม ประเมินผลตามนโยบาย แผนระดับชาติ และกฎหมาย ว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ด้านสถิติ ด้านอุตุนิยมวิทยา รวมทั้งด้านความมั่นคงปลอดภัยทางไซเบอร์

อำนาจหน้าที่

พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ 17) พศ. 2559 (เพื่อจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) หมวด 8/1 มาตรา 21/1 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีอำนาจหน้าที่เกี่ยวกับการวางแผนส่งเสริม พัฒนา และดำเนินกิจการเกี่ยวกับดิจิทัลเพื่อเศรษฐกิจและสังคม การอุตุนิยมวิทยา การสถิติ และราชการอื่นตามที่มีกฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หรือส่วนราชการที่สังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

มาตรา 21/2 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีส่วนราชการ ดังนี้

1. สำนักงานรัฐมนตรี
2. สำนักงานปลัดกระทรวง
3. กรมอุตุนิยมวิทยา
4. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ
5. สำนักงานสถิติแห่งชาติ

นอกจากนี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมยังมีหน่วยงาน องค์การมหาชนและรัฐวิสาหกิจในสังกัดอีก 5 แห่งประกอบด้วย

1. บริษัท ทีโอที จำกัด (มหาชน)
2. บริษัท กสท โทรคมนาคม จำกัด (มหาชน)
3. บริษัท ไปรษณีย์ไทย จำกัด
4. สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
5. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

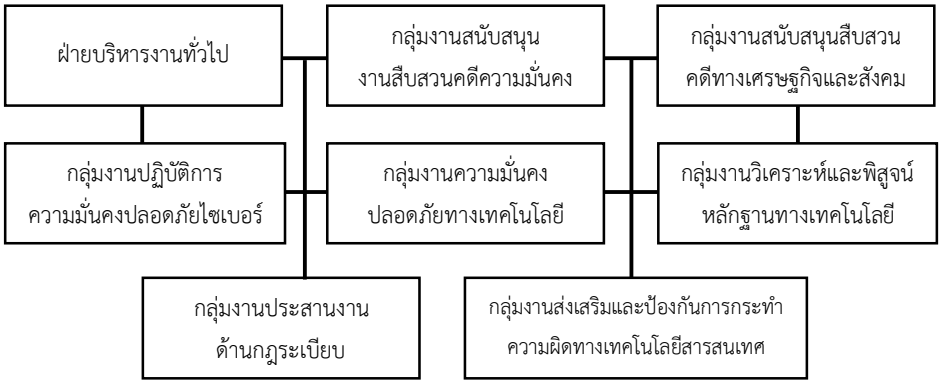
ยุทธศาสตร์

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัล และส่งเสริมการใช้เทคโนโลยีดิจิทัลเพื่อพัฒนาเศรษฐกิจและสังคม

ยุทธศาสตร์ที่ 2 ส่งเสริมการบริหารจัดการองค์กรอย่างมีประสิทธิภาพ

ยุทธศาสตร์ที่ 3 เสริมสร้างความมั่นคงปลอดภัยและความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

โครงสร้างหน่วยงาน



ภาพที่ 2-5 โครงสร้างหน่วยงานกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

7.1.5 สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ

ความเป็นมา

การก่อตั้งกองพิสูจน์หลักฐาน พ.ศ.2475 ขณะนั้นมีประชากรประมาณ 14 ล้านคนได้มีพระบรมราชโองการในพระบาทสมเด็จพระปรมินทรประชาธิปก พระปกเกล้าเจ้าอยู่หัว ได้จัดวางโครงการตำรวจขึ้นใหม่ โดยเปลี่ยนชื่อกรมตำรวจภูธรเป็นกรมตำรวจและให้เสนาบดีกระทรวงมหาดไทย จัดแบ่งแผนงานรายย่อยออกไปตามสมควรแก่รูปการในปีเดียวกันนั้นพระยา จ่าเสนาบดีศรีบริบาล รัฐมนตรีกระทรวงมหาดไทย ได้จัดแบ่งแผนงาน ในกรมตำรวจสำหรับตำรวจสันติบาลนั้นได้ประกาศไว้ดังนี้ ตำรวจสันติบาล มีหัวหน้าเป็นผู้บังคับการหนึ่งนาย แบ่งเป็น กองที่หนึ่ง กองที่สอง กองที่สาม และ กองตำรวจแผนกสรรพกร

กองที่สาม มีระเบียบงานดังนี้

กองนี้เป็นกองวิทยาการตำรวจ ซึ่งต้องใช้ผู้มีความรู้พิเศษ เช่น การตรวจพิสูจน์ลายมือของผู้ต้องหา หรือผู้ที่สมัครเข้ารับราชการว่าเคยต้องโทษมาแล้วหรือไม่ บันทึกประวัติ ของผู้กระทำผิด การตรวจพิสูจน์ของกลางประเภทต่างๆ ออกรูปพรรณของหายและออกประกาศสืบจับผู้ร้ายซึ่งหลบหนี คดีอาญา ซึ่งกองที่สาม ของตำรวจสันติบาล ในสมัยนั้น คือจุดกำเนิดของงานวิทยาการตำรวจ กองที่สามแบ่งออกเป็นสี่แผนก มีอยู่แผนกหนึ่งในกองที่สามเป็นจุดกำเนิด ของงานวิทยาการตำรวจ พ.ศ.2476 ขณะนั้นมีประชากรประมาณ 14 ล้านคน ได้มีพระราชกฤษฎีกาจัดวางระเบียบราชการกรมต่างๆ ในกระทรวงมหาดไทย กำหนดงานของกรมตำรวจขึ้นใหม่ สำหรับกองตำรวจสันติบาล ได้กำหนดไว้ดังนี้

กองกำกับการ 1 สืบสวนปราบปรามโจรผู้ร้าย

กองกำกับการ 2 สืบสวนราชการพิเศษ

กองกำกับการ 3 เทคนิคตำรวจแบ่งออกเป็น 5 แผนก คือ

1. แผนกทะเบียนพิมพ์ลายนิ้วมือ
2. แผนกบันทึกแผนประทุษกรรม

3. แผนกพิสูจน์หลักฐาน
4. แผนกบัญชีโจรผู้ร้าย
5. แผนกเนรเทศ

กองกำกับการ 4 ทะเบียนตำรวจ

พ.ศ.2483 ขณะนั้นมีประชากรประมาณ 16 ล้านคน ได้มีการปรับปรุงและขยายงานของกรมตำรวจ ได้จัดตั้งกองบัญชาการตำรวจสอบสวนกลางขึ้นใหม่ โดยแยกงานทางด้านวิทยาการ ซึ่งเดิมสังกัดอยู่กับกองบังคับการตำรวจสันติบาล มาขึ้นตรงต่อกองบัญชาการตำรวจสอบสวนกลาง

พ.ศ. 2493 ขณะนั้นมีประชากรประมาณ 20 ล้านคน กิจการของตำรวจสอบสวนกลางได้เจริญรุดหน้าไป จึงยกฐานะขึ้นเป็นกองบัญชาการตำรวจสอบสวนกลาง ในกองบัญชาการตำรวจสอบสวนกลางนั้น มีกองกำกับการหนึ่งซึ่งเรียกว่า กองกำกับการวิชาการ และได้ยกฐานะกองกำกับการขึ้นเป็น กองพิเศษ กองพิเศษซึ่งจัดตั้งขึ้นใหม่นี้เป็นรากฐานของ “กองพิสูจน์หลักฐาน” และ “กองทะเบียนประวัติอาชญากร”

พ.ศ.2497 ขณะนั้นมีประชากร ประมาณ 23 ล้านคน กองบัญชาการตำรวจสอบสวนกลางได้มีการปรับปรุง หน่วยงานให้กว้างขวางยิ่งขึ้นโดยเพิ่มกองบังคับการใหม่ขึ้นอีก 4 กอง และมีอยู่กองหนึ่งที่เป็นส่วนหนึ่งของ กองพิสูจน์หลักฐาน และกองทะเบียนประวัติอาชญากร คือ กองวิทยาการ และได้มีการยุบกองพิเศษไปรวม กับกองวิทยาการที่ตั้งขึ้นใหม่ เพื่อต้องการให้การดำเนินงานด้านการพิสูจน์วัตถุพยาน ซึ่งเป็นงานของ กองพิสูจน์หลักฐาน และการตรวจพิสูจน์ค้นคว้าตัวบุคคล ซึ่งเป็นงานกองทะเบียนประวัติอาชญากร รวมอยู่ใน หน่วยเดียวกัน กองวิทยาการ ได้แบ่งออกเป็น 3 กองกำกับการ คือ

กองกำกับการ 1 ประกอบด้วยแผนกถ่ายรูปสถานที่เกิดเหตุ แผนกเอกสารและวัตถุแผนกหอทดลองและแผนกพิพิธภัณฑ์ทางคดี

กองกำกับการ 2 ประกอบด้วยแผนกตรวจสอบพิมพ์ลายนิ้วมือ แผนกตรวจเก็บพิมพ์ลายนิ้วมือ แผนกบัญชีการต้องโทษ แผนกประทุษกรรม

กองกำกับการ 3 ประกอบด้วยแผนกสถิติคดีอาชญากร แผนกสถานดูตัว แผนกสืบจับและของหายได้คืน พ.ศ.2503 ขณะนั้นมีประชากรประมาร 26 ล้านคน กองบัญชาการตำรวจสอบสวนกลางได้มีการปรับปรุงหน่วยงานต่างๆใหม่โดยยุบ “กองวิทยาการ” ซึ่งตั้งมาได้ 8 ปี 4 เดือน 10 วัน ออกจาก สารบบทำเนียบราชการตำรวจ โดยแยกงานของกองนี้ออกเป็น 2 กอง คือ

1. กองพิสูจน์หลักฐาน
2. กองทะเบียนประวัติอาชญากร

โดยการแยกงานด้านการตรวจพิสูจน์วัตถุพยานและงานตรวจพิสูจน์ค้นคว้าในด้านตัวบุคคลออกจากกันและได้มีการปรับปรุงหน่วยงานทั้งสองให้กว้างขวางยิ่งขึ้น ดังนั้น กองพิสูจน์หลักฐานและกองทะเบียนประวัติอาชญากร จึงได้ถือกำเนิดและเป็นหน่วยงานระดับ กองบังคับการขึ้นตรงต่อกองบัญชาการตำรวจสอบสวนกลาง ตามพระราชกฤษฎีกา แบ่งส่วนราชการ กรมตำรวจ ตั้งแต่วันที่ 13 กันยายน พ.ศ.2503 เป็นต้นมา พ.ศ.2535 ได้มีพระราชกฤษฎีกา แบ่งส่วนราชการ กรมตำรวจ กระทรวงมหาดไทย (ฉบับที่ 18)

พ.ศ. 2535 ซึ่งได้ประกาศในราชกิจจานุเบกษา เล่ม 109 ตอนที่ 10 มาตรา 4 จัดตั้งสำนักงานวิทยาการตำรวจ โดยให้สำนักงานวิทยาการตำรวจแบ่งออกเป็น 7 กองบังคับการ คือ

1. กองบังคับการอำนวยการ แบ่งเป็น 3 กองกำกับการ
2. กองพิสูจน์หลักฐาน แบ่งเป็น 6 กองกำกับการ
3. กองทะเบียนประวัติอาชญากร แบ่งเป็น 5 กองกำกับการ
4. กองวิทยาการภาค 1 แบ่งเป็น 4 กองกำกับการ
5. กองวิทยาการภาค 2 แบ่งเป็น 4 กองกำกับการ
6. กองวิทยาการภาค 3 แบ่งเป็น 4 กองกำกับการ
7. กองวิทยาการภาค 4 แบ่งเป็น 4 กองกำกับการ

พ.ศ.2537 โดยมติ ก.ตร. ครั้งที่ 19/2537 เมื่อวันที่ 16 พฤศจิกายน 2537 ได้มีมติอนุมัติเปลี่ยนแปลง การกำหนดตำแหน่งใหม่ในสำนักงานวิทยาการตำรวจ ทำให้ส่วนราชการในสังกัดกองพิสูจน์หลักฐาน มีหน่วยงานเทียบเท่ากองกำกับการเพิ่มขึ้น คือ “ศูนย์ตรวจพิสูจน์ลายนิ้วมือแฝง” ในปี 2548 ได้มีพระราชกฤษฎีกาแบ่งส่วนราชการ สำนักงานตำรวจแห่งชาติ พ.ศ.2548 และ กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนวิชาการ ที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ.2548 เป็นผลให้สำนักงานวิทยาการตำรวจ เปลี่ยนชื่อหน่วยงานเป็น “สำนักงานนิติวิทยาศาสตร์ตำรวจ”ตามกฎหมายดังกล่าว โดยแยกกองทะเบียนประวัติอาชญากรออกไปสังกัดสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ตั้งแต่บัดนั้นเป็นต้นมา ต่อมาในปี 2552 ได้มีพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552 และกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการ หรือส่วนราชการที่เรียกชื่อ อย่างอื่นใน ตร. พ.ศ.2552 ยกเลิกส่วนราชการเดิมและจัดตั้งส่วนราชการใหม่ ประกอบกับมติ ก.ตร. ในการประชุมครั้งที่ 6/2552 เมื่อ 5 มิถุนายน 2552 อนุมัติให้ยุบเลิกตำแหน่งต่างๆ ในส่วนราชการเดิมและกำหนด ตำแหน่งให้กับส่วนราชการใหม่ โดยพระราชกษฎีกานี้ ได้ประกาศในราชกิจจานุเบกษาลง 6 กันยายน 2552 ให้มีผลใช้บังคับ ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไปนั้น เป็นผลให้ สำนักงานนิติวิทยาศาสตร์ตำรวจ เปลี่ยนชื่อหน่วยงานเป็นสำนักงานพิสูจน์หลักฐานตำรวจ และมี หน่วยราชการในสังกัดใหม่ ระดับกองบังคับการ และกองกำกับการดังนี้

1) กองบังคับการอำนวยการ
2) กองพิสูจน์หลักฐานกลาง
3) ศูนย์พิสูจน์หลักฐาน 1-10
4) สถาบันฝึกอบรมและวิจัยการพิสูจน์หลักฐานตำรวจ
5) กองทะเบียนประวัติอาชญากร
6) ศูนย์ข้อมูลวัตถุระเบิด (ผกก.หน.)
7) กลุ่มงานพิสูจน์เอกลักษณ์บุคคล (ผกก.หน.)

ซึ่งทำให้กองพิสูจน์หลักฐานได้เปลี่ยนชื่อหน่วยงานเป็น "กองพิสูจน์หลักฐานกลาง" และได้นำกองทะเบียนประวัติอาชญากรมาสังกัดสำนักงานพิสูจน์หลักฐานตำรวจ ตั้งแต่บัดนั้นเป็นต้นไป

วิสัยทัศน์

“เป็นหลักประกันความยุติธรรม ด้านพิสูจน์หลักฐาน และวิทยาการตำรวจที่มีมาตรฐานสากล”

พันธกิจ

1. เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติในการวางแผน ควบคุม ตรวจสอบให้คำแนะนำและเสนอแนะการปฏิบัติงานตามอำนาจหน้าที่ของ สำนักงานพิสูจน์หลักฐานตำรวจและหน่วยงาน ในสังกัด

2. ดำเนินการเกี่ยวกับการพิสูจน์หลักฐานตำรวจ วิทยาการตำรวจ การตรวจสถานที่เกิดเหตุ การถ่ายรูปการทะเบียนประวัติอาชญากร การจัดเก็บสารบบลายพิมพ์นิ้วมือ และการตรวจสอบประวัติในการกระทำความผิดของผู้ต้องหา และบุคคลทั่วราชอาณาจักร เพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยงานอื่น

3. ดำเนินการเกี่ยวกับการตรวจพิสูจน์เอกลักษณ์ของบุคคล ลารส่งกลับในกรณีเหตุวินาศภัย หรือเหตุพิเศษอื่น

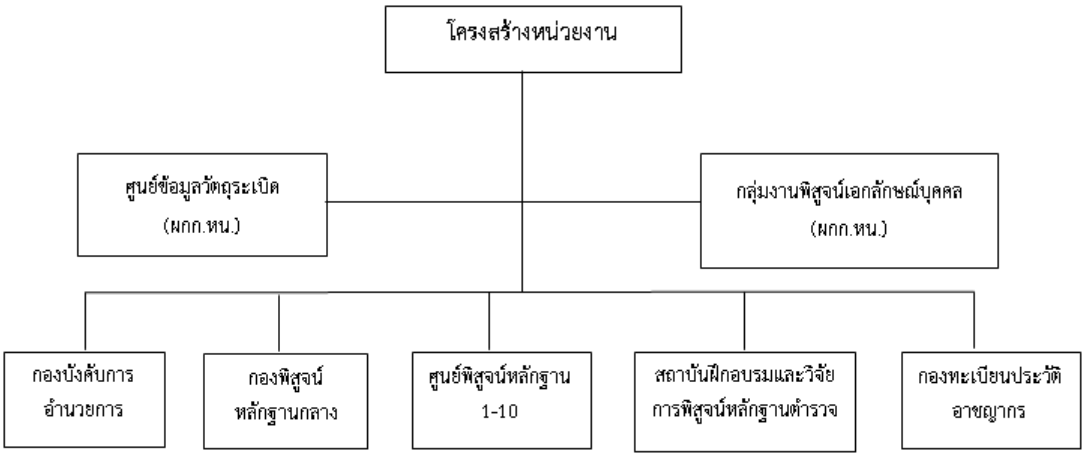
4.ดำเนินงานเกี่ยวกับงานฐานข้อมูลวัตถุระเบิด รวมทั้งสนับสนุนด้านวิชาการ การตรวจพิสูจน์ วิเคระห์ เก็บกู้ และทำลายวัตถุระเบิด เฉพาะกรณีที่มีลักษณะพิเศษ

5. ดำเนินการเกี่ยวกับการฝึกอบรมงานด้านพิสูจน์หลักฐาน และงานด้านวิทยาการตำรวจของสำนักงานตำรวจแห่งชาติ

6. ประสานความร่วมมือกับหน่วยงานของรัฐหรือองค์กรอื่นที่เกี่ยวข้องกับงานพิสูจน์หลักฐานและงานวิทยาการทั้งในและต่างประเทศ

7. ปฏิบัติงานร่วมกันหรือสนับสนุนการปฏิบัติงานของหน่วยงาน อื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

โครงสร้างหน่วยงาน



ภาพที่ 2-6 โครงสร้างหน่วยงานสำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ

7.2 หน่วยงานสนับสนุน

7.2.1 กองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร

ความเป็นมา

บก.สสท. เป็นหน่วยงานจัดตั้งตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552 มีอำนาจหน้าที่ดำเนินการเกี่ยวกับการตรวจสอบการกระทำผิดกฎหมายโดยใช้เครื่องมือเทคโนโลยีสารสนเทศและการสื่อสาร ศึกษา วิเคราะห์ วิจัย และพัฒนาระบบงานเทคโนโลยีสารสนเทศและการสื่อสาร สร้างมาตรฐานด้านคอมพิวเตอร์ ตลอดจนฝึกอบรมเทคโนโลยีสารสนเทศและการสื่อสารให้แก่ข้าราชการตำรวจ พนักงานราชการ และลูกจ้างในสำนักงานตำรวจแห่งชาติ ปฏิบัติงานร่วมกับหรือ สนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือได้รับมอบหมาย โดยได้นำหน้าที่การงานบางส่วนระดับกองกำกับการของศูนย์เทคโนโลยีสารสนเทศกลาง (ศทก.)และหน้าที่การงานของ ศูนย์ตรวจสอบและวิเคราะห์การกระทำผิดทางเทคโนโลยี(ศตท.) มารวมไว้ด้วยกัน ดังนี้

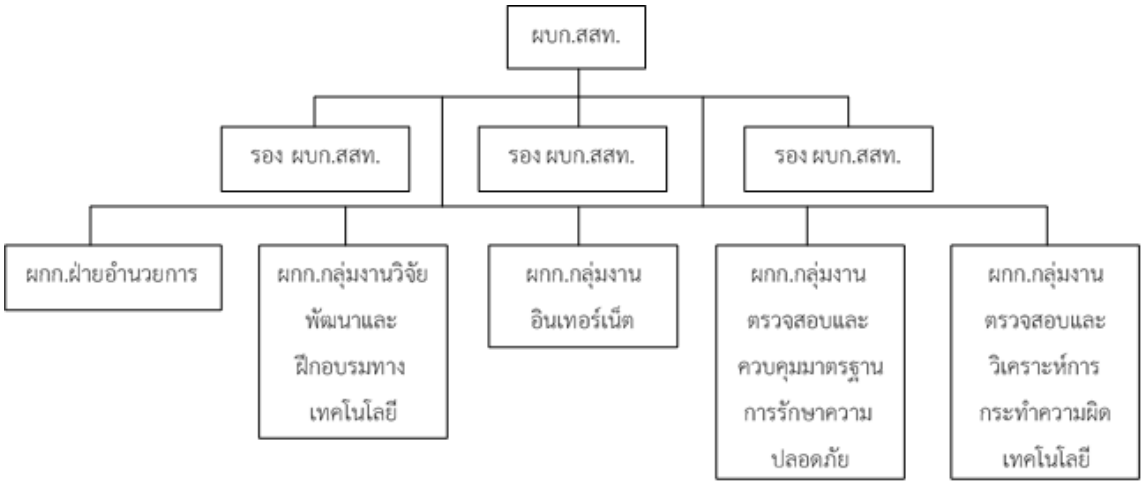
1) ฝ่ายอำนวยการ
2) กลุ่มงานวิจัยพัฒนาและฝึกอบรมเทคโนโลยี
3) กลุ่มงานอินเทอร์เน็ต

เนื่องจากในภาวการณ์ปัจจุบัน การใช้อินเทอร์เน็ตได้เข้ามามีบทบาทและแทบจะถือได้ว่าเป็นปัจจัยที่สำคัญอย่างหนึ่งในการดำเนินชีวิตในปัจจุบัน ทั้งต่อหน้าที่การงาน เพื่อติดต่อสื่อสารระหว่างกัน อีกทั้งเพื่อค้นหาข้อมูลต่างๆ เพื่อพัฒนาหน่วยงานหรือองค์กร ตลอดจนเป็นแหล่งรวบรวมความบันเทิงในรูปแบบต่างๆ อีกทั้งสามารถเป็นตัวชี้วัดได้อีกทางหนึ่งว่าองค์กรของเรานั้นมีศักยภาพ หรือมีประสิทธิภาพเท่าเทียมกับ

องค์กรอื่นได้หรือไม่ ประกอบกับได้มีการกำหนดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ซึ่งมีผลบังคับใช้ตั้งแต่วันที่ 18 กรกฎาคม 2550 ขึ้น

จึงทำให้กลุ่มงานอินเทอร์เน็ตตระหนักและเล็งเห็นความสำคัญของการใช้งานอินเทอร์เน็ตจึงได้เกิดแนวความคิดด้านการจัดระเบียบการใช้และบริหารจัดการอินเทอร์เน็ตให้สามารถบ่งชี้ตำแหน่งของเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ ณ เวลาหนึ่งๆของทุกเครื่องคอมพิวเตอร์ที่เชื่อมต่ออินเตอร์เน็ต ตลอดจนเพื่อตอบสนองความต้องการของบุคลากรในองค์กรให้สามารถ ใช้งานอินเทอร์เน็ตอย่างมีประสิทธิภาพเท่าเทียมกันและทั่วถึง ตลอดจนเพื่อเป็นการลดค่าใช้จ่ายในการจัดหาระบบอินเทอร์เน็ตมาใช้งานของแต่ละหน่วยให้สามารถใช้ทรัพยากรที่มีอยู่ร่วมกันอย่างมีประสิทธิภาพ และสามารถบริหารจัดการหรือซ่อมบำรุงได้อย่างสะดวกและ รวดเร็ว ตามคำสั่ง สตช.ที่ 428/2552 ลงวันที่ 7 ก.ย. 2552 เรื่องแต่งตั้งข้าราชการตำรวจตามิได้มีพราะราชกฤษฎีกาการแบ่งส่วนราชการของสำนักงานตำรวจแห่งชาติ พ.ศ. 2552 และกฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการที่เรียกชื่ออย่างอื่นในสำนักงานตำรวจ แห่งชาติ พ.ศ. 2552 ทำให้กลุ่มงานอินเทอร์เน็ต แต่เดิมสังกัดอยู่กับศูนย์เทคโนโลยีสารสนเทศกลาง มาสังกัดกองบังคับการสนับสนุนทางเทคโนโลยีกลุ่มงานตรวจสอบและควบคุมมาตรฐานการรักษาความปลอดภัย และกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี

โครงสร้างหน่วยงาน



ภาพที่ 2-7 โครงสร้างหน่วยงานกองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร

7.2.2 กรมสอบสวนคดีพิเศษ

ความเป็นมา

สืบเนื่องจากสถานการณ์ของโลกมีการเปลี่ยนแปลงอย่างรวดเร็วการพัฒนาด้านเทคโนโลยีส่งผลกระทบต่อระบบเศรษฐกิจ สังคมการเมืองวัฒนธรรม สิ่งแวดล้อม ตลอดถึงการก่ออาชญากรรม ซึ่งพัฒนาจากการใช้ความรุนแรง เป็นอาชญากรรมที่ก่อให้เกิดความเสียหายทางเศรษฐกิจที่มีมูลค่ามหาศาล ส่งผลกระทบต่อประชาชนเป็นจำนวนมาก การใช้เทคโนโลยีคุณภาพสูงและช่องว่างของกฎหมายปิดบังความผิดของตน มีอิทธิพลและเครือข่ายองค์กร โยงใยทั้งภายในและภายนอกประเทศ ทำให้ยากต่อการสืบสวนสอบสวนดำเนินคดี จึงต้องมีการจัดตั้งกรมสอบสวนคดีพิเศษขึ้นโดยอยู่ภายใต้สังกัดกระทรวงยุติธรรม ก่อตั้งขึ้นเมื่อวันที่ 3 ตุลาคม 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545 ใช้ชื่อภาษาอังกฤษว่า “DEPARTMENT OF SPECIAL INVESTIGATION” มีชื่อย่อว่า “DSI” ซึ่งมีบุคลากรที่มีความรู้ความชำนาญในด้านต่าง ๆ พัฒนารูป แบบการทำงานให้มีประสิทธิภาพ เป็นองค์กรหนึ่งซึ่งเป็นยุทธศาสตร์ในการปฏิรูประบบราชการ ทำให้ประชาชนและประเทศชาติได้รับความเป็นธรรมและประโยชน์สูงสุด

หน่วยงานในสังกัด

1) สำนักบริหารกลาง
2) กองกฎหมาย
3) สำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ
4) สำนักคดีการเงินการธนาคาร
5) สำนักคดีความมั่นคง
6) สำนักคุ้มครองผู้บริโภคและสิ่งแวดล้อม
7) สำนักคดีทรัพย์สินทางปัญญา
8) สำนักคดีเทคโนโลยีและสารสนเทศ
9) สำนักคดีภาษีอากร
10) สำนักคดีการเงินการธนาคาร
11) สำนักคดีอาญาพิเศษ 1
12) สำนักคดีอาญาพิเศษ 2
13) สำนักคดีอาญาพิเศษ 3
14) สำนักเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ
15) สำนักนโยบายและยุทธศาสตร์
16) สำนักปฏิบัติการคดีพิเศษภาค
17) สำนักงานปฏิบัติการพิเศษ
18) สำนักพัฒนาและสนับสนุนคดีพิเศษ

วิสัยทัศน์

"เป็นองค์การหลักในการบังคับใช้กฎหมายกับอาชญากรรมพิเศษตามมาตรฐานสากล"
โดยกำหนดความหมายของวิสัยทัศน์ ดังนี้

การบังคับใช้กฎหมาย หมายถึง การใช้อำนาจการสืบสวนสอบสวนตามที่กำหนดไว้ตามประมวลกฎหมายวิธีพิจารณาความอาญา และพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 และแก้ไขเพิ่มเติม อาชญากรรมพิเศษ หมายถึง อาชญากรรมซึ่งมีลักษณะแตกต่างจากอาชญากรรมพื้นฐาน เป็นอาชญากรรมที่มีความสำคัญและจำเป็นต้องได้รับความสนใจเป็นกรณีพิเศษ โดยมีความละเอียดและซับซ้อน ยุ่งยาก และร้ายแรง อาทิ อาชญากรรมทางเศรษฐกิจ (White Collar Crime) องค์กรอาชญากรรม (Organization Crime) อาชญากรรมข้ามชาติ (Transnational Crime)

มาตรฐานสากล หมายถึง หลักเกณฑ์มาตรฐานที่เป็นไปตามเกณฑ์ตัวชี้วัดหลักนิติธรรมขององค์การสหประชาชาติ (The United Nations Rule of Law Indicators) ประกอบด้วย หลักประสิทธิภาพในการปฏิบัติงาน, หลักความเที่ยงตรง เป็นกลาง ความรับผิดชอบและความโปร่งใส, หลักการคุ้มครองบุคคลที่มีความเสี่ยงต่อการถูกละเมิด และหลักศักยภาพ โดยมีการประเมินด้วยตัวชี้วัด (KPIs) จำนวน 7 ตัว ได้แก่ 1) การบรรลุเป้าหมายและผลผลิต 2) ความเชื่อมั่นจากสังคม 3) การทำงานที่ยึดถือเป้าหมายและความรับผิดชอบร่วมกัน 4) ความโปร่งใส 5) ความพร้อมด้านอุปกรณ์ เครื่องมือ 6) ความพร้อมด้านทรัพยากรบุคคล และ 7) ประสิทธิภาพในการบริหารงาน

ทั้งนี้ การดำเนินการตามมาตรฐานดังกล่าว อยู่บนหลักพื้นฐานของมาตรา 29 (ว่าด้วยการรับโทษทางอาญา) และมาตรา 68 (ว่าด้วยสิทธิของบุคคลในกระบวนการยุติธรรม) ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

พันธกิจ

ป้องกัน ปราบปราม สืบสวน สอบสวนและดำเนินคดีพิเศษอย่างมีประสิทธิภาพด้วยความเป็นธรรม

ภารกิจ

เกี่ยวกับการป้องกัน การปราบปราม การสืบสวนและการสอบสวนคดีความผิดทางอาญาที่ต้องดำเนินการสืบสวนและสอบสวนโดยใช้วิธีการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ

อำนาจหน้าที่

(1) รับผิดชอบงานเลขานุการของคณะกรรมการตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ และกฎหมายที่เกี่ยวข้อง

(2) ป้องกัน ปราบปราม สืบสวน และสอบสวนคดีพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษและตามหลักเกณฑ์ที่คณะกรรมการคดีพิเศษประกาศกำหนดหรือตามมติของคณะกรรมการคดีพิเศษ ตลอดจนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นอันเกี่ยวกับความผิดทางอาญาที่เป็นคดีพิเศษ

(3) ศึกษา รวบรวม จัดระบบ และวิเคราะห์ข้อมูลเพื่อประโยชน์แก่การปฏิบัติหน้าที่ของคณะกรรมการตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ และเพื่อป้องกัน ปราบปราม สืบสวนและสอบสวนคดีพิเศษ

(4) จัดให้มีการศึกษา อบรม และพัฒนาระบบงานการสืบสวนและสอบสวนคดีพิเศษการพัฒนาความรู้และการประเมินสมรรถภาพการปฏิบัติหน้าที่ของข้าราชการ พนักงานราชการและลูกจ้างของกรม และบุคลากรที่เกี่ยวข้อง ไม่ว่าจะมีฐานะเป็นพนักงานสอบสวนคดีพิเศษหรือเจ้าหน้าที่คดีพิเศษหรือไม่

(5) ดำเนินการเกี่ยวกับงานกฎหมายและระเบียบที่อยู่ในอำนาจหน้าที่ของกรมและงานอื่นที่เกี่ยวข้อง

(6) ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกรม หรือตามที่รัฐมนตรี หรือคณะรัฐมนตรีมอบหมาย

โครงสร้างหน่วยงาน

ภาพที่ 2-8 โครงสร้างหน่วยงานกรมสอบสวนคดีพิเศษ

8. หน่วยงานงานป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของต่างประเทศ

คณะผู้วิจัยได้ทำการทบทวนวรรณกรรมของการปฏิบัติงานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในต่างประเทศ ในอเมริกา ยุโรป และเอเชีย เพื่อนำมาทำการปรับปรุงโครงสร้างของหน่วยงานป้องกันและปราบปรามอาชญากรรมของตำรวจ ซึ่งประกอบด้วยประเทศต่าง ๆ ดังนี้

1) สหรัฐอเมริกา
2) ประเทศอังกฤษ
3) ประเทศเยอรมัน
4) ประเทศออสเตรเลีย
5) ประเทศญี่ปุ่น
6) สาธารณรัฐสิงคโปร์
7) ไต้หวัน สาธารณรัฐจีน
8) สาธารณรัฐสังคมนิยมเวียดนาม
9) สาธารณรัฐฟิลิปปินส์

1) สหรัฐอเมริกา

1.1) สำนักงานสอบสวนกลาง (Federal Bureau of Investigation: FBI)

เป็นหน่วยงานด้านข่าวกรองและความมั่นคงภายในของสหรัฐ และเป็นหน่วยงานบังคับใช้กฎหมายในระดับกลางของสหรัฐ ปฏิบัติหน้าที่ภายในเขตอำนาจของกระทรวงยุติธรรมสหรัฐ ทั้งเป็นสมาชิกของประชาคมข่าวกรองสหรัฐ รายงานตรงต่อทั้งอัยการสูงสุดสหรัฐและผู้อำนวยการข่าวกรองแห่งชาติ อนึ่ง เอฟบีไอยังเป็นองค์การหลักของสหรัฐในการต่อต้านการก่อการร้าย การต่อต้านข่าวกรอง และการสืบสวนอาชญากรรม โดยมีเขตอำนาจเหนือการละเมิดกฎหมายในกลุ่มอาชญากรรมกลางกว่า 200 กลุ่ม

สำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. (Washington, D.C.) และยังมีสำนักงานอยู่ตามเมืองยุทธศาสตร์ที่สำคัญอีก 58 แห่ง ทั่วหรัฐอเมริกา และเปอร์โตริโก

โครงสร้างองค์กร

สำนักงานสอบสวนกลาง ผู้ช่วยผู้อำนวยการฝ่ายบริหารมีหน้าที่จัดการสาขาต่าง ๆ แบ่งออกเป็นสาขาการทำงาน ได้แก่

- สาขาข่าวกรอง
- สาขาความมั่นคงแห่งชาติ
- **สาขาอาชญากรรม, ไซเบอร์, ตอบโต้, และบริการ**
- สาขาวิทยาศาสตร์และเทคโนโลยี
- สาขาข้อมูลและเทคโนโลยี
- สาขากำลังพล

อาชญากรรมไซเบอร์

FBI ในส่วนนี้ทำหน้าที่จัดการกับอาชญากรรมไซเบอร์ในลักษณะที่ประสานงาน กับทีมไซเบอร์ที่ได้รับการฝึกมาเป็นพิเศษที่สำนักงานใหญ่ของ FBI และในสำนักงานเขต 56 แห่ง มีเจ้าหน้าที่และตัวแทนวิเคราะห์ที่ปกป้องและตรวจสอบการบุกรุกคอมพิวเตอร์ การโจรกรรมทรัพย์สินทางปัญญาและข้อมูลส่วนบุคคล ภาพอนาจารเด็ก และการฉ้อโกงออนไลน์ มีทีมปฏิบัติการไซเบอร์ใหม่ที่เดินทางไปทั่วโลก เพื่อจัดการปัญหาอาชญากรรมไซเบอร์ที่อันตรายต่อความมั่นคงของประเทศและต่อเศรษฐกิจของอเมริกา

1.2) สำนักข่าวกรองกลาง (Central Intelligence Agency : CIA)

เป็นหน่วยงานราชการด้านข่าวกรองของรัฐบาลกลางสหรัฐ เป็นหน่วยสืบราชการลับมีหน้าที่รวบรวม ประมวลผล และวิเคราะห์ข้อมูลที่เป็นภัยต่อความมั่นคงของชาติจากทั่วโลก โดยผ่านการข่าวกรองทางมนุษย์เป็นส่วนใหญ่ เพื่อรายงานต่อ ผู้อำนวยการข่าวกรองแห่งชาติ และจะเน้นไปที่การหาข่าวกรองให้ประธานาธิบดีสหรัฐ และ คณะรัฐมนตรีสหรัฐ เป็นหลัก

แนวโน้มความเป็นไปในเรื่องต่าง ๆ จะต้องมีนักวิเคราะห์ก็มีหลายตำแหน่ง ดังนี้

นักวิเคราะห์ทางการทหาร – เป็นนักวิเคราะห์ที่จะคอยวิเคราะห์ความเป็นไปทางเรื่องการก่อการร้าย อาวุธสงคราม และความสามารถทางการทหารของประเทศอื่น ๆ ว่าส่งผลต่อทางการทหารของอเมริกาหรือไม่

นักวิเคราะห์ทางการเมือง – เป็นนักวิเคราะห์ที่จะเข้ามาวิเคราะห์ความแปรปรวนทางการเมืองและนอกจากนี้ก็จะยังมีเจ้าหน้าที่ที่เข้าไปวิเคราะห์การเมืองของแต่ละประเทศที่จะเข้าไปตรวจสอบดูนโยบายว่ามีผลต่อสหรัฐอเมริกาอย่างไร ซึ่งเจ้าหน้าที่ที่เข้าไปก็จำเป็นที่จะต้องมีความชำนาญในการใช้ภาษาอย่างแต่ละประเทศนั้นเป็นอย่างดี

นักวิเคราะห์ความเป็นผู้นำ – เป็นฝ่ายที่คอยดูผู้นำของประเทศอื่นเพื่อที่จะเข้าใจอารมณ์และทำให้ง่ายต่อการสานความสัมพันธ์ระหว่างประเทศได้อย่างราบรื่นมากยิ่งขึ้นโดยจะอาศัยหลักจิตวิทยาเข้ามาเกี่ยวข้องด้วย

นักวิเคราะห์ผู้ก่อการร้าย – การวิเคราะห์ด้านนี้จะเข้ามามีส่วนร่วมในเรื่องของการทำนายความเป็นไปได้ขอการก่อการร้ายและสืบหาว่ามีใครบ้างที่สนับสนุนผู้ก่อการร้ายรายนี้ และทำการวิเคราะห์หาแผนการทำงานของผู้ก่อการร้ายและแรงจูงใจในการก่อเหตุแต่ละครั้งด้วย

ลำดับความสำคัญ (พ.ศ. 2556) 5 อย่าง คือ

- การต่อต้านการก่อการร้าย
- การป้องกันการแพร่กระจายของ อาวุธนิวเคลียร์ และ อาวุธอานุภาพทำลายล้างสูงอื่นๆ
- แจ้งเตือน/รายงาน เหตุการณ์ที่สำคัญในต่างประเทศให้แก่ผู้นำของอเมริกา
- ต่อต้านการข่าวกรองของต่างประเทศ
- **การข่าวกรองทางไซเบอร์**
- ไม่สนับสนุนการก่อการร้ายทุกรูปแบบ

โครงสร้างองค์กร

- **กองอำนวยการนวัตกรรมดิจิตัล**
- กองอำนวยการการวิเคราะห์
- กองอำนวยการการปฏิบัติการณ์
- กองอำนวยการสนับสนุน
- กองอำนวยการวิทยาศาสตร์และเทคโนโลยี

2) ประเทศอังกฤษ (England)

ศูนย์รักษาความปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Centre: NCSC)

เพื่อเตรียมพร้อมรับมืออาชญากรรมทางไซเบอร์ จุดประสงค์เพื่อป้องกันการโจมตีระบบโครงสร้างพื้นฐานสำคัญของประเทศ (critical infrastructure) หน่วยงานนี้เป็นหน่วยงานภายใต้กระทรวงดิจิทัลและอุตสาหกรรมเชิงสร้างสรรค์ตั้งอยู่ในกรุงลอนดอน มีผู้เชี่ยวชาญกว่า 700 คน หนึ่งใน**ภารกิจสำคัญของ NCSC คือการร่วมมือกับธนาคารกลางแห่งประเทศอังกฤษ (Bank of England) เพื่อสร้างความตระหนักด้านภัยคุกคามทางไซเบอร์ที่มีผลกระทบกับหน่วยงานด้านการเงิน**

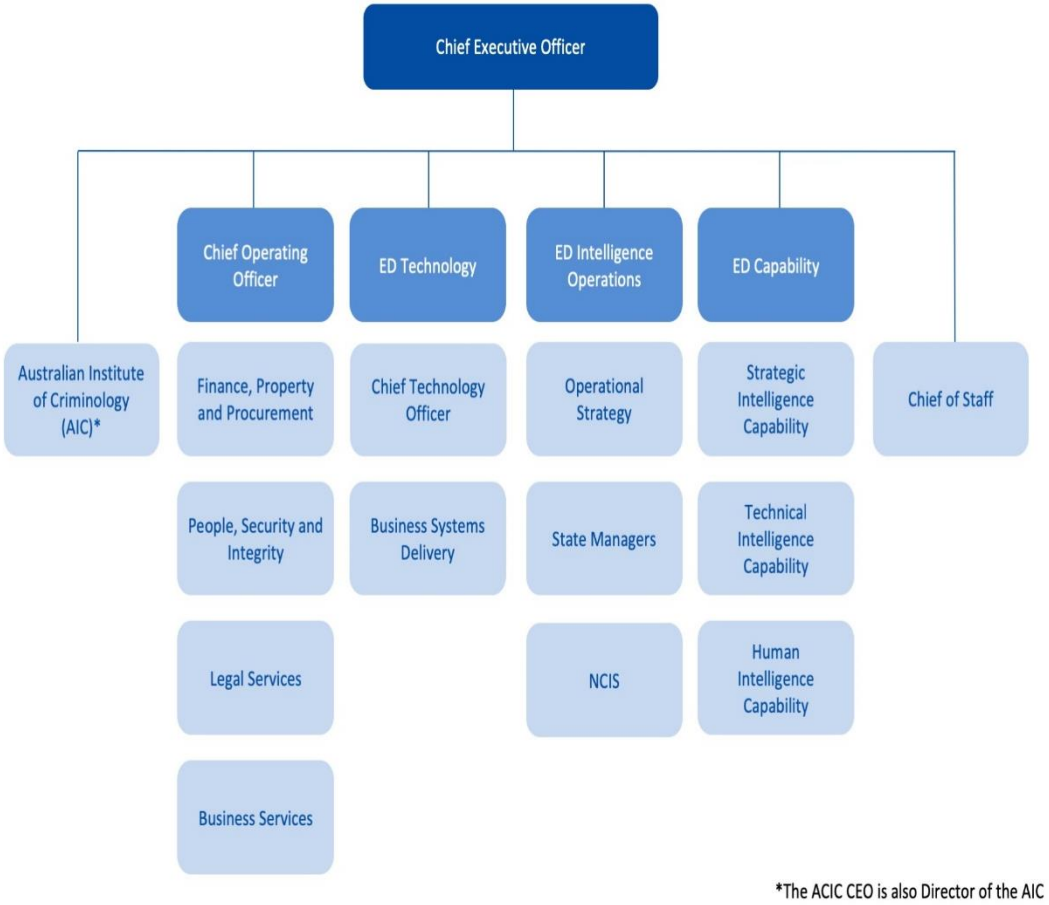
3) สหพันธ์สาธารณรัฐเยอรมนี (Federal Republic of Germany)

สำนักงานความปลอดภัยของข้อมูลแห่งชาติเยอรมัน (Federal Office for Information Security: FOIS)

เป็นหน่วยงานระดับสูงของรัฐบาลเยอรมันที่รับผิดชอบด้านการจัดการความปลอดภัยคอมพิวเตอร์และการสื่อสารสำหรับรัฐบาลเยอรมัน ความเชี่ยวชาญและความรับผิดชอบของหน่วยงาน ครอบคลุมถึงความปลอดภัยของแอปพลิเคชันคอมพิวเตอร์การป้องกันโครงสร้างพื้นฐานที่สำคัญความปลอดภัยของอินเทอร์เน็ต การเข้ารหัสลับการดักฟังการรับรองผลิตภัณฑ์ด้านความปลอดภัยและการรับรองห้องปฏิบัติการทดสอบความปลอดภัย ตั้งอยู่ในกรุงบอนน์และมีพนักงานมากกว่า 600 คน

4) เครือรัฐออสเตรเลีย (The Commonwealth of Australia)

เครือรัฐออสเตรเลียมีองค์กรที่จัดตั้งขึ้นในปี ค.ศ. 2016 มีการจัดตั้ง **The Australian Criminal Intelligence Commission (ACIC)** เพื่อเป็นองค์กรในการดำเนินการ และประสานงานกับตำรวจของแต่ละรัฐ ทางด้านอาชญากรรม โดยทำงานร่วมกับรัฐ ในระดับประเทศและระหว่างประเทศในการสืบสวนและรวบรวมข้อมูล เพื่อปรับปรุงความสามารถระดับชาติในการตอบสนองต่ออาชญากรรมที่ส่งผลกระทบต่อออสเตรเลีย เพิ่มศักยภาพในการรวบรวมข่าวกรอง ให้การสนับสนุนที่สำคัญต่อกลยุทธ์ระดับชาติเพื่อต่อสู้กับอาชญากรรมที่ร้ายแรง และระบบอาชญากรรมไซเบอร์ที่เป็นภัยคุกคามความมั่นคงแห่งชาติ ซึ่งปัจจุบันมีบุคลากรปฏิบัติงานมากกว่า 1,000 คน มีโครงสร้าง ดังนี้



ภาพที่ 2-9 Organizational Structure

ที่มา: https://www.acic.gov.au/about-us/organisational-structure

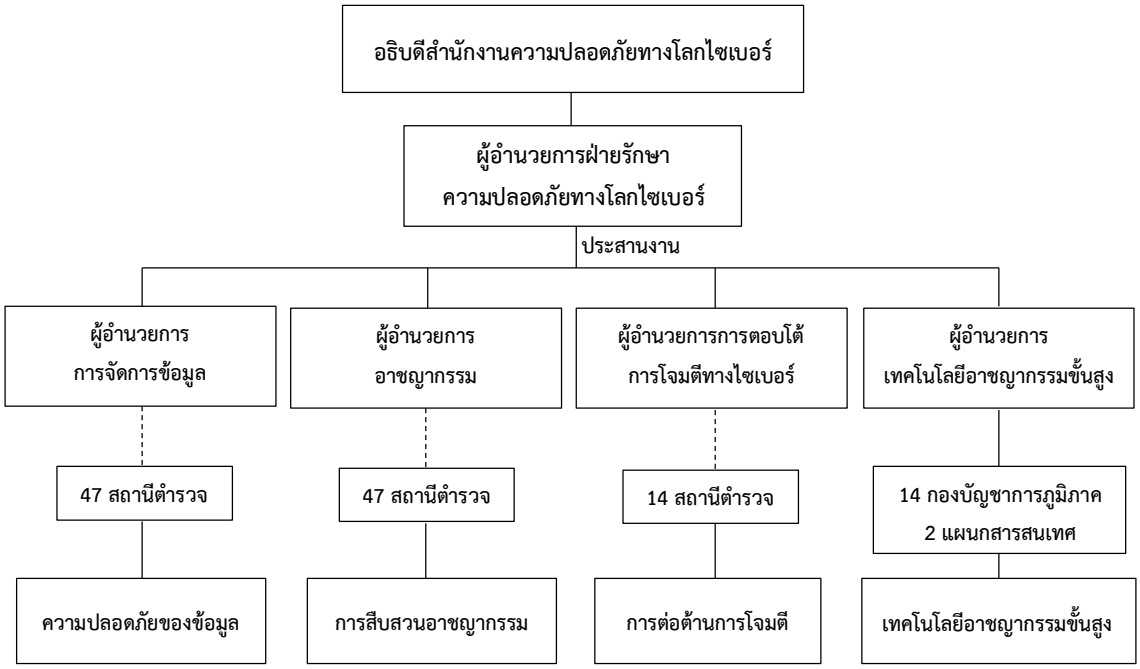
5) ประเทศญี่ปุ่น (Japan)

ประเทศญี่ปุ่นมีหน่วยงานหรือองค์กรที่รับผิดชอบในด้านความปลอดภัยของประชาชน คือ หน่วยงานของตำรวจ แต่มีการแบ่งหน้าที่รับผิดชอบในการดูแลด้านความปลอดภัยทางอาชญากรรมไซเบอร์เป็นการเฉพาะมีกลยุทธ์การรักษาความปลอดภัยทางไซเบอร์เพื่อจัดการกับภัยคุกคามในไซเบอร์สเปซ สร้างระบบที่ใช้ทรัพยากรมนุษย์ และวัสดุที่ดีที่สุดของตำรวจบนพื้นฐานของการคร่อมสายงาน เพื่อให้มีการประสานงานได้อย่างเต็มที่ สอดคล้องกับการเปลี่ยนแปลงในสถานการณ์ทางสังคมอย่างเหมาะสม ในการขจัดภัยคุกคามต่าง ๆ ผ่านความพยายามเชิงรับและเชิงรุก สาระสำคัญของกลยุทธ์มีดังนี้

1) มาตรการเชิงรุกด้วยการวิเคราะห์การเปลี่ยนแปลงของสถานการณ์

2) สร้างความร่วมมือระหว่างผู้มีส่วนได้ส่วนเสียที่หลากหลาย และ

3) สร้างความร่วมมือข้ามพรมแดนและข้ามองค์กร โดยมีโครงสร้างของหน่วยงานความปลอดภัยด้านอาชญากรรมไซเบอร์ ดังนี้



ภาพที่ 2-10 Structural for Cyber Security

ที่มา: Police of Japan (2018)

อาชญากรรมไซเบอร์ทวีความรุนแรง และก่อให้เกิดความเสียหายต่อประเทศต่าง ๆ อย่างมากมาย แต่ละประเทศจึงมีความพยายามในการป้องกัน และปราบปราบอาชญากรรมดังกล่าว ซึ่งต้องอาศัยความร่วมมืออย่างใกล้ชิดของแต่ละประเทศ ในการแลกเปลี่ยนข้อมูล เพื่อให้สามารถตรวจจับ กวาดล้างอาชญากรไซเบอร์เหล่านั้นได้

ภาพที่ 2-11 Organizational Structure of NPA (2018)

ที่มา: Police of Japan, 2018

6) สาธารณรัฐสิงคโปร์ (Republic of Singapore)

หน่วยงานบังคับใช้กฎหมาย

หน่วยงานที่ทำหน้าที่บังคับใช้กฎหมายในการสืบสวนสอบสวนคดีอาชญากรมของสิงคโปร์ มีหลายหน่วยงานด้วยกัน

สำนักงานตำรวจแห่งชาติสิงคโปร์ (Singapore police Force : SPF) เป็นหน่วยงานบังคับใช้กฎหมายอาญาหลักของสิงคโปร์อยู่ภายใต้สังกัดมหาดไทย (Ministry of Home Affairs) มีหน้าที่ในการปกป้องประชาชนที่อาศัยในสิงคโปร์จากอาชญากรรมและอันตรายจากอาชญากรรมทุกรูปแบบ

สำนักงานตำรวจแห่งชาติสิงคโปร์ได้วางวิสัยทัศน์และเป้าหมายว่าจะทำให้สิงคโปร์เป็นประเทศที่ปลอดภัยที่สุดในโลก

สำนักงานตำรวจแห่งชาติสิงคโปร์จัดโครงสร้างองค์กรตามลักษณะงาน ซึ่ง ประกอบด้วย หน่วยอำนวยการ (Staff Department) มี13 หน่วยงาน ได้แก่ กรมกำลังพล กรมกิจการภายใน กรมบริหารและการเงิน กรมส่งกำลังบำรุง ฯลฯ

หน่วยเชี่ยวชาญเฉพาะ (Specialist Staff Departments) มี 3 หน่วยงาน ได้แก่ กรมกิจการค้า (Commercial Affairs Department) กรมสืบสวนสอบสวนอาชญากรรม (Criminal Investigation Department) กรมการข่าวกรองตำรวจ (Police Intelligence Department) และหน่วยเชี่ยวชาญเฉพาะและบังคับบัญชา (Specialist and Line Unit) มี 14 หน่วย ได้แก่ ตำรวจสนามบิน ตำรวจจราจร ตำรวจชายฝั่ง ตำรวจท้องที่ต่าง ๆ

หน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติสิงคโปร์ที่สำคัญและเกี่ยวข้องกับการดำเนินคดีอาญาโดยตรง ได้แก่

กรมสืบสวนสอบสวนคดีอาชญากรรม (Criminal Investigation Department: Co) มีหน้าที่รับผิดชอบคดีอาชญากรรมพิเศษ **อาชญากรรมสำคัญและอาชญากรมทางคอมพิวเตอร์** เช่น การพนันแบบมีเครือข่ายโยงใย (syndicated gambling) สมาคมลับ การละเมิดทรัพย์สินทางปัญญา การลักลอบค้าอาวุธปืน การปล้นและการข่มขืน

กรมกิจการค้า (Commercial Affairs Department CAD) เป็นหน่วยงานสืบสวนคดีอาชญากรรมทางเศรษฐกิจหลักของประทศสิงคโปร์ มีภารกิจในการป้องกันบ้องปราม และสืบสวนจับกุมคดีอาชญากรรมทางเศรษฐกิจ

กรมประสานความร่วมมือระหว่างประเทศ (The International Cooperation Department: ICO) เป็นหน่วยกลางในการติดต่อประสานงานและดำเนินความร่วมมือระหว่างสำนักงานตำรวจแห่งชาติสิงคโปร์กับตำรวจสากล (NTERPOL) และทำหน้าที่เป็นสำนักงานกลางแห่งชาติตำรวจสากล (INTERPOL NATIONAL Central Bureau : NEB) ของสิงคโปร์

7) ประเทศไต้หวัน สาธารณรัฐจีน (Taiwan, Republic of China)

การแบ่งงานของศูนย์อาชญากรรมทางคอมพิวเตอร์ของกรมสืบสวนสอบสวนกระทรวงยุติธรรมไต้หวัน.

- กองนโยบายและแผน
- กองบริหารและงานธุรการ
- กองกำกับดูแลผู้เสียหายจากภัยคุกคามทางคอมพิวเตอร์
- กองกำกับสืบสวนความผิดและป้องกันการกระทำผิดจากอุปกรณ์คอมพิวเตอร์
- กองตรวจสอบอุปกรณ์คอมพิวเตอร์ทางนิติวิทยาศาสตร์
- กองวิเคราะห์และศึกษาให้ความรู้ในการใช้อุปกรณ์คอมพิวเตอร์
- ภารกิจอื่น ๆ และความมั่นคง

8) สาธารณรัฐสังคมนิยมเวียดนาม (The Socialist Republic of Vietnam)

วิวัฒนาการขององค์กรตำรวจเวียดนาม มีความเป็นมาพร้อมกับประวัติศาสตร์ความเปลี่ยนแปลงทางการเมือง การปกครองประเทศ ตั้งแต่ตกเป็นอาณานิคมของฝรั่งเศส กระทั่งการจัดตั้งพรรคคอมมิวนิสต์เวียดนามที่ถือเป็นจุดเปลี่ยนครั้งสำคัญของประวัติศาสตร์การปฏิวัติประเทศ นำไปสู่การกำเนิด **"กองกำลังตำรวจประชาชนเวียดนาม"** มีการก่อตั้งหน่วยงานสำคัญ ได้แก่ หน่วยตำรวจลับ หน่วยบริการตำรวจในภาคเหนือ หน่วยบริการสอดส่องฝ่าระวังในภาคกลาง หน่วยรักษาความปลอดภัยแห่งชาติในภาคใต้ รวมทั้งหน่วยงานตำรวจในเกือบทุกจังหวัดของประเทศที่เป็นหน่วยบริการด้านการข่าวเมื่อมีการรวมประเทศเวียดนามเหนือและเวียดนามใต้เข้าเป็นผืนแผ่นดินเดียวกัน งานรักษาความมั่นคงภายในรวมถึงตำรวจจึงอยู่ภายใต้ความรับผิดชอบของกระทรวงความมั่นคงสาธารณะเวียดนาม โครงสร้างองค์กรของหน่วยงานตำรวจในเวียดนาม แบ่งออกเป็น 4 ระดับ คือ กรมตำรวจเวียดนาม ตำรววจังหวัด ตำรววอำภอ/เขต มีอำนาจสอบสวนดำเนินคดี ตำรวจตำบล/แขวง ไม่มีอำนาจสอบสวน ทำหน้าที่แค่ป้องกันและรับแจ้งเบื้องต้นส่งให้ตำรวจอำเภอ/เขตไปดำเนินกาสอบสวนกำลังพลตำรวจเวียดนามมีประมาณ 280,000 นาย ชั้นยศแบบทหาร มีสถานการศึกษาและฝึกอบรมหลัก คือ โรงเรียนตำรวจประชาชนเวียดนาม การเกษียณอายุของพวกเขาไม่เท่ากัน แบ่งเป็น 3 กลุ่ม ตั้งแต่กลุ่มตำรวจทั่วไปในระดับปฏิบัติการ หรือชั้นประทวน ผู้ชายเกษียณที่อายุ 55 ปี ผู้หญิงเกษียณที่อายุ 5 ปี ผู้บริหารระดับกลาง หรือระดับสารวัตถึงรองผู้บังคับการของไทย ผู้ชายจะเกษียณที่อายุ 58 ปี ผู้หญิงอายุ 53 ปี และผู้บริหาระดับสูงเทียบเท่านายพลขึ้นไปของไทย ผู้ชายจะเกษียณที่อายุ 60 ปี ผู้หญิงอายุ 55 ปี

บทบาทและหน้าที่ของตำรวจเวียดนามในพื้นที่นอกเหนือจากการปฏิบัติหน้าที่ด้านการป้องกันและปราบปรามอาชญากรรมการสืบสวนสอบสวนแล้ว ตำรวจยังมีหน้าที่เกี่ยวข้องกับงานทะเบียนราษฎร์ งานทะเบียนยานพาหนะทั้งรถยนต์ รถจักรยานยนต์อีกด้วย อย่างไรก็ตาม เวียดนามปกครองด้วยระบบสังคมนิยมคอมมิวนิสต์ การสร้างหุ้นส่วนเพื่อความปลอดภัยสารรณะจึงมิได้เป็นไปตามแนวคิดการตำรวจชุมชนแบบใน

ประเทศประชาธิปไตยตะวันวันตก เวียดนามใช้การตำรวจชุมชนเป็นส่วนหนึ่งของระบบควบคุมสังคมมวลชน มีวัตถุประสงค์เพื่อใช้เจ้าหน้าที่ตำรวจต่อประชากรน้อยที่สุด แต่ให้เกิดประสิทธิภาพมากที่สุดในการควบคุมอาชญากรรม ยุทธศาสตร์การตำรวจชุมชนไม่เพียงแต่เป็นวิธีการควบคุมทางสังคมโดยการ สร้างวินัยและให้การศึกษาแก่ประชาชนเท่านั้นแต่ยังเป็นกลไกการเฝ้าระวังที่มีประสิทธิภาพ ตรงนี้เองทำเวียดนามมีอัตราการเกิดอาชญากรรมต่ำ เพราะมีการควบคุมทางสังคมและการตรวจสอบจากรัฐบาลอย่างเข้มงวด

อาชญากรรมคอมพิวเตอร์เป็นอีกปัญหาที่เกิดขึ้นในเวียดนาม มีความซับซ้อนในการกระทำผิดมากขึ้น**มีระดับของคอมพิวเตอร์ส่วนบุคคลที่ติดไวรัสมากในระดับ 7 ของโลก** มีการใช้ซอฟแวร์ที่ไม่ได้รับอนุญาตหรือหมดอายุอย่างแพร่หลาย วายร้ายไซเบอร์ไม่ได้มุ่งโจมตีเพียงปัจเจกบุคคลเพื่อข้อมูลส่วนบุคคลเท่านั้น แต่ยังมีเป้าหมายที่เจาะข้อมูลทางเศรษฐกิจภาคธุรกิจ ข้อมูลทางการเมืองของหน่วยงานรัฐบาลต่างประเทศในเวียดนาม

หน่วยงานบังคับใช้กฎหมาย

หน่วยงานที่รับผิดชอบด้านการบังคับใช้กฎหมายในเวียดนาม คือ สำนักงานตำรวจป้องกันปราบปรามอาชญากรรม (The General Police Department for Crime Prevention and Suppression) อยู่ภายใต้กระทรวงมั่นคง (Ministry of Security) มีหน้าที่รักษากฎหมาย ระเบียบ และความปลอดภัยภายในประเทศป้องกันปราบปรามและสืบสวนอาชญากรรม ให้คำปรึกษาแก่รัฐบาล เกี่ยวกับวิธีการและนโยบายเพื่อป้องกันและปราบปรามอาชญากรรมข้ามชาติ

โครงสร้างของหน่วยงานประกอบด้วย

- สำนักงานกลางเพื่อป้องกันอาชญากรรมและการควบคุมยาเสพติด
- งานสืบสวนอาชญากรรมต่อชุมชนและสังคม
- งานป้องกันปราบปรามการทุจริต
- งานสอบสวนคดีอาชญากรรม
- งานฐานข้อมูลอาชญากรรม
- **งานอาชญากรรมทางคอมพิวเตอร์**
- งานป้องกันปราบปรามยาเสพติด
- งานคดีอาชญากรรมทางเศรษฐกิจ
- งานอาชญากรรมด้านสิ่งแวดล้อม
- งานผู้ลี้ภัย
- งานทรัพยากรมนุษย์
- ตำรวจสากล
- สถาบันนิติวิทยาศาสตร์
- งานด้านการเมืองและส่งบำรุง
- งานด้านความมั่นคงและตรวจตรา

9) สาธารณรัฐฟิลิปปินส์ (Republic of the Philippines)

สำนักงานตำรวจแห่งชาติฟิลิปปินส์ (Philippines National Police: PNP)

สำนักงานตำรวจแห่งชาติฟิลิปปินส์ เป็นหน่วยงานภายใต้กระทรวงมหาดไทยและรัฐบาลท้องถิ่น (Department of Interior and Local Government) มีหน้าที่ในการบังคับใช้กฎหมาย รักษาความสงบเรียบร้อย ป้องกันและสืบสวนคดีอาชญากรรมรวมและนำตัวผู้กระทำผิดเข้าสู่กระบวนการยุติธรม ใช้อำนาจหน้าที่ตามที่รัฐธรรมนูญของฟิลิปปินส์และกฎหมายที่เกี่ยวข้อง กำหนดควบคุมตัวผู้ถูกจับกุมไม่เกินระยะเวลาควบคุม ดำเนินการตามกฎหมายและระเบียบต่าง ๆ ว่าด้วยการควบคุมอาวุธและวัตถุระเบิดและกำกับและควบคุมการฝึกอบรมและการปฏิบัติการของหน่วยงานความมั่นคง

สำนักงานตำรวจแห่งชาติฟิลิปปินส์ มีกำลังพลทั่วประเทศรวมประมาณ 145,000 คน จัดแบ่งองค์กรออกเป็นหลายสาขา ประกอบ

- กลุ่มงานความปลอดภัยทางการบิน (Aviation Security Group)
- หน่วยปฏิบัติการพิเศษ (Special Action Force)
- สำนักงานบริหารจัดการโครงการ (Program Management Office)
- กลุ่มงานตำรวจทางทะเล (Maritime Group)
- กลุ่มงานข่าวกรอง (Intelligence Group)
- กองรักษาความปลอดภัยสาธารณะในภูมิภาค (Regional Public Safe Battalion)
- กลุ่มงานความมั่นคงและคุ้มครอง (Security and Protection Group)
- **กลุ่มงานต่อต้านอาชญากรรมทางคอมพิวเตอร์ (Anti-Cybercrime Group).**
- กลุ่มตำรวจชุมชนสัมพันธ์ (Community Relation Group)
- กลุ่มงานตำรวจทางหลวง (Highway Patrol Group)
- กลุ่มงานความปลอดภัยพลเรือน (Civil Security Group)
- กลุ่มงานต่อต้านการลักพาตัว (Anti - Kidnapping Group)

9. งานวิจัยที่เกี่ยวข้อง

ณรงค์ กุลนิเทศ (2557) ได้ทำการศึกษาวิจัย เรื่อง รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร ผลการวิจัยพบว่า 1. สภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย สามารถแบ่งเป็นประเด็นสำคัญ คือ 1) ปัญหาด้านข้อกฎหมาย - ฐานความผิด - เขตอำนาจ - ใครต้องเป็นผู้รับผิด – ลักษณะพยาน 2) ปัญหาด้านเทคนิค - เทคนิคพัฒนาต่อเนื่อง - การศึกษา – เทคนิคในการเก็บหลักฐาน 3) แนวทางการปฏิบัติ - การประสานแนวทางปฏิบัติ ระหว่าง - ตำรวจ - อัยการ – ศาล 4) วัฒนธรรม – วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ 2. กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ที่สำคัญ เช่น พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น และกำหนดกฎของระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ 4 ข้อ ได้แก่ 1) ความสมบูรณ์ของหลักฐาน 2) ระบุที่มาของหลักฐานได้ 3) บุคคลที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ และ 4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย 3. รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์ ที่สำคัญคือ การนำ ส่งวัตถุพยานในการตรวจพิสูจน์ทางอาชญากรรมไซเบอร์ เช่น อย่าเปิดเครื่องอุปกรณ์ถ้าหากว่าเครื่องปิดอยู่ เป็นต้น ด้านมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ เช่น ควรเร่งการออกกฎหมายให้ครอบคลุม การกระทำความผิด มากขึ้น เป็นต้น

ศิริรัตน์ ศรีสว่าง (2558) ได้ทำการศึกษาวิจัย เรื่อง ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ ผลการวิจัยพบว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ได้รับอิทธิพลจากปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูลและประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน โดยส่งผ่านการรับรู้ต่อสภาวะคุกคาม การรับรู้ความสามารถในการจัดการกับภัยคุกคาม และแรงจูงใจในการป้องกัน โมเดลเชิงสาเหตุพฤติกรรม การป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์มีความไม่แปรเปลี่ยนของรูปแบบโมเดลและค่าพารามิเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ

นูรา ออล มูตาวา (Noora Al Mutawa และคณะ,2561) ได้ทำการศึกษาวิจัยเรื่อง แบบจำลองนิติวิทยาศาสตร์ดิจิทัลเชิงพฤติกรรม: ฝังการวิเคราะห์หลักฐานเชิงพฤติกรรมลงในการสืบสวนอาชญากรรมดิจิตอล ผลการวิจัยพบว่า การปฏิบัติงานที่ล้ำสมัยแสดงให้เห็นถึงการรับรู้ที่เพิ่มขึ้น แต่การยอมรับที่จำกัดของกระบวนการวิเคราะห์หลักฐานเชิงพฤติกรรม (BEA) ภายในกระบวนการสอบสวนทางนิติวิทยาศาสตร์ดิจิทัล (DF) ซึ่งในปัจจุบันยังไม่มีรูปแบบกระบวนการและแนวทางปฏิบัติที่บังคับใช้ BEA สำหรับ ผู้ตรวจสอบ DF เพื่อปฏิบัติตามเพื่อใช้ประโยชน์จากแนวทางดังกล่าว บทความนี้เสนอตัวแบบจำลองนิติวิทยาศาสตร์เชิงพฤติกรรม โดยใช้วิธีการแบบสหวิทยาการซึ่งรวม BEA เข้าสู่การสอบสวนในห้องปฏิบัติการ (เช่น อาชญากรรมทางดิจิทัลที่เกี่ยวข้องกับการปฏิสัมพันธ์ระหว่างมนุษย์กับผู้กระทำความผิดและเหยื่อ) รูปแบบดังกล่าวได้รับ

การออกแบบตามการใช้งานของ BEA แบบดั้งเดิมไปจนถึง การนำมาใช้ใน 35 คดี และประเมินโดยใช้คดีอาชญากรรมดิจิทัลจริง 5 คดี โดยข้อมูลทั้งหมดมาจากคลังข้อมูลตำรวจดูไบ อย่างไรก็ตามบทความนี้ให้รายละเอียดของคดีเดียวเท่านั้นจากกลุ่มคดีนี้ เมื่อเทียบกับผลลัพธ์ของคดีเหล่านี้โดยใช้กระบวนการตรวจสอบ DF แบบใหม่แสดงประโยชน์มากมาย โดยให้มีการมุ่งเน้นการสืบสวนที่มีประสิทธิภาพมากขึ้น และให้ใช้เป็นแนวทางในการระบุตำแหน่งของหลักฐานที่เกี่ยวข้องเพิ่มเติม นอกจากนี้ยังช่วยให้เข้าใจ และตีความพฤติกรรมของเหยื่อ/ผู้กระทำความผิดได้ดีขึ้น (เช่น แรงจูงใจของผู้กระทำผิดที่เป็นไปได้ และวิธีการกระทำ) ซึ่งจะช่วยอำนวยความสะดวกในการทำความเข้าใจเชิงลึกของอาชญากรรมโดยเฉพาะ

ฮูมาร์รา อาชาด (Humaira Arshad และคณะ, 2561) ได้ทำการศึกษาวิจัยเรื่อง การรวบรวมหลักฐาน และ การพิสูจน์หลักฐานทางเครือข่ายสังคมออนไลน์ : ความท้าทายและทิศทางการวิจัย พบว่า หลักฐานของ Social Media (SM) เป็นขอบเขตใหม่และเกิดขึ้นอย่างรวดเร็วในนิตินิติวิทยาศาสตร์ เส้นทางของข้อมูลดิจิตอลบนโซเชียลมีเดียหากสำรวจอย่างถูกต้องสามารถให้การสนับสนุนในการสืบสวนคดีอาชญากรรม อย่างไรก็ตาม การสำรวจเครือข่ายสังคมออนไลน์เพื่อหาหลักฐานที่เป็นไปได้และการนำเสนอหลักฐานเหล่านี้ในชั้นศาลนั้นไม่ใช่เรื่องง่าย โดยหลักฐานทางโซเชียลมีเดียจะต้องรวบรวมโดยกระบวนการทางนิติวิทยาศาสตร์ที่เหมาะสมตามกฎหมาย และสอดคล้องกับสิทธิความเป็นส่วนตัวของบุคคลการปฏิบัติตามกระบวนการทางกฎหมายเป็นงานที่ท้าทายสำหรับผู้ปฏิบัติงานด้านกฎหมาย และผู้ตรวจสอบ เนื่องจากลักษณะของเครือข่ายสังคมออนไลน์ที่มีการเปลี่ยนแปลง และมีความหลากหลาย ผู้ตรวจสอบทางนิติวิทยาศาสตร์สามารถดำเนินการตรวจสอบ รวบรวมหลักฐานทางกฎหมายที่มีประสิทธิภาพหากมีเครื่องมือที่ทันสมัยในการจัดการความหลากหลายและขนาดของเนื้อหาเครือข่ายสังคมออนไลน์ บทความนี้ อธิบายถึงสถานะปัจจุบันของการได้รับหลักฐานการยอมรับและเขตอำนาจศาลในการพิสูจน์หลักฐานทางโซเชียลมีเดีย นอกจากนี้ยังอธิบายถึงความท้าทายสำหรับการรวบรวมการวิเคราะห์การนำเสนอและการตรวจสอบความถูกต้องของหลักฐานสื่อสังคมออนไลน์ในกระบวนการทางกฎหมาย และมีการนำเสนอช่องว่างการวินิจฉัยในโดเมนและวัตถุประสงค์การวิจัยเล็กน้อยที่มีทิศทางการวิจัยที่เป็นไปได้

บทที่ 3
วิธีดำเนินการวิจัย

การศึกษาวิจัย เรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามทางเทคโนโลยี ผู้วิจัยได้นำเสนอประเด็นต่าง ๆ ในการดำเนินการวิจัย โดยมีรายละเอียดดังต่อไปนี้

1. ระเบียบวิธีวิจัย
2. ประชากรและกลุ่มตัวอย่าง
3. เครื่องมือในการวิจัย
4. การเก็บรวบรวมข้อมูล
5. การวิเคราะห์ข้อมูล
6. แผนการดำเนินงานวิจัย
7. การจัดกิจกรรมประชุมกลุ่มย่อย
8. การสัมภาษณ์เชิงลึก

1. ระเบียบวิธีวิจัย

การศึกษาวิจัยนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative research) โดยการจัดการสนทนากลุ่มย่อย (focus group discussion) มาดำเนินการ และหลังจากนั้นผู้วิจัยจะนำข้อค้นพบที่ได้รับมาถอดบทเรียน โดยนำแนวคิดทฤษฎีที่เกี่ยวข้องที่ได้จากการศึกษาเอกสาร และงานวิจัยที่เกี่ยวข้อง จึงทำการสัมภาษณ์แบบเจาะลึก (in-depth interview) จากผู้แทนจากหน่วยงานต่าง ๆ ที่ทำหน้าที่เกี่ยวข้องกับการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามทางเทคโนโลยี ที่ทำหน้าที่ด้านการบริหาร และดำเนินการจัดการสนทนากลุ่มย่อย (focus group discussion) แล้ว โดยจะจัดขึ้น ณ กรุงเทพมหานคร รวม 3 ครั้ง

2. ประชากรและกลุ่มตัวอย่าง

ผู้วิจัยคัดเลือกจากประชากรซึ่งมีประสบการณ์เกี่ยวกับการทำสำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี รวมทั้ง การพัฒนาหน่วยงานตำรวจ ที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยเลือกจากผู้ที่มีความรู้ และประสบการณ์ที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี การวิจัยประเภทนี้ จะเป็นกลุ่มตัวอย่าง ที่เป็นผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญพิเศษเฉพาะด้านที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี สอดคล้องกับประเภทของอาชญากรรมไซเบอร์ ซึ่งแบ่งออกเป็น 2 กลุ่ม ดังนี้

1) กลุ่มตัวอย่างที่ใช้ในการสัมภาษณ์เชิงลึก ได้แก่

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) พนักงานสอบสวน ฝ่ายสืบสวน และฝ่ายป้องกันและปราบปรามของสถานีตำรวจนครบาล และสถานีตำรวจภูธร

(3) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

(4) อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมทางเทคโนโลยี

2) กลุ่มตัวอย่างที่ใช้ในการประชุมกลุ่มย่อย (focus group) ได้แก่

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) เจ้าหน้าที่ตำรวจกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจ

(3) เจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(4) เจ้าหน้าที่ตำรวจสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.)

(5) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES)

3. เครื่องมือในการวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยเลือกใช้เครื่องมือในการศึกษาครั้งนี้ คือ การดำเนินการสัมภาษณ์เชิงลึกและการประชุมกลุ่มย่อย (focus group) เกี่ยวกับการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมทั้งความรู้ ประสบการณ์ และความเชี่ยวชาญทางด้านกฎหมาย การทำสำนวนการสอบสวน รายงานการสืบสวน การรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล ภัยบนอินเตอร์เน็ต และรูปแบบการกระทำผิดทางด้านอาชญากรรมทางเทคโนโลยี เพื่อค้นหาแนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดย มีประเด็นในการวิเคราะห์ ดังนี้

ประเด็นที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสัมภาษณ์

ประเด็นที่ 2 ประเด็นเกี่ยวกับแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ประเด็นที่ 3 ประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ

ประเด็นที่ 4 ประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 5 ประเด็นเกี่ยวกับสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 6 ข้อเสนอแนะเพิ่มเติม

ขั้นตอนการสร้างเครื่องมือที่ใช้ในการวิจัย

1) ศึกษาแนวคิด และทฤษฎี เอกสารงานวิจัยที่เกี่ยวข้องต่าง ๆ เพื่อเป็นแนวทางในการสร้างเครื่องมือที่ใช้ในการวิจัยตามรายละเอียดที่เสนอข้างต้น

2) สร้างแบบสัมภาษณ์ให้ครอบคลุมกรอบแนวความคิดในการวิจัย ซึ่งจะต้องครอบคลุมและสอดคล้องกับวัตถุประสงค์สำหรับการวิจัยที่กำหนดไว้

3) นำเครื่องมือที่ใช้ในการวิจัยเสนอต่อผู้ทรงคุณวุฒิ เพื่อพิจารณาตรวจสอบความถูกต้อง ความสมบูรณ์ของเนื้อหา และความเหมาะสมของความหมาย และภาษาที่ใช้

4. การเก็บรวบรวมข้อมูล

ผู้วิจัยได้กำหนดการเก็บรวบรวมข้อมูลโดยทำการถอดบทเรียนจากการจัดการประชุมกลุ่มย่อยโดยการนำข้อมูลที่กระจัดกระจายอยู่ในตัวบุคคลหรือเอกสาร มาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์การสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพโดยความรู้มี 2 ประเภท คือ ความรู้ที่ฝังอยู่ในคน (Tacit Knowledge) เป็นความรู้ที่ได้จากประสบการณ์พรสวรรค์หรือสัญชาตญาณของแต่ละบุคคลในการทำความเข้าใจในสิ่งต่าง ๆ เป็นความรู้ที่ไม่สามารถถ่ายทอดออกมาเป็นคำพูดหรือลายลักษณ์อักษรได้โดยง่าย เช่น ทักษะในการทำงาน หรือการคิดเชิงวิเคราะห์ บางครั้งจึงเรียกว่าเป็นความรู้แบบนามธรรม และความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่สามารถรวบรวมถ่ายทอดได้โดยผ่านวิธีต่าง ๆ เช่น การบันทึกเป็นลายลักษณ์อักษร ทฤษฎี คู่มือต่าง ๆ และบางครั้งเรียกว่าความรู้แบบรูปธรรม ซึ่งการถอดบทเรียนในครั้งนี้จะเป็นการถอดบทเรียนเฉพาะประเด็นที่สำคัญ และเน้นกิจกรรมที่สำคัญในการปฏิบัติงาน โดยสามารถนำผลการถอดบทเรียนจากกิจกรรมนี้ไปใช้เพื่อเป็นประโยชน์ในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้ประสบความสำเร็จในอนาคต

5. การวิเคราะห์ข้อมูล

ผู้วิจัยได้นำผลการศึกษาดังกล่าวข้างต้นมาดำเนินการวิเคราะห์ข้อมูล โดยใช้วิธีการวิเคราะห์โดยการนำข้อมูลต่าง ๆ ที่ได้จากการศึกษามาพัฒนาเป็นองค์ความรู้ทางทฤษฎีซึ่งเป็นข้อมูลปลายเปิด (open ended)

6. แผนการดำเนินงานวิจัย

ตารางที่ 3-1 แผนการดำเนินงานวิจัย

ที่	รายละเอียดกิจกรรม	ระยะเวลาการดำเนินงาน (เดือน)											
		1	2	3	4	5	6	7	8	9	10	11	12
1	**การดำเนินการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่าง** - ศึกษาถึงการดำเนินงานทางด้านอาชญากรรมทางเทคโนโลยีในสถานการณ์ปัจจุบัน และกรณีศึกษาที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี	✓	✓										
2	**จัดการประชุมครั้งที่ 1 ณ กรุงเทพมหานคร** - ศึกษารวบรวมระเบียบ กฎหมายจากเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้อง - ศึกษากรณีศึกษาคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีที่สำคัญ หรือเป็นที่น่าสนใจที่เกิดขึ้นในปัจจุบัน รวมทั้งกรณีศึกษาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ทันสมัย			✓	✓	✓							
3	**จัดการประชุมครั้งที่ 2 ณ กรุงเทพมหานคร** - ศึกษารวบรวมระเบียบ กฎหมายจากเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้อง - ศึกษากรณีศึกษาที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี - ศึกษาการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี						✓	✓	✓				
4	**จัดประชุมครั้งที่ 3 ณ กรุงเทพมหานคร** - ศึกษารวบรวมระเบียบ กฎหมายจากเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้อง - ศึกษากรณีศึกษาที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี - ศึกษาการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี									✓	✓		
5	- จัดทำเล่มฉบับสมบูรณ์ และคู่มือการพัฒนาการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำเสนอ สกว.											✓	✓

7. การจัดกิจกรรมประชุมกลุ่มย่อย

การจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) ประชุมร่วมกันระหว่างทีมถอดบทเรียนโดยเชิญกลุ่มเป้าหมาย เพื่อปรับปรุงและเสนอแนะงานวิจัยให้มีความสมบูรณ์มากยิ่งขึ้น โดยได้จัดขึ้น ณ กรุงเทพมหานคร รวม 3 ครั้ง มีรายละเอียด ดังนี้

ครั้งที่ 1 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 มกราคม พ.ศ. 2562

ครั้งที่ 2 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 7 สิงหาคม พ.ศ. 2562

ครั้งที่ 3 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 สิงหาคม พ.ศ. 2562

7.1 การจัดกิจกรรมประชุมกลุ่มย่อย ครั้งที่ 1

โดยมีวัตถุประสงค์ของการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) เพื่อให้ผู้เข้าร่วมประชุมกลุ่มย่อยเกี่ยวกับการศึกษารวบรวมระเบียบ กฎหมาย จากเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้อง ศึกษากรณีศึกษาคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีที่สำคัญ หรือเป็นที่น่าสนใจที่เกิดขึ้นในปัจจุบัน รวมทั้งกรณีศึกษาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ทันสมัย จากการเข้าร่วมกิจกรรมการประชุมกลุ่มย่อย และการเล่าเรื่องจากผู้เข้าร่วมเพื่อการแสดงความรู้ และประสบการณ์ คณะผู้วิจัยได้ทำการถอดบทเรียน และสกัดความรู้ที่ได้จากการจัดประชุมแลกเปลี่ยนเรียนรู้ เพื่อนำเสนอเป็นบันทึกการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) เป็นรายบุคคล โดยจัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 มกราคม พ.ศ. 2562 ณ ห้องประชุม 26109 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา






ภาพที่ 3-1 การจัดประชุมกลุ่มย่อย ครั้งที่ 1 เมื่อวันที่ 14 มกราคม พ.ศ. 2562 ณ ห้องประชุมคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

7.2 การจัดกิจกรรมประชุมกลุ่มย่อย ครั้งที่ 2

โดยมีวัตถุประสงค์ของการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) เพื่อให้ผู้เข้าร่วมประชุมกลุ่มย่อยเกี่ยวกับการศึกษากรณีศึกษาคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีที่สำคัญ หรือเป็นที่น่าสนใจที่เกิดขึ้นในปัจจุบัน รวมทั้งกรณีศึกษาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ทันสมัย จากการเข้าร่วมกิจกรรมการประชุมกลุ่มย่อย และการเล่าเรื่องจากผู้เข้าร่วมเพื่อการแสดงความรู้ และประสบการณ์ คณะผู้วิจัยได้ทำการถอดบทเรียน และสกัดความรู้ที่ได้จากการจัดประชุมแลกเปลี่ยนเรียนรู้ เพื่อนำเสนอเป็นบันทึกการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) โดยจัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 7 สิงหาคม พ.ศ. 2562 ณ ห้องประชุม 26109 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

ภาพที่ 3-2 การจัดประชุมกลุ่มย่อย ครั้งที่ 2 เมื่อวันที่ 7 สิงหาคม พ.ศ. 2562 ณ ห้องประชุมคณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

7.3 การจัดกิจกรรมประชุมกลุ่มย่อย ครั้งที่ 3

โดยมีวัตถุประสงค์ของการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) เพื่อให้ผู้เข้าร่วมประชุมกลุ่มย่อยเกี่ยวกับการศึกษากรณีศึกษาในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ทันสมัย จากการเข้าร่วมกิจกรรมการประชุมกลุ่มย่อย และการเล่าเรื่องจากผู้เข้าร่วมเพื่อการแสดงความรู้และประสบการณ์ คณะผู้วิจัยได้ทำการถอดบทเรียน และสกัดความรู้ที่ได้จากการจัดประชุมแลกเปลี่ยนเรียนรู้เพื่อนำเสนอเป็นบันทึกการจัดกิจกรรมประชุมกลุ่มย่อย (Focus Group) เป็นรายบุคคล โดยจัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 สิงหาคม พ.ศ. 2562 ณ ห้องประชุม 26109 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

8. การสัมภาษณ์เชิงลึก

ผู้วิจัยเลือกใช้เครื่องมือในการดำเนินการสัมภาษณ์เชิงลึก เพื่อค้นหาแนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดย มีประเด็นในการวิเคราะห์ดังนี้

ประเด็นที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสัมภาษณ์

ประเด็นที่ 2 ประเด็นเกี่ยวกับแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ประเด็นที่ 3 ประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ

ประเด็นที่ 4 ประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 5 ประเด็นเกี่ยวกับสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ประเด็นที่ 6 ข้อเสนอแนะเพิ่มเติม

โดยมีกลุ่มตัวอย่างที่ใช้ในการสัมภาษณ์เชิงลึก ได้แก่

(1) ตัวแทนของผู้บริหารหน่วยงานตำรวจของสถานีตำรวจนครบาล และสถานีตำรวจภูธร รวมทั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

(2) พนักงานสอบสวน ฝ่ายสืบสวน และฝ่ายป้องกันและปราบปรามของสถานีตำรวจนครบาล และสถานีตำรวจภูธร

(3) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

(4) อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมทางเทคโนโลยี

บทที่ 4
ผลการวิจัย

การศึกษาวิจัย เรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
2. เพื่อกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
3. เพื่อสร้างองค์ความรู้และคู่มือการพัฒนางานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

การศึกษาวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ โดยทำการวิจัยที่เกี่ยวกับการมีส่วนร่วม จัดให้มีประชุมกลุ่มย่อยจำนวน 3 ครั้ง รวมทั้งการสัมภาษณ์แบบเจาะลึกผู้ให้ข้อมูลเป็นผู้ทรงคุณวุฒิจากอดีตผู้บัญชาการสำนักงานพิสูจน์หลักฐานตำรวจ อดีตผู้ทรงคุณวุฒิสำนักงานตำรวจแห่งชาติ ผู้แทนสำนักงานอธิบดีผู้พิพากษาภาค 7 ผู้แทนจากสำนักงานอัยการพิเศษฝ่ายคดีอาญา 2 สำนักงานอัยการสูงสุด ผู้แทนจากกรมสอบสวนคดีพิเศษ ผู้แทนจากกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม ผู้แทนจากสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ผู้แทนจากพนักงานสอบสวนในสังกัดกองบัญชาการตำรวจนครบาล ผู้แทนจากพนักงานสอบสวนในสังกัดกองบัญชาการตำรวจภูธร และผู้เชี่ยวชาญการพิสูจน์หลักฐานทางอาชญากรรมไซเบอร์ ศูนย์พิสูจน์หลักฐาน 7 สำหรับการประชุมกลุ่มย่อยจำนวน 3 ครั้ง มีรายละเอียด ดังนี้

ครั้งที่ 1 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 มกราคม 2562

ครั้งที่ 2 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 7 สิงหาคม 2562

ครั้งที่ 3 จัดการประชุมที่กรุงเทพมหานคร เมื่อวันที่ 14 สิงหาคม 2562

ได้ทำการทบทวนวรรณกรรมทั้งต่างประเทศและในประเทศ ได้ผลการวิจัยโดยสรุปในประเด็นตามวัตถุประสงค์ ดังต่อไปนี้

1. การศึกษาพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากผลการศึกษาวิจัยที่ได้จากการจัดประชุมกลุ่มย่อย และการสัมภาษณ์เชิงลึก นักวิจัยได้ตั้งประเด็นในการศึกษาเพื่อนำมาเป็นแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ดังนี้

1) แนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยมีประเด็นศึกษาให้ได้ข้อมูลเพิ่มเติม คือ

- ด้านบุคลากร (เช่น การขาด/เพิ่มกำลังพลให้สอดคล้องกับการปฏิบัติหน้าที่)
- ด้านการฝึกอบรม (เช่น การจัด หรือเข้าร่วมการอบรมให้กับเจ้าหน้าที่ตำรวจ เพื่อเสริมสร้างทักษะความรู้ต่างๆ)
- ด้านงบประมาณ (เช่น เพิ่มงบประมาณในการทำสื่อประชาสัมพันธ์ให้ประชาชนรับทราบถึงภัยของอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ)
- ด้านเครื่องมือและอุปกรณ์ (เช่น เพิ่มอุปกรณ์ในการสืบสวน หาข่าว และการจัดเก็บวัตถุพยานต่าง ๆ เป็นต้น)
- ด้านเทคโนโลยี (เช่น ติดตั้ง และปรับปรุงซอฟต์แวร์ที่ช่วยในการทำงานเพิ่มเติม)
- ด้านบริหารการจัดการ (เช่น ผู้บังคับบัญชาเล็งเห็นความสำคัญในการบริหารจัดการอย่างเป็นระบบหรือมีการสร้างแรงจูงใจในการทำงาน)
- ด้านโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (มีการกำหนดนโยบายที่ความชัดเจน และมีการวิเคราะห์บทบาทของหน่วยงานให้สอดคล้องกับการปฏิบัติงานจริง)
- ด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน (เช่น ปรับปรุงภารกิจและความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง /เสนอขอแก้ไขกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้องให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี)
- ด้านการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยี และด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างไรให้เกิดประสิทธิภาพในการทำงานอย่างสูงสุด

2) รูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ โดยมีประเด็นศึกษาให้ได้ข้อมูลเพิ่มเติม คือ

- รูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพควรลักษณะอย่างไร

- ด้านเทคนิคในการบริหารงานเกี่ยวกับด้านอาชญากรรมทางเทคโนโลยีให้ประสบความสำเร็จมีการดำเนินการอย่างไร

- ด้านการพัฒนารูปแบบที่ทำให้เกิดประโยชน์สูงสุดในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีควรเป็นอย่างไร

3) สถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีประเด็นศึกษาให้ได้ข้อมูลเพิ่มเติม คือ

- หน่วยงานตำรวจที่ปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แก่ ภารกิจและความรับผิดชอบ ระเบียบ ข้อบังคับ กฎหมาย และการบูรณาการระหว่างหน่วยงาน

- การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้แก่ ยุทธศาสตร์วิธีการ ป้องกันและปราบปราม มาตรการและวิธีการป้องกันและปราบปราม และบทบาทหน้าที่ของหน่วยงานตำรวจ

- การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แก่ สาเหตุการก่ออาชญากรรม รูปแบบอาชญากรรม และการวิเคราะห์อาชญากรรม

- องค์ความรู้ และความชำนาญงานเกี่ยวกับอาชญากรรมทางเทคโนโลยีได้แก่ ระดับการศึกษา ประสบการณ์การทำงาน และความรู้ทางด้านเทคโนโลยี

- การพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี ได้แก่ เครื่องมือ และอุปกรณ์ การตรวจสถานที่เกิดเหตุ และการครอบครองพยานหลักฐาน

- การสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยี ได้แก่ เทคนิคในการสืบสวน และสอบสวน การแสวงหาข้อเท็จจริงและหลักฐาน และผู้มีอำนาจ และเขตอำนาจการสืบสวนและสอบสวน

4) สภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

- ปัญหาด้านบุคลากร (เช่น ปัญหาการขาดบุคลากร ปัญหาเจ้าหน้าที่ขาดความรู้และทักษะในการปฏิบัติหน้าที่ ปัญหาความเครียดและความกดดันจากการทำงาน เป็นต้น)

- ปัญหาด้านงบประมาณ (เช่น การขาดงบประมาณในการจัดทำสื่อประชาสัมพันธ์ให้ประชาชนรับทราบถึงภัยของอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ เป็นต้น)

- ปัญหาด้านเครื่องมือ และอุปกรณ์ (เช่น ปัญหาการขาดแคลนอุปกรณ์ในการสืบสวน หาข่าว และการจัดเก็บวัตถุพยานต่างๆ เป็นต้น)

- ปัญหาด้านเทคโนโลยี (เช่น ขาดการปรับปรุงซอฟต์แวร์ที่ช่วยในการทำงานให้เป็นปัจจุบัน หรือมีแต่ไม่มีประสิทธิภาพ เป็นต้น)

- ปัญหาด้านบริหารการจัดการ (เช่น ผู้บังคับบัญชาไม่มีการบริหารจัดการอย่างเป็นระบบ หรือไม่มีการสร้างแรงจูงใจในการทำงาน)

- ปัญหานโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (เช่น นโยบายไม่มีความชัดเจนและไม่สามารถนำมาปฏิบัติได้อย่างเป็นรูปธรรม/ในปัจจุบันไม่มีมาตรการในการปฏิบัติงานจริง)

- ปัญหาด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน (เช่น ภารกิจและความรับผิดชอบที่ซ้ำซ้อนกัน/ไม่มีหน่วยงานใดเป็นเจ้าภาพที่แท้จริง ปัญหาข้อกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้อง)

รายละเอียดตามตารางที่ 4-1 – ตารางที่ 4-4

1) ประเด็นที่เกี่ยวกับแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานใน การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น รายละเอียดตามตารางที่ 4-1

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน

ผู้ให้ความเห็น	บุคลากร	ฝึกอบรม	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 1	ควรมีการกำหนดกรอบอัตราจำนวนที่เพียงพอต่อการปฏิบัติหน้าที่ และกระจายบุคลากรลงไปให้ทั่วถึง ทันต่อเหตุการณ์ มิใช่กระจุกตัวอยู่แต่ในส่วนกลาง	ควรจัดให้มีการฝึกอบรมตามรอบระยะเวลาที่เหมาะสม มีหลักสูตรระดับต้น-กลาง-สูง เพื่อเสริมสร้างทักษะความรู้ต่าง ๆ ให้ทันต่อเหตุการณ์ การเรียนรู้อาจมีทั้งเข้าอบรม หรือศึกษาด้วยตนเองจากบทความวิชาการ แล้วให้เป็นหน่วยกิต บทความละ 1 – 3 หน่วยกิต ต้องเก็บได้อย่างน้อยปีละ 20 หน่วยกิต	ควรเพิ่มงบประมาณให้เพียงพอแก่การประชาสัมพันธ์ให้ประชาชนรับทราบให้มากที่สุด สื่อที่ใช้ควรมีหลายรูปแบบ เพื่อให้เข้าถึงประชาชนทุกกลุ่ม	เพิ่มอุปกรณ์ เครื่องมือในการสืบสวนหาข่าว จัดเก็บวัตถุพยานต่าง ๆ ให้มีประสิทธิภาพ น่าเชื่อถือ เป็นไปตามมาตรฐานนานาชาติ ข้อมูลหรือผลลัพธ์ที่ได้ นำไปใช้ได้ทุกประเทศต่าง ๆ ทั่วโลก	ควรมีการติดตั้ง ปรับปรุง software ที่ทันสมัย (อย่างน้อยก็ควรจะทันสมัยกว่าอาชญากรทางคอมพิวเตอร์) เพื่อให้พัฒนาขีดความสามารถได้เท่าทันกับอาชญากรทางเทคโนโลยี
คนที่ 2	ความเห็นส่วนตัวจากประสบการณ์ในการทำงานร่วมกับเจ้าหน้าที่ตำรวจสำนักงานตำรวจแห่งชาติ พบว่า สตช.ยังขาดแคลนบุคลากรที่มีความรู้ความสามารถในการดำเนินคดีอาชญากรรมทางเทคโนโลยีเป็นอย่างยิ่ง แต่ทราบว่า สตช.ได้พยายามเพิ่มอัตรากำลัง และฝึกอบรมบุคลากรด้านนี้เพิ่มเติมอยู่ กองบังคับการปราบปรามการกระทำความผิด เกี่ยวกับอาชญากรรมทางเทคโนโลยี และกองบังคับการปราบปราม	ความเห็นส่วนตัวฯ การจัดอบรมให้กับเจ้าหน้าที่ตำรวจยังมีน้อย เมื่อเทียบกับความจำเป็นเร่งด่วนในการสร้างบุคลากรให้ทันต่อการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี	-	ความเห็นส่วนตัวฯ สตช.ยังขาดแคลนงบประมาณในการจัดหาเครื่องมือและอุปกรณ์ ให้เพียงพอต่อการดำเนินคดีอาชญากรรมทางเทคโนโลยีในภูมิภาคต่าง ๆ ทั่วประเทศ	ความเห็นส่วนตัวฯ สตช.ควรนำเทคโนโลยีใหม่ๆ มาช่วยเจ้าหน้าที่ตำรวจทั้งด้านสืบสวน และสอบสวน เพื่อลดภาระในการทำงาน โดยเฉพาะในปัจจุบันที่เทคโนโลยีการสื่อสาร และการทำธุรกรรมต่างๆ ทำให้พยานหลักฐานแต่ละเรื่อง กระจายอยู่ในหลายท้องที่ ซึ่งมีความยุ่งยากในการรวบรวม

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บุคลากร	ฝึกอบรม	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 3	ยังขาดบุคลากรที่มีความรู้ ความสามารถ ทักษะและประสบการณ์ ที่มีความเหมาะสมในการทำงาน และสร้างผู้เชี่ยวชาญเฉพาะด้านเพื่อทำหน้าที่ที่ปรึกษา	ควรจัดการฝึกอบรมให้ครอบคลุม และเพียงพออย่างสม่ำเสมอ	ยังขาดงบประมาณอย่างมากทั้งในเรื่องการจัดตั้งหน่วยงาน, การจัดหาเครื่องมือที่ทันสมัย และเพียงพอ ตลอดจนการพัฒนาบุคลากรอย่างต่อเนื่อง	ต้องจัดหาเครื่องมือในการทำงานที่จำเป็น ทันสมัยและมีประสิทธิภาพสูง รวมทั้งต้อง Upgrade/ปรับปรุงอยู่ตลอดเวลา ให้ครอบคลุมในทุก ๆ ภารกิจ	ด้านเทคโนโลยีต้องได้รับการพัฒนาอย่างสม่ำเสมอและต่อเนื่อง รวมทั้งควรมีแผนกวิจัยค้นคว้าและพัฒนาอุปกรณ์เครื่องมือใหม่ ๆ ด้วย
คนที่ 4	- ขาดกำลังพลที่มีทักษะความเชี่ยวชาญในการปฏิบัติงาน - การรักษาบุคลากรให้คงอยู่กับหน่วยงาน - การสร้างความเจริญก้าวหน้าในสายงาน	- ควรมีการอบรมอย่างต่อเนื่องให้เหมาะสมกับเจ้าหน้าที่ตำรวจในแต่ละระดับ - พัฒนาระบบ e-learning เพื่อให้เจ้าหน้าที่ตำรวจสามารถเรียนรู้ได้ทั่วประเทศ - เพิ่มทักษะความเชี่ยวชาญในการฝึกอบรมในต่างประเทศ	- ควรมีค่าตอบแทนพิเศษเพื่อป้องกันมิให้เกิดปัญหาสมองไหล - ควรมีงบประมาณอย่างต่อเนื่องเพื่อพัฒนาเครื่องมือ และบุคลากร	- ควรมีการปรับปรุงเครื่องมือให้ทันสมัยอยู่ตลอดเวลา - จัดหาเครื่องมือที่ทันสมัยเพื่อช่วยในการทำงานให้มีประสิทธิภาพ	- ควรมีหน่วยวิจัยเพื่อวิเคราะห์ และสืบสวนหาร่องรอยพยานหลักฐานทางอิเล็กทรอนิกส์ให้ตรงกับความต้องการ - พัฒนาระบบบริหารจัดการคดี เพื่อเชื่อมโยงข้อมูลในคดีต่าง ๆ ในอดีต ซึ่งจะช่วยให้การสืบสวนมีประสิทธิภาพมากขึ้น
คนที่ 5	กองกำกับการสืบสวนตำรวจนครบาล 8 เป็นหน่วยงานที่รับผิดชอบการสืบสวนคดีสำคัญที่เกิดขึ้นในพื้นที่กองบังคับการตำรวจนครบาล 8 ซึ่งโดยส่วนมากจะเป็นคดีอาชญากรรมทั่วไป บุคลากรโดยส่วนมากจะมีความรู้ด้านเทคโนโลยีเฉพาะการใช้เทคโนโลยีที่ช่วยในการสืบค้นข้อมูลและการสืบสวน แต่ไม่มีองค์ความรู้หรือประสบการณ์ในการสืบสวนอาชญากรรมทางเทคโนโลยี	ทางสำนักงานตำรวจแห่งชาติจะมีการจัดการอบรมการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี แต่จำนวนที่ได้รับจัดสรรมายังหน่วยงานใต้บังคับบัญชา (กองบัญชาการตำรวจนครบาล) มีไม่มาก และส่วนมากจะไม่ได้จัดสรรมาถึงระดับกองกำกับการ เนื่องจากอาจไม่ได้มีหน้าที่ในการสืบสวน อาชญากรรมทางเทคโนโลยีโดยเฉพาะ จึงเห็นควรให้กระจายและเพิ่มจำนวนการฝึกอบรมให้มากขึ้นและทั่วถึง	ปัจจุบันอาชญากรรมเทคโนโลยีมีจำนวนเพิ่มมากขึ้น ซึ่งเป็นอาชญากรรมที่สามารถสร้างความเสียหายได้ในวงกว้างต่อประชาชนและมีโอกาสสร้างมูลค่าความเสียหายได้จำนวนมาก เห็นว่าจะควรเพิ่มงบประมาณในด้านนี้ให้เพียงพอ และควรเป็นลักษณะจัดงบประมาณที่กำหนดเฉพาะในส่วนของอาชญากรรมทางเทคโนโลยี ที่จะสร้างศักยภาพให้สามารถป้องกันและสืบสวนปราบปรามอาชญากรรมทางเทคโนโลยี	ปัจจุบันหน่วยงานที่มีเครื่องมือสืบสวนทางเทคโนโลยี จะมีอยู่เฉพาะหน่วยงานส่วนกลางหรือหน่วยงานพิเศษเท่านั้น ควรจะกระจายให้หน่วยงานระดับท้องที่ด้วย เช่น กองบัญชาการตำรวจนครบาล หรือภูธรภาคต่าง ๆ การทำงานที่ผ่านมามีการสร้างช่องทางให้ส่งพยานหลักฐานหรือ ของกลาง ไปตรวจสอบ แต่ในการทำงานจริงนั้น บางครั้งพฤติการณ์ในคดีอาจจะยังไม่ถึงขั้นการดำเนินคดี	อาชญากรรมทางเทคโนโลยีเป็นอาชญากรรมที่มีการปรับเปลี่ยนรูปแบบรวดเร็ว ที่เทคโนโลยีที่ใช้ในการป้องกันหรือสืบสวนปราบปรามจำเป็นที่ต้องจะปรับตัวให้ทันกับสถานการณ์ที่เกิดขึ้น การซื้อเทคโนโลยี อุปกรณ์เครื่องมือ หรือโปรแกรมต่าง ๆ จากบริษัทต่างประเทศ หรือ เอกชนแต่เพียงอย่างเดียว อาจทำให้การพัฒนาเทคโนโลยีของฝ่ายเจ้าหน้าที่ทำได้ช้ากว่าอาชญากรเสมอ จึงเห็นว่าควรมีหน่วยงานเฉพาะในการวิจัย พัฒนาเทคโนโลยีเฉพาะทาง

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บุคลากร	ฝึกอบรม	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 5 (ต่อ)	ซึ่งหากต้องการพัฒนาบุคคลากรด้านนี้โดยเฉพาะ เห็นควรรับบรรจุผู้ที่มีวุฒิด้านนี้โดยเฉพาะ และควรมีการจัดการให้บุคคลากรที่มีความรู้ด้านเทคโนโลยีโดยเฉพาะนี้ สามารถทำงานและมีความเจริญก้าวหน้าในสายงานในสำนักงานตำรวจแห่งชาติได้ โดยอาจกำหนดเป็นแท่งพิเศษหรือเป็นตำรวจประเภทไม่มียศ	-	ได้อย่างมีประสิทธิภาพและทั่วถึง ในปัจจุบันหน่วยงานในสำนักงานตำรวจแห่งชาติที่อยู่ในระดับภูมิภาคยังไม่มีขีดความสามารถในการดำเนินคดีอาชญากรรมทางเทคโนโลยีได้เลย ประชาชนซึ่งไม่ได้อยู่ในบริเวณกรุงเทพมหานครและปริมณฑลอาจเป็นเหยื่อในอาชญากรรมดังกล่าว แต่อาจเข้าไม่ถึงการช่วยเหลือได้	ยังเป็นเพียงการสืบสวนเบื้องต้น การส่งไปตรวจพิสูจน์ที่กองพิสูจน์หลักฐานนั้นไม่สามารถทำได้ หรือจะขอให้หน่วยงานที่มีเครื่องมือมาสนับสนุนการปฏิบัติงานนั้นอาจกระทำได้อย่างมีข้อจำกัด การกระจายเครื่องมือสืบสวนไปยังหน่วยงานปฏิบัติในระดับท้องที่จึงมีความจำเป็นอย่างยิ่ง	ที่เหมาะสมกับสถานการณ์ด้านอาชญากรรมเทคโนโลยีที่เกิดขึ้นภายในประเทศไทย
คนที่ 6	สำนักงานตำรวจแห่งชาติพยายามเพิ่มเติมกำลังพลผู้ปฏิบัติงานด้านการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ให้แก่สำนักงานพิสูจน์หลักฐานตำรวจ โดยคาดว่าจะสามารถเพิ่มได้ปีละประมาณ 10 นาย จนครบจำนวน การเพิ่มพูนความรู้และการรักษามาตรฐานในการปฏิบัติงานจะแบ่งเป็น 2 ส่วน คือ (1) การอบรมเพื่อเป็นผู้ชำนาญด้านการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ จะเป็นการฝึกอบรมโดยหลักสูตรของสำนักงานพิสูจน์หลักฐานตำรวจ รวมระยะเวลาประมาณ 1 ปี	-	ไม่มีงบประมาณในการทำสื่อประชาสัมพันธ์ให้ประชาชนรับทราบถึงภัยของอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ เป็นการเฉพาะ	ขาดแคลนเครื่องมือในการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ รวมถึงไม่มีพื้นที่ที่เหมาะสมสำหรับจัดตั้งห้องปฏิบัติการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์	ขาดแคลน software ที่มีลิขสิทธิ์ถูกต้องในการปฏิบัติงาน ทั้ง Software ที่ใช้ในการตรวจพิสูจน์โดยตรง และ Software พื้นฐานที่สนับสนุนในการปฏิบัติงาน เช่น ระบบปฏิบัติการ Windows. Microsoft Office, โปรแกรม Photoshop เป็นต้น

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บุคลากร	ฝึกอบรม	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 6 (ต่อ)	(ภาคทฤษฎี 4 เดือน , ภาคปฏิบัติ 8 เดือน) โดยภาคปฏิบัติจะทำหน้าที่ผู้ช่วยผู้ตรวจพิสูจน์และเก็บสะสมคดีให้ครบ 100 เรื่อง หากไม่ครบให้ขยายเวลาจนครบจำนวน) เมื่อครบเกณฑ์ที่กำหนดแล้ว จะต้องเข้ารับการทดสอบจากคณะกรรมการกลางของสำนักงานพิสูจน์หลักฐานตำรวจ เมื่อสอบผ่านจึงจะได้รับอนุมัติและมีสิทธิในการตรวจพิสูจน์พยานหลักฐานด้วยตนเอง (2) การฝึกอบรมระยะสั้น เป็นการเพิ่มพูนความรู้ ด้านเครื่องมือหรือเทคนิคในการตรวจพิสูจน์ที่ก้าวหน้าทันสมัย โดยวิทยากรผู้เชี่ยวชาญทั้งจากในประเทศ และองค์กรตำรวจต่างประเทศ เช่น FBI (อเมริกา) AFP(ออสเตรเลีย) และ JICA (ญี่ปุ่น) เป็นต้น				

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 1	ผู้บังคับบัญชาควรจะมีความรู้พื้นฐานเกี่ยวกับเรื่องอาชญากรรมทางคอมพิวเตอร์ เพื่อที่จะได้เข้าใจการทำงานของผู้ใต้บังคับ บัญชา และเป็นผู้ให้คำชี้แนะแก่ผู้ใต้บังคับบัญชา หากเกิดปัญหาขัดข้อง	มีการกำหนดนโยบายที่มีความชัดเจน มีเป้าหมายที่แน่นอน มีแนวทางปฏิบัติที่เป็นขั้นเป็นตอน สอดคล้องกับนโยบายหลัก เพื่อให้การขับเคลื่อนขององค์กรเป็นไปในทิศทางเดียวกัน	มีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐทุกแห่งที่มีส่วนเกี่ยวข้องมิใช่ต่างคนต่างทำ ข้อมูลไม่สามารถนำมาใช้ประโยชน์ร่วมกันได้ นอกจากนี้ควรมีการบูรณาการร่วมกันระหว่างภาครัฐและภาคประชาชน หรือเอกชนด้วย เพื่อให้ได้มุมมองที่กว้างออกไป และเป็นการรับฟังความคิดเห็นของภายนอกด้วย	ควรพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยี ให้มีอิสระสามารถขับเคลื่อนองค์กรไปได้ตามพันธะภารกิจให้เกิดประสิทธิภาพสูงสุด บุคลากรของหน่วยงานควรได้รับการส่งเสริมให้มีความก้าวหน้าในหน่วย ตำแหน่งบริหารของหน่วยงานควรเป็นบุคลากรภายในเพื่อเป็นขวัญและกำลังใจของคนในหน่วย	-
คนที่ 2	-	-	การมีส่วนร่วมของหน่วยงานภาครัฐอื่น และภาคเอกชน มีความสำคัญในการช่วยเหลือเจ้าหน้าที่ตำรวจทั้งฝ่ายสืบสวนและสอบสวนได้มาก แต่ค่านิยมของคนไทย และสภาพสังคม ทำให้หน่วยงานภาครัฐอื่น และภาคเอกชน มักมองว่าเป็นหน้าที่ของเจ้าหน้าที่ตำรวจแต่เพียงฝ่ายเดียว ขาดการใส่ใจช่วยเหลือ ทั้งกรณีที่เป็นหน้าที่ตามกฎหมาย และกรณีที่สมควรจะช่วยเหลือได้ แม้ไม่มีหน้าที่โดยตรง การใช้มาตรการทางสังคมที่จะส่งเสริมให้ภาคเอกชน เข้ามามีส่วนร่วมในการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ตำรวจ จะช่วยเสริมประสิทธิภาพในการดำเนินคดีได้	ในระยะเร่งด่วน ควรสร้างองค์ความรู้พื้นฐานของคดีอาชญากรรมทางเทคโนโลยีประเภทต่าง ๆ แบบสำเร็จรูป ให้ง่ายต่อการทำความเข้าใจ และมีตัวอย่างคำแนะนำ และแนวทางแก้ปัญหาให้เจ้าหน้าที่ตำรวจในหน่วยงานย่อยท้องที่ต่าง ๆ สามารถศึกษาและจัดการคดีอาชญากรรมทางเทคโนโลยีในระดับที่ไม่ยุ่งยากซับซ้อนด้วยตัวเองได้ ในระยะยาว ควรเพิ่มเติมองค์ความรู้เฉพาะทางของคดีอาชญากรรมทางเทคโนโลยีประเภทต่างๆ ให้แก่หน่วยงานเฉพาะด้านของ สตช. ที่มีภารกิจเฉพาะด้านและหน่วยงานในท้องถิ่น เพื่อรับมือกับคดีอาชญากรรมทางเทคโนโลยีทุกระดับที่จะเพิ่มปริมาณขึ้นในอนาคต รวมถึงการสร้าง	-

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 2 (ต่อ)				บุคลากรของหน่วยงานให้สามารถเติบโตได้อย่างมีความพร้อมในการปฏิบัติหน้าที่ และมีขวัญกำลังใจ เพื่อทำงานในหน่วยงานเฉพาะด้านระยะยาวได้	
คนที่ 3	ต้องให้ความสำคัญเป็นอันดับต้น ๆ ส่งเสริมและสนับสนุนต่อการทำงานเป็นดี	ต้องวิเคราะห์ทั้งปัจจุบันและอนาคต มองภาพในระยะยาวและมุ่งการทำงานในแบบบูรณาการ	การบูรณาการหรือการทำงานร่วมกันทั้งหน่วยงานราชการ ภาคเอกชน และระหว่างประเทศ จะมีความสำคัญและส่งผลสำเร็จในการทำงานเป็นอย่างมากในอนาคต	ต้องมีการวางแผนและกำหนดวัตถุประสงค์ให้ชัดเจน มีการจัดวางโครงสร้างหน่วยงาน และระบบการทำงานที่ชัดเจน มีการสนับสนุนงบประมาณอย่างเพียงพอ มีแผนในการพัฒนาบุคลากรที่ชัดเจนเป็นระบบและต่อเนื่อง จัดหาเครื่องมือที่ทันสมัยและเหมาะสม มีการประสานความร่วมมือกับหน่วยงานอื่น ๆ มีการวิจัยและพัฒนานวัตกรรม สิ่งใหม่ ๆ	ต้องมีการสร้างผู้เชี่ยวชาญเฉพาะด้านเพื่อเป็นที่ปรึกษาช่วยเหลือในการทำงาน
คนที่ 4	- ควรพัฒนาระบบการประเมินผลงานแบบ 360 องศา เพื่อแก้ปัญหาการประเมินไม่เป็นธรรม	- ควรเน้นมาตรการป้องกัน เพื่อลดช่วยโอกาสในการกระทำความผิด เช่น ลงทะเบียนซิมโทรศัพท์ การใช้ Free WiFi ที่สามารถระบุตัวตนผู้ใช้บริการได้	- ควรมีเจ้าภาพกลางในการรับฟังสภาพปัญหา เพื่อนำไปสู่การแก้ไขปัญหาการบังคับใช้กฎหมาย	- เพิ่มศักยภาพเจ้าหน้าที่ตำรวจตามสถานีตำรวจทั่วประเทศให้สามารถทำคดีทั่วไปที่เกี่ยวข้องกับทางเทคโนโลยีได้ - ปรับการทำงานของ บก.ปอท.เป็นระดับ บช. - พัฒนาหน่วยงานด้านวิจัยโดยจ้าง Outsource	-
คนที่ 5	ในงานตำรวจ การบริหารจัดการในรูปแบบเดิมนั้นที่เหมาะสมและสอดคล้องกับอาชกรรมชีวิต ร่างกาย	ปัญหาในการป้องกันและปรามปรามอาชญากรรมเทคโนโลยีมีในทุกมิติ เช่น บุคคลกร องค์ความรู้ เทคโนโลยี	การร่วมกันระหว่างหน่วยงานราชการนั้น ในปัจจุบันก็มีการร่วมมือกันในบางส่วนอยู่แล้ว ที่แต่สิ่งที่เป็นปัญหา	ดังกล่าวมาแล้วโดยโครงสร้างเดิมของงานตำรวจไม่อาจตอบสนองอาชญากรรมเทคโนโลยีได้ การพัฒนา	-

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 5 (ต่อ)	ทรัพย์สิน ทั่วไป เช่น การบริหารงานในระดับสถานีตำรวจ มีการแบ่งเป็นฝ่าย ป้องกันปราบปราม ฝ่ายสืบสวน ฝ่ายจราจร ในระดับกองบังคับการก็จะมีกองกำกับการสืบสวน เป็นหน่วยที่สืบสวนคดีที่ใหญ่ขึ้น มีความซับซ้อนมากขึ้น ในระดับกองบังคับการก็จะมีกองบังคับการสืบสวนที่สืบสวนคดีที่มีความสำคัญขึ้นไปอีก แต่เมื่อมองอาชญากรรมทางเทคโนโลยีที่เขตพื้นที่ในการก่ออาชญากรรมแทบไม่มีความสำคัญเพราะเหยื่อและอาชญากรไม่จำเป็นต้องพบกันหรืออยู่ใกล้เคียงกันเลยก็ได้ การบริหารจัดการในรูปแบบคงไม่สามารถตอบสนองการป้องกันและสืบสวนปราบปราม จึงควรมีการบริหารจัดการแบบใหม่เฉพาะอาชญากรรมประเภทนี้ ยกตัวอย่างเช่น - งานป้องกัน มีสายตรวจคอยตรวจตราในพื้นที่เพื่อป้องกันเหตุ แต่ในโลกอินเตอร์เน็ตไม่มีสายตรวจคอยตรวจตราหรือเฝ้าระวังภัย ส่วนมากจะมีการดำเนินคดีก็ต่อเมื่อมีผู้เสียหายได้รับความเสียหายแล้วมาแจ้งความ	ความตะหนักรู้ของประชาชนและเจ้าหน้าที่ผู้บังคับใช้กฎหมาย แต่ปัญหาดังกล่าวก็มีการแก้ไขและปรับตัวเองไปตามสภาพสังคมปัจจุบันในบางส่วนแล้วแต่กฎหมาย ระเบียบข้อบังคับต่าง ๆ ที่จะใช้เป็นเครื่องมือในการป้องกัน หรือสืบสวนปราบปรามนั้นดูจะล้าหลัง ไม่สามารถตอบสนองการดำเนินการต่าง ๆ ของเจ้าหน้าที่ได้เลย ยกตัวอย่างเช่น ถ้ามีคดีการทำร้ายร่างกายกัน เจ้าหน้าที่ตำรวจก็จะมีฐานข้อมูลคดี ประวัติผู้กระทำความผิด หรือฐานข้อมูลทะเบียนราษฎร์ให้ผู้เสียหาชี้ยืนยันคนร้าย แต่ถ้าเป็นการฉ้อโกงกันผ่าน Facebook หรือ Hack Facebook หรือ e-mail กัน เจ้าหน้าที่ตำรวจแทบไม่สามารถเข้าถึงข้อมูลต่างๆ เพื่อระบุตัวคนร้ายได้เลย ดังนั้นนโยบายและยุทธศาสตร์เร่งด่วน จึงควรแก้ไขกฎหมาย เพื่อเพิ่มเติมขีดความสามารถที่จะเข้าถึงข้อมูลต่างๆ ด้านเทคโนโลยีให้เจ้าหน้าที่เพื่อให้ป้องกันและสืบสวนการกระทำความผิด	อย่างมากในปัจจุบันคือ หน่วยงานเอกชนที่มักจะปฏิเสธการขอความร่วมมือจากเจ้าหน้าที่ตำรวจ ในการขอตรวจสอบข้อมูลต่าง ๆ หรือร่วมมือแต่ดำเนินการช้ามากจะไม่ทันต่อการป้องกันหรือสืบสวนปราบปรามเลย	หรือปรับปรุงเล็ก ๆ น้อย ๆ จึงไม่เพียงพอ จึงควรสร้างโครงสร้างหรือหน่วยงานใหม่โดยเฉพาะของตำรวจให้มีศักยภาพในป้องกัน และสืบสวนปราบปรามอาชญากรรมเทคโนโลยีได้อย่าง “มีประสิทธภาพและทั่วถึง” บก.ปอท. และ บก.สนับสนุนทางเทคโนโลยี เป็นหน่วยงานที่มีประสิทธิภาพแล้ว แต่ไม่ทั่วถึงที่จะดำเนินการต่ออาชญาดังกล่าวที่เพิ่มมากขึ้นและกระจายไปในวงกว้างได้ และในภาพรวมก็ยังขาดมิติในด้านการป้องกันและประชาสัมพันธ์ ไม่มีหน่วยงานในรับผิดชอบในงานด้านนี้โดยเฉพาะ	

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 5 (ต่อ)	- งานสืบสวน ฝ่ายสืบสวนก็จะทำการสืบสวนคดีต่างที่เกิดขึ้นโดยอาศัยเครื่องมือต่างๆ เช่น ฐานข้อมูลบุคคล กล้องวงจรปิดในบริเวณที่เกิดเหตุ ข้อมูลการติดต่อสื่อสารทางโทรศัพท์มือถือ เป็นต้น แต่การสืบสวนในอาชญากรรมทางเทคโนโลยี แทบไม่มีเครื่องมือที่จะช่วยในการสืบสวนเหล่านั้นเลย - การประชาสัมพันธ์ จะมีฝ่ายตำรวจชุมชนสัมพันธ์ ที่คอยให้ความรู้ สร้างเครือข่ายในการป้องกันภัยอาชญากรรม แต่โลกอินเตอร์เน็ตไม่มีเขตพื้นที่รับผิดชอบ ไม่มีใครมีหน้าที่ในการดำเนินการประชาสัมพันธ์ดังกล่าวเลย - โดยรวมคือ โครงสร้างเดิมของงานตำรวจไม่สามารถที่จะดำเนินการต่ออาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพและทั่วถึงได้เลย การเพิ่มเติม ปรับปรุง หรือพัฒนาเล็กๆน้อยคงจะไม่เพียงพอ ควรออกแบบโครงสร้างรูปแบบการดำเนินการ หรือการบริหารจัดการในรูปแบบใหม่ เพื่อตอบสนองต่ออาชญากรรมเทคโนโลยีได้				

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 6	จากปัญหาการขาดแคลนทั้งบุคลากร เครื่องมือ และความแออัดของพื้นที่ในห้องปฏิบัติการ และการเพิ่มขึ้นของปริมาณงาน ซึ่งผู้ตรวจพิสูจน์แต่ละรายจะต้องรับงานตรวจพิสูจน์ไม่น้อยกว่า 2-300 เรื่องต่อปี ผู้บังคับบัญชาได้เล็งเห็นและหาทางแก้ในส่วนที่จะสามารถทำได้แล้ว แต่สิ่งนี้ต้องใช้เวลาและงบประมาณจำนวนมาก ปัจจุบันจึงเยียวยาและรักษาประสิทธิภาพกำลังผลผู้ปฏิบัติงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ โดยการให้สิทธิประโยชน์ตามระเบียบของทางราชการด้านอื่น ๆ เช่น การให้เงินเพิ่มพิเศษประจำตำแหน่งผู้ปฏิบัติงานด้านนิติวิทยาศาสตร์และการให้เงินล่วงเวลาในการปฏิบัติงานนอกเวลาราชการ ซึ่งสามารถจูงใจให้มีผู้ปฏิบัติงานด้านนี้ต่อเนื่องไปได้ในระดับหนึ่ง	ปัจจุบันสำนักงานตำรวจแห่งชาติได้เล็งเห็นถึงปัญหาการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่ต้องใช้การบูรณาการหน่วยงานที่มีความชำนาญต่างกันให้มาทำงานร่วมกัน โดยดำเนินการใน 2 ส่วน คือ (1) สนับสนุนงบประมาณและกำลังพล (ที่มีจำกัด) ให้แก่หน่วยงานที่ทำหน้าที่ด้านนี้ (2) ใช้อำนาจในทางบริหารของสำนักงานตำรวจแห่งชาติ ในการออกคำสั่งแต่งตั้งคณะทำงานเพื่อแก้ปัญหาการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในภาพรวม ซึ่งเป็นการออกคำสั่งโดยรวบรวมฝ่ายปฏิบัติและฝ่ายเทคนิคที่มีความชำนาญในแต่ละด้านอย่างแท้จริงให้มาทำงานร่วมกัน โดยมีขอบเขตหน้าที่และมีการมอบหมายภารกิจที่ชัดเจน รวมถึงมีระบบติดตามประเมินผลการปฏิบัติที่เคร่งครัด จึงส่งผลให้การปฏิบัติในด้านนี้มีผลงานเป็นที่ประจักษ์ในปริมาณและคุณภาพของการอำนวยความยุติธรรมที่เพิ่มขึ้นอย่างต่อเนื่อง	การปฏิบัติงานเพื่อตรวจพิสูจน์หลักฐานในทุกด้านของสำนักงานพิสูจน์หลักฐานตำรวจ เป็นการสนับสนุนการปฏิบัติของพนักงานสอบสวน โดยสำนักงานพิสูจน์หลักฐานตำรวจไม่มีอำนาจในการครอบครองวัตถุพยานตั้งแต่แรกเริ่ม(ตั้งแต่ตรวจพบในสถานที่เกิดเหตุ การครอบครองวัตถุพยานเป็นอำนาจของพนักงานสอบสวน และเป็นดุลพินิจของพนักงานสอบสวนที่จะส่งวัตถุพยานใดมาทำการตรวจพิสูจน์) ปัจจุบันอยู่ระหว่างปรับปรุงกฎหมายที่เกี่ยวข้อง เพื่อให้เจ้าหน้าที่พิสูจน์หลักฐานมีอำนาจในการครอบครองวัตถุพยานได้ตั้งแต่เมื่อพบในสถานที่เกิดเหตุ ทั้งนี้เพื่อที่จะได้นำส่งมาตรวจพิสูจน์โดยเร็ว มิต้องรอให้พนักงานสอบสวนทำเรื่องส่งมาให้ตรวจพิสูจน์ในภายหลังซึ่งอาจใช้ระยะเวลานาน โดยการตรวจพิสูจน์วัตถุพยานที่ล่าช้าอาจส่งผลเสียหายต่อคดีและกระบวนการยุติธรรมได้ รวมถึงเป็นการปรับห่วงโซ่ของพยานหลักฐานให้ถูกต้อง ลดผลกระทบที่อาจเกิดความเสียหายต่อคดีได้เช่นกัน		

ตารางที่ 4-1 ความเห็นในประเด็นแนวทางการพัฒนาหน่วยงาน (ต่อ)

ผู้ให้ความเห็น	บริหารการจัดการ	นโยบายและยุทธศาสตร์	การบูรณาการร่วมกัน	ประสิทธิภาพ	อื่น ๆ
คนที่ 6 (ต่อ)			นอกจากนี้ สำนักงานพิสูจน์หลักฐานตำรวจ ได้เคยร่าง พ.ร.บ. วิชาชีพนิติวิทยาศาสตร์ พ.ศ. .... โดยมีวัตถุประสงค์ให้มีองค์กรตามกฎหมาย ทำหน้าที่ควบคุมคุณภาพและมาตรฐานการปฏิบัติงานในภาพรวมของประเทศ		

2) ประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ รายละเอียดตามตารางที่ 4-2

ตารางที่ 4-2 ความคิดเห็นในประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีที่ดี

ผู้ให้ความเห็น	รูปแบบในการปฏิบัติงาน	เทคนิคในการบริหารงาน	การพัฒนารูปแบบ
คนที่ 1	ควรปฏิบัติตามแนวทางที่กำหนดไว้อย่างเคร่งครัด โปร่งใส สามารถตรวจสอบขั้นตอนต่าง ๆ ได้ มีการส่งมอบงานต่อกัน โดยมีการปฏิบัติตามห่วงโซ่ของการครอบครองพยานหลักฐาน (chain of custody) สามารถอธิบายขั้นตอนต่าง ๆ ได้ แนวทางที่ปฏิบัติควรได้รับความน่าเชื่อถือ และเป็นไปตามมาตรฐานที่นานาชาติกำหนด ทั้งนี้เพื่อให้พยานหลักฐานที่ได้มาสามารถนำมาใช้ในขั้นพิจารณา ผู้พิพากษาสามารถนำมาชั่งน้ำหนักพยานหลักฐานได้อย่างมั่นใจ	ควรมีการสรุปบทเรียนจากคดีต่าง ๆ ที่เกิดขึ้นมาว่าประสบความสำเร็จ โดยใช้เทคนิคการบริหารงานอย่างไร เพื่อที่จะได้นำมาเป็นแนวทางในการบริหารงานเกี่ยวกับอาชญากรรมทางเทคโนโลยีให้ประสบความสำเร็จ	ควรมีการสรุปรูปแบบการปฏิบัติงานที่ผ่านมาว่าประสบความสำเร็จในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีหรือไม่อย่างไร รูปแบบใดที่มักจะประสบความสำเร็จ รูปแบบดังกล่าวสามารถที่จะพัฒนาต่อไปได้อีกหรือไม่ เพื่อให้เกิดประโยชน์สูงสุดในการปฏิบัติงาน
คนที่ 2	คดีอาชญากรรมทางเทคโนโลยี จะต้องอาศัยความรวดเร็วในการรวบรวมพยานหลักฐาน ซึ่งจะต้องมีองค์ความรู้ และได้รับความร่วมมือจากผู้ให้บริการด้านต่างๆ ที่เป็นผู้ครอบครองพยานหลักฐาน	ผมเสนอวิธีบริหารจัดการเพื่อแก้ปัญหาฯ การขาดแคลนบุคลากรและงบประมาณแบบเร่งด่วน ดังนี้ 1. การจัดแบ่งคดีอาชญากรรมทางเทคโนโลยี ออกเป็นประเภทต่างๆ และแบ่งระดับความยากง่าย เช่น ประเภทที่การกระทำผิดอยู่ในระบบเทคโนโลยีโดยตรง (เช่น ฉ้อโกงขายสินค้าทางอินเทอร์เน็ต , ลักลอบทำธุรกรรม E – Banking ฯลฯ) กับประเภทที่การกระทำผิดไม่ได้อยู่ในระบบเทคโนโลยี แต่ใช้เทคโนโลยีเฉพาะการสื่อสาร หรือการทำธุรกรรมที่เกี่ยวข้อง (เช่น การขายสิ่งของผิดกฎหมาย แล้วมีการติดต่อสื่อสารกันด้วยโทรศัพท์ หรือโปรแกรมสนทนาผ่านอินเทอร์เน็ต ฯลฯ) แล้วแยกระดับความยากง่ายของคดี การทำแบบฟอร์มสำเร็จรูป และกำหนดช่องทางรวบรวมพยานหลักฐานจากผู้ให้บริการต่าง ๆ จะช่วยให้เจ้าหน้าที่ตำรวจได้รับความสะดวกมากยิ่งขึ้น สามารถใช้กับคดีที่ไม่ยุ่งยากซับซ้อน ลดภาระ	**ประเด็นที่ 1** ควรยกปัญหาสำคัญในหลายๆ ด้านขึ้นมาพิจารณาแก้ไขอย่างเป็นระบบ ไม่ใช่ปล่อยให้เจ้าหน้าที่ตำรวจทั้งฝ่ายสืบสวนและสอบสวนไปแก้ไขเองเป็นรายสำนวน เช่น - ปัญหาเรื่องการขอข้อมูลจากผู้ให้บริการประเภทต่างๆ ทั้งที่เกี่ยวกับระบบคอมพิวเตอร์และธุรกรรมการเงิน ที่โต้แย้งอำนาจเจ้าหน้าที่ของรัฐอย่างไม่สมเหตุผล ให้ข้อมูลล่าช้า หรือปฏิเสธการให้ข้อมูล การเรียกรับค่าใช้จ่ายจากเจ้าหน้าที่ของรัฐ ฯลฯ ทั้งนี้ อาจหามาตรการจูงใจต่างๆ เพื่อให้ผู้ให้บริการฯ เต็มใจให้ความร่วมมือกับเจ้าหน้าที่ของรัฐ เช่น การให้คำรับรองหรือประกาศชมเชย ว่าเป็นหน่วยงานที่มีความรับผิดชอบทางสังคม (Social Accountability) สำหรับองค์กรที่ทำ ISO หรือใช้มาตรการทางภาษี เช่น การให้สิทธินำไปคิดเป็นค่าใช้จ่ายของหน่วยงาน คำขอละ 20 บาท เป็นต้น

ตารางที่ 4-2 ความคิดเห็นในประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีที่ดี (ต่อ)

ผู้ให้ความเห็น	รูปแบบในการปฏิบัติงาน	เทคนิคในการบริหารงาน	การพัฒนารูปแบบ
คนที่ 2 (ต่อ)		ค่าใช้จ่าย และระยะเวลาทำคดีได้ 2. จัดแบ่งเจ้าหน้าที่ ออกเป็น 3 กลุ่ม เพื่อรับมือกับคดีที่มีความยากง่ายต่างกัน ได้แก่ 2.1 ระดับที่ใช้ความรู้อย่างเดียว หรือใช้เทคโนโลยีที่มีอยู่ทั่วไปในการบริหารจัดการคดีได้ 2.2 ระดับที่ต้องใช้เครื่องมือพิเศษที่จะต้องมีความรู้เป็นการเฉพาะในการทำงาน เช่น การใช้โปรแกรมตรวจพิสูจน์ และ 2.3 ระดับที่จะต้องใช้ทั้งเครื่องมือพิเศษและความรู้พิเศษในการจัดการคดีที่มีความยุ่งยากซับซ้อนทางเทคโนโลยีโดยตรง เช่น การลักลอบเข้าถึงระบบคอมพิวเตอร์ของหน่วยงานภาครัฐ หรือสถาบันการเงินแล้ว ก่อความเสียหายในรูปแบบต่าง ๆ สภาพปัญหาส่วนนี้คือ การแก้ปัญหาโดยเข้าใจว่า คดีอาชญากรรมทางเทคโนโลยีมีความยุ่งยากซับซ้อนสูง ต้องรอให้มีผู้เชี่ยวชาญพิเศษ พร้อมเครื่องมือและงบประมาณ จึงจะทำคดีได้ กลายเป็นว่าคดีอาชญากรรมทางเทคโนโลยีจำนวนมากที่ไม่ถึงขั้นยุ่งยาก เพียงแต่ต้องอาศัยความรู้เบื้องต้น เจ้าหน้าที่ส่วนใหญ่ ยังไม่สามารถทำคดี หรือวางแผนการรวบรวมพยานหลักฐานได้ ผู้บังคับบัญชาในแต่ละหน่วย จะต้องประเมินความยากง่ายของคดี และจัดเจ้าหน้าที่ตำรวจรับผิดชอบคดีแต่ละระดับอย่างเหมาะสม โดยคดีที่มีความยุ่งยากเกินขีดความสามารถของหน่วยย่อยในท้องที่ต่างๆ จะต้องมีคณะทำงานพิเศษในกลุ่มที่ 2.2 และ 2.3 ลงไปช่วยเหลือ 3. ศึกษาสภาพปัญหาและแนวทางการดำเนินคดี เพื่อหาแนวทางการดำเนินคดีที่มีประสิทธิภาพ ลดกระบวนงานที่ไม่จำเป็นหรือ	- การกระตุ้นให้หน่วยงานที่มีหน้าที่กำกับดูแลผู้ให้บริการแต่ละประเภท ตรวจสอบดำเนินการเพื่อให้ปฏิบัติตามกฎหมาย โดยเฉพาะการร่วมมือกับในการดำเนินคดีฯ - ปัญหาเรื่องพยานหลักฐานอยู่ต่างท้องที่กับเจ้าหน้าที่ - ปัญหาด้านภาษาต่างประเทศ - ปัญหาเรื่องการขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา **ประเด็นที่ 2** ควรพิจารณาแนวทางการสอบสวนในรูปแบบใหม่ๆ ที่จะช่วยลดภาระด้านเวลา ค่าใช้จ่ายให้แก่เจ้าหน้าที่ทั้งฝ่ายสืบสวนและพนักงานสอบสวน - การสอบปากคำผ่านระบบ Video Conference - การแบ่งงานบางส่วนให้ฝ่ายสืบสวน รวบรวมพยานหลักฐานในรูปแบบที่สามารถนำไปใช้เป็นพยานหลักฐานในสำนวนการสอบสวนได้ - การจัดทำแบบฟอร์มมาตรฐานในการสอบปากคำ หรือขอข้อมูล เพื่ออำนวยความสะดวก สำหรับผู้เสียหาย หรือพยานบางประเภท - การใช้เอกสารอิเล็กทรอนิกส์ที่มีความน่าเชื่อถือและชอบด้วยกฎหมาย ในการติดต่อขั้นตอนต่างๆ สามารถนำมาใช้เป็นพยานหลักฐาน และมีสภาพบังคับตามกฎหมายได้ - การใช้อาสาสมัคร หรือนักศึกษาฝึกงาน มาช่วยให้คำแนะนำแก่ผู้เสียหาย ในการจัดเตรียมข้อมูลและพยานหลักฐานเบื้องต้นให้แก่พนักงานสอบสวน

ตารางที่ 4-2 ความคิดเห็นในประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีที่ดี (ต่อ)

ผู้ให้ความเห็น	รูปแบบในการปฏิบัติงาน	เทคนิคในการบริหารงาน	การพัฒนารูปแบบ
คนที่ 2 (ต่อ)		กระบวนงานที่ไม่สามารถทำได้ (เช่น การขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาหลายกรณี ที่ไม่ทันเวลา หรือไม่ได้รับความร่วมมือจากต่างประเทศ) แล้วใช้บุคลากรดำเนินคดีด้วยแนวทางที่เหมาะสมในแต่ละสถานการณ์	
คนที่ 3	มีมาตรฐานในการทำงาน กำหนดขั้นตอนในการปฏิบัติที่ชัดเจนและเป็นสากล	ควรกำหนดมาตรฐานและขั้นตอนใน การทำงานให้ละเอียดในทุก ๆ ประเภทและลักษณะของคดี และให้ครอบคลุมในทุก ๆ เรื่องที่เกี่ยวข้องกับการทำงาน	ควรมีการวิเคราะห์รูปแบบของคดีที่ผ่านมา จัดทำเป็นกรณีศึกษาเพื่อเป็นรูปแบบมาตรฐานในการทำงานต่อไป
คนที่ 4	- มีความรอบรู้และเข้าใจเทคโนโลยี - รู้ข้อจำกัดของตนเอง ข้อกฎหมาย - ไม่เปลี่ยนแปลงพยานหลักฐานทางอิเล็กทรอนิกส์ หากจำเป็นให้เปลี่ยนแปลงให้น้อยที่สุด - เข้าใจหลักการ hashing เพื่อใช้ในการยืนยันว่าพยานหลักฐานทางพยานหลักฐานทางอิเล็กทรอนิกส์ ไม่มีการเปลี่ยนแปลง - ใช้หลัก Chain of custody เพื่อรักษาห่วงโซ่ของพยานหลักฐาน - เข้าใจวิธีการยึดพยานหลักฐานทางอิเล็กทรอนิกส์แต่ละประเภท	- ระบุสาเหตุของปัญหาต่าง ๆ ได้ตรงจุด เพื่อให้สามารถยืนยันได้ว่า ปัญหาที่เกิดขึ้นสามารถแก้ไขได้หรือไม่ สามารถป้องกันมิให้เกิดได้หรือไม่ เป็นปัญหาที่เครื่องมือ บุคลากรหรือองค์ความรู้ และจะต้องมีการพัฒนาเพื่อเตรียมความพร้อมในการแก้ไขปัญหาอย่างไร	- ควรจัดทำเป็นกรณีศึกษา และแนวทางในการสืบสวนดำเนินคดีเพื่อให้เจ้าหน้าที่สามารถเรียนรู้จากประสบการณ์ของผู้อื่นได้ - มีการจำลองสถานการณ์ เพื่อฝึกความพร้อมของเจ้าหน้าที่ในการปฏิบัติงาน
คนที่ 5	ควรมี 2 ส่วนหลัก คือ การดำเนินการส่วนกลาง และส่วนพื้นที่ - ในส่วนกลางมีดำเนินการงานต่าง ๆ ที่เป็นภาพรวมของประเทศ เช่น การประชาสัมพันธ์ การป้องกันระวังภัยคุกคามที่อาจจะเกิดขึ้น การพัฒนาองค์ความรู้และเทคโนโลยี และการสืบสวนคดีที่เป็นคดีสำคัญหรือมีความซับซ้อน - ในส่วนพื้นที่ ควรกระจายหน่วยงานไปอยู่ในระดับภูมิภาค เพื่อให้ประชาชนสามารถแจ้งความ ร้องทุกข์ หรือเข้ามาปรึกษา	ควรแยกการบริหารงานจากโครงสร้างเดิมของตำรวจในระดับปฏิบัติการ เพราะบุคคลากร ลักษณะงาน เครื่องมืออุปกรณ์ต่าง ๆ นั้นแตกต่างจากงานตำรวจปกติค่อนข้างมาก จึงควรแยกให้เกิดความชำนาญเฉพาะด้าน	การพัฒนารูปแบบควรจะทำในลักษณะ ปรับเปลี่ยนกระบวนทัศน์ของการทำงานด้านอาชญากรรมเทคโนโลยี เพราะเพียงการพัฒนาและปรับปรุงเล็กน้อยต่อการทำงานของตำรวจเดิม ไม่อาจตอบสนองต่ออาชญากรรมดังกล่าว อันเนื่องจากแม้จะเป็นงานด้านป้องกันและสืบสวนปราบปรามอาชญากรรมเหมือนกันก็จริง แต่กลับมีความแตกต่าง ๆ อย่างมากในด้านอื่น ๆ เช่น บุคลากร ลักษณะงาน เครื่องมือ องค์ความรู้ และข้อกฎหมายต่าง ๆ

ตารางที่ 4-2 ความคิดเห็นในประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานทางด้านอาชญากรรมทางเทคโนโลยีที่ดี (ต่อ)

ผู้ให้ความเห็น	รูปแบบในการปฏิบัติงาน	เทคนิคในการบริหารงาน	การพัฒนารูปแบบ
คนที่ 5 (ต่อ)	ขอความช่วยเหลือได้เมื่อตกเป็นเหยื่อของอาชญากรรมทางเทคโนโลยี โดยดำเนินการสืบสวนเบื้องต้นได้ระดับหนึ่งแล้วมอบคดีต่อให้กับหน่วยงานส่วนกลาง		
คนที่ 6	การปฏิบัติงานด้านการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ที่ดี และไม่ส่งผลเสียหายต่อการดำเนินคดีในกระบวนการยุติธรรม ประกอบด้วย 5 ด้าน คือ (1) มีอำนาจหน้าที่ คือ ผู้ปฏิบัติงานจะต้องมีอำนาจหรือหน้าที่ตามที่กฎหมาย ระเบียบ หรือคำสั่งที่กำหนด (2) มีความรู้ความสามารถ คือ ผู้ปฏิบัติงานจะต้องมีคุณวุฒิ มีประสบการณ์ หรือ ผ่านการฝึกอบรมเพื่อให้มีความรู้ความสามารถอย่างแท้จริง (3) มีเครื่องมือที่เหมาะสม คือ เครื่องมือที่ใช้ต้องเป็นที่ยอมรับเที่ยงตรง ทันสมัย และมีมาตรฐาน (4) มีการปฏิบัติตามขั้นตอน คือ มีการกำหนดขั้นตอนการปฏิบัติที่ชัดเจน ถูกต้องตามหลักวิชา และปฏิบัติตามขั้นตอนที่กำหนดไว้ (5) มีการอธิบายหรือถ่ายทอดที่เข้าใจ คือ การอธิบายหรือการออกรายงานผลการตรวจพิสูจน์ที่ชัดเจน ครบถ้วน ถูกต้องตามหลักวิชา และสามารถเบิกความให้การในฐานะพยานผู้เชี่ยวชาญในกระบวนการยุติธรรมได้อย่างถูกต้องปราศจากข้อสงสัย	-	-

3) ประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

รายละเอียดตามตารางที่ 4-3

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 1	หน่วยงานตำรวจที่รับผิดชอบมักจะอยู่ส่วนกลาง ขณะที่ส่วนภูมิภาคไม่มีหน่วยงานตำรวจรับผิดชอบโดยตรง ในขณะที่อาชญากรรมทางเทคโนโลยีจะเกิดขึ้นทั่วประเทศ ระเบียบข้อบังคับ กฎหมายที่ใช้อยู่ในปัจจุบันยังตามหลังเทคโนโลยี ในการกระทำความผิดเสมอ นอกจากนี้การบูรณาการระหว่างหน่วยงานยังไม่เป็นไปในทิศทางเดียวกัน	ความก้าวหน้าของเทคโนโลยีเปลี่ยนแปลงค่อนข้างเร็วมาก ดังนั้นเมื่ออาชญากรใช้เทคโนโลยีระดับสูงในการกระทำความผิด ยุทธศาสตร์วิธีการป้องกันและปราบปราม มาตรการและวิธีการป้องกันและปราบปรามจึงต้องไล่ตามเทคโนโลยีที่อาชญากรใช้ให้ทัน หน่วยงานตำรวจที่ทำหน้าที่ต้องทำในลักษณะเชิงรุก ไม่ใช่ตั้งหลักรอแต่ให้ผู้เสียหายเข้ามาร้องทุกข์จึงจะดำเนินการให้	รูปแบบอาชญากรรมใน การทำความผิดจะยุ่งยากสลับซับซ้อนมากยิ่งขึ้น การวิเคราะห์อาชญากรรมก็จะต้องใช้องค์ความรู้ที่จะต้องมีการบูรณาการความรู้ในสาขาวิชามากขึ้น	ระดับการศึกษาของเจ้าหน้าที่ประสบการณ์การทำงานของเจ้าหน้าที่ และความรู้ทางด้านเทคโนโลยีของเจ้าหน้าที่หน่วยงานตำรวจที่ปฏิบัติงานในปัจจุบัน จัดว่ามีเพียงพอ องค์ความรู้ความชำนาญงาน ของเจ้าหน้าที่มีเพียงพอที่จะปฏิบัติงานป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในปัจจุบัน	เครื่องมือและอุปกรณ์การตรวจสถานที่เกิดเหตุในปัจจุบันมีการพัฒนาและได้รับงบประมาณเพิ่มเติมดีขึ้นกว่าในอดีตมาก อาจจะไม่เพียงพอที่จะใช้ในการปฏิบัติงาน อุปกรณ์บางตัวมีราคาสูง แต่ในแง่ของการครอบครองพยานหลักฐานยังดูแล้วน่าเป็นห่วง โดยเฉพาะเจ้าหน้าที่อื่นที่ร่วมทำงานด้วย เช่น เจ้าหน้าที่กู้ภัย เพราะยังมีองค์ความรู้ในเรื่องดังกล่าวน้อย	ปัจจุบันเจ้าหน้าที่มีเทคนิคในการสืบสวนสอบสวนพัฒนาดีขึ้นกว่าในอดีตมาก มีความรู้ในการแสวงหาข้อเท็จจริงและหลักฐานดี แต่บางครั้งอาจจะมีปัญหาในเรื่องเขตอำนาจการสอบสวนที่อาจจะมีการทับซ้อนกันอยู่บ้าง
คนที่ 2	ความเห็นส่วนตัวฯ ปัญหาการดำเนินคดีอาชญากรรมทางเทคโนโลยี มีมาก แต่ไม่มีการช่วยเหลือกันในหน่วยงาน และระหว่างหน่วยงานเพื่อแก้ไขปัญหาต่าง ๆ อย่างเป็นระบบ ไม่เฉพาะแต่ สตช. แต่หน่วยงานอื่นก็มีปัญหาเหล่านี้ ซึ่งเป็นอุปสรรคต่อการดำเนินคดีอาชญากรรมทางเทคโนโลยีเช่นกัน	ไม่ทราบแน่ชัด	ความเห็นส่วนตัวฯ มาตรการระบุตัวตนของผู้ใช้งานในระบบคอมพิวเตอร์และอินเทอร์เน็ต และการทำธุรกรรมต่าง ๆ ทั้งการสื่อสารและการเงิน ยังไม่มีประสิทธิภาพเพียงพอ ทำให้คนร้ายมีโอกาสในการกระทำผิดและปกปิดตัวตนได้ง่าย	เจ้าหน้าที่ตำรวจส่วนใหญ่ ทั้งฝ่ายสืบสวนและพนักงานสอบสวน ยังขาดแคลนองค์ความรู้พื้นฐานในการดำเนินคดีอาชญากรรมทางเทคโนโลยี ซึ่งเป็นปัญหาสำคัญ ในบริหารจัดการดำเนินคดีอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับระบบคอมพิวเตอร์และอินเทอร์เน็ต	หน่วยงานของ สตช. หลายหน่วยยังขาดแคลนอุปกรณ์และเครื่องมือที่จะใช้ในการเข้าถึงพยานหลักฐานที่เป็นข้อมูลต่าง ๆ ในระบบคอมพิวเตอร์และอินเทอร์เน็ต	เจ้าหน้าที่ตำรวจฝ่ายสืบสวนส่วนใหญ่ มีองค์ความรู้ด้านเทคนิคและมีช่องทางในการสืบสวนคดีอาชญากรรมทางเทคโนโลยีได้ค่อนข้างดี แต่ขาดองค์ความรู้ในการจัดเก็บและเรียบเรียงข้อมูลต่าง ๆ ให้นำมาใช้เป็นพยานหลักฐานที่มีน้ำหนักในการพิสูจน์ข้อเท็จจริง

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 3	ต้องมีการทบทวนภารกิจระเบียบกฎหมาย การบูรณาการ การทำงานร่วมกันกับหน่วยงานอื่นอย่างสม่ำเสมอ เนื่องจากมีการเปลี่ยนแปลงบ่อย ทั้งนโยบาย, กฎหมาย สถานการณ์ต่างๆครบด้าน	ต้องมองภาพทุกอย่างให้รอบด้าน และกำหนดให้ชัดเจน และต้องทบทวนตลอดเวลา	ต้องวิเคราะห์เพิ่มเติมถึงเทคโนโลยี และนวัตกรรมต่าง ๆ ที่เปลี่ยนแปลงไปด้วย ตลอดจนสภาพแวดล้อมต่าง ๆ เทคนิค, วิธีการ, สภาพชีวิตความเป็นอยู่ในปัจจุบัน และอนาคต ตลอดจนการบังคับใช้กฎหมายให้ได้ผลอย่างแท้จริง และการแก้ไขกฎหมายให้เท่ากันต่ออาชญากรรมด้วย	ความรู้ ความสามารถ ทักษะ และประสบการณ์ ที่เหมาะสมเฉพาะทาง โดยเป็นเรื่องที่สำคัญต่อการทำงาน	ทุกอย่างมีความสำคัญและเกี่ยวข้องกันอย่างเป็นระบบ ต้องมีมาตรฐาน และความเชี่ยวชาญสูง ในการทำงานจะขาดสิ่งใดไปไม่ได้เลย	ต้องมีการวิเคราะห์ข้อเท็จจริงและพยานหลักฐาน, การตรวจพิสูจน์, และความร่วมมือระหว่างประเทศเพิ่มเติม
คนที่ 4	- สถานีตำรวจเป็นหน่วยงานหลักในการดำเนินคดีอาญาที่เกี่ยวข้องกับทางเทคโนโลยี - ในขณะที่ บก.ปอท. มุ่งเน้นในการดำเนินคดีด้านอาชญากรรมทางเทคโนโลยีโดยตรง - ส่วนหน่วยงานเฉพาะทางอื่น ๆ รับผิดชอบในส่วนคดีที่ตนรับผิดชอบ ซึ่งเกี่ยวพันกับเทคโนโลยี	- ปัจจุบันการป้องกันปราบปรามไม่สามารถกระทำโดยหน่วยงานของตำรวจเพียงหน่วยเดียว จำเป็นต้องอาศัยการบูรณาการทั้งภาครัฐ และเอกชน ดังนั้น รัฐบาลจำเป็นต้องมอบหมายให้ระดับรองนายกรัฐมนตรีลงมากำกับดูแลโดยตรง เพื่อมุ่งเน้นกลไกการระบุตัวตนในโลกออนไลน์เพื่อลดช่องโอกาสในการกระทำความผิด	- สาเหตุหรือแรงจูงใจ ส่วนใหญ่จะเป็นเรื่องของเงิน รูปแบบที่พบเจอมากที่สุดคือการหลอกลวง เช่น คดีแก๊งค์ Call center ,หลอกขายของ เป็นต้น เมื่อวิเคราะห์จะพบว่าสาเหตุที่มีคดีเกิดขึ้นเป็นจำนวนมาก เพราะภาครัฐมิได้บังคับใช้กฎหมายการระบุตัวตนอย่างจริงจัง	- ปัจจุบันหน่วยงานของตำรวจมีองค์ความรู้ และความชำนาญในด้านอาชญากรรมทางเทคโนโลยีในระดับดี แต่ไม่สามารถรักษาบุคลากรให้เจริญเติบโตมีความชำนาญในสายอาชีพได้	- ปัจจุบันในส่วนของตำรวจมีหน่วย พฐก.ทำหน้าที่ในการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ โดยมี บก.สสท. เป็นหน่วยเสริมที่พบปัญหาที่มีความซับซ้อน ซึ่งในส่วนของการยึดพยานหลักฐานเป็นหน้าที่ของตำรวจที่ไปตรวจยึดพื้นที่เกิดเหตุ และส่งตรวจต่อไป	- สภาพปัญหาที่พบในปัจจุบันคือ สื่อสังคมออนไลน์ส่วนใหญ่เป็นของต่างประเทศ และไม่ค่อยได้รับความร่วมมือ - นอกจากนี้ข้อมูลในส่วนของผู้ให้บริการอินเตอร์เน็ตในประเทศไทย ก็ไม่ได้รับความร่วมมือเช่นกัน ทำให้ยากต่อการสืบสวนดำเนินคดี

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 5	- บก.ปอท. เป็นหน่วยงานตรงที่รับผิดชอบอาชญากรรมทางเทคโนโลยี ซึ่งมีความรู้ความสามารถ และความชำนาญในการสืบสวนอาชญากรรมดังกล่าว แต่เนื่องจากการเพิ่มขึ้นของอาชญากรรมทางเทคโนโลยีจำนวนมาก อาจทำให้ไม่เพียงพอต่อการปฏิบัติงาน - ในบางกรณีที่เป็นอาชญากรรมปกติ แต่อาศัยเทคโนโลยีเป็นเครื่องมือในการก่ออาชญากรรม เช่น การหมิ่นประมาททาง Social Media , การฉ้อโกงทางอินเตอร์เน็ต ในปัจจุบันมีจำนวนมหาศาลและอาจไม่เข้าลักษณะงานโดยตรงของ บก.ปอท. เป็นความรับผิดชอบของงานตำรวจในพื้นที่ แต่เมื่อผู้เสียหายมาแจ้งความที่สถานีตำรวจที่รับผิดชอบอาชญากรรมทั่วไป ก็จะมีขีดความสามารถในการสืบสวนทางเทคโนโลยีไม่เพียงพอ	ปัจจุบันโดยส่วนมากจะเป็นลักษณะที่เกิดเหตุขึ้น แล้วมีผู้เสียหายได้รับความเสียหายมาแจ้งความร้องทุกข์กับเจ้าหน้าที่ตำรวจ จากนั้นก็จะเข้าสู่กระบวนการสืบสวนสอบสวน ถ้าเป็นการแจ้งความกับพนักงานสอบสวนในระดับสถานีตำรวจ ก็เป็นการสอบสวนไปตามขั้นตอน เช่น ทำหนังสือสอบถามข้อมูลไปหน่วยงานต่าง ๆ เช่น ข้อมูลการโอนเงิน ข้อมูลอินเตอร์เน็ต ซึ่งส่วนมากก็จะไม่ได้รับความร่วมมือจากบริษัทเอกชน หรือได้รับแต่ล่าช้ามาก แต่หากว่าผู้เสียหายไปแจ้งความร้องทุกข์ที่ บก.ปอท. ซึ่งมีเจ้าหน้าที่ตำรวจที่มีความชำนาญเฉพาะก็จะมีการสืบสวนที่มีประสิทธิภาพมากกว่า และเข้าถึงข้อมูลต่างๆ ในลักษณะการสืบสวนเชิงลึกได้ แต่ดังที่กล่าวไปแล้วว่าเจ้าหน้าที่ตำรวจ บก.ปอท. ก็มีอยู่ในจำนวนจำกัด	โอกาสผู้ที่จะตกเป็นเหยื่อของอาชญากรรมเทคโนโลยี กระจายตัวเพิ่มมากขึ้น แต่เดิมที่ผู้ที่เข้าถึงเทคโนโลยีอาจจำกัดอยู่ในวงแคบ แต่ในปัจจุบันมีการกระจายตัวไปสู่ทุกระดับอายุ กลุ่มอาชีพ หรือภูมิภาคต่าง ๆ เช่นการโอนเงินผ่านโทรศัพท์มือถือ การมีบัญชี social media หรือการสืบสวนผ่านแอพลิเคชั่นไลน์ เป็นต้น เมื่อช่องทางการเข้าถึงเหยื่อมากขึ้น โอกาสก็จะมากขึ้นไปด้วยเช่นกัน อาชญากรจะสามารถจะคิด ค้นหากลลวง หรือช่องทางต่าง ๆ ที่จะหลอกลวงหรือกระทำต่อเหยื่อได้หลากหลายยิ่งขึ้น	เจ้าหน้าที่ตำรวจทั่วไป มีจำนวนน้อยมากที่มีความรู้และความชำนาญในการสืบสวนอาชญากรรมเทคโนโลยี ส่วนมากจะอยู่ที่ บก.ปอท. ในช่วง 5 ปี ที่ผ่านมา มีการรับเจ้าหน้าที่ตำรวจในวุฒิการศึกษาทางคอมพิวเตอร์เฉพาะ แต่ส่วนมากก็จะปฏิบัติหน้าที่ในส่วนของฝ่ายอำนวยการเป็นหลัก มีจำนวนไม่มากที่ได้อยู่ในฝ่ายปฏิบัติ	มีหน่วยงานกองพิสูจน์หลักฐานรับผิดชอบ ซึ่งมีเครื่องมือและเจ้าหน้าที่ที่มีประสิทธิภาพ แต่จะมีเฉพาะที่ส่วนกลาง	การสืบสวนมีอยู่ 2 ส่วนหลัก คือ การระบุตัวตนผู้กระทำผิด และการรวบรวมพยานหลักฐาน การระบุตัวตนผู้กระผิด เนื่องจากไม่สามารถเข้าถึงข้อมูลหลักหรือข้อมูลทางเทคนิคของระบบต่างๆ ได้ เช่น facebook , e-mail , Line การสืบสวนจึงต้องอาศัยการสืบสวนทางข้าง เช่น ข้อมูลรูปภาพ ข้อมูลต่างๆ ที่เคยโพสหรือส่งของผู้ต้องสงสัย หรือร่องรอยต่างๆ ที่พบอยู่ในลักษณะที่สามารถเข้าถึงได้โดยทั่วไป ส่วนการรวบรวมพยานหลักฐานนั้น ถ้าจะยืนยันว่าคนร้ายเป็นผู้กระทำผิดได้นั้น เนื่องจากไม่สามารถเข้าถึงข้อมูลทางเทคนิคของระบบได้ดังที่กล่าวข้างต้น จำเป็นที่จะต้องเข้าถึงข้อมูลปลายทางที่อยู่ที่ตัวคนร้าย เช่น โทรศัพท์มือถือ หรือเครื่องคอมพิวเตอร์ ของคนร้าย แล้วตรวจยึดส่งตรวจพิสูจน์ แต่โอกาสที่จะถูกลบข้อมูลต่าง ๆ ทิ้งก็มีสูง อีกทั้งด้วยเทคโนโลยีเข้ารหัสใน

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 5 (ต่อ)	- และงานการป้องกัน หรือประชาสัมพันธ์ อาชญากรรมทางเทคโนโลยี ยังไม่มีหน่วยงานใดของตำรวจเป็นผู้รับผิดชอบโดยตรง	อาจไม่เพียงพอต่อคดีที่เกิดขึ้นจำนวนมากได้ และไม่มีหน่วยงานของ บก.ปอท. ที่กระจายไปรับแจ้งความร้องทุกข์ในต่างจังหวัด				ปัจจุบันก็มีการป้องกันการกู้ข้อมูลจากหน่วยความจำ เป็นส่วนมากแล้ว เจ้าพนักงาน ตาม พรบ. คอมพิวเตอร์ ฯ มีเฉพาะเจ้าหน้าที่ส่วนกลาง การสืบสวนและรวบรวมพยานหลักฐานของเจ้าหน้าที่ตำรวจพื้นที่จึงต้องใช้อำนาจปกติตาม ป.วิ.อาญา
คนที่ 6	มีหน้าที่และความรับผิดชอบเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐานและของกลางในคดีเกี่ยวกับคอมพิวเตอร์และเทคโนโลยี โดยปฏิบัติหน้าที่ ดังนี้ 1) ตรวจพิสูจน์ข้อมูลดิจิตอลที่บันทึกในหน่วยบันทึกข้อมูลหรือหน่วยความจำคอมพิวเตอร์ 2) ตรวจพิสูจน์คอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ 3) ตรวจพิสูจน์การตัดต่อสื่อบันทึกเสียงและวีดิทัศน์ 4) ตรวจพิสูจน์เปรียบเทียบร่องรอยบนแผ่นซีดี	ทำหน้าที่สนับสนุนการปฏิบัติงานของพนักงานสอบสวน และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับการการกระทำความผิดทางเทคโนโลยี โดยทำหน้าที่เป็นนักวิทยาศาสตร์ผู้ชำนาญการตรวจพิสูจน์วัตถุพยาน ของสำนักงานตำรวจแห่งชาติ เพื่อแสวงหาข้อเท็จจริงทางคดีที่บันทึกด้วยกระบวนการทางดิจิตอล และทำหน้าที่เป็นพยานผู้เชี่ยวชาญในชั้นศาล	ตรวจวิเคราะห์ข้อมูลทางดิจิตอลในวัตถุพยานตามประเด็นคำถามที่พนักงานสอบสวนร้องขอ และเชื่อมโยงความสัมพันธ์ของรูปแบบแผนประทุษกรรมทางคดีเพื่อสนับสนุนการสืบสวนของเจ้าหน้าที่ตำรวจ	นักวิทยาศาสตร์ที่ปฏิบัติงานด้านการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ทุกนาย จะต้องมีระดับปริญญาไม่ต่ำกว่าปริญญาตรีทางวิทยาศาสตร์ด้านวิทยาการคอมพิวเตอร์ คอมพิวเตอร์เทคโนโลยี คอมพิวเตอร์สารสนเทศ หรือ สาขาวิชาฟิสิกส์ โดยจะต้องทำการฝึกอบรมในหลักสูตรการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ (ภาคทฤษฎี) และฝึกปฏิบัติเป็นผู้ช่วยผู้ตรวจพิสูจน์ทำการเก็บสะสมคดีไม่น้อยกว่า 100 คดี (ภาคปฏิบัติ)	เครื่องมือที่ใช้ในห้องปฏิบัติการ ตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ประกอบด้วยอุปกรณ์ทาง Hardware และ Software เช่นเดียวกับที่มีใช้ในห้องปฏิบัติการชั้นนำของโลก ปัญหาที่ประสบคืออุปกรณ์ต่างๆ ล้วนแต่มีราคาแพง โดยเฉพาะอย่างยิ่ง Software จำเป็นต้องใช้ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย มิเช่นนั้นจะส่งผลเสียต่อความถูกต้องและความน่าเชื่อถือของผลการตรวจพิสูจน์ในกระบวนการยุติธรรม	การตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ของสำนักงานพิสูจน์หลักฐานตำรวจ เป็นการใช้กระบวนการทางวิทยาศาสตร์ ในการสืบค้นข้อมูลทางดิจิตอลในวัตถุพยานที่พนักงานสอบสวนส่งมาให้ตรวจพิสูจน์ การครอบครองและอำนาจการสืบค้นหาข้อมูลเป็นการใช้อำนาจของพนักงานสอบสวนที่มีอำนาจหน้าที่ตามกฎหมาย การปฏิบัติงานของผู้ชำนาญเป็นการใช้ความรู้ทางวิทยาศาสตร์ และกระบวนการปฏิบัติตามหลักวิชาและมาตรฐานสากล

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 6 (ต่อ)	5) อื่นๆ ตามที่ผู้บังคับบัญชามอบหมาย			และมีระยะเวลาการเรียนรวมปฏิบัติไม่น้อยกว่า 1 ปี (สะสมประสบการณ์) จึงจะมีสิทธิขอรับการทดสอบ เมื่อผ่านการทดสอบ จะได้รับอนุมัติจากสำนักงานพิสูจน์หลักฐานตำรวจ ให้สามารถทำการตรวจพิสูจน์สาขาอาชญากรรมคอมพิวเตอร์ และออกรายงานผลการตรวจพิสูจน์ด้วยตนเองได้ต่อไป	ปัญหาด้านการขาดแคลนงบประมาณ(ซึ่งเป็นปัญหาหลักของรัฐบาล)และการขาดความเข้าใจที่แท้จริงของผู้บริหารที่มีหน้าที่พิจารณาจัดสรรงบประมาณ โดยตัดเครื่องมือบางอย่างที่จำเป็นออกทั้งที่มีความสำคัญ จะเป็นปัจจัยที่สำคัญอย่างยิ่งต่อการพัฒนาหรือขยายการตรวจพิสูจน์หลักฐานด้านนี้ออกไปสู่ส่วนภูมิภาค ส่วนการตรวจสถานที่เกิดเหตุกรณีอาชญากรรมคอมพิวเตอร์ รวมถึงหลักการครอบครองวัตถุพยาน ตามหลักสากล ปัจจุบันได้ทำการถ่ายทอดความรู้ด้านนี้ให้แก่พนักงานสอบสวนในหลักสูตรต่าง ๆ ของสถาบันการศึกษาตำรวจ คือ สถาบันส่งเสริมงานสอบสวน สำนักงานตำรวจแห่งชาติ โดยถ่ายทอดความรู้ด้านให้แก่พนักงานสอบสวนนี้ไปแล้วประมาณ 1,000 นาย และ	ในการแสวงหาข้อเท็จจริงสนับสนุนการปฏิบัติงานของพนักงานสอบสวน

ตารางที่ 4-3 ความเห็นในประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	หน่วยงานตำรวจที่ปฏิบัติงาน	การป้องกันปราบปราม	การกระทำความผิด	องค์ความรู้ความชำนาญงาน	การพิสูจน์หลักฐาน	การสืบสวนสอบสวน
คนที่ 6 (ต่อ)					ถ่ายทอดเพิ่มเติมให้แก่เจ้าหน้าที่ฝ่ายปฏิบัติการของคณะทำงานปราบปรามการละเมิดเด็กและสตรี สำนักงานตำรวจแห่งชาติ (TICAC) จำนวนประมาณ 100 นาย	

4) ประเด็นเกี่ยวกับสภาพปัญหาด้านการบริหารจัดการของหน่วยตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

รายละเอียดตามตารางที่ 4-4

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ

ผู้ให้ความเห็น	บุคลากร	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 1	ยังขาดบุคากรที่มีความรู้ความเชี่ยวชาญอยู่มาก ค่าตอบแทนที่รัฐจ่ายให้บุคลากรด้านนี้ยังน้อยเกินไป บางครั้งเจ้าหน้าที่อาจจะมีปัญหาความเครียดและความกดดันจากการทำงานเพราะต้องทำงานแข่งกับเวลา	งบประมาณในการประชาสัมพันธ์ยังน้อยเกินไป ประเภทของสื่อที่ใช้ประชาสัมพันธ์มีไม่กี่ประเภท บางครั้งไม่สามารถสื่อไปถึงประชาชนได้ทุกกลุ่ม	เจ้าหน้าที่ขาดแคลนเครื่องมืออุปกรณ์ในการสืบสวนหาข่าวและจัดเก็บวัตถุพยาน บางครั้งต้องใช้ทุนทรัพย์ส่วนตัวในการจัดหาเครื่องมืออุปกรณ์การปฏิบัติงาน	เจ้าหน้าที่ยังคงใช้ซอฟแวร์รุ่นเก่าในการทำงาน ซึ่งอาจจะใช้ปฏิบัติหน้าที่ได้ แต่อาจจะมีประสิทธิภาพสูงสู้ซอฟแวร์รุ่นปัจจุบันไม่ได้
คนที่ 2	- ควรหาทางแบ่งเบาภาระในบางขั้นตอนให้แก่พนักงานสอบสวนในแต่ละคดี - พนักงานสอบสวนควรมีเจ้าหน้าที่อื่นช่วยเหลือในการปฏิบัติหน้าที่ และมีผู้บังคับบัญชาที่พร้อมช่วยแก้ปัญหาสำหรับการสอบสวนในขั้นตอนหรือคดีที่เกินความสามารถของพนักงานสอบสวน	-	-	ด้านโปรแกรมตรวจพิสูจน์และโปรแกรมอื่น มีค่าลิขสิทธิ์ และค่าใช้จ่ายสูง ทั้งยังจำเป็นต้องใช้งานในระยะยาว จึงควรหาทางพัฒนาโปรแกรมที่สามารถเข้าถึงและเรียกดูพยานหลักฐาน ในระบบคอมพิวเตอร์และอินเทอร์เน็ตเบื้องต้น เพื่อลดค่าใช้จ่าย และสร้างองค์ความรู้ขึ้นเอง ลดการพึ่งพาโปรแกรมต่าง ๆ ที่ต้องจัดซื้อจากต่างประเทศ
คนที่ 3	ยังไม่ได้ให้ความสำคัญ พัฒนาและสนับสนุนเท่าที่ควร	ต้องใช้งบประมาณมากขึ้นเรื่อย ๆ	เครื่องมือในการทำงานที่จำเป็น และสำคัญต้องมีอย่างเพียงพอ และต้องปรับปรุงประสิทธิภาพอยู่ตลอดเวลา	ต้องอาศัยงบประมาณ และสนับสนุนอยู่ตลอดเวลา
คนที่ 4	- ขาดแคลนบุคลากร เนื่องจากบรรจุไม่ครบตำแหน่งที่ว่าง หรือมีการยืมตัวไปช่วยราชการที่อื่น - ขาดความเชี่ยวชาญในการปฏิบัติหน้าที่ทางเทคโนโลยี	- ขาดแคลนงบประมาณในการจัดหาเครื่องมือที่ทันสมัย ตลอดจนฝึกอบรมให้มีความชำนาญเฉพาะทางอย่างต่อเนื่อง	- ขาดแคลนเครื่องมือที่จำเป็นต้องใช้ในการปฏิบัติงานทั้งด้านการสืบสวน หาข่าว และจัดเก็บพยานหลักฐานทางอิเล็คทรอนิกส์	- ขาดซอฟแวร์ที่ทันสมัยเพื่อช่วยในการเก็บและวิเคราะห์ข้อมูล
คนที่ 5	มีจำนวนไม่เพียงพอ ส่วนที่เคยรับข้าราชการตำรวจวุฒิคอมพิวเตอร์เฉพาะส่วนมากก็จะอยู่ฝ่ายอำนวยการ ไม่ได้ปฏิบัติหน้าที่สืบสวนปราบปราม	งบประมาณไม่ได้มีกำหนดเฉพาะสำหรับงานด้านอาชญากรรมเทคโนโลยี ซึ่งเป็นงานที่ต้องใช้งบประมาณสูง	มีเฉพาะในส่วนกลาง เช่น บก.ปอท. , กองพิสูจน์หลักฐานกลาง	มีเฉพาะในส่วนกลาง ไม่ได้กระจายใช้งานในตำรวจระดับท้องที่

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	บุคลากร	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 5 (ต่อ)	และการโยกย้ายบุคลากรในตำแหน่งที่ต้องอาศัยความรู้ทางเทคโนโลยีเฉพาะ ก็ไม่ได้มีหลักเกณฑ์เฉพาะ			
คนที่ 6	ในภาพรวมขององค์กร ปัจจุบันมีผู้ปฏิบัติงานด้านการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ประมาณ 12 นาย ทำหน้าที่ตรวจพิสูจน์หลักฐาน ใน 3 หน่วยงานหลัก คือ (1) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง รับผิดชอบพื้นที่ ทั่วประเทศ (ผู้ปฏิบัติงาน 6 นาย) (2) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 7 รับผิดชอบพื้นที่ภาคตะวันตกถึงภาคใต้ และ ทั่วประเทศ ในคดีเกี่ยวกับการละเมิดเด็กและสตรี (ผู้ปฏิบัติงาน 2 นาย) (3) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 10 รับผิดชอบพื้นที่ 3 จว.ชายแดนภาคใต้ (ผู้ปฏิบัติงาน 1 นาย) (4) สำหรับศูนย์พิสูจน์หลักฐาน 1 (ปทุมธานี) ศูนย์พิสูจน์หลักฐาน 3 (นครราชสีมา) และ ศูนย์พิสูจน์หลักฐาน 5 (ลำปาง) มีผู้ชำนาญแห่งละ 1 นาย แต่ไม่สามารถปฏิบัติงานได้เนื่องจากไม่มีเครื่องมือหรือ มีแต่อุปกรณ์ Hardware แต่ขาด Software ที่จะทำงานร่วมกัน	ไม่มีงบประมาณด้านการจัดทำสื่อประชาสัมพันธ์เป็นการเฉพาะ ปัจจุบันใช้วิธีการนำเสนอข้อมูลที่น่าสนใจในการปฏิบัติงานหรือข้อมูลเพื่อเตือนภัยแก่ประชาชนผ่าน website ของสำนักงานพิสูจน์หลักฐานตำรวจ คือ www.forensic.police.go.th	ขาดแคลนเครื่องมือในการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ปัจจุบันมีเครื่องมือและสามารถทำการตรวจพิสูจน์ใน 3 หน่วยงาน คือ กองพิสูจน์หลักฐานกลาง ศูนย์พิสูจน์หลักฐาน 7 (ไม่มีเครื่องมือเป็นของตนเองแต่ใช้เครื่องมือในการปฏิบัติร่วมกับห้องปฏิบัติการ Digital Forensic) ของคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ซึ่งได้รับการสนับสนุนจากต่างประเทศ) และ ศูนย์พิสูจน์หลักฐาน 10 ส่วนศูนย์พิสูจน์หลักฐาน 1 2 3 4 5 6 8 และ 9 ยังไม่มีเครื่องมือไม่สามารถทำการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ได้	การตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ จำเป็นอย่างยิ่งที่ต้องใช้อุปกรณ์ทาง Hardware ประสิทธิภาพสูง และ Software ที่มีการอัพเดทให้ทันสมัยตลอดเวลา เพื่อให้สามารถเข้าไปสืบค้นในอุปกรณ์ต่าง ๆ ที่พัฒนาก้าวหน้าในแต่ละปี อุปกรณ์ในการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ส่วนมากจะเป็นอุปกรณ์ที่ออกแบบเป็นการเฉพาะ มีราคาแพงและมักจะต้องจัดหาจากต่างประเทศ ปัจจุบันยังมีผู้บริหารและผู้ที่เกี่ยวข้องกับระบบงบประมาณบางราย ที่มิได้ตระหนักถึงข้อเท็จจริงนี้ จึงอาจเกิดกรณีที่หน่วยงานเสนอของบประมาณแล้วมิได้รับจัดสรรหรือ จัดสรรให้แต่อุปกรณ์ Hardware (ซึ่งจับต้องได้) แต่มิได้จัดสรรงบประมาณในการจัดซื้อ Software (ทั้งที่เป็นส่วนสำคัญ) ซึ่งเป็นสาเหตุให้การปฏิบัติงานในบางหน่วยเป็นไปอย่างไม่มีประสิทธิภาพ หรือมิอาจปฏิบัติงานได้ในบางกรณี

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	บุคลากร	งบประมาณ	เครื่องมือและอุปกรณ์	เทคโนโลยี
คนที่ 6	กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ สำนักงานพิสูจน์หลักฐานตำรวจ มีอัตรากำลังเต็มจำนวน (กองพิสูจน์หลักฐานกลาง , ศูนย์พิสูจน์หลักฐาน 1 – 10) ประมาณ 50 นาย (ขาดอยู่ 38 นาย) โดยใน พ.ศ.2561 สำนักงานตำรวจแห่งชาติอนุมัติบรรจุเพิ่มเติมให้จำนวน 10 นาย กระจายลงในศูนย์พิสูจน์หลักฐานที่ยังไม่มีบุคลากรด้านนี้ และในปี พ.ศ.2562 คาดว่าจะมีการเพิ่มเติมให้อีก 10 นาย	-	-	-

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	การบริหารจัดการ	ปัญหานโยบายและยุทธศาสตร์	ด้านบูรณาการร่วมกันระหว่างหน่วยงาน	ข้อเสนอแนะเพิ่มเติม
คนที่ 1	บางครั้งบางช่วงเวลาผู้บังคับบัญชาของหน่วยงานอาจจะไม่มีความรู้ความชำนาญเรื่องดังกล่าว หรือไม่มีการบริหารจัดการที่เป็นระบบ ซึ่งจะส่งผลให้ผู้ใต้บังคับบัญชาขาดแรงจูงใจในการทำงาน	นโยบายบางครั้งเป็นแต่เพียงข้อความที่สวยหรู แต่ไม่มีความชัดเจน และบางครั้งเป็นนามธรรม ไม่สามารถปฏิบัติได้ ดังนั้นนโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีควรจะชัดเจน ปฏิบัติได้อย่างเป็นรูปธรรม	ปัญหาหลักน่าจะเป็นหน่วยงานที่เกี่ยวข้องต่างฝ่ายต่างทำงาน งานบางส่วนก็มีความซ้ำซ้อนกัน ไม่มีหน่วยงานใดเป็นเจ้าภาพหลัก นอกจากนี้การตีความปัญหาข้อกฎหมาย ข้อบังคับ และระเบียบที่เกี่ยวข้องของหน่วยงานแต่ละแห่งก็ไม่เหมือนกัน ทำให้เกิดปัญหาในการบูรณาการการทำงานร่วมกันได้	-
คนที่ 2	-	-	-	-
คนที่ 3	ต้องบริหารจัดการอย่างเป็นระบบ ทั้งโครงสร้าง อำนาจหน้าที่บุคลากร วัสดุอุปกรณ์ เครื่องมือ มาตรฐานในการทำงาน	ต้องกำหนดให้ชัดเจนและวางแผนในระยะยาว, พัฒนาปรับปรุงเป็นระยะ ๆ	ต้องทำความตกลงชัดเจน พัฒนาอย่างต่อเนื่อง รักษาความสัมพันธ์อย่างต่อเนื่อง	แนวทางในการพัฒนาในการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี ต้องเริ่มจากการวิเคราะห์ Swot, วางแผนการทำงานทั้งในระยะสั้น และระยะยาว, กำหนดนโยบาย ทิศทางในการทำงานให้ครอบคลุมและชัดเจนลงรายละเอียดไปถึงการปฏิบัติ เน้นการสร้างมาตรฐานในการทำงาน, การพัฒนาบุคลากร การจัดหาเครื่องมือที่ทันสมัย, งบประมาณเพียงพอ, การสร้างความเชี่ยวชาญการสร้างความร่วมมือรอบด้าน, ปรับปรุงกฎหมายให้มีประสิทธิภาพ, วิจัยพัฒนาสร้างนวัตกรรม
คนที่ 4	- ขาดการสร้างแรงจูงใจในการทำงาน ทั้งผลตอบแทน และความเจริญก้าวหน้าในอาชีพ	- ปัญหาการบังคับใช้ตามกฎหมายให้มีประสิทธิภาพ	- ปัญหาการบูรณาการจากกรณีที่กำหนดในกฎหมายกับอำนาจหน้าที่มีความขัดแย้งกัน เช่น กระทรวง DC ดูแล พรบ. คอมพิวเตอร์ แต่ผู้ให้บริการอินเตอร์เน็ตเชื่อฟัง กสทช.มากกว่า เพราะมีอำนาจในการยกเลิกในอนุญาตเป็นต้น	-

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	การบริหารจัดการ	ปัญหานโยบายและยุทธศาสตร์	ด้านบูรณาการร่วมกันระหว่างหน่วยงาน	ข้อเสนอแนะเพิ่มเติม
คนที่ 5	ยังไม่มีการบริหารจัดการ ที่กำหนดเฉพาะสำหรับงานอาชญากรรมเทคโนโลยี ซึ่งแตกต่างจากอาชญากรรมทั่วไป	ที่ผ่านมามีความพยายามพลักดัน แก้กฎหมาย หรืออำนาจในการเข้าถึงข้อมูลเพื่องานการป้องกันและสืบสวนปราบปรามอาชญากรรมเทคโนโลยี แต่ก็ยังไม่สำเร็จ อันอาจมีสาเหตุมาจากการรู้สึกไม่ปลอดภัยที่จะถูกเข้าถึงข้อมูลต่าง ๆ จากภาครัฐ ทางภาครัฐหรือเจ้าหน้าที่ตำรวจ ตระหนักถึงภัยคุกคามด้านอาชญากรรมเทคโนโลยีเป็นอย่างดี เพราะได้รับทราบถึงสถานการณ์ที่เกิดขึ้นผ่านการแจ้งความร้องทุกข์ต่าง ๆ จำนวนมาก แต่แนวนโยบายยุทธศาสตร์หรือกลยุทธที่จะนำไปสู่การฏิบัติงานที่มาแก้ปัญหาดังกล่าวก็เป็นเรื่องยาก เนื่องจากเป็นสภาวะการณ์ที่เกิดขึ้นใหม่ อีกทั้งยังไม่ได้รับความร่วมมือจากทางภาคเอกชน หรือประชาชนโดยส่วนรวม	คดีความเป็นอาชญากรรมทั่วไป ที่ใช้เทคโนโลยีเป็นเครื่องมือ ยังเป็นช่องว่างในการปฏิบัติงานอยู่ กล่าวคือ อาจไม่ใช่หน้าที่ความรับผิดชอบของ บก.ปอท. โดยตรง และก็เกินขีดความสามารถของเจ้าหน้าที่ตำรวจระดับท้องที่ ซึ่งปัจจุบันมีจำนวนมาก และมีแนวโน้มที่จะเพิ่มมากขึ้น กฎหมายที่จะใช้เป็นเครื่องมือในการเข้าถึงข้อมูลต่าง ๆ เพื่อการสืบสวนระบุตัวค้นร้ายหรือใช้เป็นพยานหลักฐานในการดำเนินคดี ไม่มีประสิทธิภาพพอที่จะใช้บังคับกับภาคเอกชนที่เป็นผู้ครอบครองเหล่านั้นได้ โดยเฉพาะอย่างยิ่งถ้าเป็นผู้ให้บริการในต่าง ๆ ประเทศ	-
คนที่ 6	ผู้บังคับบัญชาในปัจจุบันทั้งจากภายในหน่วยงานคือสำนักงานพิสูจน์หลักฐานตำรวจ และระดับสูง คือ สำนักงานตำรวจแห่งชาติ ได้เล็งเห็นถึงความสำคัญของอาชญากรรมด้านนี้ โดยพยายามสนับสนุน บรรจุแต่งตั้งกำลังพลเพิ่มเติมให้ และสนับสนุนด้านงบประมาณการจัดซื้ออุปกรณ์ต่าง ๆ ที่เกี่ยวข้องให้แล้ว สามารถบรรเทาปัญหาได้ในชั้นต้นบางส่วน แต่เนื่องมาจากข้อจำกัดด้านงบประมาณและกำลังพลในภาพรวมของสำนักงานตำรวจแห่งชาติ จึงมิอาจแก้ปัญหาให้ลุล่วงได้ในเร็ววัน	สำนักงานพิสูจน์หลักฐานตำรวจ มีการกำหนดมาตรฐานในการปฏิบัติงานแต่ละด้านไว้อย่างชัดเจนแล้ว โดยผู้ชำนาญการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ของสำนักงานพิสูจน์หลักฐานตำรวจ ไม่ว่าจะอยู่ในสังกัด กองพิสูจน์หลักฐานกลาง หรือ ศูนย์พิสูจน์หลักฐาน 1 – 10 ต่างต้องยึดถือและปฏิบัติตามมาตรฐานของสำนักงานพิสูจน์หลักฐานตำรวจ ปัจจุบันห้องปฏิบัติการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ อยู่ระหว่างดำเนินการขอคำรับรองระบบมาตรฐาน ISO 17025 ซึ่งเป็นการรับรองตามระบบสากลต่อไป	ไม่พบปัญหาระหว่างการปฏิบัติร่วมกับหน่วยงานอื่น ภาพรวมของสำนักงานพิสูจน์หลักฐานตำรวจ มีภาพลักษณ์ในการสนับสนุนกระบวนการยุติธรรมต่อสาธารณะและต่อหน่วยงานอื่นในระดับที่ดี จึงส่งผลให้ทุกหน่วยงานที่ทำหน้าที่ตรวจพิสูจน์หลักฐานในสังกัด ได้รับความเชื่อถือให้เกียรติ ไม่ประสบกับปัญหาในการประสานการปฏิบัติแต่อย่างใด ตัวอย่างการบูรณาการ คือ ระหว่างศูนย์พิสูจน์หลักฐาน 7 ซึ่งมีอำนาจหน้าที่ในการตรวจพิสูจน์ มีผู้ชำนาญ แต่ไม่มีเครื่องมือ กับ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ ที่มีเครื่องมือ มีคณาจารย์	-

ตารางที่ 4-4 ความเห็นในประเด็นสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจ (ต่อ)

ผู้ให้ความเห็น	การบริหารจัดการ	ปัญหานโยบายและยุทธศาสตร์	ด้านบูรณาการร่วมกันระหว่างหน่วยงาน	ข้อเสนอแนะเพิ่มเติม
คนที่ 6 (ต่อ)			ที่มีความรู้ความสามารถ แต่ไม่มีหน้าที่ในการตรวจพิสูจน์ทางคดี เมื่อบูรณาการร่วมกัน ส่งผลดังนี้ (1) ศูนย์พิสูจน์หลักฐาน 7 สามารถทำการเปิดการตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ได้ทัดเทียมกองพิสูจน์หลักฐานกลาง โดยมีคณาจารย์จากคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจเป็นที่ปรึกษาทางวิชาการ สามารถตรวจพิสูจน์ได้อย่างรวดเร็วมีประสิทธิภาพ และใน 2 ปีที่ผ่านมาถือเป็นหน่วยงานหลักในการตรวจพิสูจน์สนับสนุนการป้องกันปราบปรามการละเมิดต่อเด็กและสตรี (TICAC) ของสำนักงานตำรวจแห่งชาติ ตามนโยบายรัฐบาล (2) คณาจารย์จากคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ สามารถนำตัวอย่างการปฏิบัติจริงทางคดีและเป็นปัจจุบันไปสอนหรือถ่ายทอดให้แก่นักเรียนนายร้อยตำรวจตลอดจนนักศึกษาระดับปริญญาโท และสามารถนำไปสู่การวิจัยหรือพัฒนาเพื่อความก้าวหน้าทางวิทยาการด้านนี้ได้อย่างกว้างขวางต่อไป (3) นักเรียนนายร้อยตำรวจ มีความรู้ทั้งภาคทฤษฎีและภาคปฏิบัติ สามารถนำไปใช้ในการฝึกงานยังสถานีตำรวจ และสามารถใช้ในการปฏิบัติจริงเมื่อสำเร็จการศึกษาและบรรจุเป็นนายตำรวจชั้นสัญญาบัตรประจำแต่ละสถานีตำรวจได้	

หมายเหตุ

ผู้ให้ความเห็นคนที่ 1 ผู้ทรงคุณวุฒิจากสำนักงานอธิบดีผู้พิพากษาภาค 7

ผู้ให้ความเห็นคนที่ 2 ผู้ทรงคุณวุฒิจากสำนักงานอัยการพิเศษ ฝ่ายคดีอาญา 2 สำนักงานอัยการสูงสุด

ผู้ให้ความเห็นคนที่ 3 ผู้ทรงคุณวุฒิจากสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ

ผู้ให้ความเห็นคนที่ 4 ผู้เชี่ยวชาญเฉพาะด้านพิเศษ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

ผู้ให้ความเห็นคนที่ 5 ผู้ทรงคุณวุฒิจากกองกำกับการสืบสวนสอบสวน กองบังคับการตำรวจนครบาล 8

ผู้ให้ความเห็นคนที่ 6 ผู้ทรงคุณวุฒิจากกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 7 สำนักงานพิสูจน์หลักฐานตำรวจ

2. การปรับปรุงโครงสร้างหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรมเกี่ยวกับโครงสร้างในการปฏิบัติงานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของต่างประเทศ พบว่า โครงสร้างของหน่วยงานที่ปฏิบัติงานมีลักษณะโครงสร้างดังนี้

1) สหรัฐอเมริกา: มีหน่วยงานสาขาอาชญากรรม, ไซเบอร์, ตอบโต้และบริการขึ้นอยู่กับสำนักงานสอบสวนกลาง (FBI) กระจายออกไป มีสำนักงานเขต 56 แห่ง ทำงานประสานงานกับสำนักงานข่าวกรองกลาง (CIA) เกี่ยวกับการข่าวกรองทางไซเบอร์

2) ประเทศอังกฤษ: มีหน่วยงานระดับศูนย์รักษาความปลอดภัยไซเบอร์แห่งชาติ (NCSC) ในการเตรียมพร้อมรับมืออาชญากรรมทางไซเบอร์ มีผู้เชี่ยวชาญกว่า 750 คน กระจายออกทั่วประเทศ

3) ประเทศเยอรมัน: มีหน่วยงานระดับสำนักงานความปลอดภัยของข้อมูลแห่งชาติเยอรมัน (FOIS) ซึ่งเป็นหน่วยงานระดับสูงของรัฐบาลเยอรมันที่รับผิดชอบด้านการจัดการความปลอดภัยคอมพิวเตอร์ มีพนักงานมากว่า 600 คน ที่มีความเชี่ยวชาญและรับผิดชอบ กระจายออกทั่วประเทศ

4) ประเทศออสเตรเลีย: มีหน่วยงานที่เรียกว่า Australian Criminal Intelligence Commission (ACIC) เป็นองค์กรในการดำเนินการและประสานงานกับตำรวจในแต่ละรัฐ ให้การสนับสนุนที่สำคัญต่อกลยุทธระดับชาติ เพื่อต่อสู้ต่อระบบอาชญากรรมไซเบอร์ที่เป็นภัยคุกคามความมั่นคงแห่งชาติ ซึ่งปัจจุบันมีบุคลากรปฏิบัติงานมากกว่า 1,000 คน

5) ประเทศญี่ปุ่น: มีหน่วยงานตำรวจที่ปฏิบัติหน้าที่ในการดูแลความปลอดภัยทางอาชญากรรมไซเบอร์เป็นการเฉพาะ มีหน่วยงานระดับกองบัญชาการที่เรียกว่า กองบัญชาการคมนาคมสารสนเทศรับผิดชอบ

6) สาธารณรัฐสิงคโปร์: มีหน่วยงานที่เรียกว่าสำนักงานตำรวจแห่งชาติสิงคโปร์ (Singapore Police Force: SPF) ซึ่งจะมีกรมสืบสวนคดีอาชญากรรมสังกัดอยู่ในหน่วยงานนี้ ใช้อยู่กับกรมสืบสวนสอบสวนคดีอาชญากรรม (Criminal Investigation Department: CID) ซึ่งทำหน้าที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์

7) ไต้หวัน สาธารณรัฐจีน: ศูนย์อาชญากรรมทางคอมพิวเตอร์ของไต้หวันขึ้นอยู่กับกรมสืบสวนสอบสวนกระทรวงยุติธรรมของไต้หวัน

8) สาธารณรัฐสังคมนิยมเวียดนาม: งานอาชญากรรมทางคอมพิวเตอร์ขึ้นอยู่กับสำนักงานตำรวจป้องกันและปราบปรามอาชญากรรมอยู่ภายใต้กระทรวงความมั่นคง

9) สาธารณรัฐฟิลิปปินส์: งานต่อต้านอาชญากรรมทางคอมพิวเตอร์จะขึ้นอยู่กับสำนักงานตำรวจแห่งชาติฟิลิปปินส์

และจากการศึกษาการปฏิบัติงานของหน่วยงานทางด้านอาชญากรรมทางเทคโนโลยีของต่างประเทศ พบว่ามีขยายออกทั่วประเทศ คณะผู้วิจัยจึงมีความเห็นว่า ในการพัฒนางานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีใน 3 ระดับ คือ

1. หน่วยงานในระดับสถานีตำรวจ
2. หน่วยงานของ ปอท. และ ปอศ.
3. หน่วยงานศูนย์พิสูจน์หลักฐาน สำนักงานพิสูจน์หลักฐานตำรวจ

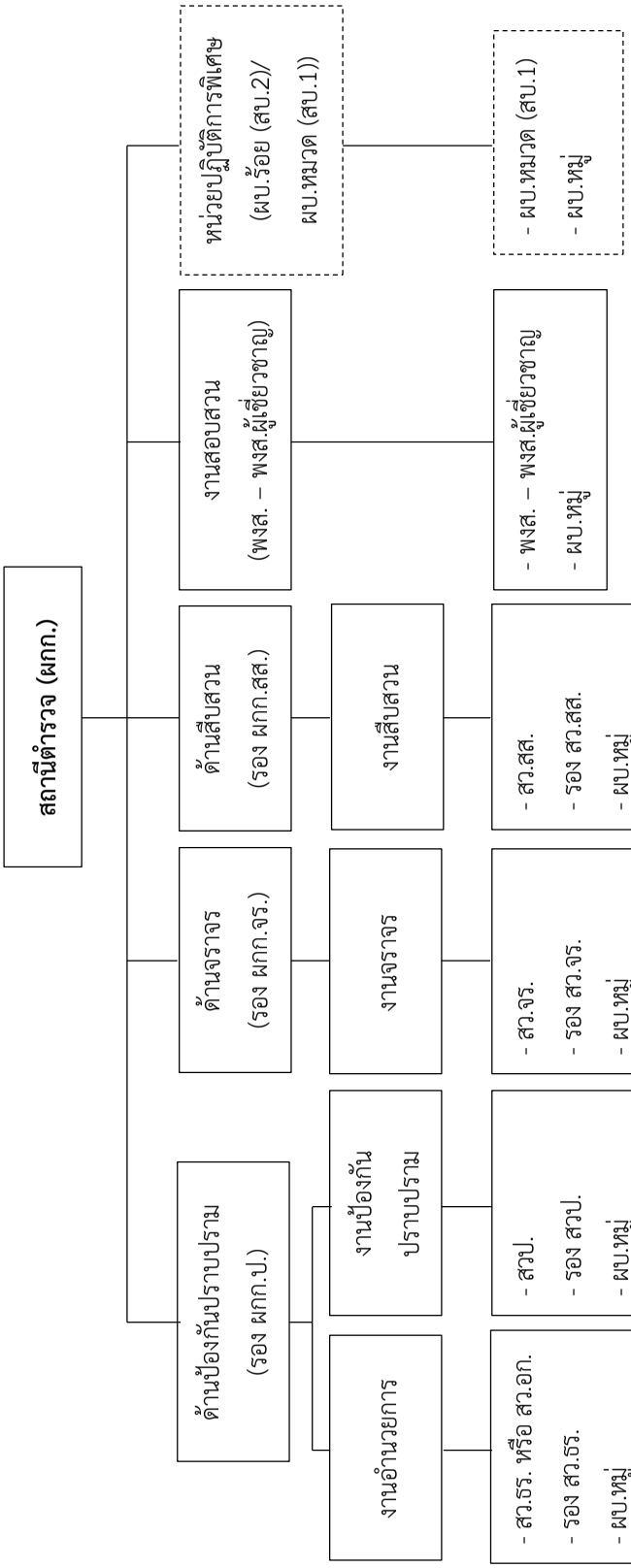
1. หน่วยงานในระดับสถานีตำรวจ

ในโครงสร้างปัจจุบันของสถานีตำรวจมีจำนวน 5 ด้าน คือ

- ด้านป้องกันปราบปราม
- ด้านจราจร
- ด้านสืบสวน
- งานสอบสวน
- หน่วยปฏิบัติการพิเศษ (หน่วยปฏิบัติการพิเศษจะกำหนดให้ตามสถานการณ์และความจำเป็น)

ในงานวิจัยครั้งนี้ได้นำข้อมูลจากผู้ทรงคุณวุฒิที่ให้ความเห็นจากการประชุมกลุ่มย่อยและการสัมภาษณ์เชิงลึก รวมทั้ง การศึกษาของหน่วยงานทางด้านการป้องกันอาชญากรรมทางเทคโนโลยีจากต่างประเทศ มีความเห็นว่าควรเพิ่มงานการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอีกงานหนึ่งในสถานีตำรวจอย่างชัดเจนให้อยู่ในงานด้านสอบสวน

- ด้านป้องกันปราบปราม
- ด้านจราจร
- ด้านสืบสวน
- งานสอบสวน
- งานป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
- หน่วยปฏิบัติการพิเศษ



ภาพที่ 4-1 โครงสร้างสถานีตำรวจ (เดิม)

หมายเหตุ 1. รองผู้กำกับการป้องกันปราบปราม เป็นหัวหน้างานอำนวยการ และงานป้องกันปราบปราม
2. รองผู้กำกับการจราจร เป็นหัวหน้างานจราจร
3. รองผู้กำกับการสืบสวน เป็นหัวหน้างานสืบสวน
4. พนักงานสอบสวนที่อาวุโสสูงสุด เป็นหัวหน้างาน
5. หน่วยปฏิบัติการพิเศษ จะกำหนดให้ตามสถานการณ์และความจำเป็น

ภาพที่ 4-2 โครงสร้างสถานีตำรวจ (ใหม่)

หมายเหตุ 1. รองผู้กำกับการป้องกันปราบปราม เป็นหัวหน้างานอำนวยการ และงานป้องกันปราบปราม

2. รองผู้กำกับการจราจร เป็นหัวหน้างานจราจร

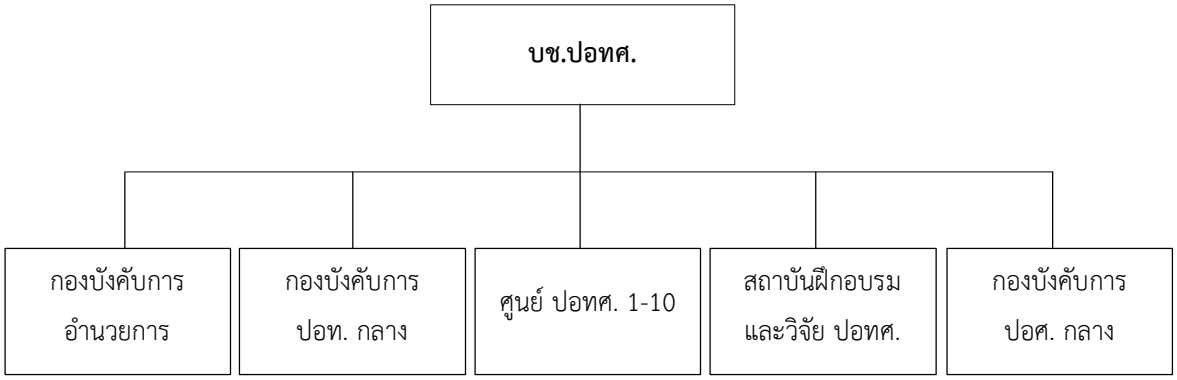
3. รองผู้กำกับการสืบสวน เป็นหัวหน้างานสืบสวน

4. พนักงานสอบสวนที่อาวุโสสูงสุด เป็นหัวหน้างาน

5. หน่วยปฏิบัติการพิเศษ จะกำหนดให้ตามสถานการณ์และความจำเป็น

2. หน่วยงานของ ปอท. และ ปอศ.

การปรับปรุงโครงสร้างของหน่วยงานที่ปฏิบัติหน้าที่เกี่ยวกับการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยการปรับเปลี่ยนโครงสร้างหน่วยงาน (ใหม่) กองบัญชาการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.) โดยการขยายหน่วยงาน บก.ปอท. และ บก.ปอศ. ตั้งเป็น บช.ปอทศ. เป็นหน่วยงานระดับกองบัญชาการ โดยนำเอาหน่วยงานกองบังคับการการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจมาเป็นหน่วยงานในสังกัด บช.ปอท.



ปอท. = การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
ปอศ. = การกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ
ปอทศ. = การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ

ภาพที่ 4-3 โครงสร้างหน่วยงาน (ใหม่) กองบัญชาการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.)

เพื่อให้สอดคล้องกับโครงสร้างการปฏิบัติงานของสำนักงานพิสูจน์หลักฐาน เนื่องจากการทำงานต้องมีการประสานงานและบูรณาการร่วมกัน ระหว่างหน่วยปฏิบัติและหน่วยสนับสนุนในการใช้เครื่องมือในการตรวจพิสูจน์ของกลาง จึงให้หน่วยปฏิบัติงานของแต่ละศูนย์ ควรตั้งตัวอยู่ในพื้นที่ เช่นเดียวกับศูนย์พิสูจน์หลักฐาน 1 - 10 ดังนี้

- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 1 ตั้งอยู่ที่ จ.ปทุมธานี
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 2 ตั้งอยู่ที่ จ.ชลบุรี
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 3 ตั้งอยู่ที่ จ.นครราชสีมา
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 4 ตั้งอยู่ที่ จ.ขอนแก่น
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 5 ตั้งอยู่ที่ จ.ลำปาง
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 6 ตั้งอยู่ที่ จ.พิษณุโลก
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 7 ตั้งอยู่ที่ จ.นครปฐม
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 8 ตั้งอยู่ที่ จ.สุราษฎร์ธานี
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 9 ตั้งอยู่ที่ จ.สงขลา
- ศูนย์กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ 10 ตั้งอยู่ที่ จ.ยะลา

3. หน่วยงานศูนย์พิสูจน์หลักฐาน สำนักงานพิสูจน์หลักฐานตำรวจ

จากการศึกษาพบว่า ทางสำนักงานพิสูจน์หลักฐานได้ดำเนินการวางแผนทางด้านบุคลากรและเครื่องมือสำหรับตรวจพิสูจน์ โดยมีบุคลากรที่ปฏิบัติงานทั้ง 11 แห่งไว้ครบแล้ว แต่อุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์มีเพียง 3 แห่ง คือ กองพิสูจน์หลักฐานกลาง, ศูนย์พิสูจน์หลักฐาน 7 (นครปฐม) และศูนย์พิสูจน์หลักฐาน 10 (ยะลา) เท่านั้น ยังคงขาดเครื่องมือสำหรับตรวจพิสูจน์ที่ศูนย์พิสูจน์หลักฐานอีก 8 แห่ง จึงควรสนับสนุนงบประมาณในการจัดซื้ออุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์ให้ครบทั้ง 11 แห่ง

2. การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญงานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีรายละเอียดและสาระสำคัญโดยสรุป ดังนี้

ในการศึกษาแนวทางและขั้นตอนการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ มีรายละเอียดและหัวข้อดังต่อไปนี้

2.1 ภัยคุกคามความปลอดภัยข้อมูลเกี่ยวกับอาชญากรรม
2.2 ขั้นตอนการบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ
2.3 ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ
2.4 ขั้นตอนการรวบรวมพยานหลักฐานในสถานที่เกิดเหตุ
2.5 ขั้นตอนการบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ
2.6 ขั้นตอนการบริหารจัดการและขนส่งพยานหลักฐาน
2.7 ขั้นตอนการบริหารจัดการและจัดเก็บพยานหลักฐาน
2.8 ขั้นตอนการเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน
2.9 แนวทางคำถามสำหรับคดีด้านอาชญากรรมทางเทคโนโลยี
2.10 การตรวจพิสูจน์อาชญากรรมทางเทคโนโลยี

2.1 ภัยคุกคามความปลอดภัยข้อมูลเกี่ยวกับอาชญากรรม

(1) รูปแบบของภัยคุกคามความปลอดภัยข้อมูลบนคอมพิวเตอร์และอินเทอร์เน็ต

(1.1) ภัยจากสแปมเมล์ (Spam Mail)

สแปมเมล์ คือ อีเมล์ที่ไม่พึงประสงค์อย่างหนึ่งที่ถูกส่งมาจากที่ผู้ที่ไม่สามารถระบุตัวตนได้ว่าเป็นใคร (โดเมนที่ไม่ได้รับการยืนยันตัวตน) ซึ่งวัตถุประสงค์ที่ส่งอีเมล์ลักษณะนี้ก็เพื่อที่จะใช้เป็นการประชาสัมพันธ์, โฆษณา, ก่อกวน เป็นต้น แต่โดยส่วนใหญ่แล้วจะส่งเพื่อก่อกวน หรือกระจายข้อความที่ไม่พึงประสงค์ อาจจะมีการฝัง Script (สคลิปต์) ต่างๆไว้ในไฟล์เอกสารที่แนบมากับอีเมล์นั้นด้วย ซึ่งเมื่อเปิดไฟล์นั้นหรือดาวน์โหลดลงมาที่เครื่องคอมพิวเตอร์ อาจจะทำให้เกิดความเสียหายได้ สำหรับ Spam mail นั้นมีอยู่หลากหลายรูปแบบ ดังนี้

- Spamvertised sites (สแปมเวอร์ไทด์ ไซต์) คือ อีเมล์ที่มีเนื้อหาเกี่ยวกับการโฆษณาสินค้า, ผลิตภัณฑ์ หรือบริการ ซึ่งในบางครั้งมักจะมีการโฆษณาแอบแฝงและหลอกลวงด้วย

- Blank SPAM (แบลงค์สแปม) คือ SPAM ที่มีจุดประสงค์หลัก คือ ก่อกวนระบบอีเมล์โดยการส่งอีเมล์ที่ไม่มีเนื้อหาทำให้เกิดการติดขัดในระบบ หรือทำให้ระบบทำงานช้าลง เนื่องจากมีเมล์จำนวนมากที่ต้องจัดการโดยไม่จำเป็น

- Image SPAM (อิมเมจ สแปม) เป็นลักษณะของ Spamvertised sites ชนิดหนึ่งแต่ส่งข้อมูลมาในลักษณะของรูปภาพแทนที่จะเป็นข้อมูลตัวอักษรเพื่อให้ยากต่อการตรวจจับของระบบดักจับ Spam (Spam Filter)

- Backscatter SPAM (แบล็กสเก็ตเตอร์) คือ อีเมล์ที่มีการแนบไฟล์ที่มีการทำงานเป็น Virus (ไวรัส) หรือ มัลแวร์ โทรจัน (Malware Trojans) อีกทั้งยังมีเนื้อหาเชิญชวนให้ผู้ใช้งานทำการ run (รัน) ไฟล์ดังกล่าว เพื่อให้ไวรัสนั้น ๆ ทำงานซึ่งอาจสร้างความเสียหายแก่ข้อมูลหรือทรัพย์สิน

(1.2) ภัยจากสปายแวร์ (Spy Ware)

สปายแวร์ คือ โปรแกรมที่แฝงเข้ามาในคอมพิวเตอร์ขณะที่กำลังใช้งานอินเตอร์เน็ต เป็นโประแกรมที่ถูกเขียนขึ้นเพื่อสอดส่อง (Spy) หรือดักจับข้อมูลการใช้งานเครื่องคอมพิวเตอร์ หรือข้อมูลส่วนบุคคล เช่นรหัสพาสเวิร์ด หรือหมายเลขบัญชีบัตรเครดิต เป็นต้น โดยสปายแวร์จะทำการส่งข้อมูลตามที่กำหนดและดักจับมาได้ไปให้เครื่องคอมพิวเตอร์ปลายทางที่ได้ระบุไว้ นอกจากนี้สปายแวร์บางชนิดอาจมีเพื่อโฆษณาขายสินค้าต่าง ๆ ซึ่งบางครั้งก็จะสร้างความรำคาญให้กับผู้ใช้ สปายแวร์บางประเภทอาจทำให้ไม่สามารถใช้งานอินเตอร์เน็ตได้เช่นกัน สามารถแยกประเภทของสปายแวร์ ได้ดังนี้

- Adware เป็นสปายแวร์ที่คอยส่งข้อความโฆษณามาที่คอมพิวเตอร์ของเรา เหตุที่จัดให้ Adware เป็นสปายแวร์เนื่องจากมีส่วนประกอบของโปรแกรมที่สามารถติดตามข้อมูลของผู้ใช้และส่งข้อมูลออกไปที่อื่นได้

- Dialer เป็นสปายแวร์ที่มักจะฝังตัวอยู่ตามเวบโป๊ต่าง ๆ และทำการหมุนโทรศัพท์ทางไกลต่อไปยังต่างประเทศ

- Hijacker เป็นสปายแวร์ที่สามารถเปลี่ยนแปลงระบบของเครื่องคอมพิวเตอร์ โดยมักจะแสดงข้อความ เพื่อให้เหยื่อทำการโอนเงินให้ ซึ่งหากไม่ทำตามเงื่อนไขที่กำหนดแล้ว เครื่องคอมพิวเตอร์เครื่องนี้หรือระบบคอมพิวเตอร์ขององค์กร จะถูกลบข้อมูลทิ้งเสียทั้งหมด หรือจะถูกล๊อคการใช้งานเป็นต้น

- BHO (Browser Helper Objects) เป็นสปายแวร์ที่จะซ่อนฟังค์ชั่นที่ไม่พึงประสงค์ไว้บนเว็บบราวเซอร์

- Toolbar เป็นสปายแวร์ที่จะซ่อนฟังค์ชั่นที่ไม่พึงประสงค์ไว้บนส่วนของเครื่องมือ (Toolbar) ของเว็บบราวเซอร์

(1.3) ภัยจากมัลแวร์ (Mal Ware)

มัลแวร์ (Malware) หรือ Malicious Software เป็นชื่อเรียกโดยรวมของโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus) , วอร์ม (Worm) , โทรจัน (Trojan เป็นต้น โดยมีลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภทดังนี้

- Virus คือ มัลแวร์ที่แฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

- Worm คือ มัลแวร์ที่สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น อีเมล์ หรือระบบแชร์ไฟล์

- Trojan คือ มัลแวร์ที่ทำหน้าที่หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริงๆแล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย

- Backdoor คือ มัลแวร์ที่ทำหน้าที่เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว

- Rootkit คือ มัลแวร์ที่ทำหน้าที่เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติมเพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

(1.4) ภัยจากการล่อลวงด้วยวิธี Phishing

Phishing (ฟิชชิ่ง) คือ อีเมล์ที่มีลักษณะหลอกสอบถามข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะด้วยวิธีการหลอกล่อต่าง ๆ ผ่านเนื้อหาในจดหมาย เช่น หลอกถามข้อมูล Password หรือสอบถามข้อมูลส่วนบุคคล ซึ่งหากผู้รับไม่รู้เท่าทันแล้วส่งข้อมูลกลับไปอาจเกิดความเสียหายแก่ผู้ที่ได้รับอีเมล์ฉบับนั้น ๆ ด้วย

(1.5) ภัยจากแฮกเกอร์ (Hacker)

แฮกเกอร์ คือ ผู้ที่มีความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างสูงมาก ไม่ว่าจะเป็นเรื่องเครือข่าย, ระบบปฏิบัติการจนสามารถเข้าใจว่าระบบมีช่องโหว่ตรงไหน หรือสามารถไปค้นหาช่องโหว่ได้จากตรงไหนบ้าง เมื่อก่อนภาพลักษณ์ของ Hacker จะเป็นพวกชั่วร้าย ชอบขโมยข้อมูล หรือ ทำลายให้เสียหาย

แต่เดี๋ยวนี้ คำว่า Hacker หมายถึง Security Professional ที่คอยใช้ความสามารถช่วยตรวจตราระบบ และแจ้งเจ้าของระบบว่ามีช่องโหว่ตรงไหนบ้าง อาจพูดง่ายๆว่าเป็น Hacker ที่มีจริยธรรมนั่นเอง ในต่างประเทศมีวิชาที่สอนถึงการเป็น Ethical Hacker หรือ แฮกเกอร์แบบมีจริยธรรม ซึ่งแฮกเกอร์แบบนี้เรียกอีกอย่างว่า White Hat Hacker ก็ได้ ส่วนพวกที่นิสัยไม่ดีเราจะเรียกว่าพวกนี้ว่า Cracker หรือ Black Hat Hacker ซึ่งก็คือ มีความสามารถเหมือน Hacker ทุกประการ เพียงแต่พฤติกรรมของ Cracker นั้นจะเป็นการกระทำที่ขาดจริยธรรม เช่น ขโมยข้อมูลหรือเข้าไปทำลายระบบคอมพิวเตอร์ให้ทำงานไม่ได้ เป็นต้น

วิธีการที่ Hacker และ Cracker ใช้เข้าไปก่อกวนในระบบอินเตอร์เน็ตมีหลายวิธี แต่วิธีที่นิยมมากมี 3 วิธี ดังนี้

- Password Sniffers เป็นโปรแกรมเล็ก ๆ ที่ซ่อนอยู่ในเครือข่าย และถูกสั่งให้บันทึกการ Log on และรหัสผ่าน (Password) แล้วนำไปเก็บในแฟ้มข้อมูลลับ

- Spooling เป็นเทคนิคการเข้าสู่คอมพิวเตอร์ที่อยู่ระยะทางไกล โดยการปลอมแปลงที่อยู่อินเตอร์เน็ต (Internet Address) ของเครื่องที่เข้าได้ง่ายหรือเครื่องที่เป็นมิตร เพื่อค้นหาจุดที่ใช้ในระบบรักษาความปลอดภัยภายใน วิธีการคือ การได้มาถึงสถานภาพที่เป็นแก่นหรือราก (Root) ซึ่งเป็นการเข้าสู่ระบบขั้นสูงสำหรับผู้บริหารระบบ เมื่อได้รากแล้วจะสร้าง Sniffers หรือโปรแกรมอื่นที่เป็น Back Door ซึ่งเป็นทางกลับลับ ๆ ใส่ไว้ในเครื่อง

- The Hole in the Web เป็นข้อบกพร่องใน World-Wide-Web (WWW) ซึ่งเป็นส่วนหนึ่งที่อยู่ในอินเทอร์เน็ต เนื่องจากโปรแกรมที่ใช้ในการปฏิบัติการของ Website จะมีหลุมหรือช่องว่างที่ผู้บุกรุกสามารถทำทุกอย่างที่เจ้าของ Site สามารถทำได้

(1.6) ภัยจากโปรแกรม Peer-to Peer (P2P)

ภัยจาก P2P เป็นภัยซึ่งเกิดจากผู้ใช้เป็นหลัก เนื่องจากโปรแกรมประเภทนี้นั้นจะให้ประโยชน์กับเรื่องส่วนตัวของผู้ใช้ เช่น การใช้โปรแกรม KAZAA เพื่อดาวน์โหลด หนัง และ เพลง แบบผิดกฎหมาย หรือใช้โปรแกรม SKYPE ในการพูดคุยสื่อสารแทนการใช้โทรศัพท์ ซึ่งการใช้โปรแกรมดังกล่าวนั้นจะนำภัยสองประเภทมาสู่องค์กร ได้แก่

- การสิ้นเปลือง Bandwidth เครือข่ายขององค์กร – ปัญหานี้เกิดขึ้นเนื่องจากการใช้ Bandwidth จำนวนมาก เช่นโปรแกรม KAZAA นั้นเป็นการดาวน์ โหลดข้อมูลเถื่อน (illegal software) จากเครื่อง PC อื่นๆทั่วโลก หรือโปรแกรม SKYPE ซึ่งใช้เป็นโทรศัพท์ผ่านอินเทอร์เน็ต

- สร้างปัญหาด้าน Confidentiality – เคยพบว่ามีช่องโหว่บน KAZAA ซึ่งทำให้ Hacker สามารถเจาะมายัง Hard disk ของคนทั้งโลกที่ติดตั้งโปรแกรม KAZAA ได้ ซึ่งแน่นอนว่าจะทำให้ข้อมูลสำคัญขององค์กรหลุดรั่วไปยังมือของผู้ไม่ประสงค์ดีได้ การแก้ปัญหาสามารถทำได้โดยที่องค์กรควรจะ Implement Preventive Control โดยใช้โปรแกรมประเภท Desktop Management หรือ ANTI-Malware ซึ่งสามารถควบคุมพฤติกรรมการใช้งานคอมพิวเตอร์ของ End User รวมถึงการติดตั้งและใช้โปรแกรมต่าง ๆ บนเครื่อง

และอาจใช้โปรแกรมด้าน Network Monitoring เฝ้าระวังเครือข่ายเพิ่มเติม เพื่อเป็น Detective Control ให้กับองค์กรด้วย

(1.7) ภัยจากเครือข่ายไร้สาย

การติดตั้งเครือข่ายไร้สายเป็นเรื่องที่ค่อนข้างอันตรายเนื่องมาจากโครงสร้างเครือข่ายไร้สายอาจออกแบบมาอย่างไม่ปลอดภัย โดยภัยคุกคามที่เกิดขึ้นจากเครือข่ายไร้สาย ได้แก่

- ภัยคุกคามจากซอฟต์แวร์ที่ใช้ในการบริหารจัดการเครือข่ายไร้สาย โดยซอฟต์แวร์ที่ทำงานผิดพลาดอาจส่งผลกระทบรุนแรงจนทำให้เกิดช่องโหว่ที่ผู้โจมตีสามารถเข้าถึงเครือข่ายไร้สายหรือเข้าควบคุมระบบการบริหารจัดการเครือข่ายไร้สายได้ *ภัยคุกคามจากการใช้เทคนิคหลอกลวง โดยพบว่าผู้โจมตีจะสร้างสถานีเครือข่ายไร้สายเพื่อหลอกลวงผู้ใช้งานให้หลงเชื่อว่าเป็นเครือข่ายไร้สายชื่อเดียวกัน ซึ่งเมื่อผู้ใช้งานทำการกรอกรหัสผ่านเพื่อเข้าใช้งานก็จะทำให้ถูกดักรับข้อมูลได้ และจากนั้นผู้โจมตีจะนำรหัสผ่านดังกล่าวไปใช้งานต่อไป

- ภัยคุกคามจากการโจมตีเครือข่ายไร้สายที่จัดตั้งขึ้น เกิดจากผู้ไม่หวังดีซึ่งสืบทราบถึงกระบวนการรักษาความปลอดภัยของเครือข่ายไร้สายที่จัดตั้งขึ้น และพยายามโจมตีเครือข่ายไร้สายดังกล่าวในลักษณะของการขโมยรหัสผ่านโดยวิธีการและอุปกรณ์ที่หาซื้อได้ตามทั่วไป ยกตัวอย่างเช่น การประมวลผลเพื่อแกะรอยรหัสผ่านของการเข้ารหัสลับสัญญาณแบบ WEP

- ภัยคุกคามจากการตั้งค่าเครือข่ายไร้สายอย่างไม่ถูกวิธี เกิดจากผู้จัดตั้งเครือข่ายไม่มีความรู้ความเข้าใจในการจัดตั้งเครือข่ายไร้สาย จนทำให้ผู้โจมตีสามารถเข้าถึงเครือข่ายไร้สายได้อย่างง่ายดาย เช่น ผู้ดูแลเครือข่ายไร้สายไม่ตั้งค่าโหมดการยืนยันรหัสผ่านไว้ ทำให้บุคคลใดก็ตามที่ค้นพบสัญญาณเครือข่ายไร้สายดังกล่าว สามารถเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ตได้ทันที

- ภัยคุกคามจากการบอกรหัสผ่านผู้อื่นสำหรับเข้าใช้งานเครือข่ายไร้สายได้ การให้รหัสผ่านกับผู้อื่นในการเข้าใช้งานเครือข่ายไร้สาย ถือเป็นความเสี่ยงอย่างรุนแรง เนื่องจากผู้ดูแลเครือข่ายไร้สายเอง จะไม่ทราบเลยว่าผู้ใช้งานคนนั้นได้ใช้งานเครือข่ายไร้สายที่จัดตั้งขึ้นในทางที่ผิดอย่างไรบ้าง เช่น ผู้ใช้งานอาจใช้งานอินเทอร์เน็ตเพื่อโพสต์ข้อความหมิ่นประมาทผู้อื่น ผู้ใช้งานนำข้อมูลรหัสผ่านนี้ไปบอกต่อแก่บุคคลอื่น หรือแม้กระทั่งผู้ใช้งานมีความพยายามจะขโมยข้อมูลหรือลักลอบเข้าไปในระบบบริหารจัดการเครือข่าย เพื่อให้ได้สิทธิ์ในการควบคุมเครือข่ายไร้สายดังกล่าว ซึ่งหากเป็นเพียงการโจมตีภายในอาจพบว่าสามารถแก้ไขได้ไม่ยาก แต่หากพบว่าเป็นการใช้งานต่อสาธารณะในความผิดที่ต้องได้รับโทษทางกฎหมาย ก็จะทำให้ผู้ดูแลเครือข่ายไร้สายหรือผู้เช่าใช้งานอินเทอร์เน็ตบนเครือข่ายไร้สายนั้น ๆ ต้องกลางเป็นผู้รับผิดชอบแทนในฐานะที่เป็นผู้กระทำความผิด โดยส่วนใหญ่ อุปกรณ์เครือข่ายไร้สายส่วนบุคคลจะไม่สามารถจัดเก็บข้อมูลบันทึกการใช้งาน (Log) ไว้ในตัวอุปกรณ์

(1.8) ภัยจาก SPIM (Spam Instant Messaging)

SPIM คือ SPAM ที่ใช้ช่องทาง IM (Instant Messaging) ในการกระจาย Malicious Code โดยผู้ที่เป็น SPIMMER นั้นจะใช้ BOT เพื่อค้นหาชื่อของคนที่ใช้โปรแกรม IM อยู่ จากนั้นจึงใช้ BOT แสดง

คำพูดเพื่อให้เหยื่อ เข้าใจว่าเป็นมนุษย์ จากนั้นจึงส่ง โฆษณา ข้อมูลหลอกลวง ลิงค์เวปไซท์ หรือแม้แต่ Spyware และ Malware ต่าง ๆ ให้กับเหยื่อ

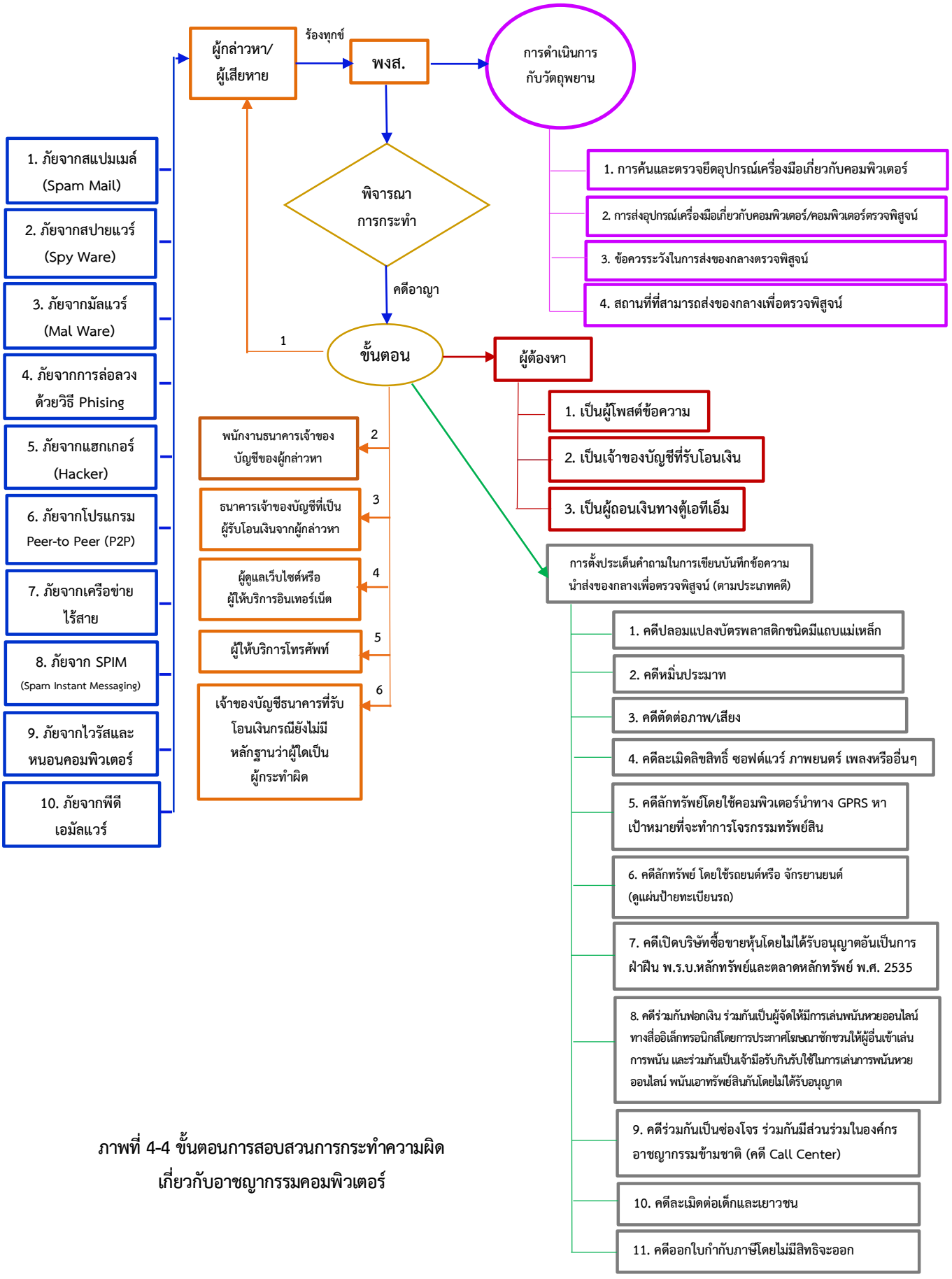
(1.9) ภัยจากไวรัสและหนอนคอมพิวเตอร์

ไวรัส (Viruses) คือโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่น ๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้า ๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปเกิดจากการที่ผู้ใช้เป็นพาหะ นำไวรัสจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง เช่นเวลาที่ส่ง E-mail โดยแนบเอกสาร หรือไฟล์ที่มีไวรัสไปด้วย การทำสำเนาไฟล์ที่ติดไวรัสไปไว้บนไฟล์เซริฟเวอร์ การแลกเปลี่ยนไฟล์โดยใช้แผ่นดิสก์เก็ต เมื่อผู้ใช้ทั่วไปรับไฟล์ หรือดิสก์มาใช้งาน ไวรัสก็จะแพร่กระจายภายในเครื่อง และจะเป็นวงจรในลักษณะนี้ต่อไป

หนอน (Worms) คือโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่งโดยอาศัยระบบเน็ตเวิร์ค (E-mail) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเอง ซึ่งจะแพร่กระจายได้อย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก

(1.10) ภัยจากพีดีเอมัลแวร์

ข้อมูลในพีดีเอสามารถที่จะเป็นพาหะของไวรัส โทรจัน หรือ Malicious Mobile Code ได้เช่นเดียวกันกับข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ ซึ่งภัยต่าง ๆ เหล่านี้ล้วนแต่เป็นการนำความรู้ทางเทคนิคมาเป็นช่องทางในการล่อลวงของผู้กระทำความผิด หรือใช้เป็นช่องทางในการได้รับข้อมูลส่วนบุคคลของประชาชนผู้ใช้งานคอมพิวเตอร์ส่วนบุคคล โทรศัพท์มือถือ หรือระบบคอมพิวเตอร์ขององค์กร ในอันที่จะนำไปใช้แสวงหาผลประโยชน์ในทางมิชอบ โดยที่มิได้รับความยินยอมหรืออนุญาตแต่อย่างใด



ภาพที่ 4-4 ขั้นตอนการสอบสวนการกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์

2.2 ขั้นตอนการบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ

การบริหารจัดการสถานที่เกิดเหตุถือเป็นหัวใจสำคัญที่เจ้าหน้าที่ต้องให้ความสำคัญอย่างมาก เนื่องจากการปฏิบัติงานต่าง ๆ ในสถานที่เกิดเหตุ หากเกิดความผิดพลาดอาจส่งผลให้เกิดความเสียหายหรือสูญไปของพยานหลักฐาน และอาจส่งผลให้พยานหลักฐานที่ได้สถานที่เกิดเหตุนั้นมีความน่าเชื่อถือลง ดังนั้น แนวทางปฏิบัติในการเก็บยึดพยานหลักฐานทางคอมพิวเตอร์ เป็นสิ่งที่จะต้องปฏิบัติในการเข้าตรวจสถานที่เกิดเหตุทางด้านคดีอาชญากรรมทางคอมพิวเตอร์ในสถานการณ์ปัจจุบัน มีดังนี้

1) ความปลอดภัยของเจ้าพนักงาน (Officer Safety) ความปลอดภัยของเจ้าพนักงานเป็นสิ่งที่สำคัญที่สุดในการปฏิบัติงานสืบสวนสอบสวนในทุกคดี ปัจจุบันนี้แทบทุกคดีจะต้องเกี่ยวข้องกับอุปกรณ์ทางคอมพิวเตอร์ และมีการใช้เทคโนโลยีในการประกอบอาชญากรรม เครื่องคอมพิวเตอร์ที่ถูกใช้ในการประกอบอาชญากรรม อาจมีพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดให้เราสืบสวนได้ ซึ่งในสภาวการณ์เช่นนี้ พนักงานสอบสวน เจ้าหน้าที่สืบสวน อย่าได้ชะล่าใจกับสภาพบุคคลหรือสถานที่เกิดเหตุที่ดูไม่น่ามีอะไรนัก เพราะอาจเป็นไปได้ว่า มีเครื่องคอมพิวเตอร์เกี่ยวข้องในการกระทำความผิดนั้น และในระหว่างทำการสืบสวนคดีอาชญากรรมทางด้านคอมพิวเตอร์หรือการดำเนินการเก็บยึดอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ พึงระวังเช่นเดียวกับกรณีคดีอื่น ๆ ทั่วไปว่า การเปลี่ยนแปลงที่ไม่คาดคิดต่อวัตถุพยานต่าง ๆ อาจก่อให้เกิดอันตรายแก่ตัวเจ้าหน้าที่ที่กำลังปฏิบัติหน้าที่ อยู่ได้ การใช้ขั้นตอนการดำเนินการที่ถูกต้องเหมาะสม จะช่วยให้มั่นใจว่าเกิดความปลอดภัยแก่เจ้าหน้าที่รวมถึงบุคคล อื่น ๆ ที่อยู่ในสถานที่เกิดเหตุนั้นด้วย

2) กฎสำคัญ (Golden Rules)

2.1) ความปลอดภัยของเจ้าพนักงาน รักษาสถานที่เกิดเหตุและจัดการให้เกิดความปลอดภัย หากเชื่ออย่างมีเหตุผลว่ามีเครื่องคอมพิวเตอร์เกี่ยวข้องในคดีที่คุณทำการสืบสวนสอบสวนอยู่ ให้ดำเนินการเก็บรักษาพยานหลักฐานโดยทันที

2.2) คำนึงว่ามีอำนาจตามกฎหมายให้เข้ายึดเครื่องคอมพิวเตอร์เรียบร้อยหรือยัง ห้ามทำการเปิดไฟล์ใด ๆ หากเครื่องคอมพิวเตอร์ปิดอยู่ ห้ามเปิดเครื่อง หากเครื่องเปิดอยู่ ห้ามทำการค้นหาไฟล์ใด ๆ บนเครื่องนั้น หากเครื่องคอมพิวเตอร์เปิดอยู่ ให้ดำเนินการตามขั้นตอนที่เหมาะสม ว่าจะต้องปิดเครื่องอย่างไร และจะต้องเตรียมการขนย้ายพยานหลักฐานอย่างไร หากมีเหตุผลที่ควรเชื่อได้ว่าเครื่องคอมพิวเตอร์กำลังทำลายพยานหลักฐาน ให้ทำการปิดเครื่องคอมพิวเตอร์โดยทันทีโดยการดึงสายไฟด้านหลังเครื่องออก หากมีกล้องไปด้วย และเครื่องคอมพิวเตอร์เปิดอยู่ ให้ทำการถ่ายภาพที่อยู่บนหน้าจอคอมพิวเตอร์ในขณะนั้น หากเครื่องคอมพิวเตอร์ปิดอยู่ ให้ทำการถ่ายภาพเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ที่เชื่อมต่ออยู่

2.3) ต้องปฏิบัติงานทุกอย่าง อย่างถูกต้องตามกฎหมาย

3) ขั้นตอนและรายละเอียดการปฏิบัติงาน

3.1) รวบรวมข้อมูลเกี่ยวกับคดี เช่น ข้อมูลด้านสถานที่ ประเภท ลักษณะ และพฤติการณ์ของความผิดความรู้ความสามารถของผู้ต้องสงสัยเกี่ยวกับคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์หรือเครื่องคอมพิวเตอร์ใดที่เกี่ยวข้องกับคดี

3.2) ให้หัวหน้าชุดปราบปรามจัดชุดรักษาความปลอดภัย เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าหรือออกสถานที่เกิดเหตุ และป้องกันมิให้เกิดการปนเปื้อนต่อพยานหลักฐานใด ๆ โดยแบ่งชุดรักษาความปลอดภัยออกเป็น 2 ส่วน คือ ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ และชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ

3.3) ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ปิดกั้นสถานที่เกิดเหตุด้วยเทปปิดกั้นพื้นที่เกิดเหตุ (Crime Scene Tape) เพื่อกำหนดพื้นที่และขอบเขตของสถานที่เกิดเหตุ และปิดกั้นไม่ให้บุคคลอื่นเข้าบริเวณดังกล่าว

3.4) ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ใช้อุปกรณ์ปิดกั้นพื้นที่ เพื่อปิดกั้นทางเข้า-ออก เช่น ถนน ทางเดินเท้า ซอยบริเวณรอบสถานที่เกิดเหตุ เป็นต้น

3.5) ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ตรวจสอบบุคลากรและเจ้าหน้าที่ที่เกี่ยวข้องเพื่อรักษาความปลอดภัยของบริเวณโดยรอบ โดยให้ความสำคัญกับขั้นตอนต่าง ๆ เช่น การจดบันทึก การเข้า-ออก สถานที่เกิดเหตุ การนำตัวผู้ต้องสงสัย บุคคลที่ไม่เกี่ยวข้อง และสัตว์เลี้ยงที่ไม่เกี่ยวข้องออกจากสถานที่เกิดเหตุทันที หรือจัดสรรพื้นที่พิเศษและจัดเจ้าหน้าที่ชุดสอบปากคำควบคุมอย่างใกล้ชิด โดยจัดชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ตรวจตราและรักษาความปลอดภัยโดยรอบสถานที่เกิดเหตุ เพื่อรักษาความปลอดภัยให้กับเจ้าหน้าที่ กรณีตรวจพบภัยคุกคามหรืออันตรายร้ายแรงตามดุลยพินิจของชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุให้อพยพเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องออกจากพื้นที่นั้น ๆ ทันที

3.6) ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุตรวจตราความปลอดภัยของเจ้าหน้าที่ผู้ปฏิบัติงานในสถานที่เกิดเหตุ โดยให้ความสำคัญกับขั้นตอนต่าง ๆ เช่น เครื่องแต่งกายของเจ้าหน้าที่ต้องเป็นชุดป้องกันไฟฟ้าสถิต (Anti-Static Suit) เช่น ถุงมือ และเสื้อคลุม เป็นต้น ไม่พกพาอุปกรณ์ใดที่อาจก่อให้เกิดสนามแม่เหล็กและห้ามมิให้เจ้าหน้าที่ใช้งานระบบสาธารณูปโภค สำรวจและตรวจสอบหาแหล่งจ่ายพลังงานไฟฟ้า และมอบหมายให้เจ้าหน้าที่ดูแลอย่างใกล้ชิด เพื่อป้องกันมิให้ผู้ประสงค์ร้ายตัดกระแสไฟฟ้า ซึ่งอาจส่งผลต่ออุปกรณ์อิเล็กทรอสิกส์ต่าง ๆ จดบันทึกรายละเอียดของสถานที่เกิดเหตุและสิ่งของที่พบเห็นโดยสังเขป ตรวจตราและรักษาความปลอดภัยภายในสถานที่เกิดเหตุ เพื่อรักษาความปลอดภัยให้กับเจ้าหน้าที่อื่น ๆ กรณีตรวจพบภัยคุกคามหรืออันตรายร้ายแรงตามดุลยพินิจของชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุให้อพยพเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องออกจากพื้นที่นั้น ๆ ทันที

3.7) ชุดสอบปากคำ ดำเนินการสอบสวนผู้ต้องสงสัย และผู้ที่เกี่ยวข้อง โดยให้ความสำคัญกับขั้นตอนต่าง ๆ เช่น ใครเป็นเจ้าของหรือผู้มีอำนาจดูแลสถานที่เกิดเหตุ จำนวนของผู้ปฏิบัติงาน พร้อมรายละเอียดของแต่ละบุคคล จำนวนเครื่องคอมพิวเตอร์ และอุปกรณ์อิเล็กทรอนิกส์ที่น่าจะเกี่ยวข้องคดีที่มีอยู่ บัญชีผู้ใช้ (Username) รหัสผ่าน (Password) และรหัสลับ (Encryption Key) อื่น ๆ ข้อมูลโครงสร้างของระบบเครือข่ายคอมพิวเตอร์ (Network Infrastructure) และแผนผังเครือข่าย (Network Diagram) และข้อมูลอื่น ๆ ที่อาจเป็นประโยชน์ต่อการสืบสวนในคดีนั้น ๆ แสดงดังภาพที่ 4-7

2.3 ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ

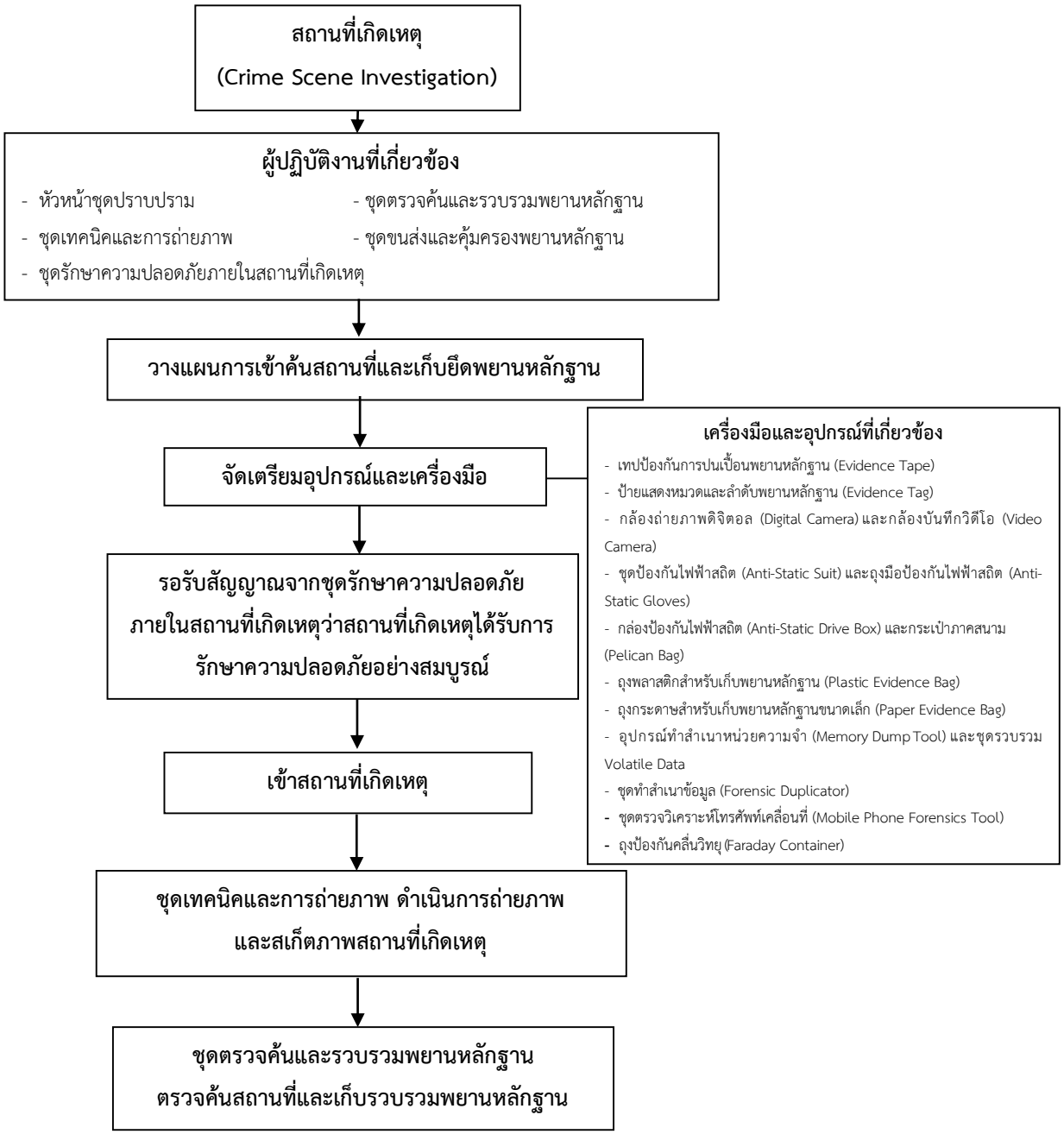
การรวบรวมพยานหลักฐานถือเป็นขั้นตอนที่ต้องให้ความสำคัญและต้องปฏิบัติตามอย่างเคร่งครัด ทั้งยังต้องให้เจ้าหน้าที่ผู้มีความรู้ความเชี่ยวชาญพิเศษ และเคยผ่านการอบรมอย่างถูกต้องเป็นผู้ตรวจค้นและรวบรวมพยานหลักฐาน โดยมีขั้นตอน ดังนี้

1) วางแผนการเข้าค้นสถานที่และเก็บยึดพยานหลักฐาน ขอหมายค้น โดยทำการแบ่งหน้าที่โดยให้หัวหน้าชุด ทำหน้าที่วางแผน ควบคุม สั่งการ ติดต่อสื่อสาร หน้าที่คุ้มกัน ทำหน้าที่รักษาความปลอดภัย หน้าที่บันทึกภาพ ทำหน้าที่สเก็ตภาพ จัดเก็บพยานหลักฐาน จดบันทึก รวบรวมพยานหลักฐาน และสัมภาษณ์ผู้ต้องสงสัย

2) จัดเตรียมอุปกรณ์และเครื่องมือ ที่จำเป็นต้องใช้ในการเก็บยึดให้พร้อม เช่น กล้องถ่ายรูป/กล้องวิดีโอ ถุงมือ/ซอง/ถุง/กล่อง/ภาชนะ เทปกาว/เทป สำหรับติดพยานหลักฐาน ไม้บรรทัด กระดานรองเขียน ปากกา ดินสอ ยางลบ กรรไกร มีด สื่อบันทึกข้อมูล เช่น แผ่นฟล็อปปี้ แผ่น CD/DVD หรือ removable media ซอฟท์แวร์สำหรับเก็บ volatile data และแบบฟอร์มสำหรับการบันทึกข้อมูลต่าง

3) การเข้าสถานที่เกิดเหตุ ทำการรักษาสถานที่เกิดเหตุ ควบคุมตัวผู้ต้องสงสัยให้อยู่ในบริเวณที่ปลอดภัยต่อเจ้าหน้าที่ ทำการตรวจสอบสถานที่ และบันทึกภาพด้วยกล้องถ่ายภาพ และ/หรือกล้องวิดีโอ และ/หรือวาดแผนผังแสดงตำแหน่งของสิ่งของต่าง ๆ และเก็บยึดพยานหลักฐานตามที่ได้แบ่งหน้าที่กันไว้ โดยมีวิธีปฏิบัติแยกออกเป็นอุปกรณ์อิเล็กทรอนิกส์ชนิดต่าง ๆ แสดงดังภาพที่ 4-8 และ 4-9

ภาพที่ 4-5 ขั้นตอนการบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ
(Crime Scene Preservation Management)



ภาพที่ 4-6 ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในที่เกิดเหตุ
(Crime Scene Search and Evidence Collection Protocol)

2.4 ขั้นตอนการรวบรวมพยานหลักฐานในสถานที่เกิดเหตุ

1) เครื่องคอมพิวเตอร์ สำหรับการเก็บรักษาพยานหลักฐานที่ถูกต้องเหมาะสม ให้ดำเนินการตามขั้นตอนต่อไปนี้

- อย่าใช้งานเครื่องคอมพิวเตอร์นั้น หรือพยายามที่จะค้นหาพยานหลักฐานในเครื่อง
- ถ่ายภาพเครื่องคอมพิวเตอร์ทั้งด้านหน้าและด้านหลัง รวมถึงสายและอุปกรณ์ต่อพ่วงต่าง ๆ ทั้งหมดที่พบ ถ่ายภาพพื้นที่รอบ ๆ นั้นก่อนทำการเคลื่อนย้ายวัตถุใด ๆ
- หากเครื่องคอมพิวเตอร์**ปิด**อยู่ ห้าม**เปิด**เครื่อง
- หากเครื่องคอมพิวเตอร์เปิดอยู่ และมีบางอย่างปรากฏอยู่บนหน้าจอ ให้ถ่ายภาพหน้าจอนั้นไว้
- หากเครื่องคอมพิวเตอร์เปิดอยู่ และหน้าจอมืดไม่มีอะไรปรากฏ ให้เลื่อนเม้าส์หรือกด space bar (จะทำให้แสดงผลหน้าจอที่เปิดอยู่ในขณะนั้น) เมื่อภาพบนหน้าจอปรากฏขึ้นมาแล้วให้ถ่ายภาพเก็บไว้
- ดึงสายไฟด้านหลังเครื่องออก
- หากเครื่องแล็ปท็อปนั้นยังไม่ได้ทำการ shutdown เมื่อดึงสายไฟออกมาแล้วให้ถอดแบตเตอรี่ออก โดยส่วนใหญ่แล้วแบตเตอรี่จะอยู่บริเวณด้านใต้และมักจะมีปุ่มเลื่อนเพื่อถอดแบตเตอรี่ออก เมื่อถอดแบตเตอรี่ออกมาแล้วอย่าใส่แบตเตอรี่กลับเข้าไปในเครื่องอีก การถอดแบตเตอรี่ออกจะช่วยป้องกันเครื่องเปิดขึ้นมาโดยไม่ได้ตั้งใจ
- วาดภาพแผนผังและติดป้ายสายไฟต่าง ๆ เพื่อดูว่าสายใดเชื่อมต่ออยู่กับอุปกรณ์ใด
- ถอดสายไฟทั้งหมดออกจากตัวเครื่อง (case) คอมพิวเตอร์
- บรรจุหีบห่อ ทำการเคลื่อนย้ายและเก็บรักษาอุปกรณ์ต่าง ๆ อย่างระมัดระวังเนื่องจากเป็นวัตถุแตกหักเสียหายได้ง่าย
- ทำการเก็บยึดสื่อบันทึกข้อมูลอื่น ๆ ที่เกี่ยวข้อง
- เก็บสื่อต่าง ๆ รวมทั้งตัวเครื่อง (case) คอมพิวเตอร์ให้อยู่ห่างจากแม่เหล็ก เครื่องรับส่งวิทยุ และสิ่งของอื่น ๆ ที่อาจก่อให้เกิดความเสียหายได้
- เก็บยึดคู่มือการใช้งาน เอกสารและบันทึกโน้ตย่อต่าง ๆ
- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ โดยละเอียด

2) สื่อบันทึกข้อมูล (Storage Media) สื่อบันทึกข้อมูลใช้สำหรับเก็บข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์

- เก็บยึดคู่มือการใช้งาน เอกสารและบันทึกโน้ตย่อต่าง ๆ
- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดสื่อบันทึกข้อมูล (บันทึกเวลาตามขั้นตอน ถ่ายรูปตามลำดับเวลา ถ่ายวิดีโอ บรรยาย)
- เก็บให้ห่างจากแม่เหล็ก เครื่องรับส่งวิทยุ และสิ่งของอื่น ๆ ที่อาจก่อให้เกิดความเสียหายได้

3) PDA, Cell Phone & Digital Camera

PDA โทรศัพท์มือถือและกล้องดิจิตอลอาจมีข้อมูลเก็บอยู่ในตัวเครื่องโดยตรงหรืออยู่ใน removable media ขั้นตอนการดำเนินการที่ถูกต้องเหมาะสมในการเก็บยึดและเก็บรักษาอุปกรณ์เหล่านี้ ดังนี้

- หากเครื่อง**ปิด**อยู่ ห้าม**เปิด**เครื่อง
- สำหรับเครื่อง PDA หรือโทรศัพท์มือถือ หากเครื่องเปิดอยู่ให้ปล่อยไว้อย่างนั้น หากเครื่องดับอาจต้องใส่พาสเวิร์ดเมื่อเปิดเครื่องใหม่ ซึ่งทำให้ไม่อาจเข้าดูพยานหลักฐานได้
- ถ่ายภาพอุปกรณ์และภาพที่ปรากฏอยู่บนหน้าจอ
- ติดป้ายและเก็บยึดสายทั้งหมด (รวมถึงสายไฟ) และให้ทำการขนย้ายไปกับเครื่องด้วย
- ให้ทำการชาร์จไฟให้กับอุปกรณ์ที่ตรวจยึดมาอยู่เสมอ
- หากไม่สามารถทำการชาร์ตไฟได้ จะต้องทำการตรวจสอบโดยผู้เชี่ยวชาญเฉพาะ ก่อนที่เครื่องจะดับ เพราะเมื่อเครื่องดับอาจทำให้สูญเสียข้อมูลไปได้
- เก็บยึดสื่อบันทึกข้อมูลอื่น ๆ มาด้วย (เช่น memory stick, compact flash เป็นต้น)
- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดเครื่องและอุปกรณ์ที่เกี่ยวข้อง

4) อำนาจในการเก็บยึดพยานหลักฐาน (Authority for Seizing Evidence)

รายละเอียดทั่วไป (Plain View) ข้อมูลทั่วไปจำเป็นต้องใช้ในการขอหมายจากศาล เพื่อให้เจ้าหน้าที่สามารถเข้าสถานที่เกิดเหตุและเก็บยึดเครื่องคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ และอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ

การยินยอม (Consent) เมื่อได้รับการยินยอมให้ดูให้แน่ใจว่าในเอกสารนั้น ได้เขียนข้อความครอบคลุมทั้ง การเก็บยึดและการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ ทั้งในส่วนของคอมพิวเตอร์ฮาร์ดแวร์ ซอฟต์แวร์ สื่ออิเล็กทรอนิกส์อื่น ๆ

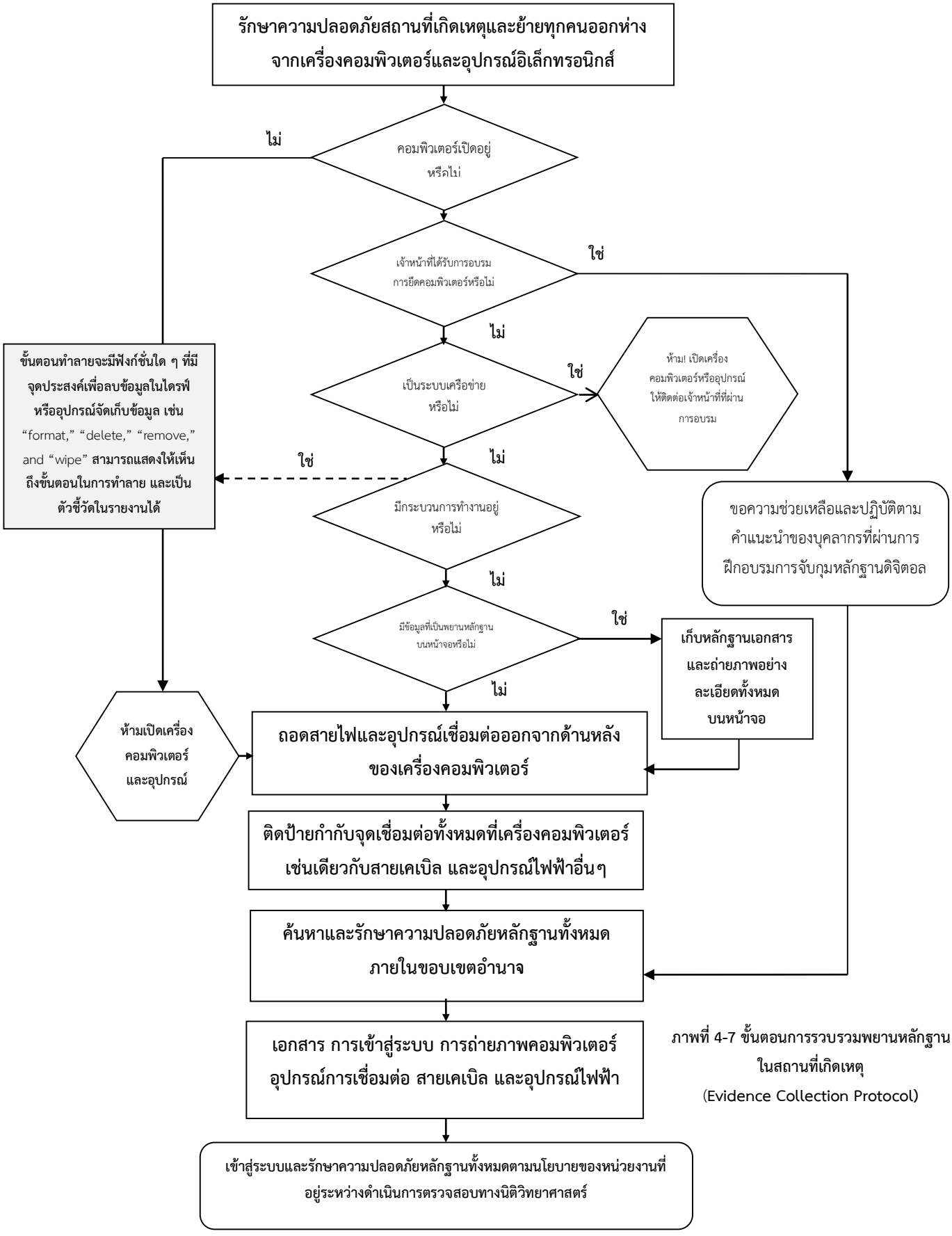
หากหน่วยงานมีแบบฟอร์มใบบันทึกการยินยอมที่ระบุถึงเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ และการตรวจพิสูจน์โดยเจ้าหน้าที่เฉพาะด้านแล้วให้ใช้แบบฟอร์มนั้น

หมายค้น (Search Warrant) หมายค้นให้อำนาจในการตรวจค้นและเก็บยึดพยานหลักฐานทางอิเล็กทรอนิกส์ที่กล่าวถึงในหมายฉบับนั้นเท่านั้น (สำหรับการค้นในสถานที่เกิดเหตุที่ได้ระบุไว้ และสำหรับการค้นอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์นี้)

หมายค้นสำหรับอุปกรณ์บันทึกข้อมูลอิเล็กทรอนิกส์ (Electronic Storage Device Search Warrant)

- การค้นและเก็บยึดฮาร์ดแวร์ ซอฟต์แวร์ เอกสาร บันทึกโน้ตย่อต่าง ๆ และสื่อบันทึกข้อมูล
- การตรวจพิสูจน์/การตรวจค้นและเก็บข้อมูล

ดังแสดงภาพที่ 4-10



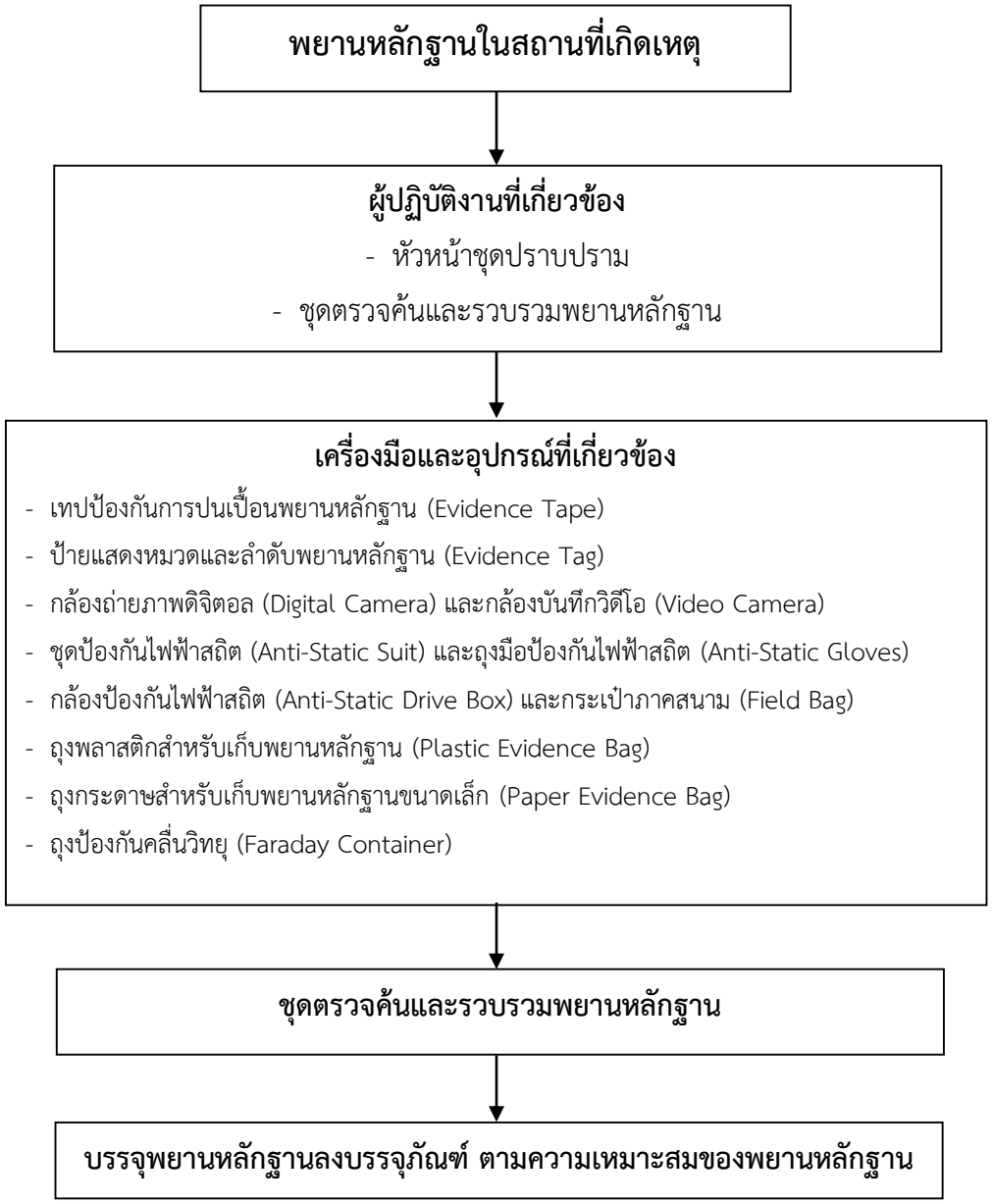
ภาพที่ 4-7 ขั้นตอนการรวบรวมพยานหลักฐาน ในสถานที่เกิดเหตุ (Evidence Collection Protocol)

2.5 ขั้นตอนการบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ

1) ชุดตรวจค้นและรวบรวมพยานหลักฐาน บรรจุหลักฐานในลงบรรจุภัณฑ์เฉพาะด้านทันทีหลังจากปฏิบัติตาม ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในที่เกิดเหตุเรียบร้อยแล้ว

2) บรรจุพยานหลักฐานลงบรรจุภัณฑ์ตามความเหมาะสมของพยานหลักฐาน

ดังแสดงภาพที่ 4-8



ภาพที่ 4-8 ขั้นตอนการบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ (Crime Scene Evidence Package Management)

2.6 ขั้นตอนการบริหารจัดการขนส่งพยานหลักฐาน (Evidence Transportation Management)

1) ชุดตรวจค้นและรวบรวมพยานหลักฐาน ตรวจสอบความถูกต้องของพยานหลักฐานทั้งหมด และลงลายมือชื่อผู้ส่งในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ก่อนนำส่งต่อชุดขนส่งและคุ้มครองพยานหลักฐาน

2) ให้ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความถูกต้องของพยานหลักฐานทั้งหมด พร้อมลงลายมือชื่อผู้รับในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานให้ครบถ้วน

3) ให้หัวหน้าชุดปราบปราม ตรวจสอบความพร้อมและเอกสารอีกครั้ง ก่อนออกคำสั่งเพื่อขนส่งพยานหลักฐานไปยังห้องปฏิบัติการ

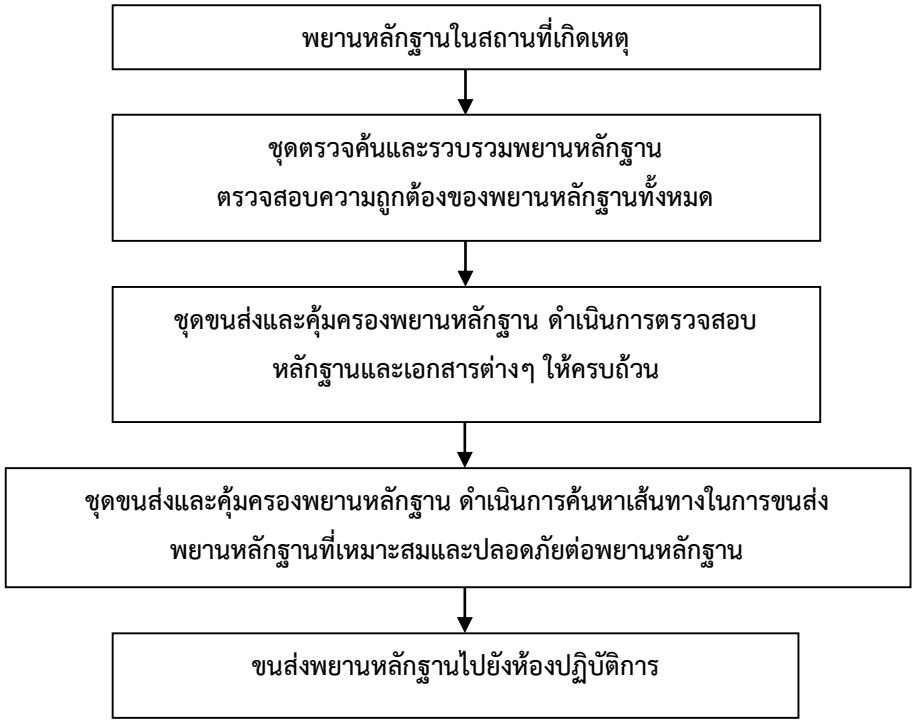
4) ให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ดำเนินการค้นหาเส้นทางในการขนส่งพยานหลักฐานที่เหมาะสมและปลอดภัยต่อพยานหลักฐาน โดยคำนึงถึงปัจจัยสำคัญที่อ้างอิงตามหัวข้อปัจจัยสำคัญที่ต้องให้ความสำคัญระหว่างการขนส่งพยานหลักฐาน

5) ขนส่งพยานหลักฐานไปยังห้องปฏิบัติการ

ปัจจัยสำคัญที่ต้องให้ความสำคัญระหว่างการขนส่งพยานหลักฐาน

- การขนส่งพยานหลักฐานต้องใช้รถขนส่งพยานหลักฐานที่ได้รับการออกแบบมาโดยเฉพาะ
- หลีกเลี่ยงการใช้งานคลื่นวิทยุหรืออุปกรณ์ใดๆ ที่อาจก่อให้เกิดคลื่นวิทยุและคลื่นสนามแม่เหล็ก
- หลักเลี่ยงเส้นทางที่มีเสาไฟฟ้าแรงสูง หรือมีคลื่นสนามแม่เหล็กแรงสูง

ดังแสดงภาพที่ 4-9



ภาพที่ 4-9 ขั้นตอนการบริหารจัดการขนส่งพยานหลักฐาน (Evidence Transportation Management)

2.7 ขั้นตอนการบริหารจัดการและจัดเก็บพยานหลักฐาน (Evidence Retention Management)

1) ชุดขนส่งและคุ้มครองพยานหลักฐาน ส่งพยานหลักฐานให้ชุดดูแลห้องเก็บพยานหลักฐาน พร้อมลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดดูแลห้องเก็บพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

2) ชุดดูแลห้องเก็บพยานหลักฐาน ทำการบันทึกข้อมูลรายการหลักฐานที่ได้รับลงในเอกสารการจัดเก็บหลักฐาน (Evidence Retention Form) พร้อมลงลายมือชื่อ

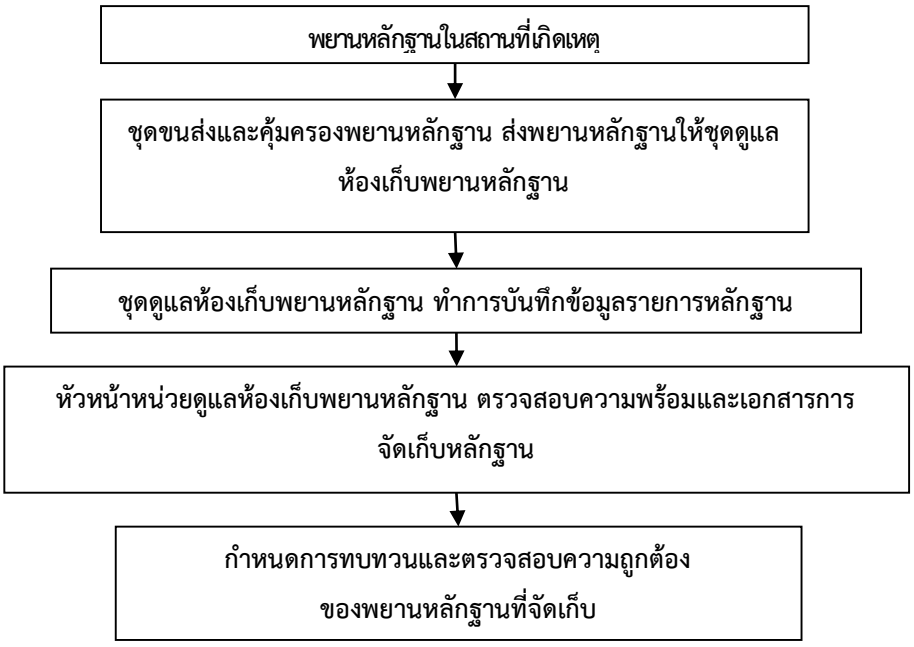
3) หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน ตรวจสอบความพร้อมและเอกสารการจัดเก็บหลักฐาน พร้อมลงลายมือชื่อรับรองความถูกต้อง

4) กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐานในฐานะผู้รับผิดชอบห้องเก็บพยานหลักฐานจำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

4.1) ความถูกต้องครบถ้วนของพยานหลักฐานที่จัดเก็บ เทียบกับรายการตามเอกสาร

4.2) ความถูกต้องสมบูรณ์ทางกายภาพของพยานหลักฐานในปัจจุบัน เทียบกับข้อมูลสภาพของหลักฐานเมื่อได้รับมา

ดังแสดงภาพที่ 4-10



ภาพที่ 4-10 ขั้นตอนการบริหารจัดการและจัดเก็บพยานหลักฐาน (Evidence Retention Management)

2.8 ขั้นตอนการเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน

1) เจ้าหน้าที่ประจำห้องปฏิบัติการ ตรวจสอบความถูกต้องและครบถ้วนของเครื่องมือที่ต้องใช้งานในแต่ละคดี

2) เจ้าหน้าที่ประจำห้องปฏิบัติการ ทดสอบความถูกต้องของโปรแกรมโดยการตรวจสอบคุณสมบัติเบื้องต้น (Function) และตรวจสอบลิขสิทธิ์ (License) ของแต่ละซอฟต์แวร์

3) เจ้าหน้าที่ประจำห้องปฏิบัติการตรวจสอบและจัดเตรียมอุปกรณ์สำหรับการจัดทำสำเนาหลักฐาน

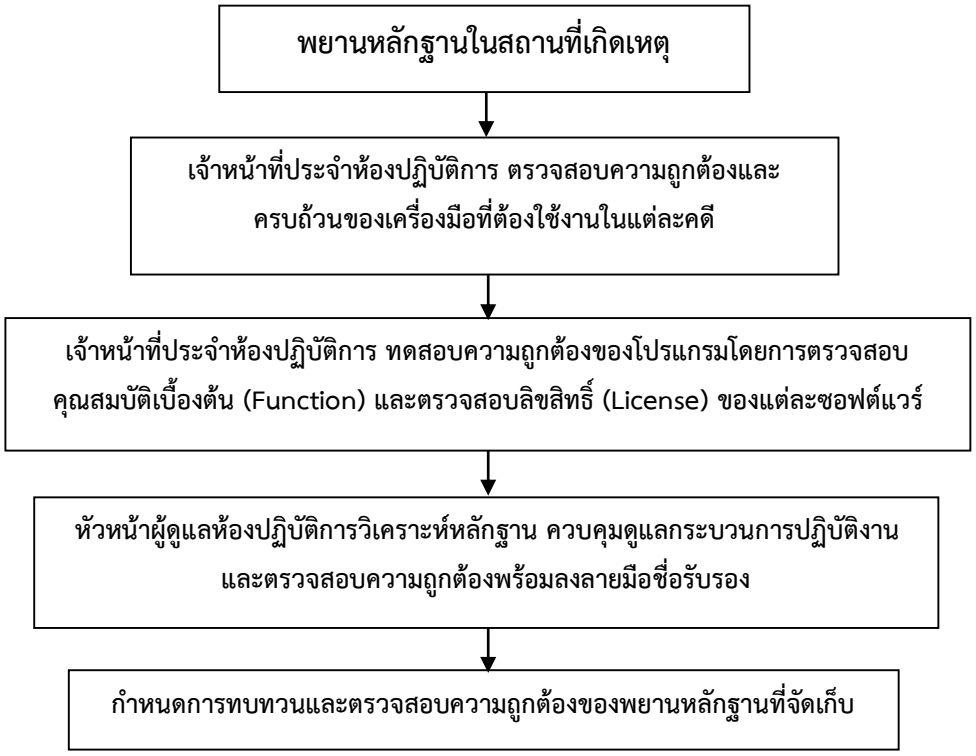
4) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน ควบคุมดูแลกระบวนการปฏิบัติงานและตรวจสอบความถูกต้องพร้อมลงลายมือชื่อรับรอง

5) กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐานในฐานะผู้รับผิดชอบห้องปฏิบัติการวิเคราะห์หลักฐานจำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของเครื่องมือและซอฟต์แวร์ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

5.1) เครื่องมือและซอฟต์แวร์สามารถใช้งานได้เป็นปกติ

5.2) เครื่องมือและซอฟต์แวร์มีลิขสิทธิ์ที่ถูกต้อง ดังแสดงภาพที่ 4-11



ภาพที่ 4-11 **ขั้นตอนการเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน (Computer Forensic Tools and Equipment Preparation)**

2.9 แนวทางคำถามสำหรับคดีทางด้านอาชญากรรมคอมพิวเตอร์

ในการใช้คำถามเหล่านี้ควรจะต้องมีข้อมูลเบื้องต้นก่อนเพื่อช่วยในการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ โดยข้อมูลเบื้องต้นที่ควรทราบมีดังต่อไปนี้

- ข้อมูลโดยสรุปของคดี เช่น รายงานการสืบสวน คำให้การของพยาน
- หมายเลข IP (ถ้ามี)
- รายการ keywords เช่น ชื่อ สถานที่ สิ่งที่ระบุถึงตัวบุคคลต่าง ๆ
- ชื่อเล่น นามแฝง เช่น ชื่อเล่นทั้งหมดที่ใช้โดยเหยื่อหรือผู้ต้องสงสัย
- พาสเวิร์ด เช่น พาสเวิร์ดทั้งหมดที่ใช้โดยเหยื่อหรือผู้ต้องสงสัย
- ข้อมูลการติดต่อ หมายถึง ชื่อของผู้ทำการสืบสวนที่ร้องขอให้ทำการตรวจพิสูจน์พยานหลักฐานคอมพิวเตอร์
- เอกสารที่เกี่ยวข้อง เช่น ใบอนุญาต หมายค้น ฯลฯ
- ชนิดของการกระทำความผิด จะต้องให้ข้อมูลที่เกี่ยวข้องกับคดี

1) คำถามทั่วไปสำหรับผู้ทำการสืบสวนสอบสวน ซึ่งอาจจะใช้ถามในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ดังต่อไปนี้

- ได้เครื่องคอมพิวเตอร์นี้มาเมื่อไหร่ เป็นเครื่องใหม่หรือเป็นเครื่องใช้แล้ว
- ใครเป็นผู้ใช้งานที่เข้าถึงฮาร์ดแวร์และซอฟท์แวร์
- สื่ออิเล็กทรอนิกส์ต่าง ๆ ของเครื่องคอมพิวเตอร์นั้น ถูกเก็บอยู่ที่ใด
- ลายพิมพ์นิ้วมือของใครที่อาจพบบนอุปกรณ์อิเล็กทรอนิกส์
- หากมีคนอื่นที่เข้าถึงเครื่องคอมพิวเตอร์นั้น ฮาร์ดแวร์หรือซอฟท์แวร์ใดที่สามารถเข้าถึงทุกสิ่งทุกอย่างที่อยู่บนเครื่องคอมพิวเตอร์ หรือเข้าถึงเพียงแค่ไฟล์ โฟล์เดอร์ หรือโปรแกรมที่ต้องการได้
- มีใครกี่คนที่ใช้เครื่องคอมพิวเตอร์เครื่องนี้ เป็นใครบ้าง
- ผู้ใช้งานคอมพิวเตอร์แต่ละคนมีประสบการณ์ในการใช้งานคอมพิวเตอร์ในระดับใด
- ผู้ใช้งานแต่ละคนนั้นใช้งานเครื่องคอมพิวเตอร์ในช่วงเวลาใดของวันบ้าง
- Username บนเครื่องคอมพิวเตอร์นั้นมีอะไรบ้าง
- โปรแกรมอะไรบ้างที่ผู้ใช้งานแต่ละคนใช้
- เครื่องคอมพิวเตอร์นั้นต้องการ username และ password ในการเข้าใช้งานหรือไม่ ถ้าใช่ username และ password นั้นมีอะไรบ้าง
- มีซอฟท์แวร์อะไรในเครื่องบ้างไหมที่ต้องใช้พาสเวิร์ด
- เครื่องคอมพิวเตอร์นั้นมีการเชื่อมต่อกับอินเทอร์เน็ตอย่างไร (ใช้ DSL, ผ่านสายโทรศัพท์ ระบบ lan หรืออื่น ๆ)
- เหยื่อหรือผู้ต้องสงสัยมีอีเมล์หรือไม่ ใช้อีเมล์ของอะไร (yahoo, AOL, gmail, hotmail หรืออื่น ๆ)
- หากมีอีเมล์เข้ามาเกี่ยวข้องในคดี ให้ถามเหยื่อหรือผู้ต้องสงสัยถึงชื่ออีเมล์ต่างๆ ของเขา

- โปรแกรมอีเมล์ใดที่ผู้ต้องสงสัยหรือเหยื่อใช้
- เหยื่อหรือผู้ต้องสงสัยสามารถเข้าถึงเครื่องคอมพิวเตอร์ของตนเองได้จากระยะไกลหรือไม่ (สามารถเข้าถึงเครื่องตัวเองเมื่ออยู่ไกลจากบ้านหรือออฟฟิศได้หรือไม่)
- มีผู้ใช้เครื่องคนใดใช้พื้นที่เก็บบันทึกข้อมูลออนไลน์หรือใช้พื้นที่เก็บบันทึกข้อมูลแบบ remote storage หรือไม่
- มีโปรแกรมใดหรือไม่ที่ถูกใช้เพื่อล้างข้อมูลในคอมพิวเตอร์นั้น
- ในเครื่องคอมพิวเตอร์นั้นมีโปรแกรมสำหรับการเข้ารหัสหรือเครื่องมือในการทำ wiping ฮาร์ดไดร์ฟหรือไม่
- เครื่องคอมพิวเตอร์นั้นเปิดทำงานอยู่ตลอดเวลาใช่หรือไม่

2) คำถามสำหรับคดีอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ ใช้ถามเจาะจงกรณีความผิดและเจาะจงกับบุคคล ดังต่อไปนี้

กรณีการขโมยข้อมูลส่วนบุคคลและคดีทางด้านการเงิน :

คำถามที่ใช้ถามผู้เสียหาย :

- คุณรู้ถึงความผิดปกติใด ๆ ที่เกิดกับ account ของคุณหรือไม่
- Account ใดที่นำข้อมูลไปใช้ให้เกิดความเสียหาย
- คุณได้ให้ข้อมูลส่วนตัวกับใครหรือหน่วยงานใดหรือไม่
- คุณให้ข้อมูลนั้นไปเพื่ออะไร
- เมื่อเร็ว ๆ นี้คุณได้กรอกข้อมูลสมัครใช้บัตรเครดิตหรือเอกสารเงินกู้ใดๆ หรือไม่
- คุณเก็บข้อมูลส่วนตัวของคุณไว้ในเครื่องคอมพิวเตอร์หรือไม่
- มีข้อมูลใบเสร็จหรือ statement ทางการเงินถูกส่งไปให้ทางเมล์อย่างผิดปกติหรือไม่
- คุณได้ตรวจสอบรายการการใช้บัตรเครดิตบ้างหรือไม่

3) คำถามที่ใช้ถามกับบุคคลเป้าหมายหรือผู้ต้องสงสัย:

- ซอฟท์แวร์ของเครื่องคอมพิวเตอร์ของคุณอยู่ที่ใด (เช่น แผ่นซีดี แผ่นฟล็อปปี้ดิสก์ ฯลฯ)
- เครื่องคอมพิวเตอร์มีโปรแกรมสำหรับใช้ทำเช็คหรือเอกสารทางการเงินอื่นๆ หรือไม่
- เครื่องคอมพิวเตอร์มีซอฟท์แวร์ในการสร้างหรือตกแต่งรูปภาพหรือไม่
- เครื่องคอมพิวเตอร์มีบัตรต่าง ๆ ที่ถูกทำขึ้นหรือที่ถูก scan เข้ามาหรือไม่
- เครื่องคอมพิวเตอร์ได้ถูกใช้งานการซื้อขายออนไลน์หรือไม่

4) อาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวข้องกับเด็ก:

คำถามที่ใช้ถามผู้เสียหาย :

- ผู้เสียหายได้ออนไลน์ให้ห้องแชทใด ๆ หรือไม่
- ผู้เสียหายใช้อินเทอร์เน็ต อีเมล์หรือแชทจากเครื่องคอมพิวเตอร์เครื่องอื่น ๆ หรือไม่ ถ้าใช่ใช้ที่ใด

- ผู้เสียหายได้ให้ข้อมูลจริงกับคนอื่นที่ออนไลน์อยู่หรือไม่ เช่น ชื่อจริง อายุ ที่อยู่ เป็นต้น
- อีเมล์ของผู้เสียหายคืออะไร หรือใช้ชื่ออะไรในการออนไลน์เล่นแชท และเล่นในห้องใด
- มีรายชื่อใครบ้างที่อยู่ในลิสต์การเล่นแชทของผู้เสียหาย
- ผู้เสียหายได้ทำการเก็บบันทึก chat logs ไว้หรือไม่
- ผู้เสียหายใช้อีเมล์หรือแชตของที่ใด ด้วยโปรแกรมอะไร
- มีพฤติการณ์ที่เน้นออกไปในทางเพศในรูปภาพหรือการติดต่อพูดคุยกันหรือไม่
- ผู้เสียหายเคยได้รับภาพหรือของขวัญจากผู้ต้องสงสัยหรือไม่

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

- เครื่องคอมพิวเตอร์ทั้งหมดของผู้ต้องสงสัยอยู่ที่ใด
- ผู้ต้องสงสัยทำการเก็บข้อมูลไว้ที่อื่นหรือไม่ เช่น เก็บใน external hard drive หรือที่เก็บข้อมูลออนไลน์ เป็นต้น
- ผู้ต้องสงสัยใช้ชื่อใดในการออนไลน์ และเข้าคุยในห้องแชตใด ด้วยชื่ออะไร
- ผู้ต้องสงสัยได้ทำการติดต่อกับใครทางอิเล็กทรอนิกส์หรือไม่
- ผู้ต้องสงสัยทำการติดต่อกับผู้อื่นนั้นด้วยวิธีได้ (ทางอีเมล์ แชต เป็นต้น)
- ผู้ต้องสงสัยดูภาพลามกอนาจารเด็กโดยใช้เครื่องคอมพิวเตอร์หรือไม่ ถ้าใช่ผู้ต้องสงสัยได้รูปภาพเหล่านั้นมาได้อย่างไร
- ผู้ต้องสงสัยได้ทำการส่งรูปภาพเหล่านั้นไปยังบุคคลอื่นๆ หรือไม่
- ผู้ต้องสงสัยตระหนักหรือไม่ว่าเขากำลังดูภาพเด็ก ๆ โดยไม่ยอมรับว่าเป็นภาพที่เครื่องคอมพิวเตอร์สร้างขึ้น
- ผู้ต้องสงสัยมีการสมัครใช้บริการ hi5, MSN, ICQ หรือไม่

5) การบุกรุกหรือการเจาะเข้าระบบ (คำถามเกี่ยวของกับระบบเครือข่าย):

คำถามระบบเครือข่ายภายในบ้าน :

- คุณสามารถทำการหาว่าสายเน็ตเวิร์คต่าง ๆ เชื่อมต่ออยู่กับเครื่องใดทั้งระบบได้หรือไม่
- เครื่องคอมพิวเตอร์แต่ละเครื่องถูกใช้งานโดยผู้ใช้แต่ละคนใช่หรือไม่
- ระบบเครือข่ายนั้นเชื่อมต่อกับอินเทอร์เน็ตหรือไม่
- ระบบเครือข่ายนั้นเชื่อมต่ออินเทอร์เนตด้วยวิธีใด (DSL ผ่ายสายโทรศัพท์ หรืออื่นๆ)
- สาย DSL หรือโมเด็มตั้งอยู่ที่ใด ตอนนี้เชื่อมต่ออยู่หรือไม่
- ใครคือ ISP
- มีเครื่องมากกว่า 1 เครื่องหรือไม่ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้
- มีระบบเครือข่ายไร้สายในที่นั้นด้วยหรือไม่

คำถามระบบเครือข่ายในองค์กรธุรกิจ :

- ใครที่สังเกตพบการกระทำที่ผิดกฎหมายเป็นคนแรก

- ทำการค้นหาว่าการกระทำนั้นผิดกฎหมายประเภทใด และหาข้อมูลการติดต่อกับพยานทุกคน
- หาตัวว่าใครคือ admin ของระบบนั้น และหาข้อมูลการติดต่อมา (admin ไม่ควรได้รับการติดต่อจากผู้ที่ทำการสืบสวนสอบสวนในขั้นต้น)
- มีพนักงานบริษัทหรืออดีตพนักงานบริษัทคนใดที่น่าสงสัยหรือไม่
- มีภาพแผนผังของระบบเครือข่ายนั้นหรือไม่
- ได้มีการเก็บ log การใช้งานไว้หรือไม่
- สามารถทำการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์-โดยทันทีเพื่อการสืบสวนสอบสวนในขั้นต่อไปได้หรือไม่
- ได้มีการติดต่อบุคคลจากหน่วยงานบังคับใช้กฎหมายอื่น ๆ หรือยัง

6) การกระทำความผิดที่เกี่ยวข้องกับอีเมล์

คำถามที่ใช้ถามผู้เสียหาย :

- ขอข้อมูลอีเมล์ของผู้เสียหายและผู้ให้บริการอีเมล์นั้น
- ขอ username และ e-mail account ทั้งหมดของผู้เสียหาย
- ขอสำเนาอีเมล์ที่ผู้เสียหายได้รับ อย่าเปิดเครื่องคอมพิวเตอร์เพื่อทำการสำเนาอีเมล์นั้น

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

- ขออีเมล์ของผู้ต้องสงสัยและผู้ให้บริการอีเมล์นั้น
- ขอ username และ e-mail account ทั้งหมดของผู้ต้องสงสัย
- ขอพาสเวิร์ดทั้งหมดและซอฟท์แวร์ที่เกี่ยวข้อง รวมทั้ง username ที่ใช้โดยผู้ต้องสงสัย

7) การกระทำความผิดที่เกี่ยวข้องกับ Instant Messaging และ IRC

คำถามที่ใช้ถามผู้เสียหาย :

- ถามผู้เสียหายว่าได้เก็บ log การใช้งานในระหว่างแชทหรือไม่
- ขอชื่อที่ผู้เสียหายใช้ในการออนไลน์รวมทั้งอีเมล์แอดเดรส
- ขอสำเนาทั้งหมดที่เหยื่อได้ทำการปริ้นท์ออกมา
- ซอฟท์แวร์ใด หรือผู้ให้บริการแชทใดที่ผู้เสียหายใช้

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

- ขอชื่อที่ผู้ต้องสงสัยใช้ในการออนไลน์รวมทั้งอีเมล์แอดเดรส
- ขอพาสเวิร์ดทั้งหมดและซอฟท์แวร์ที่เกี่ยวข้อง รวมทั้ง username ที่ใช้โดยผู้ต้องสงสัย

8) แนวทางการดำเนินการกับกรณีการขโมยข้อมูลส่วนบุคคลออนไลน์

การป้องกัน

- อย่าให้ข้อมูลต่อไปนี้กับใครที่ไม่รู้จัก

วัน/สถานที่เกิด, ที่อยู่, หมายเลขบัตรประกันสังคม, หมายเลขโทรศัพท์, หมายเลขบัตรเครดิต

- ดูรายการการใช้บัตรเครดิตอย่างน้อยปีละครั้ง

- ดูให้แน่ใจว่าการโอนเงินทางอินเทอร์เนตนั้นปลอดภัยหรือไม่ โดยสังเกตที่ลูกกุญแจล็อกที่ทางด้านล่างขวาของเว็บเบราเซอร์ก่อนทำการกรอกข้อมูลส่วนตัวใด ๆ

- หากไม่จำเป็นจริง ๆ อย่าเก็บข้อมูลทางการเงินไว้ในเครื่องคอมพิวเตอร์

- ก่อนทำการทิ้งเครื่องคอมพิวเตอร์ ให้ทำลายข้อมูลทั้งหมดที่อยู่ในฮาร์ดไดร์ฟทิ้งไป โดยใช้เครื่องมือที่ใช้ทำการ wipe เนื่องจากการ format ไม่ช่วยทำลายข้อมูลได้มากนัก

- ใช้พาสเวิร์ดที่แข็งแรงและไม่ตั้งค่าให้โปรแกรมใด ๆ จำพาสเวิร์ดไว้

- ใช้ซอฟท์แวร์ป้องกันไวรัส เพื่อป้องกันการถูกขโมยข้อมูลจากเครื่องคอมพิวเตอร์ และช่วยป้องกันการเข้ามาของโปรแกรมประสงค์ร้ายต่าง ๆ (malware) การดำเนินการ

- ติดต่อธนาคารหรือผู้ออกบัตรเครดิตเพื่อรายงานการฉ้อโกงที่เกิดขึ้น

- ใช้การเตือนการฉ้อโกง (fraud alert)

2.10 การตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์

การตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ เป็นการตรวจข้อมูลดิจิทัลที่บันทึกอยู่ในเครื่องคอมพิวเตอร์ สมาร์ทโฟน (Smart phone), สื่อบันทึกข้อมูลชนิดต่าง ๆ เช่น External Hard Disk, Thumb Drive เป็นต้น เพื่อดูรายละเอียดข้อมูลดิจิทัลดังกล่าว เพื่อยืนยันการกระทำผิดที่เกิดขึ้น

1) ของกลางที่เกี่ยวข้องกับการตรวจพิสูจน์

1.1) ของกลางในที่เกิดเหตุ/ที่พนักงานสอบสวนนำส่ง

- คอมพิวเตอร์ ซึ่งสามารถแยกย่อยออกเป็น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์ โน้ตบุ๊ก คอมพิวเตอร์แม่ข่าย (Server) เป็นต้น

- กรณีที่เป็นฮาร์ดดิสก์

- โทรศัพท์ ซึ่งสามารถแยกย่อยออกเป็น โทรศัพท์สำนักงาน โทรศัพท์มือถือ Tablet Smartphone

- แผ่นซีดี ดีวีดี/บัตรอิเล็กทรอนิกส์

- เครื่องบันทึกภาพกล้องวงจรปิด เพื่อนำมากู้ข้อมูลที่ถูกลบ ซึ่งต้องยกมาทั้งเครื่อง และมีฮาร์ดดิสก์เปล่าเพื่อนำมาเก็บข้อมูลจากเครื่องบันทึกภาพกล้องวงจรปิดที่กู้คืนขึ้นมาได้

- อุปกรณ์ไฟฟ้าหรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ ที่มีหน่วยความจำสำหรับบันทึกข้อมูลดิจิทัล

2.2) ของกลางที่เป็นประเด็นปัญหาที่พนักงานสอบสวนส่งมาให้ค้นหา

- เอกสารหน้าเฟซบุ๊กหมิ่นประมาทที่ส่งมาเปรียบเทียบ

- แฟ้มข้อมูลที่ส่งมาเปรียบเทียบ เช่น แฟ้มข้อมูลเพลงที่ถูกละเมิดลิขสิทธิ์

- แฟ้มข้อมูลเอกสารตัวอย่างที่ต้องการให้ค้นหา เช่น ใบกำกับภาษี ใบเสร็จรับเงิน เป็นต้น

2) ลักษณะของการตรวจพิสูจน์

2.1) การตรวจเปรียบเทียบข้อมูลในของกลางกับตัวอย่าง

2.2) การตรวจสอบข้อมูลจากของกลางโดยใช้โปรแกรมคอมพิวเตอร์

3) คำแนะนำในการเตรียมของกลางเพื่อตรวจพิสูจน์

วิธีการเก็บและบรรจุหีบห่อในการนำส่งของกลางเพื่อทำการตรวจพิสูจน์

3.1) คอมพิวเตอร์ส่วนบุคคล (Personal computer)

3.1.1) คอมพิวเตอร์อยู่ในสภาพ “ปิดทำงาน” ห้ามทำการเปิดเครื่อง ให้ถ่ายภาพตามขั้นตอนการถ่ายภาพเมื่อเข้าสถานที่เกิดเหตุ

3.1.2) คอมพิวเตอร์ส่วนบุคคลอยู่ในสภาพ “เปิดทำงาน”

- เมื่อพนักงานสอบสวนไปถึงสถานที่เกิดเหตุ ให้ควบคุมตัวผู้ต้องสงสัยออกจากวัตถุพยานเพื่อมิให้ผู้ต้องสงสัยเปลี่ยนแปลงข้อมูลหรือทำลายวัตถุพยานเพื่อปกปิดการกระทำความผิด

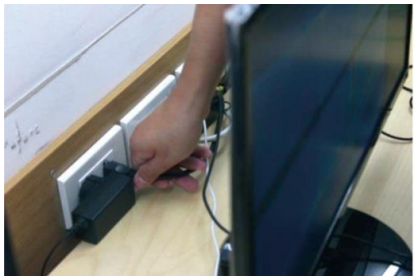
- ถ่ายภาพสถานที่เกิดเหตุและภาพวัตถุพยานที่ใช้ในการกระทำความผิด เพื่อใช้ในการยืนยันขั้นต้นว่า สถานที่เกิดเหตุมีการจัดวางเครื่องคอมพิวเตอร์รวมถึงอุปกรณ์ต่าง ๆ ไว้ในที่ตำแหน่งใดและถ่ายภาพหน้าจอของเครื่องคอมพิวเตอร์ที่ใช้ในการกระทำผิด เพื่อยืนยันว่าคอมพิวเตอร์เครื่องใด กำลังใช้งานเกี่ยวกับอะไร หรือมีโปรแกรมที่ใช้การกระทำความผิดอยู่หรือไม่ เช่น โปรแกรมเทรดหุ้น, โปรแกรมทำบัตรปลอม และแฟ้มข้อมูลเอกสารใบกำกับภาษีปลอม เป็นต้น โดยสามารถดูตัวอย่าง การถ่ายภาพเมื่อพบคอมพิวเตอร์อยู่ในสภาพ “เปิดทำงาน” ได้ตามภาพที่ 4-12 ถึง 4-18

ภาพที่ 4-12 ถ่ายภาพโดยรวมจากเครื่องคอมพิวเตอร์วัตถุพยานขณะเปิดเครื่อง

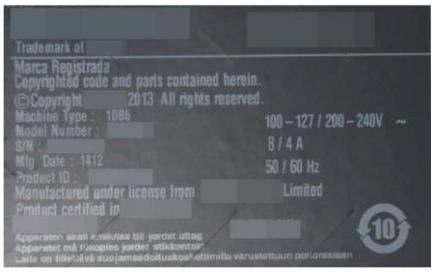
ภาพที่ 4-13 ถ่ายภาพตำแหน่งสายต่าง ๆ ของเครื่องคอมพิวเตอร์วัตถุพยาน

ภาพที่ 4-14 ทำการถอดสาย Lan จากเครื่องคอมพิวเตอร์วัตถุพยาน
เพื่อป้องกันการรีโมทเข้ามาทำลายข้อมูลภายในวัตถุพยาน

ภาพที่ 4-15 ถ่ายซูมเฉพาะหน้าจอของเครื่องคอมพิวเตอร์วัตถุพยาน
เพื่อให้ทราบว่ากำลังใช้งานโปรแกรมใดอยู่ในขณะนั้น



ภาพที่ 4-16 กรณีที่สามารถเก็บข้อมูลในหน่วยความจำ RAM ได้
ให้เก็บข้อมูลในหน่วยความจำ RAM ก่อนทำการถอดปลั๊กตามภาพ



ภาพที่ 4-17 ถ่ายรายละเอียดของฉลาก สติ๊กเกอร์ ที่ติดอยู่บนเครื่องคอมพิวเตอร์วัตถุพยาน

ภาพที่ 4-18 ควรติดฉลากแล้วเขียนตัวเลขกำกับบนเครื่องคอมพิวเตอร์วัตถุพยาน เพื่อไม่ให้เกิดการสับสนขณะนำส่งวัตถุพยาน

- ตรวจสอบในช่อง DVD, CD, Floppy disk, Card reader หรือช่องต่อ USB ต่าง ๆ ว่ามีแผ่นซีดี Thumb Drive หรืออุปกรณ์ใด ๆ ค้างอยู่หรือไม่ และควรนำส่งไปพร้อมคอมพิวเตอร์ของกลางด้วย

- การนำส่งตรวจพิสูจน์ควรใช้เทปคาดกั้นฝาปิดช่องต่ออุปกรณ์ต่าง ๆ เช่น ฝาปิดเครื่องช่องใส่ DVD หรือ USB พร้อมเซ็นชื่อกำกับ แล้วจึงบรรจุลงกล่องกระดาษหรือถุงกระดาษ ซึ่งมีวัสดุกันกระแทกให้เรียบร้อย

3.2) คอมพิวเตอร์โน้ตบุ๊ก (Notebook)

3.2.1) กรณีที่เป็นเครื่องคอมพิวเตอร์โน้ตบุ๊ก (Notebook) อยู่ในสภาพ “ปิดทำงาน” ห้ามทำการเปิดเครื่อง เนื่องจากจะเป็นการเปลี่ยนแปลงวันที่เข้าถึงครั้งสุดท้ายของเครื่องคอมพิวเตอร์โน้ตบุ๊กวัตถุพยาน ทำให้วัตถุพยานเกิดการปนเปื้อนซึ่งผิดหลัก “Chain of Custody”

3.2.2) กรณีที่เป็นเครื่องคอมพิวเตอร์โน้ตบุ๊กอยู่ในสภาพ “เปิดทำงาน” ให้ปฏิบัติตามข้อ 3.1.2) คอมพิวเตอร์ส่วนบุคคลอยู่ในสภาพ “เปิดทำงาน” แล้วจึงทำตามข้อต่อไปนี้

- ปลดล็อกรหัสผ่านเครื่องคอมพิวเตอร์โน้ตบุ๊ก
- ถอดสายไฟของเครื่องคอมพิวเตอร์โน้ตบุ๊กออกจากตัวเครื่อง และถอดแบตเตอรี่
- การนำส่งตรวจพิสูจน์ ควรใส่เครื่องคอมพิวเตอร์โน้ตบุ๊กของกลางในกระเป๋ากันกระแทก หากบรรจุกล่องอื่น ๆ ควรใส่สายชาร์จ หรืออุปกรณ์เสริมอื่น ๆ แยกจากกัน เพื่อป้องกันการกดทับซึ่งอาจทำให้เกิดความเสียหายกับตัวเครื่องคอมพิวเตอร์โน้ตบุ๊กได้

3.3) อาชญากรรมคอมพิวเตอร์ในระบบเครือข่าย หรือเครื่องแม่ข่าย (Server)

3.3.1) ขอคำปรึกษาจาก เจ้าหน้าที่กองพิสูจน์หลักฐานกลาง ศูนย์พิสูจน์หลักฐาน 1-10 หรือเจ้าหน้าที่ที่มีความชำนาญ เช่น กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ในการเข้าไปยังสถานที่เกิดเหตุ และแยกผู้ต้องสงสัยออกจากคอมพิวเตอร์ในทันที เนื่องจากผู้ต้องสงสัยอาจจะสามารถเข้าลบข้อมูลที่บันทึกอยู่ในคอมพิวเตอร์ของกลาง โดยใช้คำสั่งส่งผ่านทางอุปกรณ์พกพาขนาดเล็ก เช่น โทรศัพท์มือถือได้อย่างรวดเร็ว

3.3.2) กรณีเครื่องเป็นระบบเครือข่าย ห้ามตัดไฟจากแหล่งจ่ายไฟ หรือกระทำการอื่นใด เพราะการกระทำเช่นนั้นอาจทำให้ระบบได้รับความเสียหายสูญเสียข้อมูลสำคัญ และทำให้เจ้าหน้าที่ตำรวจต้องรับผิดชอบต่อความเสียหาย

3.4) กรณีที่เป็นฮาร์ดดิสก์

ทั้งแบบบรรจุกล่องหรือแบบเปลือย หรือ Thumb Drive ถ่ายภาพภายนอกของอุปกรณ์ และหมายเลขเครื่อง (SN) จดบันทึกรายละเอียดต่าง ๆ เช่น ยี่ห้อ ความจุ และหมายเลขอื่น ๆ ที่ปรากฏ และหยิบจับอุปกรณ์ด้วยความระมัดระวังเนื่องจากเป็นอุปกรณ์ที่ได้รับความเสียหายได้ง่าย การนำส่งต้องบรรจุใส่กล่องกระดาษหรือห่อกระดาษแบบมีวัสดุกันกระแทก ก่อนปิดผนึกให้เรียบร้อย พร้อมทั้งเซ็นชื่อกำกับ แล้วจึงนำส่งตรวจพิสูจน์

3.5) โทรศัพท์มือถือ Tablet Smartphone

3.5.1) หากโทรศัพท์มือถืออยู่ในสภาพ “ปิดทำงาน” ให้ปล่อยไว้ในสภาพ “ปิดทำงาน” ห้ามทำการเปิดเครื่อง หรือถอดแบตเตอรี่ เพื่อดูซิมการ์ดด้วยตัวเองโดยเด็ดขาด

3.5.2) หากโทรศัพท์มือถืออยู่ในสภาพ “เปิดทำงาน”

- ปล่อยโทรศัพท์ไว้ในสภาพ “เปิดทำงาน” ถ่ายภาพที่ปรากฏบนหน้าจอรวมถึงวันที่เวลาของเครื่องและบรรจุไว้ในถุงกันคลื่นแม่เหล็กไฟฟ้า (Faraday bag) ตามภาพที่ 4-19

- หากไม่มีถุงกันคลื่นแม่เหล็กไฟฟ้า ตามภาพที่ 4-20 ให้ถ่ายภาพที่ปรากฏบนหน้าจอรวมถึงวันที่เวลาของเครื่องโทรศัพท์ก่อนปิดเครื่อง

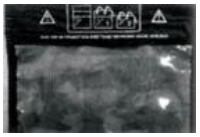
ภาพที่ 4-19 แสดงภาพโทรศัพท์มือถือบรรจุอยู่ในถุงคลื่นแม่เหล็กไฟฟ้า

ภาพที่ 4-20 แสดงภาพถุงคลื่นแม่เหล็กไฟฟ้า (FARADAY BAG)

ถ่ายภาพ และจดบันทึกรายละเอียด เช่น ยี่ห้อ รุ่น ก่อนบรรจุใส่กล่องหรือห่อกระดาษ แล้วปิดผนึก ลงลายมือชื่อกำกับ แล้วนำส่งตรวจพิสูจน์ ถ้าเป็นไปได้ให้แยก 1 เครื่องต่อ 1 ห่อ หากมีอุปกรณ์สายชาร์จแบตเตอรี่หรือสายเชื่อมต่อข้อมูลให้นำส่งมาพร้อมด้วย ตามภาพที่ 4-21

ภาพที่ 4-21 แสดงขั้นตอนการถ่ายภาพโดยละเอียดของโทรศัพท์มือถือ

โปรดทราบว่า หากท่านปล่อยโทรศัพท์ไว้ในสภาพ “เปิดทำงาน” ควรจัดส่งไปให้กองพิสูจน์หลักฐานกลางโดยเร็วที่สุด

กรณีเครื่องเปิดอยู่	
ปลด Password ไม่ได้	ปลด Password ได้
เปิดโหมดเครื่องบินหากเปิดได้	ให้ตั้งค่าตัวเครื่องไม่ให้มี password เปิดโหมดเครื่องบิน ปิด Wi Fi และปิด Bluetooth
ใส่ซองตัดสัญญาณ (FARADAY BAG) 	ใส่ซองตัดสัญญาณ (FARADAY BAG)  และบรรจุหีบห่อกันกระแทกให้เรียบร้อย

เครื่องปิดอยู่
ให้ใส่ซองกันกระแทกหรือบรรจุให้หีบห่อที่กันกระแทก
ให้สอบถามว่าเครื่องมี Password หรือไม่ ถ้ามี Password ควรสอบถามมาให้ได้

ภาพที่ 4-22 แผนผังแสดงการจัดเก็บของกลาง วัตถุพยานประเภทโทรศัพท์เคลื่อนที่

หมายเหตุ อย่าลืมนำสายชาร์จโทรศัพท์มาด้วย เพราะโทรศัพท์เคลื่อนที่แต่ละยี่ห้อ สายชาร์จจะมีขั้วที่ต่างกัน

3.6) แผ่นซีดี ดีวีดี/บัตรอิเล็กทรอนิกส์

ถ่ายภาพแผ่นด้านหน้า/หลังของบัตรและถ้าเป็นแผ่นซีดี หากของกลางมีมากกว่า 1 รายการ ควรระบุลำดับหรือข้อความที่เขียนอยู่บนแผ่นเพื่อใช้อ้างอิงกับรายละเอียดในหนังสือนำส่ง ควรจะบรรจุในซองบรรจุแผ่นซีดีหรือซองกระดาษ เช่นเดียวกับบัตรอิเล็กทรอนิกส์ ปิดหีบห่อให้เรียบร้อยก่อนนำส่งตรวจพิสูจน์ ตามภาพที่ 4-23

ภาพที่ 4-23 แสดงภาพตัวอย่างการบรรจุหีบห่อของแผ่นดีวีดีและบัตรอิเล็กทรอนิกส์

3.7) อุปกรณ์ไฟฟ้าหรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ

ถ่ายภาพ บรรจุกล่องกระดาษ/ซองกระดาษ แยกรายการให้ชัดเจน หากเป็นอุปกรณ์ขนาดเล็ก ให้ปิดผนึกด้วยซองกันกระแทกให้เรียบร้อย ลงลายมือชื่อกำกับนำส่งตรวจพิสูจน์ในทุกกรณี ถ้าเป็นไปได้ควรมีวัสดุรองรับแรงกดทับหรือแรงกระแทกเพื่อหลีกเลี่ยงความเสียหาย และควรหลีกเลี่ยงความชื้น และแสงแดด ตามภาพที่ 4-24

ภาพที่ 4-24 แสดงภาพตัวอย่างการบรรจุหีบห่อของอุปกรณ์อิเล็กทรอนิกส์

3.8) สื่อบันทึกข้อมูลดิจิทัลอื่น ๆ ที่ไม่ได้เชื่อมต่อกับเครื่องคอมพิวเตอร์

สื่อบันทึกข้อมูลดิจิทัลอื่น ๆ เช่น แผ่นซีดี ดีวีดี Floppy Disk /Thumb Drive /Sd Card /MicroSD สามารถนำส่งโดยบรรจุอยู่ในซองพลาสติกเดียวกัน หรือถุงเก็บพยานหลักฐาน รวมในใบเดียวกันได้ และควรมีวัสดุรองรับการกดทับหรือแรงกระแทกห่อหุ้มไว้ และควรติดฉลากระบุยี่ห้อ รุ่น ขนาด หรือจำนวนของกลางแต่ละรายการให้ชัดเจน ตามภาพที่ 4-25

หมายเหตุ ควรบันทึกรายละเอียดเกี่ยวกับของกลาง เช่น จำนวน ยี่ห้อ หรือรุ่น ให้ชัดเจนก่อนนำส่งตรวจพิสูจน์ และควรมีลายมือผู้นำส่งเซ็นกำกับที่หีบห่อด้วยทุกครั้ง

ภาพที่ 4-25 แสดงภาพตัวอย่างการบรรจุหีบห่อประเภทสื่อข้อมูลดิจิทัลอื่น ๆ ในกรณีเป็นหน่วยความจำแฟลช

3. องค์ความรู้และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญทางด้านการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์องค์ความรู้ และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชยากรรมทางเทคโนโลยี มีรายละเอียด และสาระสำคัญโดยสรุป ดังนี้

3.1 สภาพการณ์ทางด้านอาชญากรรมคอมพิวเตอร์

3.1.1 ปัจจุบันเจ้าหน้าที่บังคับใช้กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ดังนี้

1) ประมวลกฎหมายอาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ของลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6 และ มาตรา 269/7

2) พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

3) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และแก้ไขเพิ่มเติม พ.ศ. 2551

เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

4) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 ซึ่งให้อำนาจพนักงานเจ้าหน้าที่

5) พระราชบัญญัติการผลิต ผลิตภัณฑ์ซีดี พ.ศ. 2548

6) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

7) กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้ บริการอื่น ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

8) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

9) พระราชกฤษฎีกา ว่าด้วยการควบคุมดูและธุรกิจบริการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551

10) พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาบังคับใช้ พ.ศ. 2549

11) กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

12) กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ฉบับที่ 2 พ.ศ. 2555

13) ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนการสอบสวนและการดำเนินคดีกับผู้กระทำความผิดว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

14) ประกาศกระทรวงเทคโนโลยีและสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

15) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์และระยะเวลาการงดให้บริการโทรศัพท์เคลื่อนที่ในเขตพื้นที่จังหวัดนราธิวาส จังหวัดปัตตานี และจังหวัดยะลา พ.ศ. 2550

16) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2)

17) หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติหลักเกณฑ์ เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

18) ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ พ.ศ. 2555

19) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

20) หนังสือสำนักงานตำรวจแห่งชาติที่ 0011.26/537 ลงวันที่ 4 กุมภาพันธ์ 2556 เรื่อง แนวทางการสอบสวนและรวบรวมพยานหลักฐานในคดีการกระทำความผิดทางเทคโนโลยี

21) คู่มือการปฏิบัติงานด้านนิติวิทยาศาสตร์ในการสืบสวนสอบสวน สำนักงานตำรวจแห่งชาติ พุทธศักราช 2561

3.1.2 หน่วยงานที่รับผิดชอบดำเนินการคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ได้แก่ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสำนักงานตำรวจจะเป็นด่านแรกในการดำเนินการ สืบสวน สอบสวน ป้องกัน และปราบปราม อาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะหน่วยงานที่รับผิดชอบของสำนักงานตำรวจแห่งชาติ คือ สำนักงานเทคโนโลยีสารสนเทศ สำนักงานพิสูจน์หลักฐานตำรวจ และกองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี และสถานีตำรวจทั่วประเทศทั้งในส่วนกลางและส่วนภูมิภาค

3.2 วิธีการและขั้นตอนการสืบสวนและสอบสวนเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ปัจจุบัน มีการร้องทุกข์ให้ดำเนินคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ต เช่น กรณีผู้กระทำความผิดหลอกลวงขายสินค้าผ่านหน้าเว็บไซต์และหลอกลวงผู้ซื้อให้ชำระค่าสินค้าผ่านบัญชีธนาคาร เกิดขึ้นเป็นจำนวนมากและพบว่าในการสอบสวนดำเนินคดี มีหลายคดีที่พนักงานอัยการมีคำสั่งไม่ฟ้องผู้ต้องหาที่เป็นผู้เสนอขายสินค้าและผู้ต้องหาที่เป็นเจ้าของบัญชีเงินฝากที่ให้ผู้เสียหายโอนเงินเข้าบัญชี เนื่องจากคดีไม่มีพยานหลักฐานยืนยันว่าผู้ต้องหาได้เปิดเว็บไซต์ขายสินค้าและหลอกขายสินค้าให้กับผู้เสียหายและบุคคลทั่วไป ส่วนเจ้าของบัญชีเงินฝากนั้น พนักงานอัยการสั่งไม่ฟ้อง เนื่องจากพยานหลักฐานไม่เพียงพอที่จะทำให้เห็นได้ว่าบุคคลดังกล่าวมีส่วนเกี่ยวข้องในการกระทำความผิดอย่างไร

คดีความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์มีความยุ่งยากและซับซ้อนมากยิ่งขึ้นในปัจจุบัน ดังนั้น เพื่อให้การดำเนินการคดีกับผู้กระทำความผิดดังกล่าวเป็นไปอย่างถูกต้อง พนักงานสอบสวนมีข้อมูลที่ครบถ้วนสมบูรณ์ อันจะเป็นการพัฒนาระบบงานสอบสวนและคุ้มครองประชาชน ผู้บริสุทธิ์ให้มีประสิทธิภาพมากยิ่งขึ้น จึงกำหนดแนวทางการสอบสวนและรวบรวมพยานหลักฐานในคดีการกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ต ดังต่อไปนี้

1) ให้พิจารณาว่า คดีที่เกิดเป็นการกระทำความผิดในทางอาญา หรือเป็นการผิดสัญญาในทางแพ่ง ทั้งนี้ให้นำบทบัญญัติตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และ พ.ศ. 2560 มาประกอบการพิจารณาด้วยหากเป็นความผิดทางอาญา ให้ดำเนินคดีกับผู้กระทำความผิดฐานความผิดที่ปรากฏ

2) กรณีที่เป็นการกระทำความผิดทางอาญา ให้พนักงานสอบสวนทำการสอบสวนตามรูปคดี โดยมีแนวทางการสอบสวนเบื้องต้น ดังนี้

ก) ประเด็นคำถามในคดีด้านการเงินและการขโมยข้อมูล

1. การสอบสวนผู้กล่าวหา/ผู้เสียหาย ในประเด็น

(1) มีการตรวจพบสิ่งผิดปกติใด ๆ บ้างเกี่ยวกับบัญชีธนาคารของผู้เสียหาย

(2) พฤติการณ์การกระทำผิดและข้อเท็จจริงในคดีเป็นอย่างไร

(3) บัญชีธนาคารใดบ้างของผู้เสียหายที่ถูกแอบใช้ หรือถูกครอบครองกรรมสิทธิ์การใช้งานโดยไม่ได้รับอนุญาต

(4) ผู้เสียหายเคยให้ข้อมูลในการใช้งานกับบุคคลหรือหน่วยงานใดบ้างหรือไม่ หรือเคยให้ข้อมูลอะไร กับใครบ้าง

(5) เคยกรอกข้อมูลสมัครใช้งานบัตรเครดิต หรือเอกสารกู้ยืมใดๆ บ้างหรือไม่ อย่างไร

(6) เคยบันทึกข้อมูลสำหรับการใช้งานไว้ในเครื่องคอมพิวเตอร์ หรืออีเมล์หรือไม่ อย่างไร

(7) มีเอกสารการแจ้งหนี้หรือเอกสารการเงินที่ไม่ถูกส่งมาให้ผ่านทางอีเมล์ตามปกติหรือไม่

(8) เคยตรวจสอบรายงานการใช้บัตรเครดิตหรือไม่ ผลเป็นอย่างไร

(9) ได้มีการซื้อสินค้าทางเว็บไซต์ใด เมื่อวัน เดือน ปี และเวลา อะไร

(10) รายละเอียดของสินค้าเป็นอย่างไร ราคาเท่าไร

(11) มีการชำระเงินค่าสินค้าด้วยวิธีการอย่างไร เช่น การโอนเงินทางเครื่องเบิกถอนอัตโนมัติ (ตู้เอทีเอ็ม) ธนาคารใด สาขาอะไร เมื่อวันที่เดือนปีและเวลาอะไร โอนเงินค่าสินค้าจำนวนเท่าใด โอนไปบัญชีเลขที่อะไร ธนาคารใด ชื่อบัญชีผู้รับเงินคือใคร

(12) รายละเอียดในการติดต่อระหว่างผู้ซื้อและผู้ขาย เช่น ผู้ซื้อใช้อีเมล์อะไร ผู้โพสต์ข้อความ หรือผู้ขายใช้อีเมล์อะไร ติดต่อกันเมื่อเวลาใด และติดต่อครั้งสุดท้ายเมื่อใด

(13) ผู้ซื้อได้ใช้โทรศัพท์ติดต่อกับผู้ขายทางหมายเลขใด กี่ครั้ง เมื่อวันเวลาใด

(14) ผู้กล่าวหาได้รับความเสียหายจำนวนเท่าใด

(15) เหตุเกิดที่ไหน เมื่อใด

2. สอบสวนพนักงานธนาคารเจ้าของบัญชีของผู้กล่าวหา ในประเด็น

(1) บัญชีของผู้กล่าวหา เป็นบัญชีประเภทใด เลขที่อะไร เปิดบัญชีในนามของใคร เมื่อใด การเบิกถอนเงินจากบัญชีดังกล่าวมีเงื่อนไขอย่างไร

(2) มีเงินจ่ายค่าสินค้า โอนไปบัญชีเลขที่อะไร ที่ธนาคารใด

(3) การโอนเงินเป็นการโอนด้วยวิธีใด ดังต่อไปนี้

- โอนทางเครื่องเบิกถอนเงินอัตโนมัติ (ตู้เอทีเอ็ม) ต้องสอบสวนให้ได้ความว่าธนาคารใด ตู้เอทีเอ็มตั้งอยู่ที่ไหน โอนเงินเมื่อวันเดือน ปีและเวลาอะไร

- โอนเงินโดยทำรายการที่เคาน์เตอร์ของธนาคารใด สาขาอะไร เมื่อวันเดือนปีและเวลาอะไร เอกสารอ้างอิงเลขที่อะไร

- กรณีการโอนเงินผ่าน เวสเทิร์นยูเนียน หรือผู้บริการอื่น ๆ สอบสวนให้ได้ความว่าสถานที่ตั้งอยู่ไหน โอนเมื่อวันเดือนปีและเวลาอะไร ได้ระบุชื่อผู้รับประโยชน์คือใคร อยู่ที่ไหนเอกสารอ้างอิงหรือเอกสารการโอนเงินเลขที่ (MTCN) หมายเลขอะไร ผู้ที่มารับเงินมีเอกสารแสดงตัว (บัตรประชาชน/หนังสือเดินทาง) อะไร รับเงินที่ไหน เมื่อใด ให้ขอภาพถ่ายกล้องวงจรปิดมาประกอบสำนวนการสอบสวน

- กรณีการโอนเงินโดยใช้ช่องทางอื่น ๆ ให้สอบสวนขั้นตอนและวิธีการโอนเงินให้ชัดเจน

3. สอบสวนธนาคารเจ้าของบัญชีที่เป็นผู้รับโอนเงินจากผู้กล่าวหา ในประเด็น

(1) บัญชีธนาคารที่รับโอนเงิน เป็นบัญชีธนาคารประเภทใด เลขที่อะไร เปิดบัญชีในนามของใคร เมื่อใด การเบิกถอนเงินจากบัญชีดังกล่าว มีเงื่อนไขอย่างไร (ขอเอกสารการเปิดบัญชีประกอบ)

(2) มีเงิน (ระบุจำนวนเงินที่โอน) โอนเข้าบัญชีดังกล่าว เมื่อใด

(3) เงินดังกล่าวที่โอนมาด้วยวิธีการใด บัญชีเลขที่อะไร ธนาคารใด

(4) เงินดังกล่าวได้ถอนจากบัญชีไปเมื่อใด ถอนด้วยวิธีการอย่างไร (ถ้ามีการถอนเงินจากเอทีเอ็มให้ขอภาพจากกล้องวงจรปิดมาประกอบสำนวนการสอบสวน)

(5) ขอรายละเอียดเกี่ยวกับการโอนเงินทั้งหมดที่โอนมาเข้าบัญชีผู้กระทำผิดและมีผู้เสียหายรายอื่นร้องเรียนหรือไม่

4. สอบสวนผู้ดูแลเว็บไซต์หรือผู้ให้บริการอินเทอร์เน็ต ในประเด็น

(1) กระทู้ขายสินค้าโพสต์ในเว็บไซต์อะไร เมื่อวันเดือนปี และเวลาอะไร กระทู้ที่เท่าใด

(2) ผู้ดูแลเว็บไซต์ (WEB MASTER) เป็นใคร อยู่ที่ไหน

(3) ผู้โพสต์ ลงทะเบียนสมัครสมาชิก ในนามของใคร ระบุบัตรประจำตัวประชาชนหมายเลขอะไร พักอาศัยอยู่ที่ไหน หมายเลขโทรศัพท์อะไร ใช้อีเมล์ในการติดต่อว่าอะไร โพสต์จากหมายเลข IP และวันเดือน ปี เวลา อะไร

5. สอบสวนผู้ให้บริการโทรศัพท์ ในประเด็น

(1) โทรศัพท์ (ระบุหมายเลขที่ผู้ขายสินค้าใช้ติดต่อ) ลงทะเบียนใช้ในนามของใคร อยู่ที่ไหน บัตรประจำตัวประชาชนเลขที่อะไร

(2) มีรายการติดต่อระหว่างโทรศัพท์ (ระบุหมายเลขโทรศัพท์ผู้ซื้อและผู้ขาย) หรือไม่ติดต่อกันกี่ครั้ง เมื่อวันเดือนปีและเวลาอะไร

6. สอบสวนเจ้าของบัญชีธนาคารที่รับโอนเงิน กรณียังไม่มีหลักฐานว่าผู้ใดเป็นผู้กระทำความผิดในประเด็น

(1) บัญชีธนาคารที่รับโอนเงิน เป็นบัญชีประเภทใด หมายเลขบัญชีอะไร ที่ธนาคารใด สาขาอะไร เปิดบัญชีเมื่อใด (พร้อมเอกสารประกอบ)

(2) การเปิดบัญชีดังกล่าวเพื่อวัตถุประสงค์ใด

(3) ได้ทำเรื่องขอใช้บัตรเอทีเอ็ม หรือไม่ บัตรเอทีเอ็มอยู่กับเจ้าของบัญชีหรือส่งมอบให้กับใครไป เมื่อใด กรณีส่งมอบให้กับบุคคลอื่นที่ไม่ใช่เจ้าของบัญชี สาเหตุใดจึงมอบบัตรเอทีเอ็มพร้อมรหัสให้กับบุคคลดังกล่าว

(4) มีเงินค่าสินค้า (ระบุจำนวนเงิน) โอนเข้าบัญชีดังกล่าว หรือไม่ เมื่อวัน เดือน ปี และเวลาใด

(5) ใครเป็นผู้เบิกถอนเงินจำนวนดังกล่าว เบิกถอนที่ไหน เมื่อใดและเบิกถอนเงินด้วยวิธีการอย่างไร

(6) กรณีที่มีภาพหรือหลักฐานว่าผู้ที่มาเบิกถอนเงินไม่ใช่เจ้าของบัญชีธนาคารให้สอบสวนเจ้าของบัญชีด้วยว่ารู้จักบัคคลดังกล่าวหรือไม่ เป็นใคร และมีความเกี่ยวข้องอย่างไร

7. ผู้ต้องสงสัย

(1) ซอฟแวร์ที่ใช้งานมีอะไรบ้าง เก็บไว้ที่ไหนและอยู่ในสื่อบันทึกรูปแบบใด

(2) เครื่องคอมพิวเตอร์มีซอฟแวร์ หรือโปรแกรมสำหรับตรวจสอบรายงานทางการเงิน หรือ มีเอกสารทางการเงินใดๆ หรือไม่อย่างไร

(3) เครื่องคอมพิวเตอร์มีโปรแกรมสำหรับสำหรับตกแต่งรูปภาพหรือไม่ ถ้ามี ใช้โปรแกรมอะไร

(4) มีสำเนาข้อมูลบัตรต่างๆ เก็บไว้ในเครื่องคอมพิวเตอร์หรือไม่ เพราะเหตุใด

(5) คอมพิวเตอร์ถูกใช้ในการทำธุรกรรมซื้อขายแบบออนไลน์หรือไม่ อย่างไร

ข) ประเด็นคำถามในคดีล่วงละเมิดต่อเด็ก

การสอบสวนผู้เสียหายในประเด็น

(1) ผู้เสียหายเคยพูดเคยแบบออนไลน์ผ่านทางห้องสนทนาใดบ้าง ใช้อีเมล์และรหัสผู้ใช้อะไร

(2) ผู้เสียหายใช้อินเทอร์เน็ต อีเมล์ หรือ พูดคุย จากเครื่องคอมพิวเตอร์อื่นบ้างหรือไม่ ถ้ามีใช้จากที่ไหน

(3) ผู้เสียหายให้ข้อมูลส่วนบุคคลส่วนบุคคล อันได้แก่ ชื่อและนามสกุลจริง อายุ ที่อยู่ กับผู้อื่นที่ติดต่อผ่านทางอินเทอร์เน็ตหรือไม่ อย่างไร

(4) มีใครบ้างที่ถูกบันทึกอยู่ในรายการสำหรับผู้เสียหายติดต่อด้วยผ่านทางอินเทอร์เน็ต

(5) ผู้เสียหายเคยบันทึกประวัติการสนทนาเก็บไว้หรือไม่ อย่างไร

(6) ผู้เสียหายใช้โปรแกรมอะไรตรวจสอบอีเมล์

(7) ข้อความหรือรูปภาพอะไร ที่ระบุได้ว่าเป็นการพยายามหรือเป็นการล่วงละเมิดทางเพศกับผู้เสียหาย

(8) ผู้เสียหายเคยได้รับรูปภาพหรือสิ่งของใดๆ จากผู้ต้องสงสัยบ้างหรือไม่ อย่างไร

การสอบสวนผู้ต้องสงสัยในประเด็น

(1) เครื่องคอมพิวเตอร์ทั้งหมดของผู้ต้องสงสัยอยู่ที่ใดบ้าง

(2) ผู้ต้องสงสัยมีแหล่งเก็บข้อมูลออนไลน์ที่สามารถเข้าถึงขณะเชื่อมต่ออินเทอร์เน็ตหรือไม่ อย่างไร

(3) ผู้ต้องสงสัยใช้รหัสผู้ใช้ว่าอะไร และใช้ห้องสนทนาชื่อว่าอะไร สามารถเข้าถึงได้อย่างไร

(4) ผู้ต้องสงสัยติดต่อผ่านทางอินเทอร์เน็ตกับใครบ้าง และติดต่อด้วยวิธีการใด

(5) ผู้ต้องสงสัยเคยเผยแพร่(ดู)รูปภาพลามก(ของเด็ก)โดยใช้เครื่องคอมพิวเตอร์หรือไม่ ถ้าเคยเผยแพร่(เก็บ)ไว้ที่ใด หรือส่งไปให้ใคร

(6) ผู้ต้องสงสัยรู้หรือไม่ว่า การกระทำดังกล่าวผิดกฎหมาย(ระบุชื่อกฎหมาย)

ค) ประเด็นคำถามในคดีบุกรุก/ทำให้ระบบคอมพิวเตอร์เสียหาย

(1) ถาม - มาพบพนักสอบสวนด้วยสาเหตุใด มีความประสงค์อย่างไร

(2) ถาม - รับทราบเหตุจากผู้ใด เมื่อใด

(3) ถาม - พฤติการณ์ทางคดีเป็นอย่างไร

(4) ถาม - ระบบได้รับความเสียหายอย่างไร

(5) ถาม - ได้มีการดำเนินการแก้ไข หรือกู้ข้อมูล สำรองข้อมูล หรือไม่ อย่างไร

(6) ถาม - ใครเป็นผู้ดูแลระบบ และระบบมีรหัสผ่านการเข้าถึงระบบหรือไม่

(7) ถาม - ผู้ใดบ้างที่สามารถเข้าถึงระบบได้

(8) ถาม - ท่านได้มอบเอกสารใดให้พนักงานสอบสวนไว้เป็นหลักฐานประกอบคดีบ้าง

(9) ถาม - เคยมีสาเหตุโกรธเคืองกับผู้ใดในคดีนี้มาก่อนหรือไม่

กรณีเป็นเครือข่ายภายในบ้านพักอาศัย

(1) ท่านสามารถระบุสายทั้งหมดที่ถูกเชื่อมต่อในระบบเครือข่ายกับคอมพิวเตอร์หรือไม่อย่างไร

(2) มีการกำหนดให้เครื่องคอมพิวเตอร์ใช้กับรหัสผู้ใช้งานที่เฉพาะเจาะจงหรือไม่ อย่างไร

(3) ระบบเครือข่ายมีการเชื่อมต่อเข้ากับระบบอินเทอร์เน็ตหรือไม่ อย่างไร

(4) อุปกรณ์ที่ใช้เชื่อมต่ออินเทอร์เน็ตอยู่ที่ใด กำลังเชื่อมต่ออยู่หรือไม่

(5) ใช้บริการอินเทอร์เน็ตของผู้ให้บริการ (ISP-Internet Service Provider) รายใด

(6) เครื่องคอมพิวเตอร์สามารถใช้งานอินเทอร์เน็ตพร้อม ๆ กันได้หรือไม่

(7) มีการใช้เครือข่ายไร้สายหรือไม่ อย่างไร

กรณีเป็นเครือข่ายในธุรกิจ

(1) ใครเป็นคนแรกที่พบเห็นสิ่งผิดปกติที่เกิดขึ้น

(2) บันทึกรายละเอียดสิ่งผิดปกติต่าง ๆ ที่พยานแต่ละคนพบเห็น

(3) ใครคือผู้ดูแลระบบเครือข่าย บันทึกรายละเอียดการติดต่อ

(4) สงสัยพนักงานหรืออดีตพนักงานคนใดบ้างหรือไม่ เพราะเหตุใด

(5) มีแผนผังการเชื่อมต่อของระบบเครือข่ายหรือไม่

(6) มีการเก็บบันทึกข้อมูลประวัติการใช้งานต่าง ๆ เพื่อใช้ในการตรวจสอบย้อนหลังหรือไม่

(7) ท่านสามารถเก็บข้อมูลประวัติการใช้งานแยกออกมา เพื่อใช้สำหรับการสืบสวนได้หรือไม่

(8) มีการติดต่อในเรื่องนี้กับเจ้าหน้าที่ของหน่วยงานอื่นบ้างหรือไม่ อย่างไร

ง) ประเด็นคำถามในคดี Email Scamming

(1) ถาม - ผู้เสียหายมาพบพนักงานสอบสวนด้วยสาเหตุใด มีความประสงค์อย่างไร

ตอบ - ข้าฯ ได้รับมอบอำนาจจาก บริษัท.... ให้มาร้องทุกข์กล่าวโทษต่อพนักงานสอบสวน กรณีคนร้ายได้ส่งข้อความหลอกลวงทางจดหมายอิเล็กทรอนิกส์ (Email) ให้โอนเงิน เป็นเหตุให้บริษัท.... ได้รับความสียหาย จำนวน.... บาท จึงมามอบคดีให้พนักงานสอบสวนให้สืบสวนสอบสวนดำเนินคดีกับคนร้ายจนกว่าคดีจะถึงที่สุด

(2) ถาม - บริษัท.... ประกอบกิจการเกี่ยวกับอะไร

(3) ถาม - บริษัท.... ติดต่อธุรกิจกับลูกค้าด้วยวิธีการใด

ตอบ - ติดต่อด้วยวิธีการส่งข้อความทางจดหมายอิเล็กทรอนิกส์ (Email)

(4) ถาม - บริษัท.... ใช้อีเมล์ใดในการติดต่อส่งข้อความทางจดหมายอิเล็กทรอนิกส์ (Email) กับลูกค้า

(5) ถาม - การชำระค่าสินค้าที่ตกลงซื้อขายกัน มีวิธีการชำระอย่างไร

(6) ถาม - อีเมล์ที่แท้จริงของลูกค้าที่ใช้ติดต่อธุรกิจคืออีเมล์ใด

(7) ถาม - คนร้ายใช้อีเมล์ใดในการหลอกลวงส่งข้อความทางจดหมายอิเล็กทรอนิกส์ (Email) ติดต่อกับบริษัท....

(8) ถาม - ข้อความทางจดหมายอิเล็กทรอนิกส์ (Email) ของคนร้าย มีรายละเอียดของข้อความว่าอย่างไร

(9) ถาม - ข้อความทางจดหมายอิเล็กทรอนิกส์ (Email) ของคนร้าย หลอกลวงให้โอนเงินไปยังที่ใด

(10) ถาม - บริษัท.... ได้รับความเสียหายในคดีเป็นจำนวนเท่าใด

(11) ถาม - พฤติการณ์ในคดีนี้เป็นอย่างไร

(12) ถาม - คดีนี้เหตุเกิดที่ไหน เมื่อใด

(13) ถาม - ท่านได้มอบเอกสารใดให้พนักงานสอบสวนไว้เป็นหลักฐานประกอบคดีบ้าง

(14) ถาม - เคยมีสาเหตุโกรธเคืองกับผู้ใดในคดีนี้มาก่อนหรือไม่

จ) ประเด็นคำถามในคดี Hack Facebook

การสืบสวน สอบสวนคดีเฟสบุ๊ค อันดับแรกต้องดูว่าเฟสบุ๊คนั้นเป็นเฟสบุ๊คของจริงหรือของปลอม โดยดูจากเพื่อนที่รู้จักในชีวิตจริง ๆ ของเฟสบุ๊คนั้นว่ามีการปฏิสัมพันธ์ เช่น กดไลค์ คอมเม้นต์แล้วเจ้าของเฟสบุ๊คตอบคอมเม้นต์ แท็กรูป หรือไม่ เพราะจุดประสงค์ของเฟสบุ๊คสร้างขึ้นมาเพื่อให้คนที่รู้จักกันในชีวิตจริงได้ไปเห็นกันอีกครั้งบนหน้าจอและมีปฏิสัมพันธ์กัน ดังนั้น หากเฟสบุ๊คนั้นเป็นของจริง จะมีเพื่อนที่เขารู้จักในชีวิตจริง ๆ มาปฏิสัมพันธ์ด้วย

แต่หากเฟส์บุ๊คนั้นไม่ยืนยันตัว ลงรูปภูเขา ดอกไม้ หรือเป็นรูปคน แต่ไม่มีการปฏิสัมพันธ์ ไลค์ เม้นต์ เกิดขึ้นเลย ไม่มีเพื่อนที่น่าจะรู้จักในชีวิตจริง ๆ มาปฏิสัมพันธ์ด้วย เฟสบุ๊คนั้นก็น่าจะเป็นของปลอม

ดังนั้น เมื่อวิเคราะห์ว่าเป็นเฟสบุ๊คของจริงหรือของปลอมแล้ว หากเชื่อว่าเป็นของจริง พนักงานสอบสวนอาจออกหมายเรียกเจ้าของเฟสบุ๊คมาในฐานะพยานหรือผู้ต้องหา แล้วแต่กรณี หรือมีพยานหลักฐานอื่น เช่น ผู้เสียหายยืนยันว่ารู้จักกับผู้ต้องหานี้ในชีวิตจริง ๆ และเป็นเพื่อนกันในเฟสบุ๊คด้วย เจ้าของเฟสบุ๊คกับบุคคลที่ถอนเงินออกจากธนาคารเป็นคนเดียวกัน เป็นต้น ส่วนเจ้าหน้าที่ฝ่ายสืบสวน ไม่ออกหมายเรียกมา แต่ใช้วิธีการพิสูจน์ทราบว่าเจ้าของเฟสบุ๊คนี้เป็นใคร ชื่อนามสกุล ที่อยู่ เพื่อนสนิท พ่อแม่ ลูกเมีย ญาติพี่น้องอยู่ที่ไหน นำไปสู่การสืบสวนบนพื้นดิน สะกดรอย ปลอมตัว ถ่ายรูปหน้าบ้าน ออกหมายค้นเป้าหมาย เพื่อตรวจยึดอุปกรณ์อเล็กทรอนิกส์ คอมพิวเตอร์ สมาร์ทโฟน ไปตรวจพิสูจน์ เป็นต้น เมื่อวิเคราะห์แล้ว น่าจะเป็นเฟสบุ๊คของจริง พนักงานสอบสวนใช้การออกหมายเรียก เจ้าหน้าที่สืบสวนใช้การลงพื้นที่ตรวจสอบและออกหมายค้น แต่หากทำหนังสือไปสอบถามหน่วยงานสนับสนุนทางเทคโนโลยี จะตรวจสอบที่ตั้งเว็บไซต์นั้น จาก Whois Domaintool และตอบกลับมาว่าที่ตั้งของเว็บไซต์ เฟสบุ๊ค ไลน์ นั้นอยู่ต่างประเทศ (ความจริงก็อยู่ต่างประเทศ) ไม่ได้อยู่ภายใต้กฎหมายไทย จึงไม่สามารถทราบข้อมูลผู้ใช้เฟสบุ๊คนี้ได้ ถึงแม้ว่าจะทำหนังสือสอบถามไปก็ไม่ได้รับความร่วมมือตอบกลับมา เว้นแต่จะติดต่อช่องทางที่เขาจัดไว้ให้ เช่น ถ้าอยากขอข้อมูลหมายเลข IP Address ของผู้ใช้เฟสบุ๊คนี้ เข้าช่องทาง URL www.fackbook.com/records โดยใช้อีเมล์ Police.go.th ติดต่อไป โดยใช้ภาษาอังกฤษในการติดต่อ และความผิดที่จะขอข้อมูลไปนั้น ต้องเป็นความผิดตามกฎหมายของประเทศนั้นๆ ด้วย เช่น การก่อการร้าย ฉ้อโกง ลามกอนาจารเด็ก เป็นต้น

ประเด็นคำถาม

(1) ถาม - สมัครสมาชิก Fb ใช้ Email Address ใด

(2) ถาม - สมัครสมาชิก Fb มานานเท่าใด ใช้ชื่อบัญชี Fb ใด

(3) ถาม - ปกติเข้าใช้งาน Fb จากอะไร (สมาร์ทโฟน โน๊ตบุ๊ค PC)

(4) ถาม - นอกจากท่านแล้วมีผู้ใดรู้รหัสผ่านการเข้าใช้งาน Fb บ้าง

(5) ถาม - ท่านได้รับความเสียหายอย่างไร

(6) ถาม - ท่านได้รับทราบเหตุจากผู้ใด เมื่อใด

(7) ถาม - พฤติการณ์ในคดีนี้เป็นอย่างไร

(8) ถาม - ท่านได้มอบเอกสารใดให้พนักงานสอบสวนไว้เป็นหลักฐานประกอบคดีบ้าง

(9) ถาม - เคยมีสาเหตุโกรธเคืองกับผู้ใดในคดีนี้มาก่อนหรือไม่

ฉ) ประเด็นคำถามในคดี Romance Scam

(1) สอบถามรายละเอียดพฤติการณ์ในคดีว่ามีพฤติการณ์อย่างไร เข้าข่ายหรือไม่

(2) ผู้เสียหายได้พูดคุยกับคนร้ายผ่านทางช่องทางใด หากเป็นเว็บไซต์เฟสบุ๊ค ควรถามด้วยว่าเฟสบุ๊คดังกล่าวมี URL ว่าอะไร ผู้เสียหายรู้จักบุคคลในภาพหรือไม่ อย่างไร เคยพบเจอหรือพูดคุยติดต่อกันทางใดบ้าง ทั้งทางโลกออนไลน์และสถานที่จริง

(3) ผู้เสียหายได้ทำการโอนเงินจากธนาคารใดไปยังธนาคารใด เมื่อวันเวลาใด และจำนวนเท่าใด

(4) กลุ่มผู้ร่วมขบวนการติดต่อกับผู้เสียหายผ่านทางใดบ้าง ทั้งหมายเลขโทรศัพท์ ที่อยู่ สถานที่นัดพบ ฯลฯ

(5) ผู้เสียหายสงสัยผู้ใดในคดีนี้หรือไม่ อย่างไร

(6) ท่านได้มอบเอกสารใดให้พนักงานสอบสวนไว้เป็นหลักฐานประกอบคดีบ้าง

3) การสอบสวนผู้ต้องหา ให้พนักงานสอบสวนแจ้งให้ทราบถึงข้อเท็จจริงเกี่ยวกับการกระทำที่กล่าวหาว่าผู้ต้องหาได้กระทำผิดแล้วจึงแจ้งข้อหาให้ทราบ และสอบสวนในประเด็น (โดยให้ประยุกต์ใช้ตามความเหมาะสม)

3.1) กรณีผู้ต้องหาที่เป็นผู้โพสต์ข้อความ

(1) ถาม - ท่านจะให้การในเรื่องที่ต้องหาว่าอย่างไร

(2) ถาม - โพสต์ข้อความประกาศขายสินค้าอะไร ราคาเท่าใด ทางเว็บไซต์ใด ใช้อีเมล์อะไร เมื่อวันและเวลาใด

(3) ถาม - การโพสต์ข้อความดังกล่าวเป็นเจตนาของผู้ต้องหา หรือบุคคลใดมอบหมายให้เป็นผู้โพสต์ มีหลักฐานหรือไม่ อย่างไร

(4) ถาม - ท่านติดต่อกับผู้ซื้อสินค้าช่องทางใดบ้าง เช่น โทรศัพท์ โทรสาร SMS หรือช่องทางอื่นใดบ้าง

(5) ถาม - ท่านได้เชื่อมต่ออินเตอร์เน็ตเพื่อโพสต์ข้อความจากผู้ให้บริการอินเตอร์เน็ตรายใด และเชื่อมต่อจากหมายเลขโทรศัพท์ใด จากที่ใด

(6) ถาม - ท่านใช้คอมพิวเตอร์เชื่อมต่อจากเครื่องคอมพิวเตอร์เครื่องใด ของใคร

3.2) กรณีผู้ต้องหาเป็นเจ้าของบัญชีที่รับโอนเงิน

(1) ถาม - บัญชีที่รับโอนเงินเป็นบัญชีเงินฝากของผู้ต้องหาใช่หรือไม่ เปิดตั้งแต่เมื่อใด การเปิดบัญชีธนาคารที่รับโอนเงิน เป็นความประสงค์ของผู้ต้องหาเอง หรือบุคคลใดเป็นผู้ใช้ให้เปิดบัญชี มีรายละเอียดอย่างไร (ใครใช้, เมื่อใด, ได้รับค่าจ้างหรือไม่จำนวนเท่าใด, มอบบัตรเอทีเอ็มพร้อมรหัสให้ใคร มอบที่ไหน เมื่อใด)

(2) ถาม - ใครเป็นผู้โอนเงินบัญชีธนาคารที่รับโอนเงินดังกล่าวเกิดจากมูลหนี้อะไร มีหลักฐานหรือไม่

(3) ถาม - ใครเป็นผู้ถอนเงินเข้าบัญชีธนาคารที่รับโอน ถอนที่ไหน เมื่อใด จำนวนเงินเท่าใด ถอนด้วยวิธีการใด หากตรวจสอบพบว่าผู้ต้องหานั้นเป็นผู้รับจ้างเปิดบัญชีเงินฝาก ให้พนักงานสอบสวนพิจารณาแจ้งข้อกล่าวหาในความผิดเกี่ยวกับการฟอกเงิน ตามนัยมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 9 แห่ง พ.ร.บ.ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 แล้วแต่กรณี แก่ผู้ที่มีพฤติการณ์รับจ้างเปิดบัญชีในสถาบันการเงิน เพื่อรับโอนเงินที่ได้มาจากการทำความผิดฐานฉ้อโกงประชาชน อันเป็นความผิดมูลฐานตามพระราชบัญญัติดังกล่าว

3.3) กรณีผู้ต้องหาเป็นผู้ถอนเงินทางตู้เอทีเอ็ม

(1) ถาม - ถอนเงินจากตู้เอทีเอ็มจากบัญชีธนาคารที่รับโอน จากตู้เอทีเอ็มของธนาคารอะไร ตั้งอยู่ที่ไหน ถอนเมื่อวันที่และเวลาอะไร เงินที่ถอนในแต่ละครั้งจำนวนเท่าใด

(2) ถาม - บัตรเอทีเอ็มพร้อมรหัส เป็นของใคร และได้รับมาจากบุคคลใด ที่ไหน เมื่อใด

(3) ถาม - เงินที่ถอนมาได้ นำไปมอบให้ใคร ด้วยวิธีการอย่างไร (เช่น มอบให้บุคคลอื่นไป, โอนเงินไปบัญชีอื่น, นำเงินที่ถอนฝากเข้าเครื่องรับฝากเงินอัตโนมัติเพื่อโอนไปบัญชีอื่น หรือโอนไปบัญชีที่เปิดไว้ในต่างประเทศ, หรือวิธีการอื่นใด เป็นต้น)

(4) ถาม - มีการทำธุรกรรมรับ/โอนเงิน ทางอินเทอร์เน็ต บ้างหรือไม่ (ถ้ามีให้ระบุรายละเอียดตามรูปคดี)

4) การค้นและตรวจยึดอุปกรณ์เครื่องมือเกี่ยวกับคอมพิวเตอร์

ข้อแนะนำในการเข้าตรวจค้นและยึดพยานหลักฐานอิเล็กทรอนิกส์ในเบื้องต้นควรให้ผู้ชำนาญการเป็นผู้ดำเนินการ หากไม่มีผู้ชำนาญการให้ดำเนินการ ดังนี้

4.1) คำนึกถึงความปลอดภัยของเจ้าหน้าที่เป็นอันดับแรก

4.2) จัดทำแผนที่ห้อง หรือสถานที่ที่ทำการตรวจค้นเช่นเดียวกับคดีทั่วไป

4.3) สวมถุงมือขณะตรวจค้นและยึดเพื่อป้องกันการปนเปื้อนของพยานหลักฐาน

4.4) วางป้ายระบุลำดับที่ของจุดต่าง ๆ พร้อมถ่ายภาพไว้ในทุกขั้นตอน

4.5) กันผู้ต้องสงสัยออกจากเครื่องคอมพิวเตอร์

4.6) ตรวจสอบสถานะของเครื่องคอมพิวเตอร์ว่าเปิดอยู่หรือปิดอยู่ ถ้าเครื่องคอมพิวเตอร์ปิดอยู่ ให้ข้ามไปที่ข้อ 4.7) ถ้าไม่มั่นใจให้พิจารณา ดังนี้

(1) ตรวจจอภาพว่าพักหน้าจอ (โดยการขยับเมาส์) หรือ ปิดหน้าจออยู่ (โดยการกดปุ่มเปิด/ปิดที่หน้าจอ)

(2) ถ่ายภาพที่ปรากฏบนหน้าจอคอมพิวเตอร์ กรณีที่มีหน้าต่างซ้อนกันหลาย ๆ หน้าต่าง ให้คลิ๊กเลือกทีละหน้าต่าง และถ่ายภาพเก็บเป็นหลักฐานเอาไว้

(3) หากมีเอกสารที่ยังไม่ได้บันทึก ให้กดปุ่มบันทึก

(4) ในกรณีที่ไม่เข้าเงื่อนไขตามที่กล่าวมาแล้ว เช่น มีไฟล์กำลังถูกลบ, ติดรหัสผ่าน ฯลฯ ก็ให้ดึงปลั๊กออกจากหลังเครื่องคอมพิวเตอร์ ถ้าเป็นเครื่องคอมพิวเตอร์แบบพกพาให้ถอดแบตเตอรี่ก่อน ยกเว้นในกรณีที่เป็นเครื่องคอมพิวเตอร์แบบแม่ข่ายรันระบบปฏิบัติการ Windows Server รุ่นต่าง ๆ, ระบบ Unix ให้ใช้วิธีการ Shutdown แทนการดึงปลั๊กออกจากหลังเครื่อง (ปิดเครื่องคอมพิวเตอร์ด้วยวิธีปกติ ผลดีจะทำให้ข้อมูลไม่เสียหาย, การดึงปลั๊กออกขณะเครื่องคอมพิวเตอร์เปิดใช้งานอยู่ อาจทำให้ข้อมูลคอมพิวเตอร์หรือฮาร์ดดิสก์เสียหาย แต่มีผลดีคือทำให้ได้ข้อมูลทุกอย่างก่อนที่จะดึงปลั๊กออก)

4.7) ติดป้ายกำกับเป็นคู่ไว้บริเวณจุดเชื่อมต่อของเครื่องคอมพิวเตอร์ กับ สายที่เชื่อมต่อ

4.8) การถ่ายภาพควรถ่ายให้เห็นภาพรวม จุดเชื่อมต่อ และรายละเอียดของอุปกรณ์ที่ยึดทั้งหมด โดยเฉพาะหมายเลขประจำเครื่อง จากนั้น ดำเนินการบรรจุเครื่องคอมพิวเตอร์ที่ต้องการยึดลงในกล่องถุงพลาสติก แล้วปิดผนึกด้วยเทปกาว พร้อมลงลายมือชื่อกำกับไว้

4.9) บันทึกรายละเอียดของเครื่องคอมพิวเตอร์ที่ยึด ลงลายมือชื่อผู้ยึด พร้อมระบุวันเดือนปีและเวลาที่ยึด เมื่อมีการส่งมอบพยานหลักฐานทางอิเล็กทรอนิกส์ ให้จดบันทึกเหตุผลในการส่งมอบพร้อมลงลายมือชื่อผู้รับ และ ผู้ส่งมอบ พร้อมระบุวัน เวลา ให้ชัดเจน เพื่อเป็นการรักษาห่วงโซ่ของพยานหลักฐานให้มีความน่าเชื่อถือตลอดเวลา

4.10) ห่อเครื่องอย่างระมัดระวังหลังจากที่บันทึกรอยนิ้วมือแล้ว และทำการบรรจุหรือหีบห่อในวัสดุกันกระแทกตามหลักการเก็บวัตถุพยานของกองพิสูจน์หลักฐาน

4.11) การเคลื่อนย้ายพยานหลักฐานทางอิเล็กทรอนิกส์ ควรหลีกเลี่ยงสัญญาณวิทยุกำลังสูงภายในรถยนต์สายตรวจ สนามแม่เหล็ก โดยระวังเรื่องการกระแทก ความเปียกชื้น และความร้อนเพราะอาจทำให้พยานหลักฐานทางอิเล็กทรอนิกส์เกิดความเสียหายได้

4.12) เก็บเครื่องมือเกี่ยวกับคอมพิวเตอร์ไว้ในพื้นที่ปลอดภัย/ ไม่ควรทำรายการใด ๆ กับเครื่องคอมพิวเตอร์หลังจากตรวจยึด

4.13) เอกสารทั้งหมดต้องอยู่สถานะต้นฉบับ

4.14) หากมีกรณีที่จะต้องตรวจสอบลายนิ้วมือ ให้เก็บรอยนิ้วมือที่คีย์บอร์ด เมาส์ จอ และซีดีรอม อื่น ๆ

5) การส่งอุปกรณ์เครื่องมือเกี่ยวกับคอมพิวเตอร์/คอมพิวเตอร์ตรวจพิสูจน์

5.1) คอมพิวเตอร์ส่วนบุคคล

(1) ถ่ายภาพให้ได้อุปกรณ์ของกลางครบทุกชิ้น ใส่หมายเลขอ้างอิงให้ครบถ้วน

(2) ถอดสายไฟฟ้า สายต่อต่าง ๆ ออกให้หมดแล้วจึงบรรจุลงกล่องกระดาษหรือถุงกระดาษให้เรียบร้อยควรลงหมายเลขช่องต่อต่าง ๆ ไว้ด้วย และทำหมายเลขระบุตำแหน่งของสายที่ปลดออก เพื่อป้องกันความสับสนในการนำมาประกอบคืน

(3) ตรวจสอบในช่องใส่แผ่น CD, Floppy disk หรือ Card read หรือช่อง USB Memory ค้างอยู่หรือไม่

(4) ตัว CPU ที่มีช่องเสียบอุปกรณ์ต่าง ๆ ควรปิดผนึกด้วยกระดาษกาวแล้วบรรจุในกล่องกระดาษหรือกล่องที่เหมาะสม

(5) ลงบันทึกรายละเอียดต่าง ๆ ให้ชัดเจนมากที่สุดก่อนนำส่งเพื่อตรวจพิสูจน์และควรลงลายมือชื่อผู้นำส่งหีบห่อ

5.2) คอมพิวเตอร์โน้ตบุ๊ก/ฮาร์ดดิสก์

(1) กรณีที่เป็นฮาร์ดดิสก์ ถ่ายภาพ SN และบรรจุใส่กล่องกระดาษ หรือห่อกระดาษปิดผนึกให้เรียบร้อย บันทึกรายละเอียดต่าง ๆ เช่น ยี่ห้อ, ความจุ และ SN แล้วจึงนำส่งตรวจพิสูจน์และควรลงลายมือชื่อผู้นำส่งที่หีบห่อ

(2) กรณีที่เป็นเครื่องคอมพิวเตอร์โน้ตบุ๊ก

- หากเครื่องคอมพิวเตอร์โน้ตบุ๊กอยู่ในสภาพ “ปิดทำงาน” ให้ปล่อยทิ้งไว้อย่างนั้น ห้ามเปิดให้เครื่องคอมพิวเตอร์โน้ตบุ๊กทำงาน หากเครื่องคอมพิวเตอร์โน้ตบุ๊กอยู่ในสภาพ “เปิดทำงาน” ให้ถ่ายภาพสิ่งที่ปรากฏหน้าจอหากโปรแกรมรักษาหน้าจอเปิดทำงานอยู่ให้เคลื่อนย้ายเมาส์หรือกดแป้นพิมพ์
- ถอดแบตเตอรี่ออกจากเครื่องคอมพิวเตอร์โน้ตบุ๊ก
- ถอดปลั๊กของเครื่องคอมพิวเตอร์โน้ตบุ๊กออกจากด้านหลังของตัวเครื่องหากเสียบปลั๊กไว้
- บรรจุและเก็บแบตเตอรี่ของเครื่องคอมพิวเตอร์โน้ตบุ๊ก พร้อมทั้งสายที่ใช้ชาร์จไฟไว้ในถุงเสมอ

5.3) โทรศัพท์มือถือ

(1) ถ่ายภาพและบรรจุใส่กล่องกระดาษหรือห่อกระดาษปิดผนึกลงลายมือชื่อ แล้วนำส่งตรวจพิสูจน์ ถ้าเป็นไปได้ให้แยก 1 ถุงต่อ 1 เครื่อง ให้นำส่งอุปกรณ์สายต่อชาร์จแบตเตอรี่หรือสายเชื่อมต่อข้อมูล (Data link cable) มาด้วย (ถ้ามี)

(2) หากโทรศัพท์มือถืออยู่ในสภาพ “ปิดทำงาน” ให้ปล่อยไว้ในสภาพ “ปิดทำงาน”

(3) หากโทรศัพท์มือถืออยู่ในสภาพ “เปิดทำงาน”

- ปล่อยโทรศัพท์ไว้ในสภาพ “เปิดทำงาน” และบรรจุไว้ในถุงกันคลื่นแม่เหล็กไฟฟ้า หรือ
- หากไม่มีถุงกันคลื่นแม่เหล็กไฟฟ้า ให้ “เปิดโหมดเครื่องบิน” และ “ปิด” โทรศัพท์

(4) ในกรณีที่ปล่อยโทรศัพท์ไว้ในสภาพ “เปิดทำงาน” และบรรจุไว้ในถุงกันคลื่นแม่เหล็กไฟฟ้า ควรจัดส่งไปตรวจพิสูจน์หลักฐานในวันเดียวกันหรือโดยเร็วที่สุด

(5) หากโทรศัพท์มือถือมีการเข้ารหัสป้องกันการเปิดไว้ ให้สอบถามรหัสและแนบรหัสดังกล่าวนี้เมื่อส่งตรวจพิสูจน์หลักฐาน

5.4) แผ่นซีดี/บัตรอิเล็กทรอนิกส์

ถ่ายภาพด้านหน้า/ หลังของบัตรและถ้าเป็นแผ่นซีดี หากของกลางมีมากกว่า 1 รายการ ควรระบุลำดับหรือข้อความที่เขียนอยู่บนแผ่นเพื่อใช้อ้างอิงกับรายละเอียดในหนังสือนำส่ง ควรจะบรรจุในซองบรรจุแผ่นซีดีหรือซองกระดาษ เช่นเดียวกับบัตรอิเล็กทรอนิกส์ ปิดหีบห่อให้เรียบร้อย ลงลายมือชื่อผู้นำส่งก่อนนำส่งตรวจพิสูจน์

5.5) อุปกรณ์ไฟฟ้า/ อิเล็กทรอนิกส์ที่เกี่ยวข้อง

ถ่ายภาพ บรรจุกล่องกระดาษ/ซองกระดาษ แยกรายการให้ชัดเจน ปิดผนึกให้เรียบร้อย ลงลายมือชื่อ นำส่งตรวจพิสูจน์ในทุกกรณี ถ้าเป็นไปได้ควรหลีกเลี่ยง กล่องพลาสติก/ ถุงพลาสติกต่าง ๆ เพื่อป้องกันไฟฟ้าสถิต

5.6) คอมพิวเตอร์ในเครือข่าย

(1) ให้ปรึกษาผู้ชำนาญจากกองพิสูจน์หลักฐานกลาง หรือ ศูนย์พิสูจน์หลักฐาน 7 หรือ 10 แล้วแต่กรณี และแยกผู้ต้องสงสัยออกจากคอมพิวเตอร์ในทันที และมีข้อที่พึงระมัดระวังคือผู้ต้องสงสัยสามารถเข้าใช้งานคอมพิวเตอร์ในเครือข่ายจากระยะไกลได้และสามารถทำเช่นนั้นได้โดยอาศัยอุปกรณ์จำพวก PDA หรือโทรศัพท์มือถือ

(2) อย่าตัดไฟจากแหล่งจ่ายไฟ หรือกระทำการอื่นใด เพราะการกระทำเช่นนั้น อาจทำให้ระบบได้รับความเสียหายสูญเสียข้อมูลและอาจทำให้สำนักงานตำรวจแห่งชาติต้องรับผิดชอบต่อความเสียหาย

5.7) สิ่งบันทึกอื่น ๆ ที่ไม่ได้เชื่อมต่อกับเครื่องพิวเตอร์

สิ่งที่บันทึกอื่น ๆ เช่น แผ่น DVD, CD และ Floppy disk สามารถบรรจุอยู่ด้วยกันในถุงเก็บพยานหลักฐานเดียวกันได้ ส่วนอุปกรณ์ USB เช่น Thumb drive ควรบรรจุอยู่ในถุงกระดาษ

3.3 การตั้งประเด็นคำถามในการส่งตรวจพิสูจน์

1) ตัวอย่างการตั้งประเด็นคำถามการตรวจพิสูจน์

1.1) การตั้งคำถามของกลางประเภท คอมพิวเตอร์

(1) มีแฟ้มข้อมูลตามเอกสาร, ภาพถ่ายของกลางรายการที่...(ตามที่ส่งมาตรวจ) บันทึกอยู่ในคอมพิวเตอร์ของกลางหรือไม่

(2) มีแฟ้มข้อมูลภาพยนตร์ตามแผ่นดีวีดีของกลาง (เจ้าของลิขสิทธิ์) รายการที่...บันทึกอยู่ในคอมพิวเตอร์ของกลางหรือไม่

1.2) การตั้งคำถามของกลางประเภท โทรศัพท์เคลื่อนที่

(1) มีแฟ้มข้อมูลภาพยนตร์, แฟ้มข้อมูลภาพ บันทึกอยู่ในโทรศัพท์เคลื่อนที่ของกลางหรือไม่

(2) มีข้อมูลประวัติการโทรศัพท์หรือบัญชีรายชื่อผู้ติดต่อ บันทึกอยู่ในโทรศัพท์เคลื่อนที่ของกลางหรือไม่

(3) มีข้อมูลการสนทนาผ่านโปรแกรม WeChat, Facebook Messenger, Line บันทึกอยู่ในโทรศัพท์เคลื่อนที่ของกลางนี้หรือไม่

(4) มีแฟ้มข้อมูลภาพหรือแฟ้มข้อมูลภาพยนตร์ที่มีภาพบุคคลเปลือยกายหรือปรากฏอวัยวะเพศบันทึกอยู่ในโทรศัพท์เคลื่อนที่ของกลางหรือไม่

หมายเหตุ ควรหลีกเลี่ยงคำถามปลายเปิด เช่น โทรศัพท์เคลื่อนที่ของกลางมีคุณสมบัติใช้งานอย่างไร เป็นต้น

1.3) การตั้งคำถามของกลางประเภท แผ่นซีดี/บัตรอิเล็กทรอนิกส์

(1) มีแฟ้มข้อมูลภาพยนตร์ แฟ้มข้อมูลภาพ บันทึกอยู่ในแผ่นซีดีของกลางหรือไม่

(2) มีร่องรอยการตัดต่อแฟ้มข้อมูลภาพยนตร์หรือไม่

(3) รถยนต์ที่ปรากฏในแฟ้มข้อมูลภาพยนตร์ มี ยี่ห้อ รุ่นและหมายเลขแผ่นป้ายทะเบียนใด

(4) มีข้อมูลใดบันทึกอยู่ในบัตรพลาสติกของกลางหรือไม่

1.4) การตั้งคำถามของกลางประเภท อุปกรณ์ไฟฟ้าหรืออุปกรณ์อิเล็กหรอนิกส์อื่น ๆ เครื่องอ่านบัตรพลาสติกของกลาง สามารถอ่านและเขียนข้อมูลจากบัตรพลาสติกได้หรือไม่

1.5) การตั้งคำถามของกลางประเภทสื่อบันทึกข้อมูลดิจิทัลอื่น ๆ ที่ไม่ได้เชื่อมต่อกับเครื่องคอมพิวเตอร์

(1) มีแฟ้มข้อมูลภาพยนตร์ แฟ้มข้อมูลภาพ บันทึกอยู่ในหน่วยความจำแฟลชชนิด USB ของกลางหรือไม่

(2) มีร่องรอยการตัดต่อแฟ้มข้อมูลภาพยนตร์หรือไม่

(3) รถยนต์ที่ปรากฏในแฟ้มข้อมูลภาพยนตร์ มี ยี่ห้อ รุ่นและหมายเลขแผ่นป้ายทะเบียนใด

2) ประเด็นคำถามในการเขียนบันทึกข้อความนำส่งของกลางเพื่อตรวจพิสูจน์ (ตามประเภทคดี)

ตารางที่ 4-5 ประเด็นคำถามในการเขียนบันทึกข้อความนำส่งของกลางเพื่อตรวจพิสูจน์ (ตามประเภทคดี)

ลำดับ	ประเภทคดี	ของกลางที่เกี่ยวข้อง	จุดประสงค์ในการตรวจพิสูจน์
1.	ปลอมแปลงบัตรพลาสติกชนิดมีแถบแม่เหล็ก	1. คอมพิวเตอร์ 2. เครื่องอ่านเขียนบัตร 3. บัตรแถบแม่เหล็ก	1. มีโปรแกรมในคอมพิวเตอร์/คอมพิวเตอร์โน้ตบุ๊กของกลางหรือไม่ 2. มีข้อมูลบันทึกอยู่ในบัตรอิเล็กทรอนิกส์หรือไม่ 3. มีข้อมูลตาม ข้อ 2 หรือข้อมูลจากธนาคารบันทึกอยู่ในคอมพิวเตอร์ของกลางหรือไม่
2.	หมิ่นประมาท	1. คอมพิวเตอร์ 2. โทรศัพท์	1. มีข้อความตามเอกสารบันทึกอยู่ในคอมพิวเตอร์/คอมพิวเตอร์โน้ตบุ๊กของกลางหรือไม่ 2. มีประวัติการใช้ Facebook/Line ในคอมพิวเตอร์ /คอมพิวเตอร์โน้ตบุ๊กของกลางหรือไม่ 3. มีประวัติการใช้งานโทรศัพท์เคลื่อนที่ของกลางหรือไม่
3.	ตัดต่อภาพ/เสียง	1. คอมพิวเตอร์ 2. โทรศัพท์ 3. แผ่นซีดี 4. อื่น ๆ	1. มีร่องรอยการตัดต่อแฟ้มข้อมูลภาพ/ เสียงที่บันทึกอยู่ในของกลางหรือไม่
4.	ลิขสิทธิ์ ซอฟต์แวร์ ภาพยนตร์ เพลงหรืออื่นๆ	1. คอมพิวเตอร์ 2. โทรศัพท์ 3. แผ่นซีดี 4. อื่น ๆ	1. มีซอฟต์แวร์/ภาพยนตร์/เพลง/... ตามตัวอย่างบันทึกอยู่ในของกลางหรือไม่
5.	ลักทรัพย์โดยใช้คอมพิวเตอร์นำทาง GPRS หาเป้าหมายที่จะทำการโจรกรรมทรัพย์สิน	คอมพิวเตอร์นำทาง GPRS ในรถยนต์ หรืออื่น ๆ	มีประวัติการใช้คอมพิวเตอร์นำทาง GPRS ไปยังสถานที่ต่าง ๆ บันทึกอยู่ในคอมพิวเตอร์ของกลางหรือไม่
6.	ลักทรัพย์ โดยใช้รถยนต์ หรือ จักรยานยนต์ (ดูแผ่นป้ายทะเบียนรถ)	แฟ้มข้อมูล ภาพ หรือ แฟ้มข้อมูลภาพยนตร์	หมายเลขแผ่นป้านทะเบียนรถยนต์/รถจักรยานยนต์มีหมายเลขใด
7.	เปิดบริษัทซื้อขายหุ้นโดยไม่ได้รับอนุญาตอันเป็นการฝ่าฝืน พ.ร.บ.	1. คอมพิวเตอร์ 2. โทรศัพท์	1. มีโปรแกรมซื้อขายหุ้นที่มีลักษณะตามเอกสารตัวอย่างบันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่ 2. มีแฟ้มข้อมูลเอกสารและตารางที่ระบุถึงการ

ตารางที่ 4-5 ประเด็นคำถามในการเขียนบันทึกข้อความนำส่งของกลางเพื่อตรวจพิสูจน์ (ตามประเภทคดี)

ลำดับ	ประเภทคดี	ของกลางที่เกี่ยวข้อง	จุดประสงค์ในการตรวจพิสูจน์
	หลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535		จ่ายเงินเดือนพนักงานตามเอกสารตัวอย่างบันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่
8.	ร่วมกันฟอกเงิน ร่วมกันเป็นผู้จัดให้มีการเล่นพนันหวยออนไลน์ทางสื่ออิเล็กทรอนิกส์โดยการประกาศโฆษณาชักชวนให้ผู้อื่นเข้าเล่นการพนันและร่วมกันเป็นเจ้ามือรับกินรับใช้ในการเล่นการพนันหวยออนไลน์ พนันเอาทรัพย์สินกันโดยไม่ได้รับอนุญาต	1. คอมพิวเตอร์ 2. โทรศัพท์	1. มีข้อมูลการเข้าถึงเว็บไซต์พนันออนไลน์ชื่อ... ตามเอกสารตัวอย่างบันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่ 2. มีแฟ้มข้อมูลเอกสารหรือตารางงานที่มีคำว่า “หวยออนไลน์”, “ทายผลฟุตบอล” ตามเอกสารตัวอย่างบันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่
9.	ร่วมกันเป็นซ่องโจร ร่วมกันมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ (คดี Call Center)	1. คอมพิวเตอร์ 2. โทรศัพท์	1. มีโปรแกรม VOIP เช่น Bria Skype บันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่ และมีประวัติการใช้งานอย่างไร 2. อุปกรณ์เชื่อมต่อระบบเครือข่ายของกลางมีการตั้งค่า Configuration อย่างไร
10.	คดีละเมิดต่อเด็กและเยาวชน	1. คอมพิวเตอร์ 2. โทรศัพท์	1. มีภาพบุคคลเปลือยกายของเด็กหรือเยาวชนตามเอกสารตัวอย่างบันทึกอยู่ในคอมพิวเตอร์/โทรศัพท์ของกลางหรือไม่ 2. มีการเผยแพร่ภาพบุคคลเปลือยกายตามข้อ 1 ไปยังเครือข่ายคอมพิวเตอร์ เช่น Facebook, Line หรือไม่
11.	ออกใบกำกับภาษีโดยไม่มีสิทธิจะออก	คอมพิวเตอร์	มีแฟ้มข้อมูลเอกสาร ตารางงาน หรือรูปภาพที่ระบุคำว่า “ใบกำกับภาษี” บันทึกอยู่ในคอมพิวเตอร์ของกลางหรือไม่

ข้อควรระวังในการส่งของกลางตรวจพิสูจน์

1) ของกลางประเภทคอมพิวเตอร์

1.1) กรณีคอมพิวเตอร์ปิดอยู่ ห้ามเปิดเครื่องเพื่อพิมพ์งานลงในคอมพิวเตอร์ของกลาง

1.2) หากพนักงานสอบสวนต้องการทำสำเนาข้อมูลเพื่อส่งตรวจพิสูจน์ให้ทำสำเนามาทั้งระบบ (ทำสำเนาข้อมูลบิตต่อบิตให้เหมือนต้นฉบับทุกประการ)

1.3) หากคอมพิวเตอร์มีรหัสป้องกันให้ขอ Password มาด้วย ระวังเจ้าของคอมพิวเตอร์มักบอกว่าลืม

1.4) หากตรวจเปรียบเทียบต้องมีตัวอย่างที่ต้องการตรวจเปรียบเทียบ

1.5) เนื่องจากคอมพิวเตอร์ถูกออกแบบมาให้ควบคุมระยะไกลให้ระมัดระวังการ Remote เข้ามาลบข้อมูล

2) ของกลางประเภทโทรศัพท์

2.1) เนื่องจากโทรศัพท์สมาร์ทโฟนในยุคปัจจุบันออกแบบมาให้ควบคุมระยะไกลให้ระมัดระวังการ Remote เข้ามาลบข้อมูล

2.2) หากโทรศัพท์มีรหัสป้องกันให้ขอ password มาด้วย ระวังเจ้าของโทรศัพท์มักบอกว่าลืม

หากพบว่าผู้ให้บริการ จงใจ สนับสนุนหรือยินยอมให้มีการกระทำความผิด ในการนำสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน หรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ในระบบคอมพิวเตอร์ที่อยู่ในความครอบครองของตน เข้าข่ายเป็นความผิดตามมาตรา 14 (1) ถึง (5) แห่ง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ให้พนักงานสอบสวนพิจารณาดำเนินคดีกับผู้ให้บริการด้วย

หากมีข้อขัดข้องหรือข้อสงสัยเกี่ยวกับการสืบสวนทางเทคนิคหรือการรวบรวมพยานหลักฐานในการกระทำความผิดทางเทคโนโลยี ให้ประสานกับกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี บก.สทท.สทส. อาคาร 33 ชั้น 4 สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ โทรศัพท์ 0 2205 2627

สถานที่ที่สามารถส่งของกลางเพื่อตรวจพิสูจน์

ปัจจุบันสำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ มีหน่วยงานรับตรวจอาชญากรรมทางคอมพิวเตอร์ จำนวน 3 แห่ง ครอบคลุมพื้นที่ให้บริการดังนี้

1) กองพิสูจน์หลักฐานกลาง โทร. 0-2205-1742 (กทม. และพื้นที่อื่น ๆ)

2) ศูนย์พิสูจน์หลักฐาน 7 โทร. 0-3425-1981 (ตำรวจภูธรภาค 7 และพื้นที่อื่น ๆ)

3) ศูนย์พิสูจน์หลักฐาน 10 โทร. 0-7327-4407 (3 จังหวัดชายแดนภาคใต้ และตำรวจภูธรภาค 9)

3.3 กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

ปัจจุบันเจ้าหน้าที่บังคับใช้กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ดังนี้

1) ประมวลกฎหมายอาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ของลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6 และ มาตรา 269/7

2) พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537

3) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และแก้ไขเพิ่มเติม พ.ศ. 2551 เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

4) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 ซึ่งให้อำนาจพนักงานเจ้าหน้าที่

5) พระราชบัญญัติการผลิต ผลิตภัณฑ์ซีดี พ.ศ. 2548

6) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

7) กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้ บริการอื่น ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

8) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

9) พระราชกฤษฎีกา ว่าด้วยการควบคุมดูและธุรกิจบริการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551

10) พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาบังคับใช้ พ.ศ. 2549

11) กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

12) กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ฉบับที่ 2 พ.ศ. 2555

13) ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนการสอบสวนและการดำเนินคดีกับผู้กระทำความผิดว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

14) ประกาศกระทรวงเทคโนโลยีและสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

15) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์และระยะเวลาการงดให้บริการโทรศัพท์เคลื่อนที่ในเขตพื้นที่จังหวัดนราธิวาส จังหวัดปัตตานี และจังหวัดยะลา พ.ศ. 2550

16) ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ฉบับที่ 2)

17) หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติหลักเกณฑ์ เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

18) ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ พ.ศ. 2555

19) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

20) หนังสือสำนักงานตำรวจแห่งชาติที่ 0011.26/537 ลงวันที่ 4 กุมภาพันธ์ 2556 เรื่อง แนวทางการสอบสวนและรวบรวมพยานหลักฐานในคดีการกระทำความผิดทางเทคโนโลยี

21) คู่มือการปฏิบัติงานด้านนิติวิทยาศาสตร์ในการสืบสวนสอบสวน สำนักงานตำรวจแห่งชาติ พุทธศักราช 2561

3.4 รายการอาชญากรรมทางเทคโนโลยี และพยานหลักฐานทางดิจิตอล หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ

1) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการก่อการร้าย (Importance Evidence Related on Terrorism)

- เงินสด (Cash)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- เอกสารแสดงตัวตนปลอม (Fictitious Identification)
- ประวัติทางการเงิน (Financial Records)
- อุปกรณ์ระบุตำแหน่งและแผนที่ (GPS Equipment and Maps)
- สายเชื่อมต่อโทรศัพท์ (Phone Cables)
- โทรศัพท์ที่ถูกขโมย (Stolen Phones)
- โทรศัพท์วีโอไอพีและโปรแกรมสำหรับโทรศัพท์ (VoIP and Soft Phones)

2) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการฉ้อโกงทางคอมพิวเตอร์

- ข้อมูล Account ของผู้ใช้งานการประมูลอนไลน์
- ซอฟท์แวร์และไฟล์ทางด้านการบัญชี

- สมุดที่อยู่
- ปฏิทิน
- Chat logs
- ข้อมูลลูกค้า
- ข้อมูลบัตรเครดิต
- ฐานข้อมูล
- ซอฟท์แวร์ของกล้องดิจิตอล
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ข้อมูลทางด้านการเงินและรายการทรัพย์สิน
- ข้อมูลจราจรทางคอมพิวเตอร์

3) พยานหลักฐานสำคัญที่เกี่ยวข้องการล่วงละเมิดทางเพศ คดีภาพโป๊เด็ก และการกระทำทารุณกรรมต่อเด็ก

- ประวัติหมายเลขประจำตัวผู้โทร (Caller ID Records)
- ประวัติทางการเงิน (Financial Records)
- เอกสารทางกฎหมาย (Legal Documents)
- แผนที่ เส้นทางและอุปกรณ์ระบุตำแหน่ง (Maps, Directions and GPS Equipment)
- เว็บไซต์ส่วนตัว (Personal Web sites)
- บันทึกและไดอารีส่วนตัว (Personal Writings and Diaries)
- ประวัติการใช้งานโทรศัพท์ (Telephone Records)
- Chat logs
- ซอฟท์แวร์ของกล้องดิจิตอล
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- โปรแกรมเกมส์คอมพิวเตอร์ (Computer Games)
- ซอฟท์แวร์การเปิดภาพและตกแต่งภาพ (Digital Photo Software)
- ภาพพิมพ์รูปถ่ายต่าง ๆ (Printed Photographs)
- ข้อมูลจราจรทางคอมพิวเตอร์
- ไฟล์ภาพยนตร์
- ไดเรคทอรี่ที่การจัดแบ่งหมวดหมู่รูปภาพ
- ปฏิทินและตารางงาน (Calendars and journals)
- เครื่องพิมพ์หรือเครื่องทำสำเนา (Printers and copiers)
- เครื่องแสกนเนอร์ (Scanners)
- กล้องถ่ายภาพและสื่อจัดเก็บข้อมูล (Cameras and media)

- กล้องวิดีโอและสื่อบันทึก (Video Cameras and Medias)
- เครื่องเล่นเกมส์ (Video Games and Consoles)
- โทรศัพท์วีโอไอพีและโปรแกรมสำหรับโทรศัพท์ (VoIP and Soft Phones)

4) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการบุกรุกทางระบบคอมพิวเตอร์ หรือระบบเน็ตเวิร์ค

- เสาสัญญาณ (Antennas)
- หนังสือและเอกสารอ้างอิงการเจาะระบบ (Books and References on Hacking)
- รายการเครื่องคอมพิวเตอร์ที่เข้าถึงได้ (List of Computers Accessed)
- รายการหมายเลขไอพี (List of IP Addresses)
- อุปกรณ์เครือข่ายและอุปกรณ์เสริม (Network Devices and Components)
- เอกสารแสดงรหัสคอมพิวเตอร์ (Printed Computer Password)
- อุปกรณ์เชื่อมต่อเครือข่ายไร้สาย (Wireless Network Equipment**)**
- สมุดที่อยู่
- ไฟล์การตั้งค่าต่าง ๆ (Configuration files)
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- โปรแกรมต่าง ๆ (Executable programs)
- ข้อมูลจราจรทางคอมพิวเตอร์
- Internet protocol address และ usernames
- Log การใช้งาน IRC
- Source code
- Text files และไฟล์เอกสารที่เก็บข้อมูล usernames และ passwords

5) พยานหลักฐานสำคัญที่เกี่ยวข้องกับคดีฆาตกรรม

- ข้อมูลบัตรเครดิต (Credit Card Information)
- โปรแกรมทำธุรกรรมออนไลน์ (Online Banking Software)
- รายการสั่งพิมพ์เอกสารก่อนหน้า (Recently Printed Material)
- ลายเซ็นปลอม (Reproductions of Signatures)
- สมุดที่อยู่
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ประวัติทางการเงิน (Financial Records)
- ข้อมูลจราจรทางคอมพิวเตอร์
- พินัยกรรมและเอกสารทางกฎหมาย
- ประวัติทางการรักษา (Medical records)
- ประวัติการใช้งานโทรศัพท์และการชำระเงิน (Telephone and Billing Records)

- บันทึกและไดอารีส่วนตัว (Personal Writings and Diaries)
- แผนที่
- ภาพถ่ายของเหยื่อหรือผู้ต้องสงสัย
- ภาพถ่ายที่ระลึกถึงการฆาตกรรมต่าง ๆ

6) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการกระทำความผิดภายในประเทศ

- สมุดที่อยู่
- ไดอารี
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ข้อมูลการเงิน
- ข้อมูลเบอร์โทรศัพท์

7) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการปลอมแปลง ทุจริตออนไลน์ และการฉ้อโกงทางเศรษฐกิจ

- โปรแกรมบัญชี (Accounting Software)
- เงินสด เช็คและคำสั่งโอนเงิน (Cash, Checks and Money Orders)
- ข้อมูลของธนาคาร (Bank logs)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- ประวัติทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)
- รูปภาพเช็คหรือใบสั่งจ่ายเงินต่าง ๆ
- โปรแกรมทำธุรกรรมออนไลน์ (Online Banking Software)
- ลายเซ็นปลอม (Reproductions of Signatures)
- สมุดที่อยู่
- ปฏิทิน
- รูปภาพธนบัตรต่าง ๆ
- ข้อมูลลูกค้า
- ฐานข้อมูล
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- บัตรประชาชนปลอม
- ข้อมูลจราจรทางคอมพิวเตอร์
- รูปภาพเงินตราที่ทำการปลอมแปลง

- เครื่องพิมพ์ความละเอียดสูง (High-Quality Printers)
- เครื่องอ่านแถบแม่เหล็ก (Magnetic Strip Readers)
- เอกสารแสดงรหัสคอมพิวเตอร์ (Printed Computer Password)
- เครื่องสแกนเนอร์และเครื่องทำสำเนา (Scanners and Copiers)

8) พยานหลักฐานสำคัญที่เกี่ยวข้องกับกรณีพวกโรคจิต ทำให้อับอาย หมิ่นประมาท หรือการข่มขู่ทางอีเมล์

- ประวัติหมายเลขประจาตัวผู้โทร (Caller ID Records)
- ประวัติทางการเงิน (Financial Records)
- เอกสารทางกฎหมาย (Legal Documents)
- บันทึกและไดอารีส่วนตัว (Personal Writings and Diaries)
- คำร้องขอการคุ้มครอง (Protection Orders)
- ประวัติการใช้งานโทรศัพท์และการชำระเงิน (Telephone and Billing Records)
- สมุดที่อยู่
- ไดอารี
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ข้อมูลทางการเงิน
- รูปภาพต่าง ๆ
- ข้อมูลจราจรทางคอมพิวเตอร์
- เอกสารทางกฎหมายต่าง ๆ
- รายการโทรศัพท์
- การค้นหาข้อมูลต่าง ๆ เกี่ยวกับเหยื่อ
- แผนที่ที่อยู่อาศัยของเหยื่อ

9) พยานหลักฐานสำคัญที่เกี่ยวข้องกับคดียาเสพติด

- เงินสด (Cash)
- อุปกรณ์ป้องกันการเฝ้าระวัง (Counter Surveillance Equipment)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- เอกสารแสดงตัวตนปลอม (Fictitious Identification)
- ประวัติข้อมูลทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)
- อุปกรณ์ระบุตำแหน่งและแผนที่ (GPS Equipment and Maps)

- โปรแกรมทำธุรกรรมออนไลน์ (Online Banking Software)
- สูตรยาเสพติด และรูปถ่ายสารเสพย์ติด (Photographs of Drugs)
- สมุดที่อยู่
- ปฏิทิน
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ข้อมูลจราจรทางคอมพิวเตอร์
- ข้อมูลใบสั่งยา

10) พยานหลักฐานสำคัญที่เกี่ยวข้องการสืบสวนกรณีละเมิดลิขสิทธิ์ซอฟท์แวร์

- เงินสด (Cash)
- เครื่องเขียนข้อมูลซีดีและดีวีดี (CD and DVD burners)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- ประวัติทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)
- โปรแกรมสำหรับกำหนด Activation Code (Software Activation Codes)
- อุปกรณ์สำหรับทำสำเนาโปรแกรม (Software Duplication Equipment)
- Chat logs
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ไฟล์ภาพใบรับรองซอฟท์แวร์
- ข้อมูลจราจรทางคอมพิวเตอร์
- Serial number ของซอฟท์แวร์
- ซอฟท์แวร์สำหรับการแคร็ก
- การจัดการไฟล์ไดเรคทอรีและการตั้งชื่อไฟล์แยกตามหมวดหมู่ของซอฟท์แวร์ลิขสิทธิ์

11) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการฉ้อโกงทางด้านการสื่อสารโทรคมนาคม

- อุปกรณ์โหลดข้อมูล (Boot Loader Devices)
- ข้อมูลทางการเงิน และเงินสด (Cash)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- อุปกรณ์เขียน EPROM (EPROM Burner)
- ประวัติทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)

- โปรแกรมทำธุรกรรมออนไลน์ (Online Banking Software)
- สายเชื่อมต่อโทรศัพท์ (Phone Cables)
- เครื่องอ่าน SIM Card (SIM Card Reader)
- โทรศัพท์ที่ถูกขโมย (Stolen Phones)
- ซอฟท์แวร์สำหรับการทำสำเนา (Cloning software)
- รายการฐานข้อมูลของลูกค้า
- Electronic serial number
- หมายเลขโทรศัพท์ของบุคคลต่าง ๆ
- อีเมล์ จดหมาย และบันทึกต่าง ๆ
- ข้อมูลจราจรทางคอมพิวเตอร์

12) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการขโมยอัตภาพ

- โปรแกรมบัญชี (Accounting Software)
- เงินสด เช็คและคำสั่งโอนเงิน (Cash, Checks and Money Orders)
- ข้อมูลบัตรเครดิต (Credit Card Information)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- ประวัติทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)
- เครื่องพิมพ์ความละเอียดสูง (High-Quality Printers)
- รายชื่ออีเมล์ของเหยื่อ (Mail in Victim’s Name)
- โปรแกรมทาธุรกรรมออนไลน์ (Online Banking Software)
- ลายเซ็นปลอม (Reproductions of Signatures)
- เครื่องสแกนเนอร์และเครื่องทำสำเนา (Scanners and Copiers)
- ประวัติการเข้าใช้งานเว็บไซต์ (Web Site Transaction Records)

13) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการสืบสวนการขโมยข้อมูลส่วนบุคคล

- Tools ต่าง ๆ สำหรับฮาร์ดแวร์และซอฟท์แวร์
- Backdrops
- Credit card reader/writer
- ซอฟท์แวร์ของกล้องดิจิตอล
- ซอฟท์แวร์ของเครื่อง Scanner
- เทมเพลตของข้อมูลบุคคลต่าง ๆ
- ใบสูติบัตร

- บัตรเงินสด (Check cashing card)
- ภาพถ่ายดิจิตอล
- ใบขับขี่
- ลายเซ็นต์อิเล็กทรอนิกส์
- ข้อมูลสำหรับทำใบขับขี่ปลอม
- เอกสารการประกันภัยปลอม
- บัตรประกันสังคม
- กิจกรรมทางอินเทอร์เน็ตที่เกี่ยวข้องกับการขโมยข้อมูลบุคคล
- การโพสต์อีเมล์ หรือชื่อ newsgroup
- ไฟล์เอกสารที่ถูกลบทิ้ง
- ใบสั่งของออนไลน์
- ข้อมูลการซื้อขายออนไลน์
- ข้อมูลจราจรทางคอมพิวเตอร์
- เครื่องมือต่าง ๆ สำหรับการเจรจาต่อรอง (negotiable instruments)
- เช็คที่ออกในนามบริษัท
- แคชเชียร์เช็ค
- หมายเลขบัตรเครดิต
- เอกสารทางกฎหมายปลอม
- บัตรของขวัญปลอม
- เอกสารการกู้ยืมเงินปลอม
- ใบเสร็จปลอม
- ใบสั่งจ่ายเงินปลอม
- เช็คส่วนบุคคล

14) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการพนัน

- โปรแกรมบัญชี (Accounting Software)
- เงินสด (Cash)
- รายการลูกค้า (Client Lists)
- เอกสารแผนผังฐานข้อมูล (Database Printouts)
- รายการหรือประวัติการโอน-รับเงิน (Electronic Money Transfers)
- ประวัติทางการเงิน (Financial Records)
- เอกสารตั๋วเงินปลอม (Forged Documents)
- รายชื่อเว็บไซต์การพนัน (Lists of Online Gambling Sites)

- เอกสารอ้างอิง (References to Odds and Lines)
- สถิติการพนัน (Sports Betting Statistics)

3.5 แนวทางบริหารจัดการและจัดเก็บพยานหลักฐาน

หนึ่งในปัจจัยสำคัญของการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐานที่ได้รับจากสถานที่เกิดเหตุนั้น คือการจัดเก็บและรักษาสภาพของพยานหลักฐานในห้องเก็บพยานหลักฐาน ซึ่งมีปัจจัยที่ต้องให้ความสำคัญซึ่งและต้องปฏิบัติตามขั้นตอนอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน
- ชุดดูแลห้องเก็บพยานหลักฐาน
- ชุดขนส่งและคุ้มครองพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- ตู้เก็บพยานหลักฐาน

1) ขั้นตอนการปฏิบัติเพื่อจัดเก็บพยานหลักฐาน (Evidence Retention Protocol)

1.1) ชุดขนส่งและคุ้มครองพยานหลักฐาน ส่งพยานหลักฐานให้ชุดดูแลห้องเก็บพยานหลักฐาน พร้อมลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดดูแลห้องเก็บพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

1.2) ชุดดูแลห้องเก็บพยานหลักฐาน ทำการบันทึกข้อมูลรายการหลักฐานที่ได้รับลงในเอกสารการจัดเก็บหลักฐาน (Evidence Retention Form) พร้อมลงลายมือชื่อ

1.3) หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน ตรวจสอบความพร้อมและเอกสารการจัดเก็บหลักฐานพร้อมลงลายมือชื่อรับรองความถูกต้อง

2) กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐานในฐานะผู้รับผิดชอบห้องเก็บพยานหลักฐานจำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

2.1) ความถูกต้องครบถ้วนของพยานหลักฐานที่จัดเก็บ เทียบกับรายการตามเอกสาร

2.2) ความถูกต้องสมบูรณ์ทางกายภาพของพยานหลักฐานในปัจจุบัน เทียบกับข้อมูลสภาพของหลักฐานเมื่อได้รับมา

3.6 ปัญหาข้อขัดข้องในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์

1) ปัญหาที่เกิดก่อนการตรวจพิสูจน์
   - ความรู้ความสามารถเรื่องคอมพิวเตอร์ ของพนักงานสอบสวน ในการสอบสวนคดี
   - ตั้งคำถามไม่ตรงประเด็นและไม่เป็นประโยชน์ต่อรูปคดี
   - ยึดของกลางในปริมาณมาก และยึดของกลางที่ไม่เกี่ยวข้อง
2) ปัญหาที่เกิดระหว่างการตรวจพิสูจน์
   - ทรัพยากรในการตรวจพิสูจน์ของกลางมีไม่เพียงพอ (เช่น ผู้ปฏิบัติงาน และอุปกรณ์)
   - ข้อจำกัดของระบบคอมพิวเตอร์ หรือ Software
3) ปัญหาที่เกิดหลังการตรวจพิสูจน์
   - การอธิบายในรายงานการตรวจเป็นศัพท์ทางเทคนิคซึ่งเข้าใจได้ยาก
   - ผลการตรวจไม่เป็นประโยชน์ต่อรูปคดี
   - พนักงานสอบสวน พนักงานอัยการ ศาล ไม่เข้าใจคำตอบที่เกี่ยวข้องกับศัพท์คอมพิวเตอร์

3.7 การบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ (Crime Scene Preservation Management)

การบริหารจัดการสถานที่เกิดเหตุถือเป็นหัวใจสาคัญที่เจ้าหน้าที่ต้องให้ความสำคัญอย่างมาก เนื่องจากการปฏิบัติงานต่างๆ ในสถานที่เกิดเหตุ หากเกิดความผิดพลาดอาจส่งผลให้เกิดความเสียหายหรือสูญไปของพยานหลักฐาน และอาจส่งผลให้พยานหลักฐานที่ได้สถานที่เกิดเหตุนั้นมีความน่าเชื่อถือลง ดังนั้น แนวทางปฏิบัติในการเก็บยึดพยานหลักฐานทางคอมพิวเตอร์ เป็นสิ่งที่จะต้องปฏิบัติในการเข้าตรวจสถานที่เกิดเหตุทางด้านคดีอาชญากรรมทางคอมพิวเตอร์ในสถานการณ์ปัจจุบัน มีดังนี้

1) ความปลอดภัยของเจ้าพนักงาน (Officer Safety)

ความปลอดภัยของเจ้าพนักงานเป็นสิ่งที่สำคัญที่สุดในการปฏิบัติงานสืบสวนสอบสวนในทุกคดี ปัจจุบันนี้แทบทุกคดีจะต้องเกี่ยวข้องกับอุปกรณ์ทางคอมพิวเตอร์ และมีการใช้เทคโนโลยีในการประกอบอาชญากรรม เครื่องคอมพิวเตอร์ที่ถูกใช้ในการประกอบอาชญากรรม อาจมีพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดให้เราสืบสวนได้ ซึ่งในสภาะการณ์เช่นนี้ พนักงานสอบสวน เจ้าหน้าที่สืบสวน อย่าได้ชะล่าใจกับสภาพบุคคลหรือสถานที่เกิดเหตุที่ดูไม่น่ามีอะไรนัก เพราะอาจเป็นไปได้ว่า มีเครื่องคอมพิวเตอร์เกี่ยวข้องในการกระทำความผิดนั้น และในระหว่างทำการสืบสวนคดีอาชญากรรมทางด้านคอมพิวเตอร์หรือการดำเนินการเก็บยึดอุปกรณ์คอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์อื่นๆ พึงระวังเช่นเดียวกับกรณีคดีอื่น ๆ ทั่วไป ว่าการเปลี่ยนแปลงที่ไม่คาดคิดต่อวัตถุพยานต่าง ๆ อาจก่อให้เกิดอันตรายแก่ตัวเจ้าหน้าที่ที่กำลังปฏิบัติหน้าที่อยู่ได้

การใช้ขั้นตอนการดำเนินการที่ถูกต้องเหมาะสม จะช่วยให้มั่นใจว่าเกิดความปลอดภัยแก่เจ้าหน้าที่รวมถึงบุคคลอื่นๆ ที่อยู่ในสถานที่เกิดเหตุนั้นด้วย

2) กฎสำคัญ (Golden Rules)

มีหลักการในการปฏิบัติทั่วๆ ไปเมื่อเข้าไปถึงที่เกิดเหตุที่อาจมีเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เกี่ยวข้องด้วยอยู่หลายหลักการด้วยกัน เช่น

2.1 ความปลอดภัยของเจ้าพนักงาน

รักษาสถานที่เกิดเหตุและจัดการให้เกิดความปลอดภัย หากเชื่ออย่างมีเหตุผลว่ามีเครื่องคอมพิวเตอร์เกี่ยวข้องในคดีที่คุณทำการสืบสวนสอบสวนอยู่ ให้ดำเนินการเก็บรักษาพยานหลักฐานโดยทันที

2.2 คำนึงว่ามีอำนาจตามกฎหมายให้เข้ายึดเครื่องคอมพิวเตอร์เรียบร้อยหรือยัง (การสำรวจในขั้นเบื้องต้น, หมาย ค้น เป็นต้น)

ห้ามทำการเปิดไฟล์ใด ๆ หากเครื่องคอมพิวเตอร์ปิดอยู่ ห้ามเปิดเครื่อง หากเครื่องเปิดอยู่ ห้ามทำการค้นหาไฟล์ใดๆ บนเครื่องนั้น

หากเครื่องคอมพิวเตอร์เปิดอยู่ ให้ดำเนินการตามขั้นตอนที่เหมาะสม ว่าจะต้องปิดเครื่องอย่างไรและจะต้องเตรียมการขนย้ายพยานหลักฐานอย่างไรหากมีเหตุผลที่ควรเชื่อได้ว่าเครื่องคอมพิวเตอร์กำลังทำลายพยานหลักฐาน ให้ทำการปิดเครื่องคอมพิวเตอร์โดยทันทีโดยการดึงสายไฟด้านหลังเครื่องออก

หากมีกล้องไปด้วย และเครื่องคอมพิวเตอร์เปิดอยู่ ให้ทำการถ่ายภาพที่อยู่บนหน้าจอคอมพิวเตอร์ในขณะนั้น

หากเครื่องคอมพิวเตอร์ปิดอยู่ ให้ทำการถ่ายภาพเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ที่เชื่อมต่ออยู่

2.3 ต้องปฏิบัติงานทุกอย่าง อย่างถูกต้องตามกฎหมาย (เช่น ในบางกรณี เราต้องให้บุคคลต่อไปนี้เข้าร่วมในการปฏิบัติงานด้วย แพทย์, นักกฎหมาย, นักศาสนา, จิตแพทย์, นักหนังสือพิมพ์, นักข่าว เป็นต้น)

3) ขั้นตอนและรายละเอียดการปฏิบัติงาน

ขั้นตอนการปฏิบัติเพื่อรักษาสภาพสถานที่เกิดเหตุ (Crime Scene Preservation Protocol)

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าชุดปราบปราม
- ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ
- ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ
- ชุดสอบปากคำ

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เทปปิดกันพื้นที่เกิดเหตุ (เทปเหลือง) (Crime Scene Tape)
- อุปกรณ์ปิดกันพื้นที่ (รั้วเหล็ก)
- อุปกรณ์สำหรับการรักษาความปลอดภัย (ปืนพก และกระบอง)

3.1 รวบรวมข้อมูลเกี่ยวกับคดี เช่น ข้อมูลด้านสถานที่ ประเภท ลักษณะ และพฤติการณ์ของความผิดความรู้ความสามารถของผู้ต้องสงสัยเกี่ยวกับคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์หรือเครื่องคอมพิวเตอร์ใดที่เกี่ยวข้องกับคดี

3.2 ให้หัวหน้าชุดปราบปรามจัดชุดรักษาความปลอดภัย เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าหรือออกสถานที่เกิดเหตุ และป้องกันมิให้เกิดการปนเปื้อนต่อพยานหลักฐานใดๆ โดยแบ่งชุดรักษาความปลอดภัยออกเป็น 2 ส่วน คือ

3.2.1 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ

3.2.2 ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ

3.3 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ปิดกันสถานที่เกิดเหตุด้วยเทปปิดกันพื้นที่เกิดเหตุ (Crime Scene Tape) เพื่อกำหนดพื้นที่และขอบเขตของสถานที่เกิดเหตุ และปิดกั้นไม่ให้บุคคลอื่นเข้าบริเวณดังกล่าว

3.4 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ใช้อุปกรณ์ปิดกันพื้นที่ เพื่อปิดกั้นทางเข้า-ออก เช่น ถนน ทางเดินเท้า ซอยบริเวณรอบสถานที่เกิดเหตุ เป็นต้น

3.5 ชุดรักษาความปลอภัยรอบสถานที่เกิดเหตุ ตรวจสอบบุคลากรและเจ้าหน้าที่ที่เกี่ยวข้องเพื่อรักษาความปลอดภัยของบริเวณโดยรอบ โดยให้ความสาคัญกับสิ่งต่อไปนี้เป็นพิเศษ

3.5.1 จดบันทึก (Logging) การเข้า-ออก สถานที่เกิดเหตุตลอดระยะเวลาของการปฏิบัติงาน

3.5.2 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุนำตัวผู้ต้องสงสัย บุคคลที่ไม่เกี่ยวข้อง และสัตว์เลี้ยงที่ไม่เกี่ยวข้องออกจากสถานที่เกิดเหตุทันที หรือจัดสรรพื้นที่พิเศษและจัดเจ้าหน้าที่ชุดสอบปากคาควบคุมอย่างใกล้ชิด (กรณีที่ไม่สามารถนำตัวออกนอกสถานที่ได้)

3.5.3 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุตรวจตราและรักษาความปลอดภัยโดยรอบสถานที่เกิดเหตุ เพื่อรักษาความปลอดภัยให้กับเจ้าหน้าที่

3.5.4 กรณีตรวจพบภัยคุกคามหรืออันตรายร้ายแรงตามดุลยพินิจของชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุให้อพยพเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องออกจากพื้นที่นั้นๆ ทันที

3.6 ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุตรวจตราความปลอดภัยของเจ้าหน้าที่ผู้ปฏิบัติงานในสถานที่เกิดเหตุ โดยให้ความสำคัญกับสิ่งต่อไปนี้เป็นพิเศษ

3.6.1 เครื่องแต่งกายของเจ้าหน้าที่ต้องเป็นชุดป้องกันไฟฟ้าสถิต (Anti-Static Suit) เช่น ถุงมือ และเสื้อคลุม เป็นต้น

3.6.2 เจ้าหน้าที่ต้องไม่พกพาอุปกรณ์ใดที่อาจก่อให้เกิดสนามแม่เหล็กและห้ามมิให้เจ้าหน้าที่ใช้งานระบบสาธารณูปโภค เช่น สุขภัณฑ์ในห้องน้า อุปกรณ์ในครัว และอุปกรณ์อื่นที่ไม่ใช้ของตนขณะปฏิบัติงาน เป็นต้น

3.6.3 สำรวจและตรวจสอบหาแหล่งจ่ายพลังงานไฟฟ้า และมอบหมายให้เจ้าหน้าที่ดูแลอย่างใกล้ชิด เพื่อป้องกันมิให้ผู้ประสงค์ร้ายตัดกระแสไฟฟ้า ซึ่งอาจส่งผลต่ออุปกรณ์อิเล็กทรอสิกส์ต่างๆ

3.6.4 จดบันทึกรายละเอียดของสถานที่เกิดเหตุและสิ่งของที่พบเห็นโดยสังเขป

3.6.5 ตรวจตราและรักษาความปลอดภัยภายในสถานที่เกิดเหตุ เพื่อรักษาความปลอดภัยให้กับเจ้าหน้าที่อื่นๆ

3.6.6 กรณีตรวจพบภัยคุกคามหรืออันตรายร้ายแรงตามดุลยพินิจของชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุให้อพยพเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องออกจากพื้นที่นั้นๆ ทันที

3.7 ชุดสอบปากคำ ดำเนินการสอบสวนผู้ต้องสงสัย และผู้ที่เกี่ยวข้อง โดยให้ความสำคัญกับข้อมูลต่อไปนี้

3.7.1 ใครเป็นเจ้าของหรือผู้มีอำนาจดูแลสถานที่เกิดเหตุ

3.7.2 จำนวนของผู้ปฏิบัติงาน พร้อมรายละเอียดของแต่ละบุคคล (ชื่อ-นามสกุล เลขบัตรประชาชน ที่อยู่ หมายเลขโทรศัพท์และข้อมูลอื่นๆ ที่เกี่ยวข้อง)

3.7.3 จำนวนเครื่องคอมพิวเตอร์ และอุปกรณ์อิเล็กทรอนิกส์ที่น่าจะเกี่ยวข้องคดีที่มีอยู่

3.7.4 บัญชีผู้ใช้ (Username) รหัสผ่าน (Password) และรหัสลับ (Encryption Key) อื่นๆ

3.7.5 ข้อมูลโครงสร้างของระบบเครือข่ายคอมพิวเตอร์ (Network Infrastructure) และแผนผังเครือข่าย (Network Diagram)

3.7.6 ข้อมูลอื่นๆ ที่อาจเป็นประโยชน์ต่อการสืบสวนในคดีนั้นๆ

3.8 การปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ (Crime Scene Search and Evidence Seizure Management)

การรวบรวมพยานหลักฐานถือเป็นขั้นตอนที่ต้องให้ความสำคัญและต้องปฏิบัติตามอย่างเคร่งครัด ทั้งยังต้องให้เจ้าหน้าที่ผู้มีความรู้ความเชี่ยวชาญพิเศษ และเคยผ่านการอบรมอย่างถูกต้องเป็นผู้ตรวจค้นและรวบรวมพยานหลักฐาน

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าชุดปราบปราม
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน
- ชุดเทคนิคและการถ่ายภาพ
- ชุดขนส่งและคุ้มครองพยานหลักฐาน
- ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape)
- ป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag)
- กล้องถ่ายภาพดิจิตอล (Digital Camera) และกล้องบันทึกวิดีโอ (Video Camera)
- ชุดป้องกันไฟฟ้าสถิต (Anti-Static Suit) และถุงมือป้องกันไฟฟ้าสถิต (Anti-Static Gloves)
- กล้องป้องกันไฟฟ้าสถิต (Anti-Static Drive Box) และกระเป๋าภาคสนาม (Pelican Bag)

- ถุงพลาสติกสำหรับเก็บพยานหลักฐาน (Plastic Evidence Bag)
- ถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดเล็ก (Paper Evidence Bag)
- อุปกรณ์ทำสำเนาหน่วยความจำ (Memory Dump Tool) และชุดรวบรวม Volatile Data
- ชุดทำสำเนาข้อมูล (Forensic Duplicator)
- ชุดตรวจวิเคราะห์โทรศัพท์เคลื่อนที่ (Mobile Phone Forensics Tool)
- ถุงป้องกันคลื่นวิทยุ (Faraday Container)

1) วางแผนการเข้าค้นสถานที่และเก็บยึดพยานหลักฐาน ขอหมายค้น และทำการแบ่งหน้าที่ ที่ต้องปฏิบัติในสถานที่เกิดเหตุให้ชัดเจน

การแบ่งหน้าที่

- หัวหน้าชุด: วางแผน ควบคุม สั่งการ ติดต่อสื่อสาร
- หน้าที่คุ้มกัน รักษาความปลอดภัย
- หน้าที่บันทึกภาพ สเก็ตภาพ
- หน้าที่จัดเก็บพยานหลักฐาน
- หน้าที่จดบันทึก
- หน้าที่รวบรวมพยานหลักฐาน
- หน้าที่สัมภาษณ์ผู้ต้องสงสัย

2) จัดเตรียมอุปกรณ์และเครื่องมือ ที่จะเป็นต้องใช้ในการเก็บยึดให้พร้อม เช่น

- กล้องถ่ายรูป/กล้องวิดีโอ
- ถุงมือ
- ซอง/ถุง/กล่อง/ภาชนะ สำหรับบรรจุพยานหลักฐาน
- เทปกาว/เทปสำหรับติดพยานหลักฐาน
- ไม้บรรทัด กระดานรองเขียน ปากกา ดินสอ ยางลบ กรรไกร มีด
- สื่อบันทึกข้อมูล เช่น แผ่นฟล็อปปี้ แผ่น CD/DVD หรือ removable media
- ซอฟท์แวร์สำหรับเก็บ volatile data
- แบบฟอร์มสำหรับการบันทึกข้อมูลต่างๆ

3) การเข้าสถานที่เกิดเหตุ

- ทำการรักษาสถานที่เกิดเหตุ
- ควบคุมตัวผู้ต้องสงสัยให้อยู่ในบริเวณที่ปลอดภัยต่อเจ้าหน้าที่
- ทำการตรวจสอบสถานที่ และบันทึกภาพด้วยกล้องถ่ายภาพและ/หรือกล้องวิดีโอ และ/หรือ วาดแผนผังแสดงตำแหน่งของสิ่งของต่างๆ
- เก็บยึดพยานหลักฐานตามที่ได้แบ่งหน้าที่กันไว้ โดยมีวิธีปฏิบัติแยกออกเป็นอุปกรณ์อิเล็กทรอนิกส์ชนิดต่างๆ

4) ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในที่เกิดเหตุ (Crime Scene Search and Evidence Collection Protocol)

4.1 หลังจากได้รับสัญญาณจากชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ เพื่อให้ มั่นใจว่าสถานที่เกิดเหตุได้รับการรักษาความปลอดภัยอย่างสมบูรณ์แล้วให้หัวหน้าชุดปราบราม สั่งชุดเทคนิคและการถ่ายภาพให้ดำเนินการตรวจค้นและเก็บรวบรวมพยานหลักฐาน

4.2 ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพและสเก็ตภาพสถานที่เกิดเหตุ โดยให้ความสาคัญกับสิ่งต่อไปนี้เป็นพิเศษ

4.2.1 การถ่ายภาพนิ่งสภาพแวดล้อมทั้ง 360 องศา ของสถานที่เกิดเหตุ

4.2.2 การถ่ายภาพนิ่งสภาพแวดล้อมใน 3 ระดับได้แก่ ระยะใกล้ ระยะกลาง และระยะไกล

4.2.3 จดบันทึกรายการหลักฐานและสถานที่ที่ถ่ายภาพครบถ้วนแล้ว เพื่อใช้ตรวจสอบและยืนยันการปฏิบัติงาน

4.2.4 เมื่อชุดเทคนิคและการถ่ายภาพ ปฏิบัติงานโดยรวมเสร็จสิ้นแล้วให้ปฏิบัติงานสนับสนุนชุดตรวจค้นและรวบรวมพยานหลักฐาน เพื่อถ่ายภาพพยานหลักฐานแบบเฉพาะเจาะจงต่อไป

4.2.5 ให้ชุดเทคนิคและการถ่ายภาพ จัดสรรเจ้าหน้าที่พิเศษเพื่อดาเนินการบันทึกภาพเคลื่อนไหว (Video) การปฏิบัติงานในการตรวจค้นและรวบรวมพยานหลักฐานตลอดการปฏิบัติงาน

4.3 ชุดตรวจค้นและรวบรวมพยานหลักฐาน ตรวจค้นสถานที่และเก็บรวบรวมพยานหลักฐานที่พบ โดยให้ความสาคัญกับสิ่งต่อไปนี้เป็นพิเศษ

4.3.1 ชุดตรวจค้นและรวบรวมพยานหลักฐาน ต้องสวมชุด (Anti-Static Suit) และ ถุงมือป้องกันไฟฟ้าสถิต (Anti-Static Gloves)

4.3.2 ปฏิบัติงานด้วยความระมัดระวังเพื่อป้องกันมิให้เกิดความเสียหายต่อพยานหลักฐานทั้งยังไม่ดำเนินการใดๆ อันอาจส่งผลให้เกิดการปนเปื้อนต่อพยานหลักฐานทุกชนิด และให้ระวังกรณีดังนี้

1. กรณีเครื่องคอมพิวเตอร์ส่วนบุคคลที่ไม่ได้เชื่อมต่อเป็นเครือข่าย สำหรับการเก็บรักษาพยานหลักฐานที่ถูกต้องเหมาะสม ให้ดำเนินการตามขั้นตอนต่อไปนี้

- อย่าใช้งานเครื่องคอมพิวเตอร์นั้นหรือพยายามที่จะค้นหาพยานหลักฐานในเครื่อง
- ถ่ายภาพเครื่องคอมพิวเตอร์ทั้งด้านหน้าและด้านหลัง รวมถึงสายและอุปกรณ์ต่อพ่วงต่างๆ ทั้งหมดที่พบ ถ่ายภาพพื้นที่รอบๆ นั้นก่อนทำการเคลื่อนย้ายวัตถุใดๆ
- หากเครื่องคอมพิวเตอร์ปิดอยู่ ห้ามเปิดเครื่อง
- หากเครื่องคอมพิวเตอร์เปิดอยู่ และมีบางอย่างปรากฏอยู่บนหน้าจอ ให้ถ่ายภาพหน้าจอนั้นไว้
- หากเครื่องคอมพิวเตอร์เปิดอยู่ และหน้าจอมืดไม่มีอะไรปรากฏ ให้เลื่อนเมาส์ หรือกด space bar (จะทำให้แสดงผลหน้าจอที่เปิดอยู่ในขณะนั้น) เมื่อภาพบนหน้าจอปรากฏขึ้นมาแล้วให้ถ่ายภาพเก็บไว้

- ดึงสายไฟด้านหลังเครื่องออก

- หากเครื่องแล็ปท็อปนั้นยังไม่ได้ทำการ shutdown เมื่อดึงสายไฟออกมาแล้วให้ถอดแบตเตอรี่ออก โดยส่วนใหญ่แล้วแบตเตอรี่จะอยู่บริเวณด้านใต้และมักจะมีปุ่มเลื่อนเพื่อถอดแบตเตอรี่ออก เมื่อถอดแบตเตอรี่ออกมาแล้วอย่าใส่แบตเตอรี่กลับเข้าไปในเครื่องอีก การถอดแบตเตอรี่ออกจะช่วยป้องกันเครื่องเปิดขึ้นมาโดยไม่ได้ตั้งใจ

- วาดภาพแผนผังและติดป้ายสายไฟต่างๆ เพื่อดูว่าสายใดเชื่อมต่ออยู่กับอุปกรณ์ใด

- ถอดสายไฟทั้งหมดออกจากตัวเคสคอมพิวเตอร์

- บรรจุหีบห่อ ทำการเคลื่อนย้ายและเก็บรักษาอุปกรณ์ต่างๆ อย่างระมัดระวัง เนื่องจากเป็นวัตถุแตกหักเสียหายได้ง่าย

- ทำการเก็บยึดสื่อบันทึกข้อมูลอื่นๆ

- เก็บสื่อต่างๆ รวมทั้งตัวเคสคอมพิวเตอร์ให้อยู่ห่างจากแม่เหล็ก เครื่องรับส่งวิทยุ และสิ่งที่อื่นๆ ที่อาจก่อให้เกิดความเสียหายได้

- เก็บยึดคู่มือการใช้งาน เอกสารและบันทึกโน้ตย่อต่างๆ

- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ โดยละเอียด

2.เครื่องคอมพิวเตอร์ส่วนบุคคลที่ทำการเชื่อมต่อเป็นเครือข่าย สำหรับการเก็บรักษาพยานหลักฐานที่ถูกต้องเหมาะสม ให้ดำเนินการตามขั้นตอนต่อไปนี้

- ถอดสายไฟออกจากเราท์เตอร์หรือโมเด็ม

- อย่าใช้งานเครื่องคอมพิวเตอร์นั้น หรือพยายามที่จะค้นหาพยานหลักฐานในเครื่อง

- ถ่ายภาพเครื่องคอมพิวเตอร์ทั้งด้านหน้าและด้านหลัง รวมถึงสายและอุปกรณ์ต่อพ่วงต่างๆ ทั้งหมดที่พบ ถ่ายภาพพื้นที่รอบๆ นั้นก่อนทำการเคลื่อนย้ายวัตถุใดๆ

- หากเครื่องคอมพิวเตอร์ปิดอยู่ ห้ามเปิดเครื่อง

- หากเครื่องคอมพิวเตอร์เปิดอยู่ และมีบางอย่างปรากฏอยู่บนหน้าจอ ให้ถ่ายภาพหน้าจอนั้นไว้

- หากเครื่องคอมพิวเตอร์เปิดอยู่ และหน้าจอมืดไม่มีอะไรปรากฏ ให้เลื่อนเมาส์หรือกด space bar (จะทำให้แสดงผลหน้าจอที่เปิดอยู่ในขณะนั้น) เมื่อภาพบนหน้าจอปรากฏขึ้นมาแล้วให้ถ่ายภาพเก็บไว้

- ดึงสายไฟด้านหลังเครื่องออก ตามภาพที่ 4-26

- วาดภาพแผนผังและติดป้ายสายไฟต่างๆ เพื่อดูว่าสายใดเชื่อมต่ออยู่กับอุปกรณ์ใด

ภาพที่ 4-26 สายไฟด้านหลังเครื่อง

- ถอดสายไฟทั้งหมดออกจากตัวเคสคอมพิวเตอร์

- บรรจุหีบห่อ ทำการเคลื่อนย้ายและเก็บรักษาอุปกรณ์ต่างๆ รวมถึงเราท์เตอร์ และโมเด็ม อย่างระมัดระวัง เนื่องจากเป็นวัตถุแตกหักเสียหายได้ง่าย
- ทำการเก็บยึดสื่อบันทึกข้อมูลอื่นๆ
- เก็บสื่อต่างๆ รวมทั้งตัวเคสคอมพิวเตอร์ให้อยู่ห่างจากแม่เหล็ก เครื่องรับส่งวิทยุ และสิ่งที่อื่นๆ ที่อาจก่อให้เกิดความเสียหายได้
- เก็บยึดคู่มือการใช้งาน เอกสารและบันทึกโน้ตย่อต่างๆ
- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ โดยละเอียด

3. เครื่องคอมพิวเตอร์เครือข่ายหรือเครื่องคอมพิวเตอร์ในเครือข่ายองค์กรธุรกิจ

- ขอคำแนะนำจากผู้เชี่ยวชาญด้านคอมพิวเตอร์เพื่อการดำเนินการพิจารณาการยึดเก็บข้อมูลต่อไป
- รักษาสถานที่เกิดเหตุและไม่ให้บุคคลใดแตะต้อง เว้นแต่บุคคลที่ได้รับการฝึกอบรมเพื่อดำเนินการกับระบบเน็ตเวิร์คโดยเฉพาะ
- **ข้อพึงระวัง!** การถอดสายไฟอาจก่อให้เกิด :
  - ความเสียหายอย่างรุนแรงต่อระบบ
  - รบกวนการดำเนินงานทางธุรกิจ
  - เพิ่มภาระความรับผิดชอบให้แก่หน่วยงานและพนักงานเจ้าหน้าที่

4. เครื่องคอมพิวเตอร์พกพาที่ไม่ได้เปิดใช้งาน (Laptop Turn-off)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้อง กันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและสายเชื่อมต่ออื่นๆ
- ชุดตรวจค้นและรวบรวมพยานหลักฐานบันทึกรายละเอียดของเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน
- ชุดเทคนิคและการถ่ายภาพ ดาเนินการถ่ายภาพพยานหลักฐานอย่างชัดเจนโดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อของอุปกรณ์ และ รุ่นของอุปกรณ์ (Model) (ถ้ามี) ถ่ายภาพสายไฟและสายเชื่อมต่อตลอดจนอุปกรณ์ต่อพ่วงต่างๆ (DVD-Drive และ External Drive) ให้ครบถ้วนชัดเจนเพื่อแสดงถึงสภาพของพยานหลักฐานเมื่อเข้าเก็บหลักฐาน
- ถอดแบตเตอรี่ออกจากตัวเครื่อง
- ถอดสายไฟและสายเชื่อมต่อ ตลอดจนอุปกรณ์ต่อพ่วงออกจากเครื่องคอมพิวเตอร์
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) บริเวณจุดเชื่อมต่ออุปกรณ์ เช่น ช่องเชื่อมต่อสายไฟ ช่องเชื่อมต่อ USB ช่องเชื่อมต่อ Mouse และ Keyboard เป็นต้น

- ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพพยานหลักฐานที่ถูกปิดเทปปนเปื้อนพยานหลักฐานเรียบร้อยแล้ว เพื่อแสดงถึงสภาพของพยานหลักฐานที่เจ้าหน้าที่ได้ทำการจัดเก็บ

- ชุดตรวจค้นและรวบรวมพยานหลักฐานบรรจุอุปกรณ์คอมพิวเตอร์ลงในบรรจุภัณฑ์เฉพาะด้านอ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ

- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานหลังจากบรรจุภัณฑ์เรียบร้อยแล้ว

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน

- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยาน หลักฐานลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

5. กรณีตรวจค้นเครื่องคอมพิวเตอร์พกพาที่เปิดใช้งาน (Laptop Turn-on)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว

- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลาดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและสายเชื่อมต่ออื่นๆ

- ในกรณีที่เครื่องคอมพิวเตอร์พกพาไม่ได้ทาการเปิดหน้าจอ ให้ชุดตรวจค้นและรวบรวมพยานหลักฐานเปิดหน้าจอแสดงผล เพื่อให้ชุดเทคนิคและการถ่ายภาพถ่ายหน้าจอของเครื่องคอมพิวเตอร์

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ทำสำเนาหน่วยความจำ (Memory Dump)

- ถอดแบตเตอรี่ออกจากตัวเครื่องเพื่อป้องกันการทำงานในโหมดแบตเตอรี่

- ถอดสายไฟด้านจากเครื่องคอมพิวเตอร์พกพาในทันที ตลอดจนอุปกรณ์ต่อพ่วงออกจากเครื่องคอมพิวเตอร์ โดยไม่อนุญาตให้ทำการ Shut-down ระบบ

- ชุดตรวจค้นและรวบรวมพยานหลักฐานบันทึกรายละเอียดของเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน

- ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพพยานหลักฐานอย่างชัดเจนโดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อของอุปกรณ์ และ รุ่นของอุปกรณ์ (Model) (ถ้ามี) ถ่ายภาพสายไฟ

และสายเชื่อมต่อตลอดจนอุปกรณ์ต่อพ่วงต่างๆ (DVD-Drive และ External Drive) ให้ครบถ้วนชัดเจน เพื่อแสดงถึงสภาพของพยานหลักฐานเมื่อเข้าเก็บหลักฐาน

- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) บริเวณจุดเชื่อมต่ออุปกรณ์ เช่น ช่องเชื่อมต่อสายไฟ ช่องเชื่อมต่อ USB ช่องเชื่อมต่อ Mouse และ Keyboard เป็นต้น

- ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพพยานหลักฐานที่ถูกปิดเทปกันการปนเปื้อนพยานหลักฐานเรียบร้อยแล้ว เพื่อแสดงถึงสภาพของพยานหลักฐานที่เจ้าหน้าที่ได้ทำการจัดเก็บ

- ชุดตรวจค้นและรวบรวมพยานหลักฐานบรรจุอุปกรณ์คอมพิวเตอร์ลงในบรรจุภัณฑ์เฉพาะด้าน อ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ

- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานหลังจากบรรจุภัณฑ์เรียบร้อยแล้ว

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน

- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงานเพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

6. สื่อบันทึกข้อมูล (Storage Media)

สิ่งที่ควรรู้เบื้องต้น : สื่อบันทึกข้อมูลถูกใช้เพื่อเก็บข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์บางชนิดมีพื้นที่ความจุที่ตายตัวในตัวของมันเองแต่ในบางครั้งก็จำเป็นต้องมีการถ่ายโอนข้อมูลขึ้นมา อุปกรณ์จำนวนมากในปัจจุบันสามารถที่จะเก็บข้อมูลลงภายในพื้นที่ความจุของตัวเองและยังสามารถเก็บข้อมูลลงในสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Removable media) อีกด้วย สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้นั้นใช้ได้ทั้งเพื่อทำการถ่ายโอนข้อมูลและเพื่อเก็บข้อมูลไว้ในตัวเอง

สื่อบันทึกเหล่านี้มีหลายรูปแบบและมีการใช้งานเป็นจำนวนมาก สื่อบันทึกข้อมูลจำนวนมากที่ใช้ในปัจจุบันไม่สามารถพบเห็นได้โดยทั่วไปแม้จะมีการนำมาใช้อยู่มากในตลาดของสื่อเป็นประจำ และถึงแม้ว่าสื่อบันทึกจะมีมาตรฐานการใช้งานอยู่บ้าง แต่ก็ยังพบเห็นได้ง่ายและใช้งานได้ดี เช่น สื่อบันทึกข้อมูลใช้สำหรับเก็บข้อมูลจากอุปกรณ์คอมพิวเตอร์ต่าง ๆ

- Floppy Disk - CD (Compact Disk) - DVD (Digital Video Disk)
- MD (Mini Disc) - Ls-120 (Super Disk) - Zip

- Click - Memory Stick
- Jaz
- Flash memory card - Smart media
- Removable hard drive
- External hard drive - Micro-drive
- Magneto optical drive
- DLT tape - DAT (Digital audio tape) - DLT tape
- HiFD (High Density Floppy Disk)

การเก็บยึด

- เก็บยึดคู่มือการใช้งาน เอกสารและบันทึกโน้ตย่อต่างๆ
- จดบันทึกการกระทำทุกขั้นตอนที่เกี่ยวข้องในการเก็บยึดสื่อบันทึกข้อมูล (บันทึกเวลาตามขั้นตอนถ่ายรูปตามลำดับเวลา ถ่ายวิดีโอ บรรยาย)
- เก็บวัตถุพยานทุกชนิด ให้ห่างจากแม่เหล็กเครื่องรับส่งวิทยุ และสิ่งที่อื่นๆ ที่อาจก่อให้เกิดความเสียหายได้

7. กรณีตรวจค้นโทรศัพท์เคลื่อนที่และอุปกรณ์สื่อสาร (Mobile Phone)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว
- หากอุปกรณ์นั้นเปิดอยู่ห้ามปิดอุปกรณ์ และหากอุปกรณ์นั้นปิดอยู่ห้ามเปิดอุปกรณ์
- ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพพยานหลักฐานอย่างชัดเจนโดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อของอุปกรณ์ และ รุ่นของอุปกรณ์ (Model) (ถ้ามี) เพื่อแสดงถึงสภาพของพยานหลักฐานเมื่อเข้าเก็บหลักฐาน
- โดยให้ถ่ายหน้าจอเครื่องให้ชัดเจน และบันทึกวิดีโอตลอดกระบวนการปฏิบัติงาน
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกรายละเอียดของคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน
- ตรวจสอบสถานะของแบตเตอรี่คงเหลือ และจัดหาแหล่งจ่ายไฟหากจาเป็น
- บรรจุโทรศัพท์เคลื่อนที่และอุปกรณ์สื่อสารลงในบรรจุภัณฑ์เฉพาะด้าน อ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานหลังจากบรรจุลงบรรจุภัณฑ์เรียบร้อยแล้ว
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ตรวจความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน พร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน

- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

8. โทรสาร (Facsimile Machines)

- หากเครื่อง “ปิด” อยู่ “ห้ามเปิด” เครื่อง
- หากเครื่อง “เปิด” อยู่ให้ปฏิบัติดังต่อไปนี้
- การปิดเครื่องอาจทำให้สูญเสียหมายเลขล่าสุดที่เครื่องโทรสารนั้นทำการส่งข้อความออกไปถึงได้ หรือทำให้สูญเสียข้อมูลที่เก็บไว้ในเครื่องโทรสารไปได้ ควรศึกษาคู่มือการใช้งานก่อนการปิดเครื่องหากทำได้
- ทำการจดบันทึกข้อมูลที่ถูกบันทึกไว้ในเครื่องก่อนทำการปิดเครื่อง
- ถ่ายภาพเก็บไว้
- ควรทำการยึดอุปกรณ์และคู่มือการใช้งานทั้งหมดหากทำได้

9. บัตรสมาร์ทการ์ดและบัตรแถบแม่เหล็ก (Smart Cards & Magnetic Stripe Cards)

- ถ่ายภาพบัตรเก็บไว้
- ชื่อและลักษณะเฉพาะของบัตร
- ตรวจสอบการดัดแปลงบัตรและข้อสงสัยใดๆ ที่พบระหว่างการตรวจสอบ
- ตรวจสอบว่าใครคือผู้ครอบครองบัตรและพบบัตรนั้นที่ใด

10. สแกนเนอร์ (Scanners)

- ทำการตรวจสอบว่าเครื่องสแกนเนอร์ได้เชื่อมต่อกับเครือข่ายอยู่หรือไม่ ใช้เป็นเครื่องเดียวโดยไม่ต้องต่อกับเครือข่ายหรือไม่ หรือสามารถพกพาได้หรือไม่
- เครื่องสแกนเนอร์บางรุ่นสามารถใช้เป็นเครื่องถ่ายเอกสาร เครื่องปรินเตอร์และเครื่องโทรสารได้ด้วย
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมทั้งสายไฟมาทั้งหมดด้วย
- หากเครื่อง “เปิด” อยู่การปิดเครื่องอาจเป็นสาเหตุให้เกิดการสูญหายของข้อมูลได้

11. เครื่องปรินเตอร์ (Printers)

- หากเครื่อง “เปิด” อยู่การปิดเครื่องอาจเป็นสาเหตุให้เกิดการสูญหายของข้อมูลได้
- ทำการตรวจสอบว่าเครื่องพิมพ์บัตรได้เชื่อมต่อกับเครือข่ายอยู่หรือไม่ ใช้เป็นเครื่องเดียวโดยไม่ ต้องต่อกับเครือข่ายหรือไม่ หรือสามารถพกพาได้หรือไม่
- จดบันทึกหมายเลขโทรศัพท์ที่เครื่องปรินเตอร์ทำการเชื่อมต่ออยู่
- จดบันทึกหมายเลขโทรศัพท์ของเครือข่ายที่เครื่องปรินเตอร์ทำการเชื่อมต่ออยู่
- เครื่องปรินเตอร์บางรุ่นสามารถใช้เป็นเครื่องถ่ายเอกสาร สแกนเนอร์ และโทรสารได้ด้วย
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมทั้งสายไฟมาทั้งหมดด้วย

12. เครื่องถ่ายเอกสาร (Copiers)

- หากเครื่อง “เปิด” อยู่การปิดเครื่องอาจเป็นสาเหตุให้เกิดการสูญหายของข้อมูลได้
- ทำการตรวจสอบว่าเครื่องถ่ายเอกสารได้เชื่อมต่อกับเครือข่ายอยู่หรือไม่ ใช้เป็นเครื่องเดียวโดยไม่ต้องต่อกับเครือข่ายหรือไม่ หรือสามารถพกพาได้หรือไม่
- จดบันทึกหมายเลขโทรศัพท์ที่เครื่องถ่ายสำเนาทำการเชื่อมต่ออยู่
- จดบันทึกหมายเลขโทรศัพท์ของเครือข่ายที่เครื่องถ่ายสำเนาทำการเชื่อมต่ออยู่
- เครื่องถ่ายสำเนาบางรุ่นสามารถใช้เป็นเครื่องปรินเตอร์ สแกนเนอร์ และโทรสารได้ด้วย
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมทั้งสายไฟมาทั้งหมดด้วย

13. เครื่องทำสำเนาแผ่นซีดีและเครื่องพิมพ์ฉลาก (Compact Disk Duplicators and Labelers)

- หากเครื่อง “เปิด” อยู่การปิดเครื่องอาจเป็นสาเหตุให้เกิดการสูญหายของข้อมูลที่ถูกบันทึกอยู่ในเครื่องทั้ง 2 ชนิดนี้ได้
- ทำการตรวจสอบว่าเครื่องทำสำเนาแผ่นซีดีได้เชื่อมต่อกับเครือข่ายอยู่หรือไม่ใช้เป็นเครื่องเดียวโดยไม่ต้องต่อกับเครือข่ายหรือไม่ หรือสามารถพกพาได้หรือไม่
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้องรวมทั้งสายไฟมาทั้งหมดด้วย
- เครื่องปั๊มแผ่นบางเครื่องสามารถที่จะเก็บอิมเมจลงในฮาร์ดไดร์ฟได้

14. กล้องถ่ายภาพและกล้องวิดีโอ (Camera and Video Camera)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว

- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและสายเชื่อมต่ออื่นๆ

- ชุดตรวจค้นและรวบรวมพยานหลักฐานบันทึกรายละเอียดของอุปกรณ์ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ถอดแบตเตอรี่และหน่วยจัดเก็บข้อมูล (Memory Card) ออกจากตัวเครื่อง

- บรรจุสื่อจัดเก็บข้อมูลดิจิตอลลงในบรรจุภัณฑ์เฉพาะด้าน อ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ

- ชุดเทคนิคและการถ่ายภาพ ดาเนินการถ่ายภาพพยานหลักฐานอย่างชัดเจนโดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อของอุปกรณ์ และ รุ่นของอุปกรณ์ (Model) **(**ถ้ามี) ถ่ายภาพสายไฟและสายเชื่อมต่อตลอดจนอุปกรณ์ต่อพ่วงต่างๆ ให้ครบถ้วนชัดเจน เพื่อแสดงถึงสภาพของพยานหลักฐานเมื่อเข้าเก็บหลักฐาน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน

- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

15. เครื่องเล่นเกม (Electronic Game Devices)

- หากเครื่อง “ปิด” อยู่ “ห้ามเปิด” เครื่อง

- หากเครื่อง “เปิด” อยู่ให้ปรึกษาผู้ชำนาญการเพื่อการดำเนินการต่อไป

- กรณีที่ไม่สามารถขอคำแนะนำจากผู้ชำนาญการได้ ให้ถ่ายภาพอุปกรณ์ไว้ (เช่น จอแสดงภาพ) แล้วทำการถอดสายไฟต่างๆ ด้านหลังเครื่องออกให้หมด หากไม่สามารถทำได้ให้นำกลับไปปรึกษาผู้ชำนาญการในทันทีที่สามารถกระทำได้

- แปะเทปสำหรับแปะพยานหลักฐาน (Evidence tape) บริเวณช่องเสียบไดร์ฟ (drive slots) ช่องเสียบสื่อบันทึกข้อมูล (media slots) หรือช่องใส่แผ่นเกม เป็นต้น
- ทำการถ่ายภาพ เขียนแผนผัง และฉลากของอุปกรณ์ซึ่งแสดงการเชื่อมต่อจริงในขณะนั้น
- ติดฉลากบนชิ้นส่วนสายไฟ สายเคเบิ้ลทั้งหมด เพื่อสะดวกต่อการประกอบชิ้นส่วนใหม่หากมีความจำเป็น
- หากจำเป็นต้องทำการเคลื่อนย้ายอุปกรณ์ให้ทำการขนส่งอย่างระมัดระวัง และกระทบกระเทือนน้อยที่สุด
- ความล่าช้าในการตรวจสอบ อาจทำให้ข้อมูลที่มีอยู่หายไปได้หากแบตเตอรี่หมด
- ใช้ความระมัดระวังในการเก็บรักษาและเคลื่อนย้าย เช่น ไม่ควรเก็บในที่มีความร้อนสูงหรือในที่ที่มีความชื้นหรือความเย็น เป็นต้น
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมทั้งสายไฟมาทั้งหมดด้วย

16. เครื่องระบุตำแหน่ง (Global Positioning System: GPS)

- หากเครื่อง “ปิด” อยู่ “ห้ามเปิด” เครื่อง
- หากเครื่อง “เปิด” อยู่ให้ปรึกษาผู้ชำนาญการเพื่อการดำเนินการต่อไป
- กรณีที่ไม่สามารถขอคำ แนะนำ จากผู้ชำนาญการได้ ให้ถ่ายภาพอุปกรณ์ไว้ (เช่น จอแสดงภาพ) แล้วทำการถอดสายไฟต่างๆ ทางด้านหลังเครื่องออกให้หมด หากไม่สามารถทำได้ให้นำกลับไปปรึกษาผู้ชำนาญการในทันทีที่สามารถกระทำได้
- แปะเทปสำหรับแปะพยานหลักฐาน (Evidence tape) บริเวณช่องเสียบไดร์ฟ (drive slots) หรือช่องเสียบสื่อบันทึกข้อมูล (media slots) เป็นต้น
- ทำการถ่ายภาพ เขียนแผนผัง และฉลากของอุปกรณ์ซึ่งแสดงการเชื่อมต่อจริงในขณะนั้น หากจำเป็นต้องทำการเคลื่อนย้ายอุปกรณ์ให้ทำการขนส่งอย่างระมัดระวัง และกระทบกระเทือนน้อยที่สุด
- ความล่าช้าในการตรวจสอบ อาจทำให้ข้อมูลที่มีอยู่หายไปได้หากแบตเตอรี่หมด
- พิจารณาว่าเครื่องมือชนิดนี้เป็นเครื่องมือที่สามารถพกพาได้หรือไม่
- ใช้ความระมัดระวังในการเก็บรักษาและเคลื่อนย้าย เช่น ไม่ควรเก็บในที่มีความร้อนสูงหรือในที่ที่มีความชื้นหรือความเย็น เป็นต้น
- ควรทำการเก็บยึดคู่มือการใช้งานทั้งหมดของเครื่องและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง รวมทั้งสายไฟมาทั้งหมดด้วย
- ควรให้ความใส่ใจต่อความสามารถในการเข้าถึงระบบจากระยะไกล เนื่องจากระบบดังกล่าวนี้ มักทำการเชื่อมต่อกับบริษัทผู้ให้บริการ ข้อมูลต่างๆ ที่ต้องการ อาจจะไม่ได้ถูกบันทึกไว้ในระบบหรืออุปกรณ์นั้นก็ได้

- GPS สามารถพบได้ในลักษณะที่สามารถพกพาไปในที่ต่างๆ ได้ และบางชนิดอาจจะอยู่ในรูปของปาล์ม มินิโน้ตบุ๊ค โน้ตบุ๊ค และกล้องดิจิตอล เป็นต้น

17. เครื่องอ่านบัตรแถบแม่เหล็ก (Skimmers/Parasites) และอุปกรณ์เทคโนโลยีในการประกอบอาชญากรรมชนิดอื่นๆ (Other Criminal Technology)

- เครื่องอ่านบัตรแถบแม่เหล็ก พยานหลักฐานที่อาจพบ
    - หมายเลขบัตรเครดิตที่ถูกขโมย
    - ข้อมูลของเหยื่อที่บ่งชี้ถึงตัวเหยื่อ
    - CVC และ CVV Numbers ซึ่งสามารถทำให้ใช้บัตรนั้นได้
- วิธีปฏิบัติในการเปิดและปิดเครื่อง
    - อย่าพยายามเคลื่อนย้ายแบตเตอรี่หรือเปลี่ยนแบตเตอรี่
    - อย่าแตะปุ่มหรือสวิชต์ บางส่วนของอุปกรณ์มีลักษณะเป็นสิ่งที่ไวต่อการสัมผัสซึ่งอาจทำลายพยานหลักฐานที่มีได้
    - ควรรีบตรวจสอบอุปกรณ์ชนิดนี้เพื่อป้องกันการสูญเสียข้อมูล
- อุปกรณ์เทคโนโลยีที่ใช้ในการประกอบอาชญากรรม
    - อุปกรณ์ที่ใช้ประกอบอาชญากรรมโดยทั่วไปนั้นอาชญากรมักจะกระทำขึ้นเองซึ่งอาจเสียหายได้ง่าย ตัวอุปกรณ์เปล่านี้ถูกพัฒนาขึ้นมาเพื่อจุดประสงค์หลักในการดำเนินการฉ้อโกง หลอกลวงระบบด้วยวิธีการต่างๆ
- หลักเกณฑ์การเปิด/ปิด
    - อย่าพยายามเคลื่อนย้ายแบตเตอรี่หรือเปลี่ยนแบตเตอรี่
    - อย่าแตะปุ่มหรือสวิชต์ บางส่วนของอุปกรณ์มีลักษณะเป็นสิ่งที่ไวต่อการสัมผัสซึ่งอาจทำลายพยานหลักฐานที่มีได้
    - ควรรีบตรวจสอบอุปกรณ์ชนิดนี้เพื่อป้องกันการสูญเสียข้อมูล

18. กรณีตรวจค้นเอกสารหรือสิ่งพิมพ์ (Document) ให้ปฏิบัติดังต่อไปนี้

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพเอกสารและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลาดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและสายเชื่อมต่ออื่นๆ และบันทึกวิดีโอตลอดกระบวนการปฏิบัติงาน
- ชุดตรวจค้นและรวบรวมพยานหลักฐานบันทึกรายละเอียดของสิ่งพิมพ์ (ขนาด, สี และเนื้อหาบางส่วน) ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน
- บรรจุเอกสารในบรรจุภัณฑ์เฉพาะด้าน อ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ

- ชุดเทคนิคและการถ่ายภาพ ดาเนินการถ่ายภาพพยานหลักฐานหลังจากบรรจุลงบรรจุภัณฑ์เรียบร้อยแล้ว

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน

- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

3.9 การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ (Crime Scene Evidence Package Management)

ด้วยเหตุที่ว่าพยานหลักฐานนั้นมีความสำคัญต่อการสืบสวนเป็นอย่างมาก ดังนั้นการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงและปราศจากการปนเปื้อนจึงถือเป็นหัวใจสำคัญของการรวบรวมพยานหลักฐานในสถานที่เกิดเหตุ ดังนั้นการบรรจุพยานหลักฐานลงในบรรจุภัณฑ์ที่ถูกต้องจึงถือเป็นสิ่งที่ต้องปฏิบัติอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าชุดปราบปราม
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape)
- ป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag)
- กล้องถ่ายภาพดิจิตอล (Digital Camera) และกล้องบันทึกวิดีโอ (Video Camera)
- ชุดป้องกันไฟฟ้าสถิต (Anti-Static Suit) และถุงมือป้องกันไฟฟ้าสถิต (Anti-Static Gloves)
- กล้องป้องกันไฟฟ้าสถิต (Anti-Static Drive Box) และกระเป๋าภาคสนาม (Field Bag)
- ถุงพลาสติกสำหรับเก็บพยานหลักฐาน (Plastic Evidence Bag)
- ถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดเล็ก (Paper Evidence Bag)
- ถุงป้องกันคลื่นวิทยุ (Faraday Container)

3.10 ขั้นตอนการปฏิบัติเพื่อบรรจุพยานหลักฐานลงบรรจุภัณฑ์ในสถานที่เกิดเหตุ (Crime Scene Evidence Package Protocol)

3.10.1 ชุดตรวจค้นและรวบรวมพยานหลักฐาน บรรจุหลักฐานในลงบรรจุภัณฑ์เฉพาะด้านทันที หลังจากปฏิบัติตาม ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในที่เกิดเหตุ เรียบร้อยแล้ว

3.10.2 บรรจุพยานหลักฐานลงบรรจุภัณฑ์ตามความเหมาะสมของพยานหลักฐาน โดยให้ความสำคัญกับสิ่งต่อไปนี้เป็นพิเศษ

1) เครื่องคอมพิวเตอร์ (Computer Case)

- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) บริเวณช่องเชื่อมต่ออุปกรณ์
- บรรจุตัวเครื่องคอมพิวเตอร์ลงในถุงดาหรือถุงพลาสติกขนาดใหญ่
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบถุงให้มิดชิด
- ปิดป้ายแสดงหมวดและลาดับพยานหลักฐาน (Evidence Tag) พร้อมลงลายมือชื่อผู้เก็บรวบบรวมหลักฐานให้ชัดเจน

2) คอมพิวเตอร์พกพา (Laptop/Tablet)

- ถอดแบตเตอรี่ออกจากตัวเครื่องหากยังไม่ได้ถอด
- ปิดป้ายแสดงหมวดและลาดับพยานหลักฐาน (Evidence Tag) บนตัวเครื่อง พร้อมลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- บรรจุตัวเครื่องลงในซองป้องกันคลื่นวิทยุ (Faraday Container)
- บรรจุแบตเตอรี่ลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดกลาง-ใหญ่ (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- บรรจุตัวเครื่องลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดใหญ่ (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

3) ฮาร์ดดิสก์ (Hard Disk)

- บรรจุฮาร์ดดิสก์ลงในกล่องป้องกันไฟฟ้าสถิต (Anti-Static Drive Box)
- ปิดป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag) บนกล่องป้องกันไฟฟ้าสถิต (Anti-Static Drive Box) พร้อมลงลายมือชื่อผู้รวบรวมให้ชัดเจน
- บรรจุกล่องป้องกันไฟฟ้าสถิตลงในกระเป๋าภาคสนามอีกชั้นหนึ่ง

4) อุปกรณ์เก็บข้อมูลพกพา (Flash Drive/USB Drive)

- บรรจุสื่อจัดเก็บข้อมูลพกพาลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดเล็ก (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

- บรรจุถุงพลาสติกสำหรับเก็บพยานหลักฐานลงในถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดเล็ก (Paper Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

5) สายไฟและสายเชื่อมต่อ (Power Cable/UTP Cable)

- บรรจุสายไฟและสายเชื่อมตาอลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดกลาง-ใหญ่ (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด
- บรรจุถุงพลาสติกสำหรับเก็บพยานหลักฐานลงในถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดกลาง-ใหญ่ (Paper Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

6) กล้องถ่ายภาพและกล้องวิดีโอ (Camera and Video Camera)

- บรรจุกล้องลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดกลาง (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- บรรจุลงแบตเตอรี่และการ์ดหน่วยความจาในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดเล็ก (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด
- บรรจุถุงพลาสติกสำหรับเก็บพยานหลักฐานลงในถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดกลาง (Paper Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

7) สื่อเก็บข้อมูลดิจิตอล (Digital Media)

- บรรจุสื่อจัดเก็บข้อมูลดิจิตอลลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดกลาง-ใหญ่ (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้
เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด
- บรรจุถุงพลาสติกสำหรับเก็บพยานหลักฐานลงในถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดกลาง-ใหญ่ (Paper Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

8) สื่อสิ่งพิมพ์ (Document)

- บรรจุสื่อสิ่งพิมพ์ลงในถุงพลาสติกสำหรับเก็บพยานหลักฐานขนาดเล็ก - กลาง - ใหญ่ (Plastic Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

- บรรจุถุงพลาสติกสำหรับเก็บพยานหลักฐานลงในถุงกระดาษสำหรับเก็บพยานหลักฐานขนาดเล็ก-กลาง-ใหญ่ (Paper Evidence Bag) พร้อมบันทึกรายละเอียด และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) รอบปากถุงให้มิดชิด

3.11 การบริหารจัดการขนส่งพยานหลักฐาน (Evidence Transportation Management)

หนึ่งในปัจจัยสำคัญของการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐานนั้นก็คือ การขนส่งพยานหลักฐานจากสถานที่เกิดเหตุไปยังห้องปฏิบัติการ ซึ่งมีปัจจัยที่ต้องให้ความสาคัญซึ่งอาจส่งผลต่อพยานหลักฐานได้ดังนั้นการขนส่งพยานหลักฐานจึงต้องปฏิบัติตามขั้นตอนอย่างเคร่งครัด การขนส่งเคลื่อนย้ายพยานหลักฐาน ต้องใช้ยานพาหนะที่เหมาะสม และระมัดระวังไม่ก่อให้เกิดความเสียหายต่อพยานหลักฐาน จัดทำรายการพยานหลักฐานให้ครบถ้วน

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าชุดปราบปราม
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน
- ชุดขนส่งและคุ้มครองพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- รถขนส่งพยานหลักฐาน

3.11.1 ขั้นตอนการปฏิบัติเพื่อจัดการขนส่งพยานหลักฐานกลับสู่ห้องปฏิบัติการ (Evidence Transportation Protocol)

1) ชุดตรวจค้นและรวบรวมพยานหลักฐาน ตรวจสอบความถูกต้องของพยานหลักฐานทั้งหมด และลงลายมือชื่อผู้ส่งในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ก่อนนำส่งต่อชุดขนส่งและคุ้มครองพยานหลักฐาน

2) ให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ดำเนินการตรวจสอบหลักฐานและเอกสารต่างๆ ให้ครบถ้วน พร้อมลงลายมือชื่อผู้รับในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ครบถ้วน

3) ให้หัวหน้าชุดปราบปราม ตรวจสอบความพร้อมและเอกสารอีกครั้ง ก่อนออกคำสั่งเพื่อขนส่งพยานหลักฐานไปยังห้องปฏิบัติการ

4) ให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ดำเนินการค้นหาเส้นทางในการขนส่งพยานหลักฐานที่เหมาะสมและปลอดภัยต่อพยานหลักฐาน โดยคำนึงถึงปัจจัยสาคัญที่อ้างอิงตามหัวข้อปัจจัยสำคัญที่ต้องให้ความสำคัญระหว่างการขนส่งพยานหลักฐาน

5) ขนส่งพยานหลักฐานไปยังห้องปฏิบัติการ

3.11.2 ปัจจัยสำคัญที่ต้องให้ความสำคัญระหว่างการขนส่งพยานหลักฐาน

1) การขนส่งพยานหลักฐานต้องใช้รถขนส่งพยานหลักฐานที่ได้รับการออกแบบมาโดยเฉพาะ

2) หลีกเลี่ยงการใช้งานคลื่นวิทยุหรืออุปกรณ์ใดๆ ที่อาจก่อให้เกิดคลื่นวิทยุและคลื่นสนามแม่เหล็ก

3) หลักเลี่ยงเส้นทางที่มีเสาไฟฟ้าแรงสูง หรือมีคลื่นสนามแม่เหล็กแรงสูง

3.12 การบริหารจัดการและจัดเก็บพยานหลักฐาน (Evidence Retention Management)

หนึ่งในปัจจัยสำคัญของการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐานที่ได้รับจากสถานที่เกิดเหตุนั้น คือการจัดเก็บและรักษาสภาพของพยานหลักฐานในห้องเก็บพยานหลักฐาน ซึ่งมีปัจจัยที่ต้องให้ความสำคัญซึ่งและต้องปฏิบัติตามขั้นตอนอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน
- ชุดดูแลห้องเก็บพยานหลักฐาน
- ชุดขนส่งและคุ้มครองพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- ตู้เก็บพยานหลักฐาน

3.12.1 ขั้นตอนการปฏิบัติเพื่อจัดเก็บพยานหลักฐาน (Evidence Retention Protocol)

1) ชุดขนส่งและคุ้มครองพยานหลักฐาน ส่งพยานหลักฐานให้ชุดดูแลห้องเก็บพยานหลักฐาน พร้อมลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดดูแลห้องเก็บพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

2) ชุดดูแลห้องเก็บพยานหลักฐาน ทำการบันทึกข้อมูลรายการหลักฐานที่ได้รับลงในเอกสารการจัดเก็บหลักฐาน (Evidence Retention Form) พร้อมลงลายมือชื่อ

3) หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน ตรวจสอบความพร้อมและเอกสารการจัดเก็บหลักฐานพร้อมลงลายมือชื่อรับรองความถูกต้อง

3.12.2 กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐานในฐานะผู้รับผิดชอบห้องเก็บพยานหลักฐาน จำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

1) ความถูกต้องครบถ้วนของพยานหลักฐานที่จัดเก็บ เทียบกับรายการตามเอกสาร

2) ความถูกต้องสมบูรณ์ทางกายภาพของพยานหลักฐานในปัจจุบัน เทียบกับข้อมูลสภาพของหลักฐานเมื่อได้รับมา

3.13 การเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน (Computer Forensic Tools and Equipment Preparation)

3.13.1 การจัดเตรียมเครื่องมือสำหรับการตรวจวิเคราะห์หลักฐาน

การตรวจวิเคราะห์พยานหลักฐานถือเป็นกระบวนการสำคัญในการสืบสวนสอบสวนอาชญากรรมที่เกี่ยวกับเทคโนโลยี เนื่องจากพยานหลักฐานทางอิเล็กทรอนิกส์มีเอกลักษณ์และแตกต่างจากพยานหลักฐานชนิดอื่น จึงต้องมีกระบวนการที่เหมาะสมและและต้องใช้เครื่องมืออุปกรณ์เฉพาะทางที่มีคุณภาพ ดังนั้นการจัดเตรียมอุปกรณ์เครื่องมือก่อนดำเนินการตรวจวิเคราะห์หลักฐาน จึงถือเป็นสิ่งจำเป็นที่ต้องปฏิบัติอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน
- เจ้าหน้าที่ประจำห้องปฏิบัติการ

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เครื่องมือและโปรแกรมสำหรับการทำสำเนาหลักฐาน
- เครื่องมือและโปรแกรมสำหรับการตรวจวิเคราะห์หลักฐาน
- สื่อจัดเก็บสำเนาข้อมูล
- เอกสารการปฏิบัติงาน

3.13.2 ขั้นตอนการปฏิบัติเพื่อจัดเตรียมเครื่องมือสำหรับการตรวจวิเคราะห์หลักฐานและการทดสอบ (Computer Forensic Tools Preparation and Testing Protocol)

1) เจ้าหน้าที่ประจำห้องปฏิบัติการ ตรวจสอบความถูกต้องและครบถ้วนของเครื่องมือที่ต้องใช้งานในแต่ละคดี

2) เจ้าหน้าที่ประจำห้องปฏิบัติการ ทดสอบความถูกต้องของโปรแกรมโดยการตรวจสอบคุณสมบัติเบื้องต้น (Function) และตรวจสอบลิขสิทธิ์ (License) ของแต่ละซอฟต์แวร์

3) เจ้าหน้าที่ประจำห้องปฏิบัติการตรวจสอบและจัดเตรียมอุปกรณ์สำหรับการจัดทำสำเนาหลักฐาน

4) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน ควบคุมดูแลกระบวกการปฏิบัติงานและตรวจสอบความถูกต้องพร้อมลงลายมือชื่อรับรอง

3.13.3 กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐานในฐานะผู้รับผิดชอบห้องห้องปฏิบัติการวิเคราะห์หลักฐานจำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของเครื่องมือและซอฟต์แวร์ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

1) เครื่องมือและซอฟต์แวร์สามารถใช้งานได้เป็นปกติ
2) เครื่องมือและซอฟต์แวร์มีลิขสิทธิ์ที่ถูกต้อง

3.14 การทำลายข้อมูลในสื่อเก็บข้อมูล (Media Sanitization and Cleaned Evidence Preparation)

3.14.1 การทำลายข้อมูลด้วยวิธีการเขียนทับในสื่อเก็บข้อมูล

การทำลายข้อมูลด้วยวิธีการเขียนทับ (Wiping) ถือเป็นกระบวนการสำคัญในการรับรองความถูกต้องของสื่อเก็บข้อมูล เพื่อให้แน่ใจว่าจะไม่มีข้อมูลเดิมจากหลักฐานในคดีอื่นๆ หลงเหลืออยู่ในสื่อจัดเก็บข้อมูลดังกล่าว ซึ่งจะทำให้กระบวนการในการตรวจพิสูจน์หลักฐานมีความถูกต้อง โปร่งใสและน่าเชื่อถือ จึงต้องมีการจัดทำขั้นตอนการทำลายข้อมูลด้วยวิธีการเขียนทับในสื่อเก็บข้อมูลขึ้น

ผู้ปฏิบัติที่เกี่ยวข้อง

- หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน
- เจ้าหน้าที่ประจำห้องปฏิบัติการ

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เครื่องมือและซอฟต์แวร์สำหรับการทำลายข้อมูลด้วยวิธีการเขียนทับ
- สื่อจัดเก็บสำเนาข้อมูล
- เอกสารการปฏิบัติงาน

3.14.2 ขั้นตอนการปฏิบัติเพื่อจัดเตรียมเครื่องมือสำหรับการตรวจวิเคราะห์หลักฐานและการทดสอบ (Media Sanitization Protocol)

1) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน จัดทำรายการสื่อเก็บข้อมูลที่มีความจำเป็นต้องใช้งานหรือสำรองไว้ใช้งานในอนาคต

2) เจ้าหน้าที่ประจำห้องปฏิบัติการ รวบรวมสื่อเก็บข้อมูลตามรายการจาก หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน

3) เจ้าหน้าที่ประจำห้องปฏิบัติการ เชื่อมต่อสื่อเก็บข้อมูลเข้ากับเครื่องมือหรือซอฟต์แวร์สำหรับการทำลายข้อมูล

4) เจ้าหน้าที่ประจำห้องปฏิบัติการ ทำลายข้อมูลในสื่อเก็บด้วยวิธีการเขียนทับข้อมูลที่ใช้เลขศูนย์ (Zerorization)

5) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน ควบคุมดูแลกระบวกการปฏิบัติงานและตรวจสอบความถูกต้องอย่างใกล้ชิด พร้อมออกรายงานผลการปฏิบัติงานและลงลายมือชื่อรับรอง

6) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน ตรวจสอบรายงานผลการทำลายข้อมูลพร้อมลงลายมือชื่อรับรอง

ข้อควรจำ :

บทบาทของเครื่องคอมพิวเตอร์ (Role of the computer)

- หมายค้นควรต้องระบุว่าเครื่องคอมพิวเตอร์นั้นมีบทบาทอย่างไรในการกระทำความผิดและทำไมจะต้องเก็บยึดมา

ความสำคัญ (Nexus)

- ระบุว่าเหตุใดจึงคิดว่าจะพบพยานหลักฐานอิเล็กทรอนิกส์ในที่ที่จะไปตรวจค้น
- ระบุลักษณะพยานหลักฐานที่จะทำการตรวจค้น (Specify evidence sought)
- ระบุรายละเอียดพยานหลักฐานที่ต้องทำการตรวจค้นรวมถึงพยานหลักฐานอื่นๆ ที่อาจอยู่ในเครื่องคอมพิวเตอร์นั้น

คำพูดกำกวม (Boiler plate language)

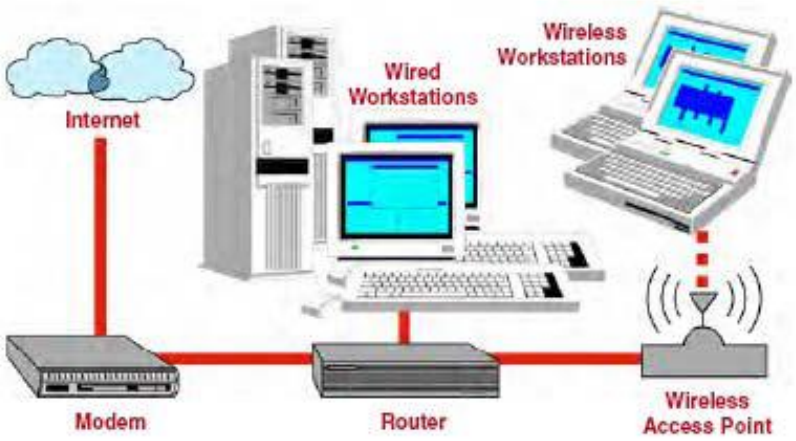
- ปรับใช้คำพูดที่เข้ากับข้อเท็จจริงในคดีนั้น หลีกเลี่ยงการใช้คำพูดที่ไม่ชัดเจน คลุมเครือ ไม่เปิดเผย (Non-Disclosure)
- อาจมีความจำเป็นต้องป้องกันความถูกต้องเที่ยงตรงของการสืบสวนสอบสวน โดยต้องปกป้องผู้ให้ข้อมูล รักษาความลับทางการค้าหรือทรัพย์สินทางปัญญา

Special Master

- การพิจาณาตามกฎหมายพิเศษเกี่ยวกับแพทย์ นักกฎหมาย คู่สามีภรรยา นักหนังสือพิมพ์และนักศาสนา เป็นต้น

3.15 องค์ประกอบพื้นฐานของระบบเน็ตเวิร์คในบ้าน (Home Network Basic Elements)

ตามที่เห็นในภาพ เน็ตเวิร์คภายในบ้านมักประกอบด้วยโมเด็ม เราท์เตอร์และเครื่องคอมพิวเตอร์ตั้งโต๊ะหรือแล็ปท็อป



ภาพที่ 4-27 เน็ตเวิร์คภายในบ้านพักอาศัย

จุดประสงค์โดยทั่วไปในการใช้งานระบบเครือข่ายภายในบ้านเรือนนั้น คือ ให้เครื่องคอมพิวเตอร์หลายๆ ตัวแชร์การใช้งานอินเทอร์เน็ตกัน เช่น ระบบ DSL ซึ่งระบบเครือข่ายภายในบ้านนี้ยังช่วยให้ผู้ใช้งานหลายๆ คนสามารถแชร์ข้อมูลกับเครื่องคอมพิวเตอร์เครื่องอื่นที่อยู่ภายในเน็ตเวิร์คได้

เมื่อต้องดำเนินการกับเครื่องระบบเครือข่ายคอมพิวเตอร์ภายในบ้านในที่เกิดเหตุ เราจะต้องทำการตัดการเชื่อมต่อกับอินเทอร์เน็ตทันทีที่สามารถทำได้ ซึ่งสามารถทำได้โดยการดึงสายพาวเวอร์ออกจากโมเด็มและ/หรือเราท์เตอร์

ข้อพึงระวัง ! ในหลายๆ กรณีที่พบว่าระบบเครือข่ายภายในบ้านนั้น ทำการเชื่อมต่อกันอยู่โดยใช้ไวร์เลสเราท์เตอร์หรือแอคเซสพอยท์ ซึ่งง่ายต่อการเก็บซ่อน

นอกจากนี้ หลายๆ กรณีที่พบว่าระบบเครือข่ายภายในบ้านเรือนยังทำงานเป็นออฟฟิศเล็กๆ ด้วย หากพบกรณีเช่นว่านี้ ควรทำการติดต่อผู้เชี่ยวชาญเฉพาะ และขอให้มาให้การช่วยเหลือในที่เกิดเหตุในการเก็บยึดพยานหลักฐานทางคอมพิวเตอร์และอิเล็กทรอนิกส์

3.16 รายการอุปกรณ์และเครื่องมือสำหรับการปฏิบัติงาน

เนื่องจากอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีนั้นมีการเปลี่ยนแปลงรูปแบบและวิธีการใหม่ๆ อยู่ตลอดเวลาดังนั้นหน่วยงานที่เกี่ยวข้องจึงจาเป็นต้องมีการพัฒนาและจัดเตรียมเครื่องมือที่ทันสมัย เพื่อให้สามารถดำเนินการสืบสวนสอบสวนอาชญากรรมได้อย่างรวดเร็วและมีประสิทธิภาพ และด้วยเหตุนี้จึงต้องมีการกำหนดรายการอุปกรณ์และเครื่องมือมาตรฐานประจาหน่วยงาน โดยมีรายละเอียด ดังนี้

3.16.1 อุปกรณ์สำหรับงานเก็บรวบรวมหลักฐาน (Electronic Crime Investigation Materials)

1) เครื่องคอมพิวเตอร์ภาคสนามสำหรับตรวจวิเคราะห์หลักฐาน (Computer Forensic Laptop)
2) เครื่องคอมพิวเตอร์วางตักสำหรับตรวจวิเคราะห์หลักฐาน (Forensic Tablet)
3) อุปกรณ์ป้องกันการเขียนทับข้อมูลภาคสนาม (Write-blocker Field Kit)
4) อุปกรณ์ตรวจวิเคราะห์โทรศัพท์เคลื่อนที่ภาคสนาม (Mobile Phone Forensic Field Kit)
5) อุปกรณ์ตรวจวิเคราะห์โทรศัพท์เคลื่อนที่จีนภาคสนาม (Chinese Phone Forensic)
6) ซองบรรจุหลักฐานแบบป้องกันคลื่นวิทยุ (Faraday Container)
7) ซองพลาสติกบรรจุหลักฐานอิเล็กทรอนิกส์ (Plastic Evidence Bag)
8) กล้องบรรจุฮาร์ดดิสก์แบบป้องกันไฟฟ้าสถิต (Anti-Static Drive Box)
9) เทปปิดกันพื้นที่เกิดเหตุ (Crime Scene Tape)
10) เทปปิดซองบรรจุหลักฐาน (Evidence Sealing Tape)
11) ป้ายปิดพยานหลักฐาน (Evidence Tag)
12) สื่อเก็บข้อมูลสำหรับบันทึกหลักฐาน

3.16.2 อุปกรณ์สำหรับงานตรวจวิเคราะห์หลักฐาน (Computer Forensic Laboratory Equipment)

1) เครื่องคอมพิวเตอร์สำหรับตรวจวิเคราะห์หลักฐาน (Computer Forensic Workstation)
2) อุปกรณ์ตรวจวิเคราะห์โทรศัพท์เคลื่อนที่ (Mobile Phone Forensics)
3) อุปกรณ์ตรวจวิเคราะห์โทรศัพท์เคลื่อนที่จีน (Chinese Phone Forensic)
4) อุปกรณ์ทำสำเนาหลักฐาน (Forensic Disk Duplicator)
5) อุปกรณ์ทำลายข้อมูลดิจิตอล (Digital Media Sanitizer)
6) อุปกรณ์เสริมศักยภาพการถอดรหัสลับ (Password Decryption Accelerator)
7) เสื้อและถุงมือป้องกันไฟฟ้าสถิต (Anti-Static Gloves and Anti-Static Suits)

3.16.3 ซอฟต์แวร์สำหรับงานตรวจวิเคราะห์หลักฐาน (Computer Forensic Software)

1) ซอฟต์แวร์ที่มีความสามารถในวิเคราะห์ข้อมูลจากสำเนาหลักฐานในรูปแบบ DD (Raw) ได้
2) ซอฟต์แวร์ที่มีคุณสมบัติในการวิเคราะห์และแสดงข้อมูลในรูปแบบเลขฐาน 16 (HEX) ได้
3) ซอฟต์แวร์ที่มีคุณสมบัติในการกู้คืนข้อมูลที่ถูกลบไปแล้วได้
4) ซอฟต์แวร์ที่มีคุณสมบัติในการวิเคราะห์ข้อมูลประวัติการใช้งาน Internet ได้
5) ซอฟต์แวร์ที่มีคุณสมบัติในการวิเคราะห์ข้อมูล Registry ได้

3.17 ห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์

ห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์ ถือเป็นหัวใจสำคัญของการตรวจวิเคราะห์หลักฐานทางอิเล็กทรอนิกส์ เนื่องจากการดำเนินกิจกรรมต่างๆ ต้องอยู่ภายใต้สภาพแวดล้อมที่เหมาะสมและปลอดภัยทั้งต่อพยานหลักฐานและเจ้าหน้าที่ผู้ปฏิบัติงาน ดังนั้นห้องปฏิบัติการฯ ควรจะมีลักษณะทางกายภาพในด้านต่างๆ ดังนี้

3.17.1 ข้อกำหนดด้านสภาพแวดล้อมของห้องปฏิบัติการ

1) อุณหภูมิต้องไม่ต่ำกว่า 25 องศาเซลเซียส
2) ระดับความชื้นสัมพัทธ์อยู่ระหว่าง 40-55%

3.17.2 ข้อกำหนดด้านความปลอดภัยทางด้านกายภาพของห้องปฏิบัติการ

1) ระบบป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต (Digital Door Lock)
2) ระบบตรวจสอบและเฝ้าระวัง (Video Surveillance)
3) ระบบทะเบียนบันทึกประวัติการเข้าปฏิบัติงานของเจ้าหน้าที่ (Log Book)
4) ระบบตรวจจับควันไฟและระบบดับเพลิงโดยใช้ก๊าซ (Fire Alarm and Suppression)
5) ระบบตรวจจับผู้บุกรุก

3.17.3 มาตรฐานบุคลากรและความรับผิดชอบ (Forensic Officer and Responsibility)

ด้วยเหตุที่ว่าอาชญากรรมที่เกี่ยวกับเทคโนโลยีนั้น ถือเป็นอาชญากรรมที่มีความซับซ้อนและแตกต่างไปจากอาชญากรรมในรูปแบบอื่น เนื่องจากอาชญากรรมดังกล่าวนั้นเกี่ยวข้องและสัมพันธ์กับระบบเครือข่ายและเทคโนโลยีคอมพิวเตอร์อยู่เสมอ จึงทำให้การสืบสวนและสอบสวนอาชญากรรมในลักษณะนี้จำเป็นต้องอาศัยเจ้าหน้าที่ผู้เชี่ยวชาญ ที่มีความรู้และความเข้าใจในเทคโนโลยีคอมพิวเตอร์และเครือข่าย เพื่อให้สามารถดำเนินการสืบสวนและสอบสวนได้อย่างมีประสิทธิภาพสมบูรณ์ ดังนั้นจึงต้องมีการกำหนดตำแหน่งและคุณสมบัติการพิจารณาเจ้าหน้าที่ขึ้น เพื่อใช้เป็นมาตรฐานในการคัดเลือกบุคลากรของหน่วยงานต่อไป

3.17.4 ความรับผิดชอบและคุณสมบัติของเจ้าหน้าที่

1) หัวหน้าห้องปฏิบัติการ (Computer Forensic Laboratory Manager)

หัวหน้าห้องปฏิบัติการมีหน้าที่บริหารจัดการและกำกับดูแลห้องปฏิบัติการวิเคราะห์หลักฐานให้สามารถดำเนินงานได้อย่างมีประสิทธิภาพ ถูกต้องสมบูรณ์และโปร่งใส และต้องมีทักษะและความชำนาญในการบริหารจัดการงานตรวจวิเคราะห์หลักฐานที่ได้รับการร้องขอจากหน่วยงานอื่น

คุณสมบัติขั้นพื้นฐานของหัวหน้าห้องปฏิบัติการ

1.1) มีประสบการณ์ด้านการตรวจวิเคราะห์หลักฐานและการบริหารงานคดีอย่างน้อย 2 ปี

1.2) มีความรู้ความเข้าใจในด้านนิติเวชวิทยาศาสตร์คอมพิวเตอร์และอุปกรณ์ดิจิตอลเป็นอย่างดี

1.3) มีความรู้ความเข้าใจในด้านคอมพิวเตอร์และระบบเครือข่าย (Computer OS, File System, Network Communication System) เป็นอย่างดี

1.4) มีความรู้ความเข้าใจในหลักห่วงโซ่ผู้ครอบครองพยานหลักฐาน (Chain of Custody) เป็นอย่างดี

1.5) มีความรู้และทักษะในการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์ไม่น้อยกว่า 15 คดี

1.6) มีความรู้และทักษะในการเก็บรวบรวมพยานหลักฐานในสถานที่เกิดเหตุไม่น้อยกว่า 20 คดี

1.7) ผ่านการอบรมหลักสูตรการวิเคราะห์หลักฐานอิเล็กทรอนิกส์

1.8) ผ่านการอบรมหลักสูตรการบริหารจัดการห้องปฏิบัติการ

2) เจ้าหน้าที่วิเคราะห์หลักฐาน (Computer Forensics Examiner)

เจ้าหน้าที่วิเคราะห์หลักฐานมีหน้าที่ตรวจวิเคราะห์พยานหลักฐานตามที่ได้รับการร้องขอจากหน่วยงานภายนอก เจ้าหน้าที่ฯ ต้องให้ความสำคัญกับความถูกต้องของพยานหลักฐานและข้อเท็จจริงจากการตรวจวิเคราะห์เป็นที่สุด

คุณสมบัติขั้นพื้นฐานของเจ้าหน้าที่วิเคราะห์หลักฐาน

2.1) มีความรู้ความเข้าใจในด้านนิติเวชวิทยาศาสตร์คอมพิวเตอร์และอุปกรณ์ดิจิตอลเป็นอย่างดี

2.2) มีความรู้ความเข้าใจในด้านคอมพิวเตอร์และระบบเครือข่าย (Computer OS, File System, Network Communication System) เป็นอย่างดี

2.3) มีความรู้ความเข้าใจในหลักห่วงโซ่ผู้ครอบครองพยานหลักฐาน (Chain of Custody) เป็นอย่างดี

2.4) มีความรู้และทักษะในการเก็บรวบรวมพยานหลักฐานในสถานที่เกิดเหตุไม่น้อยกว่า 5 คดี

2.5) มีความรู้และทักษะในการใช้งานโปรแกรมตรวจวิเคราะห์หลักฐานคอมพิวเตอร์เป็นอย่างดี

2.6) ผ่านการอบรมหลักสูตรการตรวจวิเคราะห์หลักฐาน

2.7) ผ่านการอบรมหลักสูตรการเก็บรวบรวมพยานหลักฐาน

3) เจ้าหน้าที่เก็บรวบรวมพยานหลักฐาน (Electronic Crime Scene Investigator)

เจ้าหน้าที่เก็บรวบรวมพยานหลักฐานมีหน้าที่ในการเก็บรวบรวมพยานหลักฐานในสถานที่เกิดเหตุ ซึ่งเป็นหน่วยแรกที่เข้าถึงพยานหลักฐาน และมีหน้าที่รักษาและสงวนไว้ซึ่งความถูกแท้จริงของพยานหลักฐานในขณะปฏิบัติงาน

คุณสมบัติขั้นพื้นฐาน

3.1) มีความรู้ความเข้าใจในด้านนิติเวชวิทยาศาสตร์คอมพิวเตอร์และอุปกรณ์ดิจิตอลเป็นอย่างดี

3.2) มีความรู้ความเข้าใจในด้านคอมพิวเตอร์และระบบเครือข่าย (Computer OS, File System, Network Communication System) เป็นอย่างดี

3.3) มีความรู้ความเข้าใจในหลักห่วงโซ่ผู้ครอบครองพยานหลักฐาน (Chain of Custody) เป็นอย่างดี

3.4) ผ่านการอบรมหลักสูตรการเก็บรวบรวมพยานหลักฐาน ไม่น้อยกว่า 24 ชม.

บทที่ 5
สรุปผลการศึกษา และข้อเสนอแนะ

ในการศึกษาวิจัยเรื่อง การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมเทคโนโลยี มีวัตถุประสงค์เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมทั้งกำหนดรูปแบบและขั้นตอนในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและสร้างองค์ความรู้ละการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรกมทางเทคโนโลยี ข้อมูลที่ได้รับจากการทบทวนวรรณกรรม รวมทั้งแนวคิดและทฤษฎีงานวิจัยที่เกี่ยวข้อง โดยใช้ระเบียบวิธีวิจัยทางคุณภาพ การประชุมกลุ่มย่อย และการสัมภาษณ์เจาะลึก จากผู้ทรงคุณวุฒิที่มีความรู้และความชำนาญงาน ทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี จากหน่วยงานต่างๆ ซึ่งข้อมูลที่ได้รับจะเกิดประโยชน์ต่อการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องต่างๆ คณะผู้วิจัยจึงขอสรุปผลการวิจัย และข้อเสนอแนะ ดังต่อไปนี้

1. สรุปผลการวิจัย

ในการศึกษาได้มีการประชุมกลุ่มย่อยจากผู้ทรงคุณวุฒิ จำนวน 3 ครั้ง สัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลที่สำคัญที่เป็นผู้ทรงคุณวุฒิจากหน่วยงานต่างๆ เช่น สำนักงานอธิบดีผู้พิพากษาภาค 7 สำนักงานอัยการพิเศษฝ่ายคดีอาญา 2 สำนักงานอัยการสูงสุด ผู้แทนจากกรมสอบสวนคดีพิเศษ ผู้แทนจากกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม ผู้แทนจากสำนักงานเทคโนโลยีสารสนเทศ ผู้แทนจากหน่วยงานสอบสวนสังกัดกองบัญชาการตำรวจนครบาล ผู้แทนจากพนักงานสอบสวนสังกัดกองบัญชาการตำรวจภูธร และผู้เชี่ยวชาญการพิสูจน์หลักฐานทางอาชญากรรมไซเบอร์ ศูนย์พิสูจน์หลักฐาน 7 สำนักงานพิสูจน์หลักฐานตำรวจ ในประเด็นต่าง ๆ ดังนี้

1) การศึกษาพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

แนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น คือ

(1) ด้านบุคลากร พบว่า สตช.ยังขาดแคลนบุคลากรที่มีความรู้ ความสามารถในการดำเนินคดีอาชญากรรมทางเทคโนโลยีเป็นอย่างยิ่ง แต่ทราบว่า สตช.ได้พยายามเพิ่มอัตรากำลัง และฝึกอบรมบุคลากรด้านนี้เพิ่มเติมอยู่ ควรมีการกำหนดกรอบอัตราจำนวนที่เพียงพอต่อการปฏิบัติหน้าที่และกระจายบุคลากรออกไปในส่วนภูมิภาคอย่างทันต่อเหตุการณ์มิใช่กระจุกตัวอยู่ในส่วนกลาง

(2) ด้านการฝึกอบรม พบว่า การจัดอบรมให้กับเจ้าหน้าที่ตำรวจยังมีน้อย เมื่อเทียบกับความจำเป็นเร่งด่วนในการสร้างบุคลากรให้ทันต่อการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ควรจัดให้มีการอบรม

ตามรอบระยะเวลาที่เหมาะสมมีหลักสูตรระดับต้น กลาง สูง เพื่อสริมสร้างทักษะความรู้ต่างๆ ให้ทันต่อเหตุการณ์ การเรียนรู้ อาจมีทั้งการอบรมหรือศึกษาด้วยตนเอง

(3) ด้านงบประมาณ พบว่า ควรเพิ่มงบประมาณให้เพียงพอแก่การประชาสัมพันธ์ให้ประชาชนได้รับทราบให้มากที่สุด สื่อที่ใช้ควรมีหลายรูปแบบ เพื่อให้เข้าถึงประชาชนทุกกลุ่ม

(4) ด้านเครื่องมือ และอุปกรณ์ พบว่า สตช.ยังขาดแคลนงบประมาณในการจัดหาเครื่องมือ และอุปกรณ์ ให้เพียงพอต่อการดำเนินคดีอาชญากรรมทางเทคโนโลยี ในภูมิภาคต่างๆ ทั่วประเทศ ควรเพิ่มอุปกรณ์เครื่องมือทำงานสืบสวนหาทางจัดเก็บวัตถุพยานต่างๆ ให้มีประสิทธิภาพ น่าเชื่อถือเป็นไปตามมาตรฐานของต่างประเทศ ข้อมูลหรือผลลัพธ์ที่ได้ สามารถนำไปใช้ได้ต่างได้ทั่วโลก

(5) ด้านเทคโนโลยี พบว่า สตช.ควรนำเทคโนโลยีใหม่ ๆ มาช่วยเจ้าหน้าที่ตำรวจทั้งด้านสืบสวน และสอบสวน เพื่อลดภาระในการทำงาน โดยเฉพาะในปัจจุบันที่เทคโนโลยีการสื่อสาร และการทำธุรกรรมต่างๆ ทำให้พยานหลักฐานแต่ละเรื่อง กระจายอยู่ในหลายท้องที่ ซึ่งมีความยุ่งยากในการรวบรวม รวมทั้งควรมีการติดตั้งปรับปรุง Software ที่ทันสมัยมากกว่าอาชญากรรมคอมพิวเตอร์ เพื่อให้พัฒนาขีดความสามารถได้เท่าทันอาชญากรรมเทคโนโลยี

(6) ด้านบริหารการจัดการ พบว่า ผู้บังคับบัญชาควรมีความรู้พื้นฐานเกี่ยวกับเรื่องอาชญากรรมทางคอมพิวเตอร์ เพื่อที่จะได้เข้าใจการทำงานของผู้ใต้บังคับบัญชา และเป็นผู้ให้คำชี้แนะแก่ผู้ใต้บังคับบัญชาหากเกิดปัญหาขัดข้อง

(7) ด้านโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า มีการกำหนดนโยบายที่ชัดเจน มีเป้าหมายที่แน่นอนมีแนวทางปฏิบัติหน้าที่เป็นขั้นเป็นตอนสอดคล้องกับนโยบายหลัก เพื่อให้การขับเคลื่อนขององค์กรเป็นไปในทิศทางเดียวกัน

(8) ด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน พบว่า การมีส่วนร่วมของหน่วยงานภาครัฐอื่น และภาคเอกชน มีความสำคัญในการช่วยเหลือเจ้าหน้าที่ตำรวจทั้งฝ่ายสืบสวน และสอบสวนได้มาก แต่ค่านิยมของคนไทย และสภาพสังคม ทำให้หน่วยงานภาครัฐอื่น และภาคเอกชน มักมองว่าเป็นหน้าที่ของเจ้าหน้าที่ตำรวจแต่เพียงฝ่ายเดียว ขาดการใส่ใจช่วยเหลือ ทั้งกรณีที่เป็นหน้าที่ตามกฎหมาย และกรณีที่สมควรจะช่วยเหลือได้ แม้ไม่มีหน้าที่โดยตรง การใช้มาตรการทางสังคมที่จะส่งเสริมให้ภาคเอกชน เข้ามามีส่วนร่วมในการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ตำรวจ จะช่วยเสริมประสิทธิภาพในการดำเนินคดีได้ มีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐทุกแห่งที่มีส่วนเกี่ยวข้อง รวมทั้งมีการบูรณาการร่วมกันระหว่างภาครัฐและภาคประชาชนหรือภาคเอกชน จะได้มุมมองที่กว้างและเป็นการรับฟังความคิดเห็นของภายนอกด้ว

(9) ด้านการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยี และด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า ในระยะเร่งด่วน ควรสร้างองค์ความรู้พื้นฐานของคดีอาชญากรรมทางเทคโนโลยีประเภทต่างๆ แบบสำเร็จรูป ให้ง่ายต่อการทำความเข้าใจ และมีตัวอย่าง คำแนะนำ และแนวทางแก้ปัญหาให้เจ้าหน้าที่ตำรวจในหน่วยงานย่อยท้องที่ต่างๆ สามารถศึกษาและจัดการคดีอาชญากรรมทางเทคโนโลยีในระดับที่ไม่ยุ่งยากซับซ้อนด้วยตัวเองได้ ในระยะยาว ควรเพิ่มเติมองค์ความรู้เฉพาะทางของคดี

อาชญากรรมทางเทคโนโลยีประเภทต่างๆ ให้แก่หน่วยงานเฉพาะด้านของ สตช. ที่มีภารกิจเฉพาะด้าน และหน่วยงานในท้องถิ่น เพื่อรับมือกับคดีอาชญากรรมทางเทคโนโลยีทุกระดับที่จะเพิ่มปริมาณขึ้นในอนาคต รวมถึงการสร้างบุคลากรของหน่วยงานให้สามารถเติบโตได้อย่างมีความพร้อมในการปฏิบัติหน้าที่ และมีขวัญกำลังใจเพื่อทำงานในหน่วยงานเฉพาะด้านระยะยาวได้ และการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยีให้มีอิสระสามารถขับเคลื่อนองค์กรไปได้ตามภารกิจให้เกิดประสิทธิภาพสูงสุด บุคลากรของหน่วยงานควรได้รับการส่งเสริมให้มีความก้าวหน้าในหน่วย ตำแหน่งบริหารของหน่วยงาน ควรเป็นบุคลากรภายใน เพื่อเป็นขวัญกำลังใจของคนในหน่วย

จากการศึกษาการปฏิบัติงานของหน่วยงานทางด้านอาชญากรรมทางเทคโนโลยีของต่างประเทศ พบว่ามีขยายออกทั่วประเทศ คณะผู้วิจัยจึงมีความเห็นว่า ในการพัฒนางานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยการปรับปรุงโครงสร้างหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีใน 3 ระดับ คือ

(1) หน่วยงานระดับสถานีตำรวจ – เพิ่มงานพนักงานสอบสวน ผู้เชี่ยวชาญทางด้านอาชญากรรมทางเทคโนโลยีอยู่ในงานสอบสวนในสถานีตำรวจ

(2) หน่วยงานระดับกองบัญชาการ คือ กองบังคับการอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และกองบังคับการอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ขยายหน่วยงานเป็นกองบัญชาการอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.) ขยายหน่วยงานออกเป็นศูนย์ ซึ่งเป็นหน่วยงานเทียบเท่ากองบังคับการ ออกสู่ส่วนภูมิภาคเป็น 10 ศูนย์ คือ ศูนย์ ปอทศ. 1 (ปทุมธานี) ศูนย์ ปอทศ. 2 (ชลบุรี) ศูนย์ ปอทศ. 3 (นครราชสีมา) ศูนย์ ปอทศ. 4 (ขอนแก่น) ศูนย์ ปอทศ. 5 (ลำปาง) ศูนย์ ปอทศ. 6 (พิษณุโลก) ศูนย์ ปอทศ. 7 (นครปฐม) ศูนย์ ปอทศ. 8 (สุราษฎร์ธานี) ศูนย์ ปอทศ. 9 (สงขลา) และศูนย์ ปอทศ. 10 (ยะลา) เช่น เดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

(3) หน่วยงานศูนย์พิสูจน์หลักฐาน สำนักงานพิสูจน์หลักฐานตำรวจ พบว่า ทางสำนักงานพิสูจน์หลักฐานได้ดำเนินการวางแผนทางด้านบุคลากร และเครื่องมือสำหรับตรวจพิสูจน์ โดยมีบุคลากรที่ปฏิบัติงานทั้ง 11 แห่งไว้ครบแล้ว แต่อุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์มีเพียง 3 แห่ง คือ กองพิสูจน์หลักฐานกลาง, ศูนย์พิสูจน์หลักฐาน 7 (นครปฐม) และศูนย์พิสูจน์หลักฐาน 10 (ยะลา) เท่านั้น ยังคงขาดเครื่องมือสำหรับตรวจพิสูจน์ที่ศูนย์พิสูจน์หลักฐานอีก 8 แห่ง จึงควรสนับสนุนงบประมาณในการจัดซื้ออุปกรณ์และเครื่องมือสำหรับการตรวจพิสูจน์ให้ครบทั้ง 11 แห่ง

2) การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญงานทางด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์การกำหนดรูปแบบขั้นตอนที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีรายละเอียดและสาระสำคัญโดยสรุป คือ ภัยคุกคามความปลอดภัยข้อมูลเกี่ยวกับอาชญากรรม ขั้นตอนการบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการรวบรวม

พยานหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการบริหารจัดการและขนส่งพยานหลักฐาน ขั้นตอนการบริหารจัดการและจัดเก็บพยานหลักฐาน ขั้นตอนการเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน แนวทางคำถามสำหรับคดีด้านอาชญากรรมทางเทคโนโลยี และการตรวจพิสูจน์อาชญากรรมทางเทคโนโลยี

3) องค์ความรู้และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

จากการทบทวนวรรณกรรม การประชุมกลุ่มย่อยและสัมภาษณ์เชิงลึกจากผู้ที่มีความรู้ความชำนาญทางด้านการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี ได้ทำการสังเคราะห์องค์ความรู้ และคู่มือในการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีรายละเอียด และสาระสำคัญโดยสรุป คือ สภาพการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ วิธีการและขั้นตอนการสืบสวนและสอบสวนเกี่ยวกับอาชญากรรมทางเทคโนโลยี กฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี รายการอาชญากรรมทางเทคโนโลยี และพยานหลักฐานทางดิจิตอล หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ แนวทางบริหารจัดการและจัดเก็บพยานหลักฐาน ปัญหาข้อขัดข้องในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ การบริหารจัดการเพื่อรักษาสภาพสถานที่เกิดเหตุ การปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในสถานที่เกิดเหตุ ขั้นตอนการปฏิบัติเพื่อบรรจุพยานหลักฐานลงบรรจุภัณฑ์ในสถานที่เกิดเหตุ การบริหารจัดการขนส่งพยานหลักฐาน การบริหารจัดการและจัดเก็บพยานหลักฐาน การเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน การทำลายข้อมูลในสื่อเก็บข้อมูล องค์ประกอบพื้นฐานของระบบเน็ตเวิร์คในบ้าน รายการอุปกรณ์และเครื่องมือสำหรับการปฏิบัติงาน และห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์

2. ข้อเสนอแนะ

2.1 ข้อเสนอแนะเชิงนโยบาย

2.1.1 รัฐบาลควรมีนโยบายโดยการใช้มาตรการทางสังคมที่ส่งเสริมให้ภาคเอกชนเข้ามามีส่วนร่วมในการสนับสนุนการปฏิบัติหน้าที่ของเจ้าหน้าที่ โดยมีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐและภาคประชาชน หรือภาคเอกชน เช่น ปัญหาในเรื่องการขอข้อมูลจากผู้ให้บริการประเภทต่าง ๆ ทั้งที่เกี่ยวกับระบบคอมพิวเตอร์ และธุรกรรมการเงินที่โต้แย้งอำนาจเจ้าหน้าที่ของรัฐอย่างไม่สมเหตุสมผล หรือให้ข้อมูลล่าช้า หรือปฏิเสธการให้ข้อมูลรวมทั้งการเรียกรับค่าใช้จ่ายจากเจ้าหน้าที่ของรัฐ ฯลฯ อาจหามาตรการจูงใจต่าง ๆ เพื่อให้ผู้บริการเต็มใจให้ความร่วมมือกับเจ้าหน้าที่ของรัฐ เช่น การให้คำรับรองหรือประกาศชมเชยว่าเป็นหน่วยงานที่มีความรับผิดชอบทางสังคม

2.1.2 รัฐควรมีนโยบายหรือใช้มาตรการทางภาษีให้กับหน่วยงานที่ให้บริการ หากให้ความร่วมมือกับเจ้าหน้าที่ อาจให้มีสิทธิในการนำไปคิดเป็นค่าใช้จ่าย โดยลดภาษีให้ หากไม่ให้ความร่วมมือกับเจ้าหน้าที่

หรือให้ความร่วมมือล่าช้า อาจใช้กฎหมายสรรพากรไปใช้บังคับ ในกรณีที่ผู้ให้บริการไม่ให้ความร่วมมือ ถูกเรียกเก็บภาษีเพิ่ม หรือถูกปรับทางภาษีเพิ่มเติม

2.1.3 รัฐบาลควรมีนโยบายให้มีการบูรณาการร่วมกันอย่างชัดเจนระหว่างหน่วยงาน เพราะหน่วยงานที่ปฏิบัติงานทางด้านป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีหลายหน่วยงานทั้ง กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม เช่น ให้กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคมออกกฎหมายรองรับการทำงานของเจ้าหน้าที่ตำรวจ รวมทั้งให้หน่วยงานที่เกี่ยวข้องปรับปรุงภารกิจ และความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง การเสนอขอแก้ไขกฎหมายข้อบังคับ ระเบียบที่เกี่ยวข้อง ให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี

2.1.4 รัฐบาลควรมีนโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยมีการกำหนดนโยบายที่มีความชัดเจน รวมทั้งมีการวิเคราะห์บทบาทของหน่วยงานให้สอดคล้องกับการปฏิบัติงานจริง เพื่อให้การขับเคลื่อนขององค์กรเป็นไปในทิศทางเดียวกัน โดยเฉพาะการแก้ไขกฎหมายเพิ่มเติมขีดความสามารถ และอำนาจที่จะให้เข้าถึงข้อมูลต่าง ๆ ด้านเทคโนโลยีให้กับเจ้าหน้าที่ได้อย่างรวดเร็ว เพื่อป้องกันปราบปรามและสืบสวนการกระทำผิด

2.1.5 รัฐบาลควรมีนโยบายให้ปรับปรุงโครงสร้างหน่วยงานที่ปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของสำนักงานตำรวจแห่งชาติใน 3 ระดับ คือ

(1) หน่วยงานระดับสถานีตำรวจ เพิ่มงานพนักงานสอบสวนผู้เชี่ยวชาญด้านอาขญากรรมทางเทคโนโลยี โดยรับจากผู้มีวุฒิทางด้านคอมพิวเตอร์เข้ามาปฏิบัติงานอยู่ในสถานีตำรวจ

(2) กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (ปอท.) ปรับปรุงโครงสร้างเป็นกองบัญชาการ โดยขยายออกเป็นส่วนภูมิภาค 10 ศูนย์ เช่นเดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

(3) สำนักงานพิสูจน์หลักฐานตำรวจ เพิ่มงบประมาณในการจัดซื้อเครื่องมือสำหรับการตรวจพิสูจน์อาชญากรรมทางเทคโนโลยีในส่วนภูมิภาคให้ครบทั้ง 10 ศูนย์ ให้สามารถช่วยพนักงานสอบสวนในการพิสูจน์หลักฐานข้อเท็จจริง รวมทั้งการกำหนดวิธีการตรวจให้รัดกุม การเก็บหลักฐานให้เป็นระบบ

2.2 ข้อเสนอแนะเชิงปฏิบัติการ

2.2.1 ในเรื่องอำนาจการสอบสวนมีปัญหามากระหว่างสถานตำรวจกับ บก.ปอท. และ บก.ปอศ. จึงควรเพิ่มเจ้าหน้าที่ลงในสถานีตำรวจรับจากผู้ที่มีความรู้จริง อย่างน้อยปริญญาตรีทางคอมพิวเตอร์ แล้วนำมาอบรม ส่วน บก.ปอท. และ บก.ปอศ. ซึ่งเป็นหน่วยงานระดับกองบังคับการ ควรขยายโครงสร้างของหน่วยงานเป็นระดับกองบัญชาการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีและเศรษฐกิจ (บช.ปอทศ.) ขยายงานออกตามส่วนภูมิภาคออกเป็น 10 ศูนย์ เช่นเดียวกับสำนักงานพิสูจน์หลักฐานตำรวจ

2.2.2 พนักงานสอบสวนยังขาดความรู้ความเข้าใจในเรื่องอาชญากรรมทางเทคโนโลยี เมื่อมีผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที เพราะไม่รู้ถึงกระบวนการในการทำงานที่เกิดขึ้น ซึ่งเป็นปัญหาใหญ่ที่จะต้องมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยี และกฎหมายที่เกี่ยวข้อง โดยเฉพาะประเด็นการตั้งคำถามของพนักงานสอบสวนเป็นเพราะขาดความรู้ ทำให้ตั้งคำถามอย่าง

ไม่มีทิศทาง ทั้งนี้ รวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติด้วย แต่อย่างไรก็ตามคณะผู้วิจัยได้จัดทำคู่มือในการปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยีให้กับเจ้าหน้าที่ผู้ปฏิบัติ ซึ่งคาดว่าน่าจะแก้ไขปัญหาในเรื่องนี้อยู่ในระดับหนึ่ง รวมถึงการจัดการฝึกอบรมในหลักสูตรต่างๆ ที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี

2.2.3 ควรจัดแบ่งคดีอาชญากรรมทางเทคโนโลยี ออกเป็นประเภทต่างๆ รวมทั้งแบ่งระดับความยากง่าย เช่น ประเภทที่การกระทำผิดอยู่ในระบบเทคโนโลยี โดยตรง (เช่น ฉ้อโกงขายสินค้าทางอินเทอร์เน็ต ลักลอบทำธุรกรรม E-Banking ฯลฯ) กับประเภทที่การกระทำผิดไม่ได้อยู่ในระบบเทคโนโลยี แต่ใช้เทคโนโลยีเฉพาะการสื่อสาร หรือการทำธุรกรรมที่เกี่ยวข้อง (เช่น การขายสิ่งของผิดกฎหมาย แล้วมีการติดต่อสื่อสารกันด้วยโทรศัพท์หรือโปรแกรมสนทนาผ่านอินเตอร์เน็ต ฯลฯ) แล้วแยกระดับความยากง่าย

- การทำแบบฟอร์มสำเร็จรูป ละกำหนดช่องทางรวบรวมพยานหลักฐานจากผู้ให้บริการต่างๆ จะช่วยให้เจ้าหน้าที่ตำรวจได้รับความสะดวกมากยิ่งขึ้น สามารถใช้กับคดีที่ไม่ยุ่งยากซับซ้อน ลดภาระค่าใช้จ่ายและระยะเวลาทำคดีได้

2.2.4 ควรจัดแบ่งเจ้าหน้าที่ออกเป็นกลุ่ม เพื่อรับมือกับคดีทางด้านอาชญากรรมทางเทคโนโลยีที่มีความยากง่ายต่างๆ กัน เช่น

(1) ระดับที่ใช้ความรู้อย่างเดียว หรือใช้เทคโนโลยีที่มีอยู่ทั่วไปในการบริหารจัดการคดีได้

(2) ระดับที่ต้องใช้เครื่องมือพิเศษที่จะต้องมีความรู้เป็นการเฉพาะในการทำงาน เช่น การใช้โปรแกรมตรวจพิสูจน์

(3) ระดับที่ต้องใช้ทั้งเครื่องมือพิเศษ และความรู้พิเศษในการจัดการคดีที่มีความยุ่งยาก ซับซ้อนทางเทคโนโลยีโดยตรง เช่น การลักลอบเข้าถึงระบบคอมพิวเตอร์ ของหน่วยงานภาครัฐ หรือสถาบันการเงินก่อความเสียหายในรูปแบบต่าง ๆ

สภาพปัญหาในส่วนนี้ คือ การแก้ไขปัญหาโดยเข้าใจว่า คดีอาชญากรรมทางเทคโนโลยีมีความยุ่งยากซับซ้อนสูง ต้องรอให้มีผู้เชี่ยวชาญพิเศษพร้อมเครื่องมือและงบประมาณจึงจะทำคดีได้ กลายเป็นว่าคดีที่ไม่มีความยุ่งยากเพียงแต่ต้องอาศัยความรู้เบื้องต้น เจ้าหน้าที่ส่วนใหญ่ก็ยังไม่สามารถทำคดี หรือวางแผนการรวบรวมพยานหลักฐานได้

2.2.5 ผู้บังคับบัญชาในแต่ละหน่วยต้องหาแนวทางในการดำเนินคดีที่มีประสิทธิภาพลดกระบวนการทำงานที่ไม่จำเป็น หรือกระบวนการที่ไม่สามารถทำได้ เช่น การขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาหลายกรณีที่ไม่ทันเวลา หรือไม่ได้รับความร่วมมือจากต่างประเทศ แล้วใช้บุคลากรดำเนินคดีด้วยแนวทางที่เหมาะสมในแต่ละสถานการณ์

2.2.6 ควรพิจารณาแนวทางการสอบสวนในรูปแบบใหม่ๆ ที่จะช่วยลดภาวะด้านเวลาค่าใช้จ่ายให้แก่เจ้าหน้าที่ฝ่ายสืบสวนและพนักงานสอบสวน เช่น

- การสอบปากคำผ่านระบบ Video Conference

- การแบ่งงานบางส่วนให้ฝ่ายสืบสวน รวยรวมพยานหลักฐานในรูปแบบที่สามารถนำไปใช้เป็นพยานหลักฐานในการทำสำนวนการสอบสวนได้

- การจัดทำแบบฟอร์มมาตรฐานในการสอบปากคำ หรือขอข้อมูลเพื่ออำนวยความสะดวกสำหรับผู้เสียหายหรือพยานตามประเภท

- การใช้เอกสารอิเล็กทรอนิกส์ที่มีความน่าเชื่อถือและชอบด้วยกฎหมาย ในการติดต่อขั้นตอนต่างๆ สามารถนำมาใช้เป็นพยานหลักฐานและมีสภาพบังคับตามกฎหมายได้

- การใช้อาสาสมัครหรือนักศึกษาฝึกงานมาช่วยให้คำแนะนำแก่ผู้เสียหายในการจัดเตรียมข้อมูลและพยานหลักฐานเบื้องต้นให้แก่พนักงานสอบสวน

2.2.7 พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์ในหลายกรณีไม่มีความน่าเชื่อถือ เนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of Custody) หน่วยงานที่เกี่ยวข้องจึงต้องมีระเบียบข้อบังคับที่ชัดเจนในการบันทึกหลักฐานตามลำดับเวลาเพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอน และพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้นๆ สำหรับในเรื่องนี้ คณะผู้วิจัยได้จัดทำคู่มือในการปฏิบัติงานของพนักงานสอบสวน รวมถึงขั้นตอนเกี่ยวกับพยานหลักฐานไว้ส่วนหนึ่ง

2.3 ข้อเสนอแนะในการวิจัยครั้งต่อไป

2.3.1 หน่วยงานที่ดำเนินคดีอาชญากรรมทางเทคโนโลยี มีมากแต่ไม่มีการช่วยเหลือกันในหน่วยงานและระหว่างหน่วยงานเพื่อแก้ไขปัญหาต่างๆ อย่างเป็นระบบ ไม่เฉพาะแต่สำนักงานตำรวจแห่งชาติที่มีปัญหา แต่หน่วยงานอื่นๆ ก็มีปัญหาเหล่านี้ ทั้ง กระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม (MDES) กรมสอบสวนคดีพิเศษ สำนักงานศาลและอัยการสูงสุด เป็นต้น จึงควรเข้าไปทำการศึกษาในเรื่องการมีส่วนร่วมระหว่างหน่วยงานที่เกี่ยวข้องเพื่อหาความเชื่อมโยง การสร้างเครือข่ายและการบูรณาการในการทำงานร่วมกันระหว่างหน่วยงาน ทำให้เกิดประสิทธิภาพของระบบการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2.3.2 ระบบการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีของต่างประเทศ ซึ่งในการศึกษาวิจัยครั้งนี้ ได้พยายามเข้าไปศึกษาถึงลักษณะการทำงานและโครงสร้างของหน่วยงานที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของต่างประเทศ ทั้งในอเมริกา ยุโรป และเอเชีย แต่ข้อมูลที่ได้อยู่ในระดับหนึ่งที่ยังไม่ละเอียดเท่าที่ควร จึงควรเข้าไปทำการศึกษาในเรื่องการป้องกันและปราบปรามอาชญากรรมเทคโนโลยีของต่างประเทศอย่างละเอียด โดยเฉพาะงานวิจัยทางด้านอาชญากรรม ทางด้านเทคโนโลยีของต่างประเทศ

2.3.3 ศึกษาถึงการวางรูปแบบในการขอข้อมูลจากหน่วยงานเอกชนที่ให้บริการประเภทต่างๆ ที่หน่วยงานรัฐประสบปัญหาทางด้านความล่าช้าและไม่ได้รับความร่วมมือ ทั้งการปฏิเสธและโต้แย้งอำนาจของเจ้าหน้าที่รัฐ ซึ่งอาจใช้มาตรการทางภาษี หรือใช้มาตรการของสรรพกร เพื่อนำมาแก้ไขปัญหา เพราะการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีที่จะได้ผลดีนั้น ต้องได้รับความร่วมมือจากหน่วยงานเอกชนที่ให้บริการ การศึกษาจะช่วยทำให้เกิดแนวทางในการปฏิบัติมากยิ่งขึ้น ส่งผลต่อประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

เอกสารอ้างอิง

กฤษฎา แสงเจริญทรัพย์. (2559). **พฤติกรรมอาชญากรในมุมมองทางจิตวิทยา: ศึกษากรณีทฤษฎีบุคลิกภาพคดี Nathan Leopold และ Richard Loeb**. วารสารกฎหมายสุขภาพและสาธารณสุข, 2(3), 381-392.

ญาณพล ยั่งยืน. **อาชญากรรมทางคอมพิวเตอร์ (Computer - Related Crime)**. สืบค้นเมื่อวันที่ มีนาคม 5, 2561 จาก http://elearning.aru.ac.th/402.7 Expiratory Blood 00108/hum07/topic3/linkfile/print5.htm.

ณรงค์ กุลนิเทศ. (2557). **เครือข่ายการจัดการความรู้อาชญากรรมคอมพิวเตอร์.** กรุงเทพฯ: สำนักงานกองทุนสนับสนุนการวิจัย.

ณรงค์ ทรัพย์เย็น และ ธงชาติ รอดคลองตัน. (2551). **คู่มือตำรวจ เล่มที่ 6 หมวดวิชาป้องกัน ปราบปรามอาชญากรรม.** กรุงเทพฯ: โรงพิมพ์ตำรวจ.

ณัฐฐ์วัฒน์ สุทธิโยธิน. (2554). “**ทฤษฎีอาชญาวิทยา**” ใน เอกสารประกอบการสอนชุด กฎหมายและอาชญาวิทยาชั้นสูง หน่วยที่ 5. นนทบุรี**:** มหาวิทยาลัยสุโขทัยธรรมาธิราช สาขานิติศาสตร์.

ทิพาวดี เมฆสวรรค์. (2538). **การส่งเสริมประสิทธิภาพในระบบราชการ**. กรุงเทพฯ

ธเนศ เกษศิลป์. (2560). **การพัฒนาต้นแบบการจัดสภาพแวดล้อมร่วมกับชุมชนเพื่อลดความเสี่ยงการเกิดอาชญากรรมในพื้นที่สถานศึกษา: กรณีศึกษาในพื้นที่มหาวิทยาลัยมหิดล วิทยาเขตศาลายา**. กรุงเทพฯ: สถาบันพระปกเกล้า.

ประเทือง ธนิยผล. (2548). **อาชญาวิทยาและทัณฑวิทยา.** มหาวิทยาลัยรามคำแหง.

ปริญญา หอมอเนก (2547). **เรียนรู้หลักการตรวจสอบระบบสารสนเทศ (IT Audit) อย่างมีประสิทธิภาพในทางปฏิบัติวิเคราะห์ปัญหาการตรวจสอบระบบสารสนเทศและการแก้ปัญหาในเชิงบูรณาการ**. eWeek Thailand. เมษายน 2547: หน้า 83.

ปุระชัย เปี่ยมสมบูรณ์ และคณะ. (2531). **อาชญากรรมพื้นฐานกับกระบวนการยุติธรรม: ปัญหาอุปสรรคและแนวทางควบคุม**. กรุงเทพฯ : ห้างหุ้นส่วนจำกัด การพิมพ์พระนคร.

ปุระชัย เปี่ยมสมบูรณ์. (2551). **อาชญากรรมพื้นฐานกับกระบวนการยุติธรรม**. กรุงเทพฯ : โครงการส่งเสริมเอกสารวิชาการ สถาบันบัณฑิตพัฒนบริหารศาสตร์.

ฝ่ายตำราวิชาการคอมพิวเตอร์. (2557). **พจนานุกรมคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ **:** ซีเอ็ดยูเคชั่น**.**

วอนชนก ไชยสุนทร. (2561). **พื้นฐานทางระบบสารสนเทศ.** กรุงเทพฯ**:** หจก. มีน เซอร์วิส ซัพพลาย.

ศิริรัตน์ ศรีสว่าง. (2558). **ปัจจัยที่ส่งผลต่อพฤตกิรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์**. สืบค้นเมื่อ พฤษภาคม 31, 2561 จาก http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5302037337_3439_1883.pdf

ศิริประภา รัตตัญญู. (2550). **กระบวนการสู่การกระทำความผิดในคดีฆาตกรรมของนักโทษประหาร.** วิทยานิพนธ์ปริญญา วิทยาศาสตรมหาบัณฑิต สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ มหาวิทยาลัยศรีนครินทรวิโรฒ.

ศิริรัตน์ ศรีสว่าง. (2558). **ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์**. วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

เศรษฐชัย ชัยสนิท. (2558). **เทคโนโลยีสารสนเทศเพื่อการจัดการอาชีพ.** กรุงเทพฯ : โสภณการพิมพ์.

สมพงษ์ เกษมสิน. (2550). **การบริหาร.** กรุงเทพฯ : ไทยวัฒนาพานิช.

สมภพ เองสมบุญ, พันตำรวจโท. (2551). **การตรวจสถานที่เกิดเหตุเบื้องต้น.** นครปฐม : โรงเรียนนายร้อยตำรวจ

สุขุม เฉลยทรัพย์ และคณะ. (2555). **เทคโนโลยีสารสนเทศ.** กรุงเทพฯ**:** คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏสวนดุสิต.

สุดสงวน สุธีสร. (2545). **อาชญาวิทยาและงานสังคมสงเคราะห์.** กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

สุพรรษา ยวงทอง. (2557). **ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ**. กรุงเทพฯ : บริษัท พิมพ์ดี จำกัด

สำนักงานส่งเสริมการค้าในต่างประเทศ ณ กรุงเฮก ประเทศเนเธอร์แลนด์. (2017). **ความปลอดภัยทางไซเบอร์.** สืบค้นเมื่อ กรกฎาคม 3, 2562 จาก https://www.ditp.go.th/contents_attach/207952/207952.pdf

อรรถพล แช่มสุวรรณวงศ์ และคณะ, พลตำรวจเอก. (2552). นิติวิทยาศาสตร์ 1 เพื่อการสืบสวนสอบสวน (พิมพ์ครั้งที่ 6). กรุงเทพฯ: เจ.บี.พี เซ็นเตอร์ จำกัด.

อรสา แนมใส, พิเชษฐ์ จันทวี และวีระชัย แสงฉาย. (2557). **การใช้คอมพิวเตอร์และอินเทอร์เน็ตที่เสี่ยงต่อการกระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ของนักศึกษามหาวิทยาลัยราชภัฏสงขลา**. สืบค้นเมื่อ พฤษภาคม 31, 2561 จาก https://ird.skru.ac.th/RMS/file/4740.pdf

โอภาส เอี่ยมสิริวงษ์. (2557). **วิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

Becker, S., & Neuhauser, D. (1975). **The Efficient Organization**. New York: ElsevierScientific.

Burke, R. H. (2009). **An Introduction to Criminological Theory**. (3rded.). Devon, UK: Willan Publishing.

Humaira Arshad, Aman Jantan, Esthe romolara. (2019). **Evidence collection and Forensics on social networks: Research challenges and directions.** Digital Investigation, 28, 126-128. Abstract retrived February 26, 2019, from https://www.sciencedirect.com/science/article/pii/S1742287618302937.

Hobson, Charles B. (1991). **Fire Investigation a new concept**. Illnois: Charles C. Tomas Publisher.

Inman, K. & Rudine N. (2002). **The Origin of evidence**. California: America.

Katz, D, and Kahn, R.L, (1978). **The social psychology of organizations** (2nd ed,), New York, Wiley. 32 Kerr, S.T.

Kirk, P.L. (1974). **Criminal Investigation**. Edited by John Thornton. New York: Wiley.

Lopez-Rey, M. (1975). **Criminological Manifesto**. Federal Probation, 39(3), 18-22.

Noora Al Mutawa, Joanne Bryce, Virginia N.L. Franqueira, Andrew Marrington, Janet C. Read. (2019). **Behavioural Digital Forensics Model: Embedding Behavioural Evidence Analysis into the Investigation of Digital Crimes**. Digital Investigation, 28,70-82. Abstract retrived February 26, 2019, from https://www.sciencedirect.com/science/article/pii/S1742287618301981.

Matthew Tart, Iain Brodie, Nicholas Gleed, James Matthews. (2012). **Historic cell site analysis – Overview of principles and survey methodologies**. Digital Investigation, 8, 185–193. Retrieved March 10, 2018, from http://www.sciencedirect.com/science/article/pii/S1742287611000867.

Modern Policing Community Policing in CSD. **แนวความคิดเกี่ยวกับการป้องกันปราบปรามอาชญากรรม**. สืบค้นเมื่อ มีนาคม 21, 2561, จาก http://csd.go.th/Dimensions_csd/Chapter%2002.pdf

Police of Japan. (2018). **Cyber Security**. Tokyo, Japan: National Police Agency.

The Australian Criminal Intelligence Commission. (2019). **Organizational Structure**. Available 25 July, 2019 from https://www.acic.gov.au/about-us/organisational- structure

Robert Lilly J. (2006). **Criminological Theory**. Northern Kentucky University.

ผู้มีคุณูปการ

การศึกษาวิจัยโครงการการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้รับการสนับสนุนจาก สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.) และได้รับความอนุเคราะห์จากบุคคลหลายฝ่าย ดังนี้

1.	พล.ต.ท.ดร.อดุลย์	ณรงค์ศักดิ์	อดีตผู้ทรงคุณวุฒิพิเศษ สำนักงานตำรวจแห่งชาติ ผู้ทรงคุณวุฒิประสานงานโครงการวิจัย สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม (สกสว.)
2.	นายอำพล	บุญประภากร	ผู้พิพากษา สำนักงานอธิบดีผู้พากษา ภาค 7
3.	นายปกรณ์	ธรรมโรจน์	อัยการจังหวัดประจำ สำนักงานอัยการพิเศษฝ่าย คดีอาญา 2 สำนักงานอัยการสูงสุด
4.	พ.ต.อ.ดร.สมศักดิ์	หน่องพงษ์	ผู้กำกับการสอบสวน ตำรวจภูธรจังหวัดลพบุรี
5.	พ.ต.อ.กัมปนาท	แสงเพ็ชร์	นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์ อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 7 สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ
6.	พ.ต.อ.นิเวศน์	อาภาวศิน	รองผู้บังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและสื่อสาร (สทส.) สำนักงานตำรวจแห่งชาติ
7.	พ.ต.อ.ประสงค์	อานมณี	รองผู้บังคับการสายตรวจและปฏิบัติการพิเศษ กองบังคับการสายตรวจและปฏิบัติการพิเศษ สำนักงานตำรวจแห่งชาติ
8.	พ.ต.ท.พัฒนะ	ศุกรสุต	ผู้เชี่ยวชาญเฉพาะด้านคดีพิเศษ กรมสอบสวนคดีพิเศษ (DSI) กระทรวงยุติธรรม
9.	นายอารีย์	จิวรรักษ์	ผู้อำนวยการกองป้องกันและปราบปรามการกระทำ ความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะผู้วิจัยขอขอบพระคุณทุกท่านเป็นอย่างสูงไว้ ณ โอกาสนี้

ผู้ช่วยศาสตราจารย์ (พิเศษ) พลตำรวจโท ดร.ณรงค์ กุลนิเทศ และคณะผู้วิจัย

กันยายน 2562

ภาคผนวก ก
แบบสัมภาษณ์และประชุมกลุ่มย่อย

โครงการวิจัย

“การพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี”

คำแนะนำ

1) แบบสัมภาษณ์และประชุมกลุ่มย่อยนี้มีจุดมุ่งหมายเพื่อศึกษาการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กำหนดรูปแบบที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี และสร้างองค์ความรู้และคู่มือการพัฒนาตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

2) แบบสัมภาษณ์และประชุมกลุ่มย่อยมีทั้งหมด 6 ส่วน ดังนี้

- **ส่วนที่ 1** ข้อมูลทั่วไปของผู้ตอบแบบสัมภาษณ์
- **ส่วนที่ 2** ประเด็นเกี่ยวกับแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรม ทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น
- **ส่วนที่ 3** ประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ
- **ส่วนที่ 4** ประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
- **ส่วนที่ 5** ประเด็นเกี่ยวกับสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี
- **ส่วนที่ 6** ข้อเสนอแนะเพิ่มเติม

3) แบบสัมภาษณ์และประชุมกลุ่มย่อยนี้ใช้เพื่อการวิจัยเท่านั้น ขอให้ท่านตอบคำถามตามความจริง ซึ่งผลที่ได้รับจากการตอบแบบสอบถามจะไม่ส่งผลกระทบใด ๆ ต่อท่าน และผู้วิจัยขอขอบพระคุณเป็นอย่างสูงที่ให้ความร่วมมือในการตอบแบบสอบถามในครั้งนี้

คณะผู้วิจัย
มหาวิทยาลัยราชภัฏสวนสุนันทา

ชื่อผู้ให้สัมภาษณ์.....

สถานที่ติดต่อ..... **โทร.** .....

วันที่ทำการสัมภาษณ์ วันที่ ..... **เดือน** ..... **พ.ศ. .....**

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสัมภาษณ์

1.1 เพศ

☐ 1) ชาย ☐ 2) หญิง

1.2 อายุ

☐ 1) 20 – 30 ปี ☐ 2) 31 – 40 ปี ☐ 3) 41 – 50 ปี
☐ 4) 51 – 60 ปี ☐ 5) 60 ปีขึ้นไป

1.3 ระดับการศึกษา

☐ 1) ต่ำกว่าปริญญาตรี ☐ 2) ปริญญาตรี ☐ 3) ปริญญาโท ☐ 4) ปริญญาเอก

1.4 ระดับชั้นยศ

☐ 1) สิบตำรวจตรี (ส.ต.ต.) ☐ 2) สิบตำรวจโท (ส.ต.ท.) ☐ 3) สิบตำรวจเอก (ส.ต.อ.)
☐ 4) จ่าสิบตำรวจ (จ.ส.ต.) ☐ 5) ดาบตำรวจ (ด.ต.) ☐ 6) ร้อยตำรวจตรี (ร.ต.ต.)
☐ 7) ร้อยตำรวจโท (ร.ต.ท.) ☐ 8) ร้อยตำรวจเอก (ร.ต.อ.) ☐ 9) พันตำรวจตรี (พ.ต.ต.)
☐ 10) พันตำรวจโท (พ.ต.ท.) ☐ 11) พันตำรวจเอก (พ.ต.อ.) ☐ 12) อื่น ๆ (ระบุ).....

1.5 ตำแหน่งของท่าน

☐ ตัวแทนของผู้บริหารหน่วยงานตำรวจ ระบุ
- ☐ สถานีตำรวจนครบาล
- ☐ สถานีตำรวจภูธร
- ☐ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

☐ พนักงานสอบสวน ระบุ
- ☐ ฝ่ายสืบสวน ฝ่ายป้องกันและปราบปรามของสถานีตำรวจนครบาล
- ☐ ฝ่ายสืบสวน ฝ่ายป้องกันและปราบปรามของสถานีตำรวจภูธร

☐ ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี

☐ อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมทางเทคโนโลยี

1.6 สังกัดของท่าน ระบุ .....

1.7 อายุราชการ จำนวน ..... ปี

1.8 ระยะเวลาในการดำรงตำแหน่งนี้ จำนวน ..... ปี

1.9 ท่านมี/ได้รับความรู้เรื่องที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีจากแหล่งใด (ตอบได้มากกว่า 1 ข้อ)

☐ 1.บุคคลบอกเล่า ☐ 2. วิทยากรบรรยายในการอบรม
☐ 3.เวทีแลกเปลี่ยน/เสวนา ☐ 4.การประชุม/สัมมนา
☐ 5.เอกสาร/สิ่งตีพิมพ์ ☐ 6.หนังสือ/วารสาร
☐ 7.รายงานการวิจัย ☐ 8.วิทยุ
☐ 9. โทรทัศน์ ☐ 10. ประสบการณ์ตรงจากการปฏิบัติงาน
☐ 11.อื่น ๆ ระบุ.....

1.10 ใน 3 ปีที่ผ่านมาท่านมีประสบการณ์เกี่ยวกับอาชญากรรมทางเทคโนโลยี รวม ..... ครั้ง/คดี

ส่วนที่ 2 ประเด็นเกี่ยวกับแนวทางการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพื่อนำไปสู่แนวทางในการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.1 ด้านบุคลากร (เช่น การขาด/เพิ่มกำลังพลให้สอดคล้องกับการปฏิบัติหน้าที่)

.....

.....

.....

.....

2.2 ด้านการฝึกอบรม (เช่น การจัด หรือเข้าร่วมการอบรมให้กับเจ้าหน้าที่ตำรวจ เพื่อเสริมสร้างทักษะความรู้ต่างๆ)

.....

.....

.....

.....

2.3 ด้านงบประมาณ (เช่น เพิ่มงบประมาณในการทำสื่อประชาสัมพันธ์ให้ประชาชนรับทราบถึงภัยของอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ)

.....

.....

.....

.....

2.4 ด้านเครื่องมือ และอุปกรณ์ (เช่น เพิ่มอุปกรณ์ในการสืบสวน หาข่าว และการจัดเก็บวัตถุพยานต่าง ๆ เป็นต้น)

.....

.....

.....

.....

2.5 ด้านเทคโนโลยี (เช่น ติดตั้ง และปรับปรุงซอฟต์แวร์ที่ช่วยในการทำงานเพิ่มเติม)

.....

.....

.....

.....

2.6 ด้านบริหารการจัดการ (เช่น ผู้บังคับบัญชาเล็งเห็นความสำคัญในการบริหารจัดการอย่างเป็นระบบ หรือมีการสร้างแรงจูงใจในการทำงาน)

.....

.....

.....

2.7 ด้านโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (มีการกำหนดนโยบายที่ความชัดเจน และมีการวิเคราะห์บทบาทของหน่วยงานให้สอดคล้องกับการปฏิบัติงานจริง)

.....

.....

.....

.....

2.8 ด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน (เช่น ปรับปรุงภารกิจและความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง /เสนอขอแก้ไขกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้องให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี)

.....

.....

.....

.....

2.9 ด้านการพัฒนาหน่วยงานด้านอาชญากรรมทางเทคโนโลยี และด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีอย่างไรให้เกิดประสิทธิภาพในการทำงานอย่างสูงสุด

.....

.....

.....

.....

2.10 ด้านอื่น ๆ

.....

.....

.....

.....

ส่วนที่ 3 ประเด็นเกี่ยวกับรูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพ

3.1 รูปแบบในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีที่ดี (Best Practice) ของเจ้าหน้าที่ตำรวจที่มีประสิทธิภาพควรลักษณะอย่างไร

.....

.....

.....

.....

.....

.....

.....

.....

3.2 ด้านเทคนิคในการบริหารงานเกี่ยวกับด้านอาชญากรรมทางเทคโนโลยีให้ประสบความสำเร็จมีการดำเนินการอย่างไร

.....

.....

.....

.....

.....

.....

.....

.....

3.3 การพัฒนารูปแบบที่ทำให้เกิดประโยชน์สูงสุดในการปฏิบัติงานด้านอาชญากรรมทางเทคโนโลยีควรเป็นอย่างไร

.....

.....

.....

.....

.....

.....

.....

.....

ส่วนที่ 4 ประเด็นเกี่ยวกับสถานการณ์ปัจจุบันของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

4.1 หน่วยงานตำรวจที่ปฏิบัติงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แก่ ภารกิจและความรับผิดชอบระเบียบ ข้อบังคับ กฎหมาย และการบูรณาการระหว่างหน่วยงาน

.....

.....

.....

.....

.....

4.2 การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้แก่ ยุทธศาสตร์วิธีการ ป้องกันและปราบปราม มาตรการและวิธีการป้องกันและปราบปราม และบทบาทหน้าที่ของหน่วยงานตำรวจ

.....

.....

.....

.....

.....

4.3 การกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แก่ สาเหตุการก่ออาชญากรรม รูปแบบอาชญากรรม และการวิเคราะห์อาชญากรรม

.....

.....

.....

.....

.....

.....

4.4 องค์ความรู้ และความชำนาญงานเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้แก่ ระดับการศึกษา ประสบการณ์การทำงาน และความรู้ทางด้านเทคโนโลยี

.....

.....

.....

.....

.....

.....

.....

4.5 การพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยี ได้แก่ เครื่องมือ และอุปกรณ์ การ ตรวจสถานที่เกิดเหตุ และการครอบครองพยานหลักฐาน

.....

.....

.....

.....

.....

.....

4.6 การสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยี ได้แก่ เทคนิคในการสืบสวน และสอบสวน การแสวงหาข้อเท็จจริงและหลักฐาน และผู้มีอำนาจ และเขตอำนาจการสืบสวนและสอบสวน

.....

.....

.....

.....

.....

.....

.....

ส่วนที่ 5 ประเด็นเกี่ยวกับสภาพปัญหาด้านการบริหารจัดการของหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

5.1 ด้านบุคลากร (เช่น ปัญหาการขาดบุคลากร ปัญหาเจ้าหน้าที่ขาดความรู้และทักษะในการปฏิบัติหน้าที่ ปัญหาความเครียดและความกดดันจากการทำงาน เป็นต้น)

.....

.....

.....

.....

.....

5.2 ด้านงบประมาณ (เช่น การขาดงบประมาณในการจัดทำสื่อประชาสัมพันธ์ให้ประชาชนรับทราบถึงภัยของอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ เป็นต้น)

.....

.....

.....

.....

.....

5.3 ด้านเครื่องมือ และอุปกรณ์ (เช่น ปัญหาการขาดแคลนอุปกรณ์ในการสืบสวน หาข่าว และการจัดเก็บวัตถุพยานต่างๆ เป็นต้น)

.....

.....

.....

.....

.....

5.4 ด้านเทคโนโลยี (เช่น ขาดการปรับปรุงซอฟต์แวร์ที่ช่วยในการทำงานให้เป็นปัจจุบัน หรือมีแต่ไม่มีประสิทธิภาพ เป็นต้น)

.....

.....

.....

.....

5.5 ด้านบริหารการจัดการ (เช่น ผู้บังคับบัญชาไม่มีการบริหารจัดการอย่างเป็นระบบ หรือไม่มีการสร้างแรงจูงใจในการทำงาน)

.....

.....

.....

.....

5.6 ปัญหานโยบายและยุทธศาสตร์การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (เช่น นโยบายไม่มีความชัดเจนและไม่สามารถนำมาปฏิบัติได้อย่างเป็นรูปธรรม / ในปัจจุบันไม่มีมาตรการในการปฏิบัติงานจริง)

.....

.....

.....

.....

5.7 ปัญหาด้านการบูรณาการร่วมกันระหว่างหน่วยงาน และภาคประชาชน (เช่น ภารกิจและความรับผิดชอบที่ซ้ำซ้อนกัน / ไม่มีหน่วยงานใดเป็นเจ้าภาพที่แท้จริง ปัญหาข้อกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้อง)

.....

.....

.....

.....

ส่วนที่ 6 ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

.....

.....

.....

****

ภาคผนวก ข
บันทึกการประชุมกลุ่มย่อย

การประชุมกลุ่มย่อยครั้งที่ 1 เมื่อวันที่ 14 มกราคม 2562 ได้มีผู้ทรงคุณวุฒิได้ให้ข้อคิดเห็น ดังนี้

1) อดีตผู้ทรงคุณวุฒิ สำนักงานตำรวจแห่งชาติและอดีตรองผู้บัญชาการตำรวจนครบาล ได้ให้ข้อคิดเห็นดังนี้

(1) สมัยที่ได้ได้ดำรงตำแหน่งรองผู้บัญชาการตำรวจนครบาล ซึ่งดูแลในเรื่องของคดีในช่วงหนึ่ง ปรากฏว่าในส่วนของสน.เมื่อเขาได้รับแจ้งแล้ว พนักงานสอบสวนเองแทบจะไม่มีความรู้เลย แล้วทำไม่เป็นในส่วนของตรงนี้คือสิ่งที่สำคัญ เมื่อทำไม่เป็นแล้วก็จะติดต่อประสานไปที่ ปอท. โดยปอท.ไม่รับ ได้ให้เหตุผลที่ว่ามีพนักงานสอบสวนอยู่ 40-45 ท่าน จากอัตราเต็มคือ 80 ส่วนที่เหลือไปช่วยราชการ พนักงานสอบสวนจบจากโรงเรียนนายร้อยตำรวจ 40 เหลือไม่ถึง 20 ในส่วนของตรงนี้จึงเป็นเหตุผลใหญ่ เมื่อตำรวจทำงานไม่เป็น ก็จะมาตกอยู่ที่ ปอท. ทำให้ ปอท.ไม่สามารถที่จะรับงานได้ เราจะทำอย่างไร จึงเกิดเป็นคำถามในงานวิจัยในด้านหน่วยงานของตำรวจ ในส่วนของการดำเนินโครงการนี้ มีส่วนของการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี จึงอยากให้นักวิจัยช่วยกันคิดว่าอาชญากรรมทางเทคโนโลยีที่เกิดขึ้น มันมีอะไรบ้าง อาทิเช่น ลักทรัพย์ ซึ่ง ปอท.ก็ออกประกาศในไลน์ ในเรื่องเงินที่อยู่ในบัญชีอยู่ดีๆหายโดยมีการใช้รหัสทาง True, AIS หรือทางอะไรต่าง ๆ รวมทั้งในเรื่องของการหมิ่นประมาทก็สามารถทำได้ทางเทคโนโลยี รวมทั้งอาชญากรรมทางเพศโดยหลอกลวงทางคอมพิวเตอร์ หลอกลวงเงิน หลอกลวงทรัพย์ หรือนัดหมายกันมีกิจกรรมทางเพศ แล้วตำรวจทั้ง สน.นครบาล ภูธร เขาทำไหวหรือไม่ หรือมีแนวคิดที่จะพัฒนาหน่วยของตำรวจอย่างไร ซึ่งต่อไปในอนาคต

- 2020 อาชญากรรมทางเทคโนโลยีจะเพิ่มขึ้นขนาดไหน
- 2025 AI คือหุ่นยนต์ จะเข้ามาแทนที่คน เนื่องจากเป็นหุ่นไม่มีชีวิตจิตใจ หากกระทำความผิดต้องแก้กฎหมายหรือไม่
- 2030 ต่อไปอนาคตเหมือนกับมาทำงานแทนคนได้เต็มรูปแบบ
- 2050 ทุกสิ่งทุกอย่างจะเข้ามาแทนที่ด้วยเทคโนโลยีคอมพิวเตอร์ จะรับมือกับแผนอนาคตข้างหน้าอย่างไร ไม่ใช่แต่หน่วยงานตำรวจ ทุกหน่วยงาน อัยการเดินหน้าต่ออย่างไร ก็จากการรวบรวมพยานหลักฐาน ตำรวจรวบรวมพยานหลักฐาน แต่เจ้าหน้าที่สน.ไม่สามารถทำอะไรได้เลย เพราะต้องมีหลักฐานที่จะส่งอัยการ ต้องดูในหลายๆอย่างว่าแต่ละหน่วยงานจะพัฒนาต่อไปอย่างไร

(2) เทคโนโลยี ในด้านของกฎหมาย พรบ.2550 และ พรบ.2560 มีการปรับแก้แล้วเพียงพอหรือไม่ ที่จะบังคับใช้ ในปี 2020 2025 2030 2050 ซึ่งในปี 2050 เทคโนโลยีจะเต็มรูปแบบ และมีการทำธุรกรรมทางคอมพิวเตอร์

เริ่มตั้งแต่คนที่เข้ามาแจ้งความเรื่องฉ้อฉลของสินค้า เสียหายจากเรื่องอะไร ฉ้อฉลของเรื่องทรัพย์ ฉ้อฉลของเรื่องเพศ ตัวอย่างเช่น นักการบ้านท่านหนึ่งไปฉ้อฉลเงิน เป็นค่าซื้อข้าวจากประเทศกัมพูชา คือเงินเข้ามาแล้วไม่ถึง โดยเงินนี้ไปเข้าอยู่กับสมาคม มีการติดคุกเป็นที่เรียบร้อยแล้ว หลังจากนั้นมีการพูดคุยกัน ทางเขาก็ไม่ยอม ศาลตัดสินจำคุก 20 ปี ลักษณะแบบนี้มีการดำเนินการโดยใช้แฮ็คเกอร์ โดยจำเป็นต้องตั้งกรรมการสอบสวน มีการเชิญกรรมการจาก ปอท. และเชิญทาง ICT และ DSI จนไล่เรียงแต่ละเรื่อง แล้วตั้ง

ประเด็นสอบสวนให้เขา ในส่วนของตรงนี้เราจะทำอย่างไรในส่วนขององค์กรของตำรวจ ที่ทำงานในด้านพิเศษอย่างมีคุณค่า

2) อัยการจังหวัดประจำสำนักงานอัยการสูงสุด ได้ให้ข้อคิดเห็น ดังนี้

(1) ได้ตรวจข้อสอบผู้ที่เข้ารับการประเมินหลักสูตรผู้ที่จะมาเป็นพนักงานสอบสวน ในส่วนข้อสอบส่วนแรกเป็นด้านเทคโนโลยีผู้เข้าสอบเข้าใจดี แต่ส่วนหลังผู้สอบยังไม่เข้าใจถึงกฎเกณฑ์พื้นฐานต่าง ๆ เช่น การเป็นผู้ให้บริการในประเภทต่าง ๆ ที่สำคัญในการจะเอาข้อมูลมาหลาย ๆ อย่าง และขั้นตอนลำดับเหตุการณ์ต่าง ๆ ที่จะนำไปสู่ตัวผู้กระทำความผิดกลายเป็นว่าผู้เข้าสอบยังไม่ค่อยเข้าใจ กลับมาในแง่เนื้อหาจากประสบการณ์ที่ทำงานด้านนี้มา 10 กว่าปี พบว่าปัญหาไม่ได้อยู่แค่ข้อกฎหมายแต่ยังมีปัญหาเรื่องการบริหารจัดการซึ่งสำคัญมาก ๆ ไม่น้อยกว่าข้อกฎหมาย โดยองค์ความรู้ทางด้านกฎหมายกับการบริหารจัดการโดยเฉพาะอย่างยิ่งคดีประเภทนี้ที่มีพยานหลักฐานกระจายตัวอยู่ทั้งส่วนที่เป็นองค์ความรู้ที่พนักงานสอบสวนจะต้องมี ทั้งส่วนที่เป็นเครื่องมือที่จะต้องจัดเตรียมให้พนักงานสอบสวนเพื่อที่เขาจะสามารถเข้าถึงพยานหลักฐาน ปัญหาในการรวบรวมพยานหลักฐานมีในส่วนทั้งข้อกฎหมายพนักงานสอบสวนหลายท่านก็ไม่รู้ว่าจะต้องใช้อำนาจอย่างไร เพราะว่ามีนักกฎหมายบางคนไปพูดในวงสาธารณะว่าปัจจุบันพนักงานสอบสวนไม่มีอำนาจตามป.วิอาญาที่จะเรียกพยานหลักฐานเหล่านี้ ใน พรบ.คอมพิวเตอร์ถึงแม้จะแก้ไขแล้วให้พนักงานสอบสวนสามารถร้องขอได้แต่ในการที่ให้พนักงานสอบสวนร้องขอได้ ก็ไม่ได้ตัดอำนาจพนักงานสอบสวนตามป.วิอาญาในส่วนนี้สำคัญ

ในเรื่องของวิธีบริหารจัดการสิ่งสำคัญคือเรื่องประเภทคดีเป็นตัวหนึ่งที่จะมาช่วยเรา นอกจากประเภทของคดีแล้ว ความซับซ้อนของคดีที่พนักงานสอบสวนจะต้องประเมินว่าความซับซ้อนของคดีมากน้อยแค่ไหน ต่อมาคือเราต้องมาจัดอันดับคนที่จะเข้ามาทำคดีฝ่ายสอบสวนและฝ่ายสืบสวน ได้แบ่ง level แบบอย่างออกเป็น 3 level

(1.1) คดีฉ้อโกงธรรมดา เช่น คดีฉ้อโกงในอินเตอร์เน็ต คดีหมิ่นประมาทที่เรายังไม่ได้พยานหลักฐานมาจากผู้ต้องหาสามารถบริหารคดีเบื้องต้นเฉพาะ level นี้ ประมาณ 80% ทั่วประเทศ

(1.2) อุปกรณ์ของผู้ต้องหาหรือผู้เสียหาย จะต้องมีองค์ความรู้เฉพาะด้านเช่นตรวจพิสูจน์หรือช่วยคนในlevelแรกบริหารคดีได้

(1.3) ระดับ expert คือ คนที่มีความรู้ในสองแง่มุม คือความรู้ของเทคนิคและ ความรู้ของทางสอบสวนที่จะทำคดีซับซ้อนบางประเภทที่มันจำเป็นจริง ๆ ที่มาถึง level นี้ มาช่วยอธิบายการเกิดพยานหลักฐาน เพื่อที่จะบอกว่าคดีนี้ผู้ต้องหาใช้วิธีการอย่างไร ได้ข้อมูลมาได้อย่างไร ซึ่งคดีที่มาถึง level นี้ก็มีปริมาณไม่มาก แต่เนื่องจากปัจจุบันเราไม่ได้แบ่ง จึงมองเป็นคดีทั่วไปทำให้พนักงานสอบสวน ที่สน.ขาดความรู้หากเขาไม่รู้แต่ได้ถามก็ยังดี แต่ที่ผมพบคือหลาย ๆ สำนวนไม่รู้และไม่ได้ถาม คือเขาไม่เก็บพยานหลักฐานในมุมนี้มาเลย เขาก็กลับไปเล่นในมุมของ analog หรือผู้เสียหายเก็บมาได้เท่าไหร่ก็เอาไปเท่านั้น แล้วก็ส่งสำนวน สำนวนประเภทนี้มีเยอะมาก แล้วท้ายที่สุดด้วยข้อจำกัดของการสอบสวนคดีประเภทนี้ในเรื่องของระยะเวลาที่เราจะต้องรวบรวมจิ๊กซอว์มาหาเป้าหมายปลายทางว่าใครคือผู้กระทำผิด สำคัญคือตัวหลอดไฟกล้องวงจรปิด

คอมพิวเตอร์กราฟฟิคดาต้าที่ผู้ให้บริการประเทศเรากำหนดไว้แค่ 90 วัน ขยายได้ไม่เกิน 2 ปี ซึ่งทางปฏิบัติประเด็นนี้ก็เป็นประเด็นสำคัญ บางครั้งก็มองว่าแปลกเนื่องจากทราบมาว่าบางหน่วยงานถึงขั้นต้องจัดงบขึ้นเพื่อเลี้ยงดูผู้ให้บริการเพื่อที่จะได้ข้อมูลเหล่านี้มา กลายเป็นว่าถ้าใครจ่ายก็มีโอกาสได้ข้อมูล แต่ถ้าใครไม่จ่ายก็มีข้อโต้แย้งทางกฎหมายตอบกลับมา แม้แต่กองปราบเองหากมีคดีประเภทนี้ ก็ถูกผู้ให้บริการตอบกลับมาแบบยืดยาวหลายหน้ากระดาษ ดังนั้น ประเภทนี้ไม่ใช่ปัญหาทางข้อกฎหมายแต่เป็นข้ออ้างด้านข้อมูล สิทธิส่วนบุคคล อ้างมาจนถึงนิติบัญญัติ หน่วยไหนเลี้ยงดูหน่วยนั้นได้ข้อมูลเป็นข้ออ้างไม่ใช่ปัญหาทางข้อกฎหมาย ข้ออ้างเหล่านี้ ถ้าพนักงานสอบสวนโดยทั่วไปที่มีปริมาณมากขึ้นเรื่อยๆเขาอยากจะไปต่อสู้ แต่ก็มีบางหน่วยงานที่ขัดต่อหมายเรียกก็ออกหมายจับดำเนินคดี กลายเป็นว่าอุปสรรคไม่ได้จำกัดแค่ข้อกฎหมายและเรื่องบริหารจัดการก็เป็นปัญหาที่ไม่ใหญ่ไปน้อยกว่ากัน ถ้าเรามองประเภทคดี และมองเห็นปัญหาที่จะเกิดขึ้นในรูปแบบต่าง ๆ การบริหารคดีในเชิงปริมาณช่วยได้ค่อนข้างมาก หากคดีที่ซับซ้อนจริง ๆ อย่าให้เขาโดดเดี่ยวให้เขารู้ว่าเขามีตัวช่วย ถ้าสมมติว่าเราสามารถสร้างโมเดลก็ทำให้คนที่เข้าทำงานจะแก้ปัญหาอย่างไร ให้มีผู้ช่วยจะดีมาก

(2) ควรมีเจ้าภาพหน่วยงานที่บริหารจัดการข้อมูลจราจรคอมพิวเตอร์ ซึ่งเรื่องนี้เป็นเรื่องที่สำคัญอย่างหนึ่ง เพราะว่าปัจจุบันพนักงานสอบสวนไม่เพียงพอในการบริหารคดี หลาย ๆ หน่วยงาน ภาครัฐ take อย่างเดียวไม่เคย give อะไร ในแง่ของการสืบสวนสอบสวน หากมีการร่วมมือกันระหว่างภาครัฐและเอกชนให้ข้อมูลมา ควรมีโมเดลของยุโรปซึ่งมีมาตรฐาน หากเรามาปรับแต่งนิดหน่อยให้ทุกหน่วยงานสามารถที่จะได้ประโยชน์จากข้อมูลการเงินเท่า ๆ กัน ก็จะทำให้ภาคเอกชนเขาหมดภาระที่จะจัดเตรียมข้อมูล เขาจัดเตรียมข้อมูลพื้นฐานให้เรา ภาครัฐก็สามารถเอาไปใช้ถูกต้องตามกฎเกณฑ์ของตัวเองได้

(3) ส่วนของข้อมูลอาชญากรรมคอมพิวเตอร์ หลาย ๆ คดีมีความจำเป็นมาก ก็พบว่ามีข้อูลอีกหลายส่วนที่เป็นประโยชน์ ที่บางครั้งพนักงานสอบสวนรู้ก็ขอ หากไม่รู้ก็ไม่ขอ ที่สำคัญคือผู้ให้บริการเองไม่อยากให้เนื่องจากให้แล้วเป็นภาระให้แล้วก็จะมีแต่คนจะขอเพิ่ม ในส่วนของตรงนี้เราจะทำยังไงให้ทุกฝ่ายได้ประชุมร่วมกัน ตัวอย่างเช่น

ควรมีโมเดลโดยให้ผลตอบแทนในรูปแบบของคำชมเชย หรือมีรางวัลตอบแทน หรือให้สิ่งเหล่านี้เป็นต้นทุนการลดภาษีบางส่วน คิดว่าจะเป็นแรงจูงใจที่ผู้ให้บริการมีส่วนรว่มกับภาครัฐ แต่ถ้าเรามองทีละคดีเราจะเห็นคำขอเยอะ แต่ถ้าเรามองเป็นประเภทแต่ละเดือนคำขอมีมามหาศาล อย่างผู้ให้บริการบางรายปัญหาภายในของเขากลายเป็นปัญหาภายในของเราไปด้วย ทำให้ข้ออ้างของเขาเราจะดำเนินคดีก็ดำเนินคดีไม่ได้ การบังคับใช้กฎหมายก็ไม่มีประสิทธิภาพ แล้วตัวพนักงานสอบสวนเองก็ทำงานต่อไม่ได้
ถ้าสมมติว่ามีกระทรวง ICT สามารถที่จะดึงข้อมูลพวกนี้ หรือถ้าให้ผู้บริการเหมือนเดิมจะเป็นประโยชน์ค่อนข้างมาก

ประเภทอาชญากรรมใหม่ ๆ ในการใช้คอมพิวเตอร์ล่วงละเมิดคดีทางเพศในเด็ก เป็นข่าวที่ทุกคนช่วยกันเพื่อสิทธิของเด็ก พอเข้าไปร่วมกับมูลนิธิ พบว่าเรื่องของการล่วงละเมิกทางเพศเด็กเหมือนโรคระบาดที่สามารถส่งต่อความผิดปกติ

แต่เท่าที่ฟัง เป็นเรื่องที่ impect มหาศาล เพราะว่าได้เข้าร่วมกับมูลนิธิที่ทำงานด้านนี้โดยตรง ก็พบว่า ความผิดปกติทางรสนิยมทางเพศ ให้คนนึงที่เขารู้ว่าเขาทำผิด เขาสามารถที่จะล่วงละเมิดทางเพศคนใกล้ตัว ไม่ว่าจะเป็นนักเรียนในการดูแล หรือญาติพี่น้อง หรือcaseที่ตอนนี้กลายเป็นเรื่องระบาดไปแล้วคือการปลอมโปรไฟล์ของเด็กผู้ชายให้ช่วยตัวเอง กลายเป็นว่าผู้ต้องหาที่กระทำผิดในวันนี้ คือผู้เสียหายเมื่อวานนี้ และผู้เสียหายในวันนี้ก็มีแนวโน้มเป็นผู้เสียหายในวันข้างหน้า ก็จะส่งต่อความผิดปกติทางเพศเข้าไปอีก อันนี้เป็นโมเดลที่ใกล้ตัวมาก ๆ และเพิ่มขึ้นเรื่อย ๆ

3) รองผู้บังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ได้ให้ข้อคิดเห็น ดังนี้

(1) ปัญหาที่เจอในหน่วยงานคือ มี spec บังคับทำให้กำลังพลน้อยมาก ส่งผลให้กำลังพลเริ่มย้ายออกไปยังหน่วยงานอื่นเนื่องจากเจริญก้าวหน้าได้ยาก กำลังพลจริง ๆ เต็มอัตรา สำหรับคนส่วนใหญ่ไปช่วยราชการเยอะ ทำให้ตรงนี้เป็นปัญหาการบริหารงานส่วนบุคคลที่ไม่สามารถที่จะมองข้ามได้เลย เพราะต่อให้วางระบบดีแค่ไหนแต่ถ้าผู้ใหญ่ยังสั่งการภายนอกระบบได้ก็ไม่มีทางแก้ได้ ต้องมีกลไกให้หน่วยอื่นมาช่วยตรวจสอบเด็กไปวิ่งผู้ใหญ่หมด ทำให้การบริหารงานบุคคลบิดเบี้ยวไปหมด

ในต่างประเทศแก้ไขส่วนตรงนี้สำเร็จแล้ว โดยใช้แนวความคิดอะไรในการแก้ปัญหา เพราะใช้การประเมินแบบ 360 องศา ใช้ร่วมกับคอมพิวเตอร์ เพื่อเป็นตัวจับ ทุกคนไปประเมินในระบบ แล้วไม่ต้องประเมินอะไรมาก ไม่ต้องเขียนเยอะหลายหน้า คือ ถ้ามีอยู่ 1 ตำแหน่งคุณอยากให้ใครเป็นอันดับ 1 ถ้ามี 2 ที่คุณอยากให้ใครเป็นอันดับ 1 อันดับ 2 ให้เลือกลงไป แต่ทุกคนมี waste ไม่เท่ากันผู้บังคับบัญชาระดับ 5 ก็ใช้ 5 แต้ม แล้วพอทุกคนใส่เข้าระบบแล้วจะตรวจสอบได้ว่าใครประเมินใครอะไรเท่าไหร่ก็ทำให้ประสบความสำเร็จแบบการประเมิน 360 องศา

(2) ปัญหางานบุคคลค่าตอบแทน เจ้าหน้าที่ตำรวจส่วนใหญ่เมื่อมีความสามารถไปอบรมต่างประเทศจนมีความเชี่ยวชาญ พอกลับมาก็ออกนอกหน่วยหรือออกนอกระบบไปเลย ไปอยู่การท่าอากาศยานบ้าง ไป ปอท. ไป DSI ตรงนี้เป็นเรื่องของค่าตอบแทนที่มีค่าตอบแทนอะไรบางอย่างเพิ่มเติม ถ้าเราไม่สามารถให้ค่าตอบแทนที่สูงกับคนพวกนี้ได้ เราต้องมองถึงปัญหาเรื่อง Outsource หรืออย่างเนเธอร์แลนด์ไม่มี Outsource แต่เป็นการรวมหน่วยงานด้าน forensic

โมเดล ในส่วนของด้านต่างประเทศใช้สามเหลี่ยมอาชญากรรม จะมี 3 องค์ประกอบหลัก

(2.1) แรงจูงใจ (เงิน) แก้ปัญหาโดยการใช้เงิน

(2.2) องค์ความรู้ในการกระทำความผิด ซึ่ง 2 ตัวนี้ไม่สามารถควมคุมได้

(2.3) ช่องโอกาสในการกระทำความผิด ตัวนี้สามารถควบคุมได้ คือกลไกในการป้องกัน เช่น เอา Bording pass ใช้ sim ซึ่งสามารถทำให้รู้ถึง username password ต้องเก็บให้น้อยที่สุด แต่ให้ระบุตัวตนให้ได้ หลักการคือเก็บอย่างไรก็ได้แต่ให้ระบุตัวตน

หมายเลข กลไกตัวนี้ไม่กำหนดใน พรบ.คอมพิวเตอร์ กลไกคอมพิวเตอร์ไม่ได้ไปตรวจสอบในช่วงที่ร่าง พรบ.ปี50 ได้เสนอว่าควรมีเจ้าหน้าที่ ที่สามารถเข้าไปตรวจสอบได้สามารถที่จะส่งตัวอย่าง ถ้าไม่

สามารถระบุได้ต้องดำเนินคดีทันทีก่อนที่จะมีปัญหาเกิดขึ้น ผู้ให้บริการพยายามทำทุกวิถีทางเพื่อประหยัดงบประมาณ ผลที่ตามมาคือเขาไม่เก็บข้อมูลที่มีคุณภาพ

(3) กลไกเรื่องแก้กฎหมายในการตรวจสอบ ตัวหนึ่งที่อยากให้เกิดก็คือ กลไกเรื่องของหมายเรียก electronic ให้ กสทช.เป็นเจ้าภาพ จะเอา durelop file จากผู้บริการมาไว้ตรงbig dataกลาง แล้วทำเป็น application ให้เจ้าหน้าที่ไปลงทะเบียนเพื่อให้รู้ว่าเจ้าหน้าที่เหล่านี้ผ่านการกลั่นกรองมาเรียบร้อยแล้วมีอำนาจทางกฎหมาย หลังจากนั้นทำให้สามารถมีหมายเรียกออกมาทันที เกิดเหตุว่าใครไม่ตอบตามกรอบเวลามีปัญหาว่าตรวจแล้วไม่เจอ อันนี้จะเป็นกลไกที่ทำให้ผู้บริการเกิดความเกรงกลัวแล้วจะแก้ปัญหาเรื่องทุจริตคอรัปชั่นที่ต้องให้เจ้าหน้าที่เข้าไปดูแลทุกอย่างก็ให้เป็นระบบ ประเทศไทยต้องทำเป็นระบบและมีการควบคุมกำกับดูแล

หากจะใช้ sim สาธารณะ แทนที่จะลงทะเบียนด้วยบัตรประชาชน หรือใช้พาสปอร์ตปลอมก็เข้าได้จะมองว่าไม่มีประสิทธิภาพ สิ่งที่เราควรทำคือ ระบุตัวตนให้ได้อย่างน้อยว่าคนที่มาใช้ ใช้หมายเลขโทรศัพท์อะไร พอเวลาใช้ควรมี SMS มาเป็นหลักฐาน Password ให้กรอกเข้าไป ส่วนกลไกระบุตัวตนในการใช้โทรศัพท์ การใช้ sim, wifi ฟรี ให้เสียค่าใช้จ่ายโดยหักจาก Password ที่ให้ จะทำให้คดีต่างๆลดน้อยลง การปลอมโทรศัพท์ก็จะน้อยลงไป

4) ผู้เชี่ยวชาญเฉพาะด้านคดีพิเศษ กรมสอบสวนคดีพิเศษ ได้ให้ข้อคิดเห็นดังนี้

(1) อาชญากรรมทางเทคโนโลยีเป็นปัญหาใหญ่มากในอนาคต การวิเคราะห์ปัญหากระทบมากในสังคม ความมั่นคงเศรษฐกิจ เกี่ยวโดยตรง โดยเฉพาะมูลค่าด้านการค้าขายและข้อมูลส่วนบุคคลมีการรั่วไหลและยังกระทบไปในเรื่องข้อมูล หากมองให้ลึกกว่านั้นต้องมองในเรื่องของปัญหาคิดได้หลายอย่างเอาคนเก่งมาคุยแต่ไม่สามารถปฏิบัติได้จริง ๆ สักครั้งเดียว ไม่เอาจริงเอาจังจึงกลายเป็นเรื่องเล็ก ๆ ซึ่งอาชญากรรมทางด้านนี้มองไปในวันข้างหน้าสำคัญมาก ๆ กระทบกับชีวิตมากขึ้น แต่ให้ความสำคัญน้อยมาก

(2) การจัดตั้งองค์กร โครงสร้างอำนาจหน้าที่ กำหนดแต่งตั้งหน้าที่ก็ไม่ตรงกับความรู้ความสามารถทางหน่วยงานของ DSI ระดับหัวหน้าหน่วยงานไม่ต้องเลือกคนที่มีความรู้ตรงก็สามารถทำงานได้ ก็ทำ ๆ ไป ซึ่งทำดีกับทำได้มันต่างกันเยอะ จับคนที่มีความรู้ไปวางไว้ตรงนั้นเขาคิดได้เป็น 10 step ถึงแม้จะมีคนที่มีความรู้ตรงก็ยังรักษาเขาไว้ไม่ได้อีก คนที่เก่งจริงก็ไม่ได้ดูคน ๆ นั้นไม่นานก็ไป ค่าตอบแทนคือขั้นก็จะเท่ากันแต่คนคนนั้นจะเป็นคนพิเศษแต่ได้สิทธิประโยชน์ไม่เหมือนกับคนอื่น

(3) สถิติของคดี สำคัญมากเกิดผลกระทบรุนแรง สถิติคดีเท่าไรแทบจะไม่มีใครบอกได้เลย อย่างมาแจ้งความที่โรงพักก็หายสนิทเลย คดีประเภทนี้ไม่มีอะไรที่เกิดขึ้นจริง จริง ๆ เราต้องการสถิติพวกนี้เยอะ เราต้องการรายละเอียดในการสร้าง pattern จะได้รู้ว่าทิศทางแนวโน้มไปอย่างไร จะได้แก้ปัญหาได้ถูกต้อง แนวในการป้องกัน เทคโนโลยี ในส่วนของ AI ในเชิงต้องการโดยเราใส่ข้อมูลพวกนี้เราสามารถคาดการได้ล่วงหน้าด้วยซ้ำว่าจะเกิดอะไรขึ้นจากข้อมูลที่แพร่หลาย เช่น social media สามารถจะสร้าง pattern ได้ แล้วการที่จะดำเนินคดีให้ได้ผลต้องทำอย่างรวดเร็ว เกิดปุ๊บทำได้เลยถ้าป้องกันให้ดีก่อน

(4) ที่ปรึกษาคดี เป็นเรื่องจำเป็นมาก จริง ๆ ต้องสร้างทีมที่ปรึกษา เช่น ต้องไปเก็บหลักฐานตรงนี้น่ะ เดี๋ยวหลักฐานจะอยู่ไม่นานน่ะ พยานหลักฐานชิ้นนี้สำคัญ เป็นจิ๊กซอว์ที่สำคัญ ในส่วนตรงนี้เป็น reaction หากได้หลักฐานตรงนี้มาถึงจะโอเค หากเขาไม่รู้เรื่องเลย ไม่รู้จะขออะไร แต่ถ้าไม่รู้เรื่องก็งดไป เรื่องนี้ถือเป็นเรื่องสำคัญเพราะในต่างประเทศถามเรื่องนี้สามารถตอบได้เลยเพียงสอบถามในโทรศัพท์ หากเราวางโครงสร้างประจักษ์บนในเรื่องบริหารจัดการที่ดี ในต่างประเทศที่เป็นโรงพักท้องถิ่น เขาก็มีขีดความสามารถที่เราต้องการแบบนี้เลย เขาจัดคนมีขีดความสามารถ หน่วยวิเคราะห์ หน่วยสืบ หน่วยจับ เขาทำเป็นเรื่องปกติ เคยไปร่วมงานที่เกาหลีใต้ไปกับท่านอัยการเขาถามถึงคดีในประเทศไทยเป็นอย่างไร ให้คำตอบเขาไปว่าในเรื่องของกระดาษเป็น 90% digital 10% ส่วนเกาหลีใต้ได้ให้คำตอบว่าบ้านเขา digital 90% กระดาษแทบไม่เห็นเลย ซึ่งเขาจัดคนที่มีขีดความสามารถ หน่วยวิเคราะห์ในการสร้าง pattern นี้ไว้ เพราะพื้นที่อาชญากรรมของเขาเป็น digital crime scene

(5) ความร่วมมือระหว่างประเทศ เป็นเรื่องสำคัญมาก เพราะขอความร่วมมือในประเทศยังยากการขอพยานหลักฐานต้องแน่น ยกตัวอย่างเช่น ทำความร่วมมือกับธนาคารส่งข้อมูลผ่านระบบ digital เขาแค่ส่งข้อมูลและคัดลอกตามที่เราต้องการอาชญากรรมประเภทนี้ทำเพื่อเงินการส่งข้อมูลไป

(6) Pattern ในการส่งต่อกัน จัดformat ประมาณนี้ จัด format ตามที่เราต้องการทำข้อมูลวิเคราะห์เข้าไป หากเราเจอข้อมูลตามที่เราแจ้งเบาะแสมีแค่นี้วันนี้เวลานี้เขาก็มีเอกสารรับรองให้เราแบบนี้ง่ายกว่า และข้อมูลที่ได้ที่เป็นปัญหาของข้อมูลที่เป็นกระดาษแทบนำมาวิเคราะห์อะไรไม่ได้เลย พนักงานสอบสวนไม่ได้อ่าน ถ้าเป็น digital จะง่ายขึ้น

การประชุมกลุ่มย่อยครั้งที่ 2 เมื่อวันที่ 7 สิงหาคม 2562 และการประชุมกลุ่มย่อยครั้งที่ 3 เมื่อวันที่ 14 สิงหาคม 2562 มีผู้ทรงคุณวุฒิได้ให้ข้อคิดเห็นดังต่อไปนี้

1) อดีตผู้ทรงคุณวุฒิ สำนักงานตำรวจแห่งชาติและอดีตรองผู้บัญชาการตำรวจนครบาล ได้ให้ข้อคิดเห็น ดังนี้

(1) เพื่อศึกษาการพัฒนาหน่วยงานตำรวจที่ปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เพราะฉะนั้นในการพัฒนาหน่วยงานวันนี้จะต้องหาคำตอบให้ได้ว่าโครงสร้างจะเป็นอย่างไร โดยโครงสร้างที่จะพูดถึงก็จะมี

(1.1) ในระดับตำรวจสถานีตำรวจ ทั้งภูธร นครบาล

(1.2) ในระดับของ ปอท. ปอศ.

(1.3) พิสูจน์หลักฐาน ซึ่งเมื่อสักครู่ก็ทราบว่าในเรื่องของการตรวจพิสูจน์ในด้านเทคโนโลยีมีอยู่ 3 ศูนย์ ซึ่งค่อนข้างจะสมบูรณ์แล้ว แต่ก็ยังไม่ครบถ้วนทั้ง 11 ศูนย์ ตอนนี้มีโครงการนำร่องก็เห็นภาพมาบ้างแล้ว ต่อไปในอนาคตก็คงต้องพัฒนาให้ครบทั้ง 11 ศูนย์ด้วย สิ่งที่ต้องการเห็นในวัตถุประสงค์ข้อนี้ คือ โครงสร้าง รูปแบบต่าง ๆ จะออกมายังไง มีหน้าตาเป็นยังไง ผมจะเล่าให้ฟัง ทาง DSI ตอนนั้นผมก็เป็น 1 ในทีมงานวิจัยของมหิดลในการที่จะศึกษาว่าเราจะทำหน่วยงาน DSI เมื่อก่อนไม่ได้ชื่อ DSI หน่วยงาน FBI ของประเทศไทย ตอนนั้นปี 2547 ตอนนั้นยังไม่มี DSI เราได้ศึกษารายละเอียดต่าง ๆ ศึกษาต่างประทศ เราไปดูของ FBI ว่าเป็นอย่างไร ซึ่งก็ดีที่อาจารย์ณรงค์ ได้มอบหมายให้ผู้วิจัยในทีม ซึ่งมี ผศ.ดร.ศรีปริญญา ธูปกระจ่าง และ นายอารีย์ จิวรรักษ์ ได้นำเสนอในเรื่องของต่างประเทศเข้ามา ซึ่งต่างประเทศเขานำหน้าเราไป โดยเฉพาะอย่างยิ่งสิงคโปร์ ผมมองว่าสิงคโปร์เป็นประเทศที่ก้าวล้ำนำหน้าได้อย่างฉับไว ก็เป็นส่วนหนึ่งที่ทำให้มองเห็นภาพในเอเชีย ซึ่งเวียดนาม ฟิลิปปินส์ ยังล้าหลังเรา อีกด้านหนึ่งในเรื่องของอเมริกา ยุโรป อังกฤษ เยอรมัน ก็จะเห็นภาพว่าในส่วนของเขาทำอย่างไร แล้วก็เอามาเป็นรูปแบบ เพราะฉะนั้นแล้วในส่วนของรูปแบบก็คงต้องตกผลึกแล้วว่าประเทศไทยควรจะเป็นแบบเขา ในส่วนของผมได้คุยกับท่านอาจารย์ณรงค์แล้วว่าเราจะปรับเป็นกองบัญชาการเลยดีไหม โดยรวมเอา ปอท. ปอศ. มา Matching ไปกับพิสูจน์หลักฐาน ตอนนี้พิสูจน์หลักฐานทำได้ 3 ศูนย์ พอครบ 10 ศูนย์ แล้วก็มา Matching กันอาจจะอยู่คนละกองบัญชาการ แล้วมาทำงานบูรณาการกัน แล้วก็มีพิสูจน์หลักฐานจังหวัดด้วย ตอนสมัยผมเป็นผู้การตำรวจภูธรจังหวัด เมื่อปี 50 51 ตอนนั้นพิสูจน์หลักฐานเขาก็มีพิสูจน์หลักฐานจังหวัด มีรถอยู่คันนึง คนขับก็ไม่มี น้ำมันก็ไม่มี ก็เป็นหน้าที่ของผมที่เป็นผู้บังคับการ ตอนนั้นผมให้ รปภ. ไปขับให้ น้ำมันไม่มีผมก็ต้องควักค่าน้ำมัน กองบังคับการตำรวจภูธรเชียงราย เติมให้ไม่อั้น จะไปไหนเติมได้เต็มที่ คนขับใช้ได้ตลอด เพราะเจ้าหน้าที่เขาว่างอยู่แล้ว ผมก็จัด นปพ. ขับรถให้เวลาจะไปไหน ในสมัยนั้นพิสูจน์หลักฐานมีหัวหน้าอยู่คนเดียว ลูกน้องก็ไม่มี แล้วเป็นผู้หญิงด้วย ผมให้เบี้ยเลี้ยงเดือนละ 5,000 ในฐานะที่เป็นลูกน้องผมคนนึงเอาไว้ใช้บริหารงาน แต่ตอนหลังได้ทราบว่า เขามีทีม มีนักนิติวิทยาศาสตร์ มีเจ้าหน้าที่ในด้านต่าง ๆ เพราะฉะนั้นตรงนี้ใส่ในเรื่องของเทคโนโลยีเข้าไป อย่างที่ท่านรองผู้บังคับการได้นำเสนอ ว่าถ้าครบ 11 ศูนย์ ก็จะขับเคลื่อนได้ ถ้าหากว่าเป็นกองบัญชาการ ในส่วนของตรงนี้เราจะวางกรอบอย่างไร ที่จะไปถึง อาจจะมีศูนย์พิสูจน์หลักฐาน ศูนย์อะไรต่าง ๆ หรือไม่ปรับเป็นกองบัญชาการ

ในขณะนี้มีคู่มือให้กับจังหวัด ให้กับพนักงานสอบสวน แล้วก็มีที่ปรึกษา ตอนสมัยผมจบใหม่ผมก็ทำสำนวนไม่เป็น ตอนนั้นมีอาจารย์บุญนำ สุนธรดี พิมพ์สำนวนการสอบสวนมาเป็นตัวอย่าง แล้วเราก็ลอกตามนั้นเป็นคู่มือ แล้วเวลามีปัญหาก็โทรหาอัยการ เพราะในจังหวัดเขาจะสนิทสนมกันมากระหว่างอัยการกับตำรวจ ซึ่งอัยการสามารถไกด์เราได้เป็นอย่างดี เพราะเราทำไม่เป็น ในเมื่อไม่มีคนรู้ เราก็ต้องตั้งคนรู้ขึ้นมาเป็นที่ปรึกษา ทั้งทางโทรศัพท์ และช่องทางออนไลน์ ซึ่งสามารถทำได้สะดวก อาจจะตั้งเป็นทีมที่ปรึกษา กระทรวง DE ตอนผมเป็นรองผู้บัญชาการนครบาล ก็มาช่วยกัน เขาให้คำปรึกษาอย่างดี และให้ทำสำนวนจะต้องส่งไปนู่นนี่ ผมก็ไม่รู้ ลูกน้องก็ไม่รู้ ต่างคนต่างไม่รู้ พอทางนี้เขามาเขาไกด์ สำนวนนี่หนาเป็นปึกเลย อัยการสั่งฟ้องสบายใจเลย เพราะฉะนั้นตรงนี้เราจะทำอย่างไรให้หน่วยงานตรงนี้มีประสิทธิภาพ ผมเชื่อว่าทุกท่านที่นั่งอยู่ตรงนี้ มีความรู้ในการที่จะรันตรงนี้ได้เป็นอย่างดี

(2) ขั้นตอนการกำหนดรูปแบบขั้นตอน ซึ่งผู้ทรงคุณวุฒิบอกให้ปรับมาเป็นรูปแบบขั้นตอนปฏิบัติ คือ การปฏิบัติงานในสถานีตำรวจมีขั้นตอนอย่างไร ปอท.มีขั้นตอนอย่างไร เสร็จแล้วเราจะเขียนขั้นตอนให้ทั้งใน 10 ประเภท แล้วปรับมาเป็นข้อ

(3) คือ ทำเป็นคู่มือ เป็นองค์ความรู้ให้ตำรวจไปปฏิบัติ งานวิจัยชิ้นนี้ก็จะสมบูรณ์ เรามีคู่มือให้ทุก สน. ทำ 2,000 เล่ม ส่งไปทุกสน. ส่งถึงผู้กำกับให้เขาเอาไปเรียน แล้วให้ในแต่ละจังหวัดได้อบรม ก็จะครบ 3 วัตถุประสงค์ ในส่วนของงานที่เป็นโครงสร้าง เราจะต้องวิเคราะห์จากต่างประเทศ เอารูปแบบเขามาตั้ง ของสิงคโปร์เป็นอย่างไร ของอเมริกาเป็นอย่างไร ของยุโรป อังกฤษ เยอรมันเป็นอย่างไร แล้วเราก็สังเคราะห์ออกมาว่าประเทศไทยควรเป็นอย่างไร จุดอ่อนของประเทศไทยเรามองเห็น ทุกคนรู้ดีว่า

(3.1) โรงพักไม่มีความรู้ ไม่สามารถรับแจ้งความได้ เมื่อไม่มีความรู้เราจะทำอย่างไรให้เขามีความรู้ ทำอย่างไรให้เขามีประสิทธิภาพ

(3.2) การตรวจพิสูจน์ พอไม่มีความรู้ ก็ไม่เก็บอะไรสักอย่าง แล้วที่ผ่านมานั้นท่านอัยกรปกรณ์บอกว่ามันฟ้องไม่ได้เพราะคุณไม่เก็บอะไรมาเลย ไม่มีอะไรไปฟ้องเขา มีแต่คำให้การหลักฐานไม่มี เขาก็ยกฟ้องหมด ก็เลยเป็นปัญหา อันนี้ก็จะเกี่ยวข้องกับการตรวจพิสูจน์การเก็บพยานหลักฐาน เพราะฉะนั้นในคู่มือต้องบอกด้วยว่าในแต่ละคดีต้องเก็บอะไรมาบ้าง ตรงนี้สำคัญเลย เก็บมาให้ได้ ต้องเก็บยังไง เก็บมาแล้วต้องอยู่ในมือของพนักงานสอบสวน กี่วัน มันมีระเบียบ เพราะฉะนั้นสำนักงานตำรวจแห่งชาติต้องออกระเบียบ มีงานวิจัยอยู่ชิ้นนึงที่ผมไปเป็นผู้ทรงคุณวุฒิของมหิดล เขาพูดถึงในเรื่องของการเก็บพยานหลักฐาน มีปัญหามากมายที่เมื่อมาอยู่ในการสอบสวนแล้วมันเสียไป เมื่อมาอยู่ในมือของพนักงานสอบสวน แล้วไม่ครบถ้วนจะต้องไปอยู่ในที่ต่าง ๆ ซึ่งมีรายละเอียดตรงนี้ ออกระเบียบอะไรต่าง ๆ ซึ่งมีความชัดเจน สำนักงานตำรวจแห่งชาติก็ออกระเบียบอยู่ แต่ก็ยังไม่ครบถ้วนและต้องคลี่ออกมาว่าอำนาจการสอบสวน การออกระเบียบที่เกี่ยวข้องต่าง ๆ รวมทั้งการลงทะเบียน ที่ใคร ๆ เขาพูดกันในทุก ๆ เวที ว่าต้องมีการลงทะเบียน ถ้าลงทะเบียนผมว่าอาชญากรรมหายไป 90% อาจจะ 95% ด้วยซ้ำถ้ามีการลงทะเบียน เหลืออีก 5% ก็คือมือเซียนจริง ๆ ที่เป็นแฮ็กเกอร์จริง ๆ ที่จะมาทำได้ แต่ทุกวันนี้เป็นมือสมัครเล่นทั้งนั้นเลย ที่เป็นอวตารแล้วเข้ามา เพราะฉะนั้นในวันนี้คาดว่า ทุกท่านคงจะได้ให้ข้อมูล เพื่อที่จะให้ทางทีมวิจัยของเรื่องนี้ได้สรุปให้ชัดเจน ในส่วนของผมจะ

ช่วยเข้ามาดูอีกรอบนึง หลังจากที่ได้ข้อมูลทั้งหมดมาแล้ว เขียนออกมาเป็นเล่มให้มีความชัดเจน สามารถนำไปใช้งานให้เกิดประโยชน์ต่อประเทศได้อย่างมีประสิทธิภาพ

2) รองผู้บังคับการสนับสนุนทางเทคโนโลยี สำนักงานเทคโนโลยีและการสื่อสาร ได้ให้ข้อคิดเห็นดังนี้

(1) เรื่องแรก เรื่องโครงสร้าง ผมมีมุมมองอยู่ 2-3 มุม มุมแรกคือเรื่องของโครงสร้างตำรวจในปัจจุบัน เท่าที่ดูในการนำเสนอยังขาดในส่วนของกองบังคับการสนับสนุนทางเทคโนโลยี ตรงนี้เรามีการกำหนดในอำนาจหน้าที่เลย ในการตรวจพิสูจน์พยานหลักฐาน ในการวิเคราะห์ และเป็นส่วนที่เราจะเข้าไปช่วยเสริมไอเดียตรงนี้ผมเอามาจากแนวความคิดของประเทศญี่ปุ่น เนื่องจากผมไปร่วมสัมมนาตั้งแต่ปี 2002 ก็ได้เห็นโมเดลเขา อธิบายคร่าว ๆ คือ โมเดลของเขาจะมี Cyber Edition เทียบเท่ากับ ปอท. บ้านเรา แล้วเขาก็มีหน่วยงานอีกหน่วยที่เรียกว่า High-tech Crime Center ซึ่งเทียบเท่ากับกองบังคับการสนับสนุนทางเทคโนโลยี แต่สเกลเขาใหญ่กว่าเราเยอะมาก ในส่วนของ High-tech Crime ของเขาจะเป็นวิศวะที่มีความเชี่ยวชาญในเรื่องนี้โดยตรง และเขามีกำลังคนเยอะมาก ในเรื่องของการที่จะกระจายกำลังคนหมุนเวียนไปประจำสถานีตำรวจทั่วประเทศ อันนี้คือข้อที่แตกต่างกับของเรา แล้วเวลาโปรโมชั่นต่าง ๆ เขาไม่เกี่ยวกับโรงพักเลย โปรโมชั่นเขาอยู่ที่ส่วนกลางของ High-tech Crime ที่จะประเมินผลงาน แล้วคนของเขาจะเวียนจากส่วนกลางไปส่วนภูมิภาค หมุนเวียนอย่างนี้ตลอด คนของเขาได้เงินเดือนค่อนข้างสูง เต็มโมเดลที่เป็นผู้เชี่ยวชาญคอยให้ความช่วยเหลือสถานีตำรวจทั่วประเทศ ถ้าเราบอกว่าของเรามันใหญ่ทำไม่ได้ ญี่ปุ่นประชากรเยอะกว่าเรา เขาทำมาเป็นหลาย 10 ปีแล้ว อีกส่วนนึงคือเขาจัดสัมมนาทางไซเบอร์ทุกปี ผมก็ไปร่วมประชุมแลกเปลี่ยนความรู้ทางเทคโนโลยี เขาก็จะมีคนที่มีความรู้ความเชียวชาญเรื่องเหล่านี้ พัฒนาและประสานงานกับต่างประเทศ หมุนเวียนไปตลอด อันนี้ก็เป็นจุดนึงที่ทำให้เขาค่อนข้างที่จะก้าวหน้าในเรื่องนี้ตามทันเทคโนโลยีทั้งหมด แล้วคดีของเขาเองตรงกันข้ามกับของเราเลย คดีของเขาน้อยมากเกี่ยวกับเรื่องพวกนี้ สาเหตุนึงก็คือเขาไม่ค่อยมีเบอร์โทรศัพท์แบบเติมเงิน เขาจะบังคับเลยว่าประชากรของเขา คนนึงมีเบอร์โทรศัพท์ได้มากสุด 2 หมายเลขที่ลงทะเบียน ที่เหลือที่เป็นเติมเงินเขาจะลิมิตการใช้ มี passport ไปแสดงกลไกของเขาค่อนข้างดี ดังนั้น ในการทำงานของเขาค่อนข้างที่จะง่ายกว่าเราเยอะมาก คดีเกิดน้อย และมีประสิทธิภาพ ก็เลยทำให้เขาค่อนข้างได้เปรียบเราเยอะมากในเรื่องพวกนี้ เทคโนโลยีเขาพัฒนาใหม่ทุกปี เราก็พยายามจะเก็บเกี่ยวประสบการณ์เขาเข้ามาพัฒนาต่อ

(2) อีกส่วนนึงคือ ในส่วนของสำนักงานตำรวจแห่งชาติ ทางผบ.ตร. ท่านก็ได้เห็นความสำคัญ และมีการปรับโครงสร้างในเรื่องของการสืบสวน ก็คือยกระดับหน่วยงานสืบสวนทั้งภาค ขึ้นมาอีก 1 กองกำกับทั่วประเทศ เพราะฉะนั้นก็จะมี 1,800 คนโดยประมาณที่จะเป็นเขี้ยวเล็บให้ แล้วก็มอบโจทย์นี้ให้กับหน่วยงานผมในการที่จะทำหลักสูตรเพื่ออบรม 1,800 คนทั่วประเทศ เพื่อที่จะทำให้สามารถจัดการกับปัญหาเรื่องไซเบอร์ตรงนี้ได้ อันนี้ก็เป็นอีกส่วนนึงที่น่าจะเข้าไปอยู่ในงานวิจัย มิเช่นนั้นแล้วมันจะเป็นข้อมูลที่ไม่อัพเดท จริง ๆ แล้วผมจะจัดอบรมรุ่นแรกในปีนี้ งบประมาณมีเรียบร้อย แต่ติดในเรื่องของสถานที่ที่เราจะใช้ของโรงพยาบาลตำรวจ โรงพยาบาลตำรวจบอกว่าปีนี้คิวเต็มแล้ว ต้องรอปีหน้า ก็เสียดายที่เรายังไม่ได้เริ่มต้นทำ พอปีหน้าเรา

ต้องรองบประมาณซึ่งคาดว่าจะต้องไปต้นปีหน้า ก็เป็นช่วงนึงที่อาจเสียโอกาสไป แต่ว่าในส่วนของผมเองก็มีหลักสูตรประจำในเรื่องของการสืบสวนทางไซเบอร์ครบถ้วนทุกปี เราทำมาน่าจะ 7-8 ปีแล้ว เพราะฉะนั้นตอนนี้องค์ความรู้ในเรื่องของการสืบสวนทางเทคโนโลยีผมก็ค่อนข้างมั่นใจว่าสถานีตำรวจทุกจังหวัดทั่วประเทศ มีบุคลากรด้านนี้ประจำอยู่พอสมควร สังเกตได้จากคดีที่เข้ามาในหน่วยงานผม มาให้ช่วยระบุตัวตน เขาจะถามข้อมูลแต่ละอย่างเลย เช่น ขอทราบข้อมูล IP Address ของผู้กระทำความผิดบน Facebook Line ต่าง ๆ คือเขาค่อนข้างรู้เรื่อง

(3) แต่ปัญหาอีกอย่างหนึ่งที่มากกว่านี้ คืออยากให้เห็นตรงกันว่าเรามีปัญหาในเรื่องของผู้ให้บริการไม่ให้ความร่วมมือ ตรงนี้ไม่ได้มีการประสานงาน ผมเชื่อว่าตำรวจเริ่มมีความรู้ในการขอข้อมูล แต่พอขอข้อมูลไปเพื่อที่จะระบุตัวตน เพราะมันไม่ได้ยาก จาก IP Address ก็ Matching ไปที่ตัวโทรศัพท์มือถือหรือเบอร์บ้านก็จบแล้ว เพราะฉะนั้นผมเชื่อว่าการที่เราจะต้องไปตั้งหน่วยตรงนี้เฉพาะทาง แนวทางของท่าน ผบ. ผมคิดว่าแค่นี้ก็น่าจะเพียงพอ เราอาจจะไม่จำเป็นต้องมีหน่วยงานเยอะแยะมากมาย พอหน่วยงานสืบสวนเขามีความรู้เขาสามารถไปเป็นพยานได้ ไปสืบข้อมูลได้ ปัญหาคือทำยังไงที่จะทำให้ผู้ดำเนินการให้ความร่วมมือ ปัจจุบันเราขอข้อมูลไปเดือนนึง โดยเฉลี่ยที่เขาจะให้ข้อมูลกลับมา หรือไม่ให้ เงียบไปเลย อันนี้เจอเยอะมาก ปัญหาถามว่าทำไมเขาถึงไม่ให้ความร่วมมือทั้ง ๆ ที่ พรบ.คอมพิวเตอร์ก็บังคับไว้ ก็เพราะพรบ.คอมพิวเตอร์บังคับไว้ ถ้าเก็บข้อมูลระบุตัวตนไม่ได้ เขาก็มีโทษปรับไม่เกิน 5,000 ก็เป็นเหตุผลนึงที่เขาใช้เทคโนโลยีที่เรียกว่า Proxy ทำให้ประหยัดค่าใช้จ่าย เบอร์ IP เบอร์นึงต้อง Match กับโทรศัพท์หมายเลขนึง เขาก็ใช้วิธีการ IP หมายเลขเดียวกับเบอร์โทรศัพท์เป็น 100 เบอร์ 1000 เบอร์ เพื่อประหยัดค่าใช้จ่าย มันระบุตัวตนไม่ได้ บางทีเขาก็ทำเป็นเงียบไปเลย ตรงนี้เราไม่มีกลไกในเรื่องของการเข้าไปพัฒนาแก้ปัญหาเรื่องกลไกการระบุตัวตนที่มีประสิทธิภาพ ไม่เคยมีการบังคับใช้เรื่องพวกนี้อย่างจริงจัง ยกตัวอย่างง่าย ๆ เราไม่เคยดำเนินคดีแม้แต่คดีเดียวในเรื่องของการจัดเก็บการระบุตัวตนไม่ได้ ทั้ง ๆ ที่กฎหมายกำหนดไว้ ตัวอย่างง่าย ๆ ร้านก๋วยเตี๋ยวเขียนไวไฟฟรีเบอร์โทรศัพท์ติดข้างฝาผนัง อันนี้ไม่ใช่กลไกการระบุตัวตน ถ้ามีการทำความผิดขึ้นมาเราก็ไม่รู้อยู่ดีว่ามีใครทำความผิด ตรงนี้เราอ่อนมากในเรื่องของการบังคับใช้ ก็เลยทำให้เกิดปัญหาว่า ใครกระทำความผิดง่ายมากเลย ผมไปนั่งร้านก๋วยเตี๋ยวกระทำความผิดแล้วก็เดินไป ยังไงก็จับผมไม่ได้ ถ้าไม่มีกล้องวงจรปิดในจุดนั้นที่ดูว่าใครที่ใช้ในช่วงเวลานั้น แล้วกว่าจะได้ข้อมูลก็ไม่ทันแล้ว อันนี้ก็เป็นสาเหตุที่ว่าทำไมคดีพวกนี้มันเกิดกลาดเกลื่อนเต็มไปหมดแล้ว แก้ปัญหาไม่ได้สักที มันมาจากปัญหาหลักตรงจุดนี้ที่อยากจะนำเรียนให้ทราบ

(4) ปัญหาหลักก็คือเรื่องของกลไกการระบุตัวตนที่มีประสิทธิภาพ เพราะฉะนั้นในเรื่องของการลงทะเบียนต่าง ๆ ผมลองส่งทีมงานไปมาบุญครองก็ยังสามารถซื้อซิมแบบเติมเงินโดยไม่ต้องลงทะเบียนได้ เพราะฉะนั้นกลไกนี้เราอ่อนมากจริง ๆ เราควรที่จะต้องมีชุดที่จะตรวจสอบและดำเนินคดีกับผู้ให้บริการที่ละเลยเรื่องเหล่านี้ มิเช่นนั้นจะไม่มีทางแก้ได้เลย ผู้ให้บริการเขาก็รับปาก แต่ผมยังเห็นสนามบินแจกซิมฟรีให้นักท่องเที่ยวอยู่ เราไม่เคยดำเนินคดีเรื่องเหล่านี้เลย แล้วจริง ๆ เราควรต้องมีอำนาจในการตรวจสอบด้วยว่าผมส่งข้อมูลไปแล้วลองไปถามดู ถ้าเกิดว่าตอบไม่ได้ ผมก็สามารถที่จะปรับได้เลยทันที คือปรับทุกวันถึงจะแก้ปัญหาได้ ถ้าเราไม่มีอำนาจในเรื่องนี้มันก็จะยากมาก ซึ่งค่อนข้างเสียดายที่กลไกใน พรบ. ไม่ได้เขียนเรื่องนี้

เอาไว้ แต่ผมคิดว่าถ้าทางกระทรวง DE เอาไปบัญญัติในกฎกระทรวง พนักงาน เจ้าหน้าที่มีอำนาจในการที่จะทดสอบ ตรวจสอบ คือเราทั้งจะขอความร่วมมือและก็บังคับใช้ด้วย ถ้าเกิดเขาให้ความร่วมมือดีผมว่าก็แก้ปัญหาไปได้เยอะ แต่ในที่สุดเราก็ต้องตรวจสอบ ถ้าครั้งนี้คุณอาจไม่ได้ตั้งใจ แต่เราต้องทำให้เขาอยู่ในระบบให้ได้ อีกสิ่งหนึ่งคือ หลังจากเก็บเรียบร้อยแล้ว ระบุตัวตนได้แล้ว

(5) จะต้องมีกลไกที่สามารถขอข้อมูลให้เกิดความรวดเร็ว คนร้ายกระทำความผิดไม่กี่วินาที เราใช้เวลาเป็นเดือน ผมว่าวิธีการแบบนี้ไม่มีทางที่จะต่อสู้กันได้ เพราะฉะนั้นอาจจะต้องเปลี่ยนวิธีการจากการขอข้อมูลด้วยหมายเรียกเป็นกระดาษ ใช้เป็นวิธีการอิเล็กทรอนิกส์ทำ Application ลงทะเบียนเจ้าหน้าที่รับให้เขาเกิดความมั่นใจ หลังจากที่ขอข้อมูลไปก็ต้องตอบกลับมาภายในระยะเวลาที่กำหนด ซึ่งถ้าเกิดเราคุยกันจากกระทรวง DE ตำรวจ คุยกับผู้ให้บริการเขาไม่สนใจกัน เพราะเขาถือว่าไม่มีอำนาจอะไรที่จะไปบังคับเขา ตรงจุดนี้ผมคิดว่าเราควรที่จะให้ทาง กสทช. ที่เป็นคนออกใบอนุญาต เป็นตัวกลางทำระบบ Big Data ในการเก็บข้อมูลตามพื้นที่ เขาจะได้เลิกอ้างว่าไม่มีเงินเพียงพอที่จะไปเก็บต้องมีค่าใช้จ่าย ต้องบังคับ คุณมีหน้าที่ คุณอยากเก็บของคุณไม่เป็นไร แต่ส่วนหนึ่งจะต้องมาเก็บไว้ที่ กสทช. เพื่อจะให้บริการกับหน่วยงานที่เขาจำเป็นต้องตรวจสอบ แล้วถ้าเกิดหน่วยงานภาครัฐขอเข้าไป กสทช. ก็จะเห็นว่าขอไปกี่เรื่อง ใช้เวลาเท่าไหร่ แล้วก็จะเป็นเหตุผลหนึ่งว่า ขอไป 10 เรื่อง คุณตอบว่าระบุตัวตนไม่ได้ 10 เรื่อง ถ้าปีหน้ายังไม่ปรับปรุง ออกใบอนุญาต ถ้าไม่มีกลไกตัวนี้ไม่มีทางที่จะบังคับได้ ผมคิดว่าประเทศไทยเราอาจจะต้องมีแนวทางจากประสบการณ์ของสถานที่ทำงานว่าเราจะแก้ไขปัญหากันยังไง มิเช่นนั้นก็แก้ไม่ตรงจุดสักที

(6) ในเรื่องของการลงทะเบียนที่มีการพูดว่า ถ้าเราลงทะเบียน Social Media ได้ ก็แก้ปัญหาได้ แต่ปัญหาคือจะเปิดปัญหาสังคมขึ้นเป็นจำนวนมาก แล้วในที่สุดเราก็ทำไม่ได้ เพราะฉะนั้นตรงจุดนี้ผมคิดว่า ถ้าเรามาพบกันครึ่งทาง แทนที่เราจะลงคนเดียว 100% เราใช้วิธีการลงทะเบียนภาคสมัครใจ ใครต้องการที่จะอยู่ในระบบสีขาว ซื้อขายของกันมีความปลอดภัย คุณมาลงทะเบียนกับทะเบียนราษฎร์ ไม่ต้องไปตั้งหน่วยงานใหม่ ผมเห็น พรบ. ตัวหนึ่งที่บอกว่า ทำกลไกการระบุตัวตนให้เอกชนมาดูแล ไม่รู้ผ่านหรือยัง ตรงนี้ผมคิดว่าไอเดียตัวนี้แย่มาก ถ้า ณ วันนี้เราไม่แยกภาครัฐไปให้เอกชนมาทำบริษัท แล้วแยกกันรับลงทะเบียน แยกออกเป็น 100-1,000 จบเลย ไม่มีทางที่จะได้ข้อมูล แล้วประชาชนก็จะเป็นภาระต้องไปเสียเงินให้กับผู้ให้บริการกลุ่มนี้เพื่อเก็บข้อมูลส่วนบุคคล ซึ่งกำลังจะบอกว่าเราเชื่อเอกชนมากกว่ารัฐบาล แล้วข้อมูลสำคัญไปอยู่กับเอกชนหมดเลย เพราะฉะนั้นกลไกที่ดีที่สุด ณ วันนี้ คือ ใช้ทะเบียนราษฎร์ สำนักงานทะเบียนราษฎร์หากรัฐบาลประกาศนโยบาย หรือทางกระทรวงอาจจะชูเรื่องนี้ ให้ทางทะเบียนราษฎร์รับลงทะเบียนออนไลน์หรือออฟไลน์ ผมคิดว่าไปแสดงตัวตนที่เขตดีกว่า แล้วบอกว่าตนเองเป็นเจ้าของ Facebook นี้ Line นี้ เพจนี้ Instagram ID นี้ แล้วก็ลงทะเบียนเอาไว้ แค่นี้ก็พอแล้ว แล้วก็เปิดบริการให้ประชาชนสามารถตรวจสอบได้ เช่น Instagram นี้ผมจะซื้อขายของ ผมไปเช็คทะเบียนราษฎร์ที่เปิด service ให้ ID นี้มีการลงทะเบียนหรือยัง ถ้าตอบมาว่าลงทะเบียนเรียบร้อยโดยทะเบียนราษฎร์ ผมซื้อขายของเลย ถ้ามีการโกงผมแจ้งโรงพักให้ดำเนินคดีโดยขอข้อมูลจากทะเบียนราษฎร์ คดีจะหายไปเยอะมาก

(7) คดี ณ วันนี้หน่วยงานผมที่รับจากพนักงานสอบสวนมา สมัยก่อนมีวันละเรื่องสองเรื่อง เดี๋ยวนี้มาวันละ 10 เรื่อง เยอะมาก แล้วเรื่องหลัก ๆ ก็คือ

(7.1) คดีฉ้อโกงซื้อขายของออนไลน์ ประชาชนเราให้ความรู้ไปยังไงก็ตาม ไม่มีทางที่เขาจะรู้กันหมดทุกคน เด็กรุ่นใหม่ก็ตกเป็นเหยื่อ ก็มีวงจรอย่างนี้ไปเรื่อย ๆ เพราะฉะนั้นเงินจำนวนมหาศาลที่ถูกโกงกันใน Facebook ผ่านทาง Line ที่ระบุตัวตนกันไม่ได้เยอะมาก เขาไม่รู้กลไกตัวนี้ เพราะเขาคิดว่ามีหมายเลขบัญชีเรียบร้อย ก็จะไม่มีการโกงกัน เพราะฉะนั้นผมว่าเป็นวาระที่เราจะต้องพยายามลงทะเบียน และให้ความรู้เขาว่าก่อนจะซื้อขายของกัน คุณไปตรวจสอบใน service ทะเบียนราษฎร์ ถ้ามีก็ไว้ใจได้ ถ้ามีการโกงกันรัฐบาลยินดีจ่ายเงินให้ก่อน ทำให้เกิดความมั่นใจ

(7.2) คดีฟิชชิง (Phishing) คือ ทำหน้าเว็บหลอกลวงเพื่อที่จะให้ใส่ username password รูปแบบเปลี่ยนไปเรื่อย ๆ ตรงนี้ต้องให้ความรู้กับภาคประชาชน เพราะว่าในอดีตเราให้ความรู้กับประชาชนไปแต่รูปแบบเปลี่ยนแต่เราต้องมีหลักการให้ความรู้กับเขา ณ วันนี้เขาส่งมาเพื่อให้กลัว เช่น ส่งมาบอกว่าคุณซื้อขายของบน Apple ID หากคุณไม่ได้ซื้อตามใบเสร็จนี้ให้กดลิ้งค์นี้ ซึ่งลิ้งค์ตัวนี้เป็นลิ้งค์ปลอม พอคลิกไปก็จะขึ้นหน้าของ Apple ID ซึ่งเหมือนกัน 100% แล้วประชาชนไม่มีองค์ความรู้เลยว่าจะต้องดู url ก่อนคลิกลิ้งค์ ขนาดครูอาจารย์ที่ผมไปบรรยาย ท่านก็ไม่มีความรู้ ก็ถามผมว่าอันนี้จริงไม่จริง ผมว่าองค์ความรู้ตรงนี้ควรให้ความรู้ทั้งตำรวจ และประชาชน เป็นข่าวที่ทำไม่ยาก จะรู้ได้อย่างไรว่า Facebook หรือ ลิ้งค์นี้ปลอมไม่ปลอม ก็เอาไปวางแล้วก็ดูว่ามันตรงกับ url หรือไม่ ต้องกระตุ้นให้ประชาชนมีความรู้ จะได้ไม่ตกเป็นเหยื่อ ไม่ว่าจะมารูปแบบไหนก็ตาม อันนี้ก็จะช่วยได้เยอะ

(7.3) คดีหมิ่นประมาท เยอะมาก ภรรยาน้อย บางคนก็รู้ตัว บางคนก็ไม่รู้ เนื่องจากว่ามีการทำเป็นลักษณะอวตาร ซึ่งคดีเหล่านี้จะเกิดบ่อยกับกลุ่มนักเรียน แล้วก็เกิดเป็นคดีใหม่ที่เรียกว่า ไซเบอร์บูลลี่ เป็นสาเหตุหนึ่งที่ทำให้เด็กฆ่าตัวตาย เพราะบางทีเราอาจไม่ได้คิดว่าเป็นเรื่องสำคัญ แต่เวลาที่เด็กแกล้งกันแบบนี้แล้วเอาภาพไปดัดแปลง ไปทำให้เกิดความเสียหาย เด็กอับอาย ถึงแม้ว่าเขาจะไม่ได้ทำเอง แต่คนเชื่อตามนั้น อันนี้ก็เป็นอีกเรื่องหนึ่ง เรื่องหมิ่นประมาทไซเบอร์บูลลี่

(7.4) เรื่องของการหลอกให้โอนเงินยืมเงิน อันนี้เจอเยอะมาก ใช้ทั้งรูปแบบสร้างฟอร์มขึ้นมาหรือบางทีก็ใช้ในรูปแบบของการ Hacking แล้วก็สวมรอยในการยืมเงิน ที่เจอเยอะ ณ วันนี้คือ แฮกเข้าไปในระบบอีเมลพนักงานแล้วก็คอยดูว่าเมื่อไหร่จะมีการโดนเงินล็อตใหญ่ในการซื้อขายของ เขาจะลงทะเบียนจดโดเมนชื่อใกล้ ๆ กันกับชื่อเว็บนั้น ตัวอักษรต่างกันตัวเดียว เพราะฉะนั้นคนจะไม่ทันได้สังเกต แต่โดเมนเนมต่างกัน พอเขาได้ข้อมูลมาว่าจะมีการโอนเงินเขาก็จะใช้อีเมลตัวปลอมส่งมา โดยเอาข้อมูลของจริงทุกอย่างส่งมาให้แล้วดัดแปลงหมายเลขบัญชีเป็นหมายเลขบัญชีของคนร้ายแทน เพราะฉะนั้นพอสวมรอยในลักษณะแบบนี้ ผู้เสียหายส่วนใหญ่จะไม่ได้สังเกต เคยซื้อขายของมาเป็น 10 ปี โอนครั้งละเป็น 10 ล้าน แล้วก็ shipping ของมาให้ ก็โอนไป เสร็จเรียบร้อย เกิดความสงสัยว่าปกติเคยโอนไปให้ที่อเมริกาแล้วทำไมถึงให้โอนไปที่อังกฤษ เขาก็เลยบอกว่าตอนนี้รัฐบาลอเมริกาเก็บภาษีเพิ่ม อังกฤษลดภาษี ถ้าคุณโอนมาที่นี่ภายในวันนี้ เดี๋ยวเราลด

วงเงินให้จาก 10 ล้านบาท เหลือ 9.5 ล้าน ไม่ต้องเสียภาษี เขาก็รีบโอนให้ ก็จะสิ้นสุดวิธีการ อันนี้ก็จะเป็นรูปแบบของการหลอกโอนเงินและยืมเงิน ตัวเลขเสียหายค่อนข้างเยอะ

(7.5) เรื่องของ Sex Caltion คือ หลอกเป็นเพื่อนแล้วพยายามเปิดโชว์เพื่อให้มีอารมณ์ทางเพศแล้วใช้กล้อง webcam ในการถ่ายภาพไว้ แล้วข่มขู่ผู้เสียหาย ถ้าไม่ยอมโอนเงินมาให้ภาพจะอยู่ในกลุ่ม Facebook ของเพื่อนคุณ สมัยก่อนคนร้ายจะเป็นฟิลิปปินส์ แต่ปัจจุบันคนไทยหันมาประกอบอาชีพนี้เยอะขึ้น เนื่องจากว่าไม่ค่อยไปขายบริการทางเพศ ได้เงินครั้งละเป็นแสน พยายามไปหาเหยื่อคนที่มีชื่อเสียง แล้วก็เอาหน้าตานางแบบมาล่อเป็นตัวปลอม แล้วใช้วิธีแต่งหน้าเข้ม ๆ เพื่อหลอกเหยื่อ คดีประเภทนี้หลายสิบคดี เป็นคนที่มีความรู้อย่างดี ทั้งแพทย์ วิศวกร ตำรวจ ทหาร นักการเมือง คดีประเภทนี้เป็นอีกคดีที่จะต้องให้ความรู้กับภาคประชาชน

(7.6) แรนซัมแวร์ (Ransomware) เป็นไวรัสคอมพิวเตอร์ที่พอเปิดเครื่องแล้วจะเข้ารหัสผ่านทุกอย่าง ถ้าไม่จ่ายเงินให้คนร้ายผ่านทาง บิทคอยน์ (Bitcoin) ก็จะไม่ได้ข้อมูลคืนไม่ว่าจะเป็นรูปภาพหรือไฟล์สำคัญต่าง ๆ

(7.7) คดีเกี่ยวกับภาพลามกอนาจาร ทั้งเด็กและผู้ใหญ่ ผิดทั้ง พรบ.คอมพิวเตอร์ และประมวลกฎหมายอาญา การครอบครองภาพลามกเด็ก ก็จะมีไว้ในการล่วงละเมิดต่อเด็ก

(7.8) การพนันออนไลน์ เป็นปัญหาใหญ่อีกตัวหนึ่ง ซึ่งผมพึ่งจัด course training ให้กับตำรวจทั่วประเทศ 1 รุ่น ตามนโยบายของท่านผู้ช่วยธรรมศักดิ์ ท่านต้องการที่จะเอากองปราบมาแล้วอบรมเจ้าหน้าที่ ผมเลยจัดทำ workshop ให้เขาสามารถที่จะไปวิเคราะห์แล้วเอาข้อมูลตรงนี้มาหาตัวผู้กระทำความผิดได้ ก็คิดว่าหลังจากที่เจ้าหน้าที่สืบสวนทั่วประเทศมีความรู้ในเรื่องของการวิเคราะห์ก็จะทำให้สถานการณ์ดีขึ้น เพราะแต่เดิมเขาไม่มีความรู้เลยว่าจะไปตามอย่างไร อะไรคือข้อมูลจริงไม่จริง ซึ่งตรงนี้ผมให้ความรู้เขาไปว่า โดเมนเนมที่จดปลอมได้ทุกอย่าง แต่ที่ปลอมไม่ได้มีแค่ 2 อย่าง คือ email address ที่ใช้ในการวิเคราะห์ และข้อมูลทางการเงิน ส่วนตัวชื่อ ที่อยู่ เบอร์โทรศัพท์ สามารถปลอมได้ เพราะฉะนั้นเราต้องรู้ว่าอะไรปลอมได้อะไรปลอมไม่ได้ มิเช่นนั้นเวลาเราไปให้การต่อศาล เจอทนายซักทีเดียวก็หลุดแล้ว เพราะเราไม่มีความรู้ ไม่เคยลงทะเบียนโดเมนเนม

(7.9) ขายของผิดกฎหมาย ไม่ว่าจะเป็นอาหารและยาที่ไม่ได้รับอนุญาตให้จำหน่าย ก็เอาไปจำหน่ายกัน จำพวกครีมสรรพคุณเกินจริง ยาเสพติด ปืน

เหล่านี้ก็จะเป็นกลุ่มประเภทต่าง ๆ ที่หน่วยงานผมเจอค่อนข้างเยอะ คิดว่าน่าจะเป็นประโยชน์คดีที่อยู่ในลิสต่าง ๆ เราจะได้ทราบว่าจะต้องติดตามหรือแก้ไขปัญหาอย่างไร ซึ่งแนวทางในการแก้ไขปัญหานั้นถ้าเราเห็นรูปแบบทั้งหมด เราก็จะรู้ว่าอันไหนที่จะออกมาตรการในเชิงป้องกัน อันไหนที่เราใช้กลไกการระบุตัวตนได้ ตัวที่เราใช้ในการติดตามมาก ๆ คือในเรื่องของข้อมูลทางการเงิน การธนาคาร วันนี้ก็เช่นเดียวกัน พนักงานสอบสวนหลังจากที่รู้ว่าเป็นบัญชีคนร้ายก็ไม่ได้มีการแจ้งรายงาน เขาบอกว่ากลัวโดนฟ้องกลับ อันนี้ก็เป็นปัญหาหนึ่งทำให้คนที่เปิดบัญชีปลอมขึ้นมาได้ใจ เลยจ้างคนเปิดบัญชี แล้วคำพิพากษาออกมาว่าคนที่เปิดบัญชีมาไม่มีความผิดด้วย แล้วประกาศออกไปอีก ก็เลยทำให้ธุรกิจการเปิดบัญชีเถื่อนก็ยังได้รับความนิยม

วินมอเตอร์ไซต์ได้เงิน 2,000 บาท เพื่อเอาบัญชีธนาคารกับตัวบัตร ATM ให้ คนร้ายก็ใช้ตรงนี้ในการหลอกลวงผู้อื่นต่อ โดยที่เราบอกว่าเราดำเนินคดีกับเจ้าของบัญชีไม่ได้ ทั้ง ๆ ที่ทางธนาคารก็เตือนแล้วว่าถ้าทำแบบนี้จะมีความผิด ถ้ากฎหมายไม่ผิดเราก็ต้องดำเนินให้เป็นความผิด มิเช่นนั้นแล้วจะแก้ไม่ได้ กลไกในการประสานกับแบงค์ อาจจะต้องดูจากผู้ให้บริการทั่วไปโดยเฉพาะข้อมูลทางการเงินด้วย เพราะฉะนั้นพอมีเหตุเกิดขึ้นเราจะได้มอนิเตอร์เงินเข้าเงินออก หรือติดตามแบบเรียลไทม์ ใครมากดเงินหน้าตาเป็นอย่างไร ส่งเจ้าหน้าที่ไปรวบตัวดำเนินการ มิเช่นนั้นมันจะเกิดเป็นรายวันอยู่อย่างนี้ จะแก้ปัญหาแบบ case by case แบบนี้ไม่ได้ จะต้องมีศูนย์ที่คอยเฝ้าติดตาม

3) นักวิทยาศาสตร์ (สบ.4) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 7 สำนักงานพิสูจน์หลักฐานตำรวจ ได้ให้ข้อคิดเห็น ดังนี้

ในส่วนของงานพิสูจน์หลักฐานตำรวจก็มีการมองล่วงหน้าแล้วว่าจะต้องมีหน่วยงานที่ทำหน้าที่ตรวจพิสูจน์ด้านอาชญากรรมคอมพิวเตอร์ ก็เลยมีการจัดตั้งขึ้น 11 หน่วย เป็นหน่วยงานในระดับกองบังคับการที่กองพิสูจน์หลักฐานกลาง และพิสูจน์หลักฐาน 1-10 ซึ่งแสดงให้เห็นว่าสำนักงานตำรวจแห่งชาติมองเห็นถึงความสำคัญตั้งแต่ปีนั้นแล้ว ในส่วนที่เราทำไปบ้าง ก็จะขอเรียงลำดับความคิดเห็น ในส่วนของความคิดเห็นของการปฏิบัติการ หน่วยงานของ ปอท. และ สทส. ถือว่าเป็นหน่วยงานที่มีความเข้มแข็งมาก ในส่วนของงานพิสูจน์หลักฐานตำรวจเราได้ทำการพัฒนามาโดยตลอด โดยเฉพาะอย่างยิ่งเมื่อปีที่แล้ว ถึงปีปัจจุบัน เราได้มีการบรรจุคนถือว่าทำครบเต็มจำนวน เพราะฉะนั้นในทุกศูนย์ 11 ศูนย์ของเรามีคนแล้ว เพียงแต่ว่าคนของเราที่บรรจุขึ้นมายังทำงานไม่ได้ ก็ต้องมีการฝึกอบรมเพื่อให้ได้ใบรับรองการออกรายงานก่อน เพราะฉะนั้นภายในอีก 2 ปีข้างหน้าเราจะสามารถทำงานได้อย่างมีประสิทธิภาพ ส่วนที่ความเข้มแข็งน้อยหน่อยก็คือส่วนของสถานีตำรวจ ซึ่งสำนักงานตำรวจแห่งชาติได้เริ่มแก้ไขแล้ว โดยเอาสถาบันการศึกษาหลักคือสำนักงานส่งเสริมการสอบสวนของสำนักงานตำรวจแห่งชาติ ในการถ่ายทอดความรู้โดยเป็นวิชาหลักเลย ตอนนี้เอาวิชาด้านอาชญากรรมคอมพิวเตอร์มาบรรจุไว้เป็นหนึ่งในวิชาหลัก แล้วเราก็ได้เริ่มดำเนินการต่อ เจ้าหน้าที่ตำรวจในส่วนของพนักงานสอบสวน แล้วเราก็จะทำแบบนี้กันต่อไป อันนี้ถือว่าเริ่มมีความรู้ ตรงนี้เราร่วมทำงานร่วมกัน กองพิสูจน์หลักฐานตำรวจเราทำงานร่วมกัน โดยให้แต่ละศูนย์ ถึงแม้ว่าบางศูนย์ตอนนี้เปิดการตรวจทางด้านอาชญากรรมคอมพิวเตอร์แค่ 3 ศูนย์ ในกรุงเทพฯ ศูนย์พิสูจน์หลักฐาน 7 และศูนย์พิสูจน์หลักฐาน 10 เป็นหลัก ที่เหลืออีก 8 ศูนย์จะต้องเป็นที่ปรึกษาคดี เพราะฉะนั้นถ้าตำรวจมีปัญหาสามารถโทรมาสอบถามได้ หรือจะดำเนินการอย่างไร แนวโน้มของการตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ จากที่ผมศึกษา ของผู้ต้องหาเขาปฏิเสธว่าคอมพิวเตอร์หรือโทรศัพท์ของกลาง ไม่ใช่เขาใช้งานคนเดียว มีคนอื่นด้วย ทุกคนที่นั่นจะต้องมีความรู้ด้านนี้ มันเป็นจุดอ่อนมากที่ตำรวจโรงพักจะได้รู้ รอบคอบและชัดเจน

4) ผู้เชี่ยวชาญเฉพาะด้านคดีพิเศษ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ได้ให้ข้อคิดเห็น ดังนี้

(1) สิ่งแรกเป็นข้อสำคัญที่สัมผัสได้เลย คือ การไม่ให้ความสำคัญกับเรื่องอาชญากรรมคอมพิวเตอร์เท่าที่ควร ยกตัวอย่างจากหน่วยงานของตัวเอง เช่นบอกว่าถ้าเรื่องนี้สำคัญเราก็จะวิเคราะห์ในด้านนี้ค่อนข้างเยอะ เคยมีคำถามเยอะมากว่าที่กรมก็มีคนเก่งเยอะนะ แต่ทำไมทำงานแล้วยังไม่เก่งอย่างที่ได้ตั้งใจ เมื่อวาน

ลองวิเคราะห์แล้วคุยกันเล่น ๆ เขาบอกว่าคนเก่งมีเยอะก็จริง แต่วางไม่ถูกที่ อันนี้เป็นข้อน่าคิดนะ ในเรื่องของการบริหารงานบุคคลธรรมดาพื้น ๆ นี่แหละ โดยบอกว่าทำไมไม่แต่งตั้งคนนั้น เราเขาจะเก่งขึ้นมาในทันที เหมือนว่าเอาเขาไปอยู่อีกที่นึงเขาเลยไม่เก่ง แล้วไปโทษเขาบอกทำไมไม่เก่ง ก็เอาเขากลับไปอยู่อีกที่นึง แล้วเขาก็จะเก่งเอง จริง ๆ เขาเก่งได้มากกว่านั้นด้วย ถ้าเอาเขาไปอยู่อีกที่นึง แล้วเขามีความสบายใจ มีเรื่องที่สามารถสนับสนุนบุคลากรได้หลายทาง เช่นการส่งเสริม หรืออย่างที่บางท่านได้พูดไปแล้ว บางทีมีอะไรที่พิเศษหรือการดูแลเป็นพิเศษ นอกเหนือจากทางอื่น นี่คือการมองข้ามถึงการให้ความสำคัญเรื่องบุคลากร

(2) อีกตัวอย่างหนึ่งคือ เรื่องของการแบ่งระดับการทำงาน จริง ๆ เป็นเรื่องสำคัญ ถ้าเราไม่รู้ว่าเราตั้งจุดรวมอยู่ตรงไหน การมองภาพต่อไปจะไม่เหมือนกันเลย ถ้าเราบอกว่าอันนี้เรื่องสำคัญนะ แล้วมีระดับความสำคัญมากน้อยแค่ไหน ต่อไปในเรื่องของโครงสร้างจะแตกต่างกัน บางคนบอกหน่วยงานขนาดนี้ หน่วยงานเล็ก ๆ ขนาดนี้ งั้นเอารถคันเล็กก็พอ มอเตอร์ไซต์คันเดียวก็พอ แต่ทุกหน่วยงานมีความซับซ้อนใหญ่มากขึ้น จะเป็นแบบนี้ไม่ได้ อาจจะต้องมีรถใหญ่มากกว่านี้ หรืออาจจะต้องมีรถเป็นขบวนเลยก็ได้ อยู่ที่การมองภาพว่า ถ้าเกิดเราแบ่งระดับพวกนี้ เราจะให้ความสำคัญอย่างไร เช่น จะมีหน่วยงานใดที่เกี่ยวข้อง จะมีองค์ความรู้อะไร เราต้องมีหน่วยสนับสนุนไหม ต้องมีมากน้อยแค่ไหน มีทีมที่ปรึกษาไหม มีทีมผู้เชี่ยวชาญ ซึ่งเราจะเอามาจากตรงไหน อันนี้คือเรื่องของการให้ความสำคัญ บางทีถึงบอกว่าเป็นโรงพัก หรือระดับนั้น ระดับนี้ ขีดความสามารถของเขา ในการรองรับ ถ้าเราตั้งวัตถุประสงค์ได้ถูกต้อง เราก็จะพัฒนาได้ก่อน อีกอันหนึ่งก็มีความสำคัญเช่นเดียวกัน ในเรื่องของการสร้างมาตรฐาน ที่เราคุยกันทุกวันนี้ก็คือเช่นเดียวกัน

(3) ถ้ามองไปไกลกว่านั้น ในเรื่องของสื่ออิเล็กทรอนิกส์หรือสื่อดิจิตอลมีมาตรฐานค่อนข้างสูง บางคนไม่เข้าใจ ยกตัวอย่างเช่น เราไปมองเรื่องของพยานหลักฐาน อย่างที่ได้บอก จริง ๆ แล้วเขามองไปไกลกว่าที่จะเป็นพยานหลักฐาน ยังไม่ทันระบุเลย เรายังไม่รู้ว่าพยานหลักฐานมายังไง อะไรที่มาเกี่ยวข้องที่จะเป็นพยานหลักฐานได้ อันนี้คือเกิดขึ้นก่อน แต่บางคนมองไปแล้ว ขโมยหลักฐาน อะไรที่เป็นพยานหลักฐานบ้างไม่รู้หรอก แค่หยิบมาแต่หยิบไม่ครบ หยิบมาแล้วผิด หยิบมาแล้วใช้ไม่ได้อีก อย่างที่บอก ยิ่งไปกันใหญ่เลย เลยไม่รู้ว่าความเชื่อมโยงของคดีเป็นอย่างไร อธิบายไม่ถูก กลายเป็นไม่รู้เรื่องเลย

(4) อีกเรื่องที่มีความสำคัญเช่นเดียวกันก็คือ หน่วยที่สนับสนุนต่าง ๆ ผมว่าบางทีหน่วยที่ปฏิบัติจริง ๆ เขาก็ไม่มีขีดความสามารถระดับนั้น อย่างเช่นหน่วยที่ทำหน้าที่ในเรื่องของการวิเคราะห์ คดีบางคดีไม่ได้ตรงไปตรงมา มองดูแล้วมีการปรับเปลี่ยนไปเรื่อย ๆ บางทีการวิเคราะห์แบบนี้เป็นการนำเอาข้อมูลที่ได้มาเยอะแยะมากมายแล้วมันมองไม่เห็น แต่ถ้ามีหน่วยวิเคราะห์ยังสามารถวิเคราะห์แล้วเชื่อมโยงบอกได้ว่าสิ่งที่คุณมองจริง ๆ แล้วภาพมันเป็นแบบนี้นะ มันน่าสนใจนะ แต่คือข้อมูลที่เราทุกคนต้องมองเห็นเหมือนกันไปหมด ก็เลยไม่ได้ติดใจอะไร แต่หน่วยที่วิเคราะห์มาบอก ทำให้เห็นขึ้นมาเลย มันมีความสำคัญ กับอีกส่วนหนึ่งในเรื่องของการตรวจพิสูจน์ทางคอมพิวเตอร์ ผมก็มองเหมือนกันกับที่ได้บอก แต่ผมมองเห็นลึกมากกว่านั้น บางทีจำนวนคนก็ไม่ได้บอกอะไร เพราะจำนวนคนที่มีก็มากพอแล้ว มันอยู่เรื่องของการให้บริการว่าครบถ้วนหรือเปล่า เพราะเดี๋ยวนี้มันค่อนข้างเยอะ

(5) เรื่องการตรวจพิสูจน์มีหลายมาตรฐานมาก ถามว่าเรารองรับได้ไหม เพราะพยานหลักฐานที่เข้ามาเกี่ยวกับเรื่องนั้นเรื่องนี้ ถามว่าเตรียมอุปกรณ์พร้อมไหม ตัวเจ้าหน้าที่ของเราพร้อมไหม ที่จะสร้างคนสร้างในฐานะที่เป็นผู้เชี่ยวชาญ จริง ๆ ตัวคนก็อาจจะยาก ต้องมีพื้นฐานด้านไหนบ้าง ยกตัวอย่างเช่น บางทีมีภาพ มีวิดีโอ ก็ถามว่าอันนี้ตัดต่อหรือเปล่า อาจจะต้องมีผู้เชี่ยวชาญทางด้านภาพ เสียง การตัดต่อ หรืออะไรก็แล้วแต่ อาจจะต้องมีมากกว่านี้ เพราะอีกหน่อยพยานหลักฐานที่จะเข้ามาที่เราจะใช้ประโยชน์ได้ มาวิเคราะห์อาจจะมากกว่านั้น ที่ไม่ใช่มาวิเคราะห์ในเรื่องของการใช้งานคอมพิวเตอร์อย่างเดียว หรืออะไรอย่างเดียว อาจจะมีอะไรที่หลากหลายมาก เพราะฉะนั้นต้องสร้างผู้เชี่ยวชาญให้มากขึ้นเพื่อรองรับกับเหตุการณ์ต่าง ๆ ที่เปลี่ยนแปลงไป สิ่งที่ผมมองในเรื่องของการเปรียบเทียบกับหน่วยงานของต่างประเทศ ผมคิดเหมือนกันเลยที่จะเอาแบบนั้นเหมือนกัน สิ่งที่เรามองหรือวิเคราะห์อยู่อาจจะต้องทำตามของที่นู่น พวกสิงคโปร์ หรือหน่วยงานที่เกี่ยวข้อง เราต้องทำแบบนั้นเลย แล้วก็ลงรายละเอียด โครงสร้าง ความรับผิดชอบ เครื่องมือ แนวความคิดของเขาที่ทำให้ประสบความสำเร็จ ซึ่งเป็นไอเดียที่ดีเหมือนกัน เราจะได้ไปได้มากกว่านี้ จะได้รู้ว่าแต่ละส่วนมีรายละเอียดอะไร มีแง่คิดอย่างไร หรือว่ามีความเหมาะสมอย่างไร

5) ผู้กำกับสถานีตำรวจภูธรหนองม่วง จังหวัดลพบุรี ได้ให้ข้อคิดเห็น ดังนี้

(1) จากประสบการณ์ที่เคยอยู่ ปอท. ก็พบปัญหา อยากจะเพิ่มเติมในเรื่องของคดีที่เป็นบัญชีม้า หรือบัญชีที่มีผู้เปิดรับจ้าง เคยหารือกับท่านผู้พิพากษา ท่านบอกว่าคดีม้าคนที่เปิดบัญชี แล้วโอนเข้าบัญชีผู้เปิดต้องลงเป็นผู้ร่วมกันกระทำความผิด แล้วตอนนี้ สนช. ก็มีอยู่ฝากขังศาลชั้นต้น ผมได้ประสานกับท่านว่ามีฎีกาที่ไหน ท่านรับปากว่าท่านจะตามฎีกาคดีนี้ให้ เพราะท่านบอกว่าถ้าไม่มีบัญชีม้าความผิดมันจะไม่เกิด เพราะมันเกิดจากบัญชีม้าทั้งนั้นเลย ผมอยากเรียนให้ทราบว่าตอนนี้ผมรอฎีกา ถ้าฎีกาลงพนักงานสอบสวนก็คงจะกล้าอายัดและกล้าแจ้ง อันนี้ก็คือข้อที่จะเพิ่มเติมนะครับ ทีนี้ในเรื่องของประสบการณ์ที่อยู่โรงพักมา อย่างถ้าเป็นคดีเทคโนโลยี พนักงานสอบสวนหาทางปัดได้ปัด อย่างคดีตอนที่ผมเป็นผู้กำกับอยู่ที่หนองม่วง ลพบุรี ผู้เสียหายคนหนึ่งโอนเงินผิด ซึ่งคดีนี้ก็ไม่ได้เป็นคดีอาชญากรรมอะไร เพียงแต่ว่าเขาโอนผิดบัญชีเท่านั้นเอง แล้วเขาก็มาแจ้งความ พนักงานสอบสวนบอกว่าคุณโอนเงินผิดที่ อ.ม่วงค่อม คุณต้องไปหาพนักงานสอบสวนที่ม่วงค่อม ทั้ง ๆ ที่บ้านเขาอยู่หนองม่วง ธนาคารบอกว่าต้องเอาใบแจ้งความมา แล้วภายใน 30 วันจะแจ้งให้ทราบ พอพนักงานสอบสวนไล่ออกจากโรงพัก พอดีผมเห็นเขาเดินออกมาน้ำตาซึม ผมก็เลยเรียกมาถามว่าเกิดอะไรขึ้น เขาบอกว่าโดนพนักงานสอบสวนไล่ให้ไปแจ้งความที่ม่วงค่อม ถามว่าเรื่องอะไร เขาก็บอกโอนเงินผิด ผมก็เลยให้เข้ามาคุยกับผม ผมก็เลยดำเนินการให้ ก็ขอเลขบัญชี พอรู้หมายเลขบัญชีก็กดไปถึงเจ้าของบัญชี ปรากฏว่ามีเจ้าของบัญชี 8 คน ชื่อซ้ำ นามสกุลซ้ำ ธนาคารเลยขอเลข 13 หลัก พอได้เลข 13 หลักเสร็จ ก็ทราบว่าใครเป็นเจ้าของบัญชี ผมใช้เวลาจากที่ตรวจจนได้เงินคืน ใช้เวลาไปประมาณ 27 นาที คือเราจะตอบสนองให้ความสุขแก่ประชาชนได้ทันท่วงที มันก็คือแรงขับเคลื่อนของเรา มันเป็นสิ่งเล็ก ๆ ของหน่วยงานทางเทคโนโลยี ก็ไม่ได้มีผู้ก่อเหตุเพียงแต่ว่าเขาโอนเงินผิด ซึ่งคดีแบบนี้มีเยอะ

(2) ผมไปสอนที่โรงเรียนนายร้อยตำรวจ ก็ยกตัวอย่างคดีนี้ ถือเป็นความภาคภูมิใจ การที่จะเอาเงินไปคืน พนักงานสอบสวนจะต้องเตือนอยู่แล้ว ผมอยู่โรงพักหนองม่วงในช่วงเวลาสั้น ๆ 3 รายก็ได้คืนทั้ง 3 ราย

แต่ถามว่ามีอีกคดี ผมสอนนักเรียนนายร้อยตำรวจอยู่ พนักงานสืบสวนที่อุดรก็โทรเข้ามาเลยว่า ธนาคารที่เขาโอนเงินผิดเนี่ย เขาโอนเงินคืนแล้ว เขาดีใจมากร้องไห้เลย มันเป็นสิ่งที่จับต้องได้ ที่เกี่ยวข้องกับเทคโนโลยี ถ้าพนักงานสืบสวนหรือผู้ที่ประจำสถานี ถ้าไม่มีผู้เชี่ยวชาญหรือไม่มีผู้ที่รู้จักอะไรต่าง ๆ มันก็จะตอบสนองตรงนี้ไม่ได้ ก็จะทำให้เขาทุกข์ต่อไป

(3) พนักงานสอบสวนเวลาที่เจอ จะใช้วิธีป้องกันตัวเวลามีใครมาแจ้งความ พยายามพิจารณาหลักฐานก่อน กระบวนการพนักงานสอบสวนผมเคยเรียกว่าหล่น แล้วเขาก็บอกว่าพอคนมาแจ้งความไม่รู้จะเริ่มต้นอย่างไร จะรับอย่างไร เริ่มต้นจากจุดไหน ผมก็ถามรู้จัก IP Address ไหม เขาก็ถามว่าคืออะไร แล้วรู้จัก Phishing ไหม คืออะไรตกปลาหรอ เพราะฉะนั้นพนักงานสืบสวนผมได้ยินมาว่า เวลาคนจับเขาเอามือถือมา คุณจะต้องให้เขาบันทึกอีมี่ไว้ด้วย เพราะมันมีหลายเคสที่ตอนผมอยู่

(4) มีหลายเคสที่จับแล้วยึดโทรศัพท์ของคนร้ายได้ มีหลักฐานอยู่ในโทรศัพท์เยอะแยะเลย แต่พอไปถึงเจ้าหน้าที่ตรวจพิสูจน์ ปรากฏว่ารุ่นเดียวกัน ยี่ห้อเดียวกันทุกอย่าง แต่เป็นคนละเครื่อง พอตรวจพิสูจน์ออกมาก็ไม่ใช่เครื่องเดียวกันเป็นวิธีที่เปลี่ยน และนี่ก็คือปัญหาของพนักงานสอบสวนแล้วมันก็ลามไปต่อที่ว่าพอไปขึ้นศาลโดนตั้งก่อการทุจริตแล้ว เพราะไม่มีผู้ซื่อสัตย์ ทั้งเรื่องของท่านที่พูดไว้ในเรื่องความกลาดเคลื่อนเป็นปัญหาที่เกิดขึ้นจริง

(5) เรื่องโรแมนซ์สแกม ผู้ที่ใช้รูป Facebook ปลอม แล้วเอาโฆษณาใครเหงาเรียกกันได้ แล้วก็เบอร์จริง ๆ ของคนนั้นไปเลย แล้วก็คนที่เปิดคือใครก็ไม่รู้ แกล้งกันเดี๋ยวนี้มีคนบอกว่าเป็นการฆ่าคนตายก็มีคดีไปติดเช็คติดอะไรต่าง ๆ เค้าบอกให้โอนแล้วไม่ได้เป็นเงินดอลล่าร์ หรือว่าสกุลบาท เป็นสกุลทางไอที เป็นบิทคอยน์ มันก็ตามยากนะ แล้วยังมีอีกสกุลหนึ่งที่ชื่อลิบร้า (Libra) ถ้าเกิดขึ้นในโลกสะเทือนเลย ลิบร้าของ Facebook จะพ้นผิดขนาดไหน ลิบร้าตัวนี้ในปัจจุบัน เรามีโครงสร้างอย่างสวยหรู ไหน ๆ ก็ไหน ๆ แล้วขอพูดความคับใจนิดหนึ่ง ว่าผมเป็นผู้กำกับ ปอท. ผมจบโทไอที ซึ่งมีกำหนดสเปคอยู่แล้ว ขึ้นรองผู้การได้โดยไม่ต้องวิ่งเต้นอะไร แต่ผมก็ไม่ได้ สุดท้ายตำแหน่งก็มีการขอยกเว้นเอาคนนี้ที่ไม่มีความรู้ไอทีมาเป็นรองผู้การ แล้วผมก็เป็นผู้กำกับเหมือนเดิม อันนั้นคือสำหรับโครงสร้างอย่างที่เราทำ เพราะสุดท้ายจะปรับจริงมันจะได้ไหม ผมก็หน้าแตก เรากางดูแล้วตำแหน่งนี้มีรองสารวัตรไอที ผู้บังคับหมวดไอทีเต็มเลย เรียกมาประชุม ใครเชี่ยวชาญเรื่องไหน ทุกคนเงียบกันหมดเลย

(6) ในเรื่องของการกักเก็บไฟล์พรบ.คอมพิวเตอร์ ถ้าบังคับใช้ได้ ถ้าไม่เกี่ยวกับไฟล์มันปรับถึง 500,000 แล้วสุดท้ายยังไม่เห็นมีใครเคยโดนปรับเลย แล้วใครจะกล้าทำการดำเนินคดี มีแรงพอไหม มีพาวเวอร์พอที่จะดำเนินคดีกับเขาไหม เพราะฉะนั้นแต่ละบริษัทพวก ISP ก็จะใหญ่ ผมก็เห็นด้วยว่าจะทำยังไง อันนี้คือสื่อเขาพูดไปถึงเรื่องจริงพูดถึงความเป็นจริงว่าการขอข้อมูลจาก ISP ก็ดีจาก Bank ก็ดีจะถามว่าปัจจุบันใครได้ประโยชน์ รัฐบาล แต่พอผมขอ ผมใช้เวลา 3 ชั่วโมง 5 ชั่วโมง วันรุ่งขึ้นผมได้เลย บางคนก็จะถามว่าผมได้ได้อย่างไร อันนี้ก็ต้องเรียนกันตรง ๆ เลยว่าถ้าเราไม่มี connection ข้าง ๆ ไม่มีทางได้ พอตามไป เขาจะพูดมาเลยว่ามีคดีส่งมาเป็นตั้ง ๆ ทีนี้เราต้องเรียงตามลำดับ แต่ถ้าเรารู้จักข้าง ๆ เราก็จะได้เร็ว

6) ผู้อำนวยการการป้องกันและปราบปรามการกระทำความผิด ทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ให้ข้อคิดเห็น ดังนี้

(1) ในเรื่องของโครงสร้างผมเห็นความเหลื่อมล้ำของหน่วยราชการ สมัยก่อนตอนที่ยึดอำนาจเพื่อนกันหลาย ๆ คน กินนอนด้วยกัน ตอนนี้เขาเป็นพลโท บางคนพลเอกไปแล้ว แต่เรายังเท่าเดิมอยู่ ทหารทำไมไปไวจัง ตำรวจก็เหมือนกัน ตำรวจผมเห็นศูนย์พิสูจน์หลักฐานเยอะแยะเลย สูงสุดในนั้นก็ยังเป็นพันเอกอยู่เลยเขาก็ไม่ได้มีกำลังใจในการทำงาน ทั้ง ๆ ที่งานเขาก็เยอะแยะไปหมดเลย แต่ถ้าเป็นอีกหน่วยงานหนึ่ง ถ้าเป็นทหารจะไปไวมากเลย ทีนี้ผมเห็นตำรวจมีการยึดแท่งสอบสวน ผมถามเพื่อนหลายคนเขาบอกไม่อยากอยู่แล้ว งานก็เยอะ ทำไม่ถูก ทำไม่ไวก็โดนด่า

(2) ทีนี้หน่วยงานทางด้านเทคโนโลยี ผมอยากให้เป็นเทียบเท่ากับกรม สูงสุดน่าจะเป็นพลโทคอยดูแลและวงล้อมันจะได้เจริญ ต่อไปงานทางด้านเทคโนโลยีจะมีความซับซ้อนเยอะขึ้น คดีมันหลากหลาย อยากให้เป็นระดับกรมไปเลย แล้วคนที่ทำงานตรงนี้อาจจะต้องไปฝึกอบรมอะไรสักอย่าง ใครจะมาอยู่ตรงนี้ได้ต้องผ่านหลักสูตรนี้ก่อน แล้วก็ให้วนเวียนอยู่ตรงนี้ ถ้าจะย้ายเขาไปที่อื่นก็ต้องหาคนมาแทนให้ได้ เพราะผมเห็นหลายหน่วยงาน อย่างที่ผมเคยทำงานกับปอท. ผู้การแปปเดียวก็ไปแล้ว ทีนี้คนที่มาอยู่ก็ต้องมาเรียนรู้ใหม่ ทีนี้ก็ต้องมามองเรื่องอะไรต่าง ๆ อาจจะมีปัญหาหน่อย ตอนที่ผมไปฝึกอบรม ผมเห็นน้องคนหนึ่ง ผมถามว่าคุณอยู่ที่ไหน เขาบอกว่าเขาย้ายมาจากตำรวจทางหลวง จริงๆคนที่จะทำงานหน่วยงานนี้ อาจจะต้องฝึกอบรมอะไรสักอย่าง เพื่อเป็นกำลังใจ หรือว่าจะหาเงินเพิ่มเป็นพิเศษอะไรอย่างนี้ อย่างผมเป็นนักคอมพิวเตอร์ ก็จะมีตำแหน่งอะไรพิเศษให้

7) นักวิทยาศาสตร์ (สบ.4) กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ ศูนย์พิสูจน์หลักฐาน 7 สำนักงานพิสูจน์หลักฐานตำรวจ ได้ให้ข้อคิดเห็นเพิ่มเติม ดังนี้

(1) เรื่องเลื่อนตำแหน่ง ในหน่วยงานผมทำงานด้านไอทีมีความเชี่ยวชาญ ต้องเรียนว่าไม่มีเงินประจำตำแหน่งเลย ก็เป็นส่วนหนึ่งที่ต่อสู้มาค่อนข้างนานมาก เขามองว่าตำรวจหน่วยนี้ไม่ใช่ฝ่ายปราบปราม ไม่ใช่สืบสวน เลยไม่ต้องได้เลยสักอย่างหนึ่ง เราไม่ได้อยู่ในสเปคที่จะได้เลยแม้แต่อย่างเดียว ผมก็สงสัยว่าตำรวจที่เป็นยามเฝ้าหน้า ตร. ก็ยังได้เขาบอกว่าปราบปรามก็ต้องปราบปราม อย่างผมสืบสวนทางเทคโนโลยีช่วยวิเคราะห์ระบุตัวผู้กระทำความผิดหมดเลย เขาบอกว่าไม่เกี่ยวข้อง ไม่ได้อันนี้ก็ต้องต่อสู้ครับ ผมก็ต่อสู้ 2 ประเด็น คือ เรื่องแรกก็คือขอเงินพิเศษ เขาบอกว่าต้องเป็นคุณวุฒิโดยตรง เป็นทางคอมพิวเตอร์ถึงจะได้ ผมมาประชุมในฐานะตัวแทนหน่วย ผมยืนยันว่าถ้ามีคุณวุฒิครบเอาตามนี้ ใครไม่มีคุณวุฒิครบไม่ต้องแต่งตั้งเลยก็ได้ขอให้เป็นหน้าที่ตัวเอง ไม่มีความจำเป็นเลยครับ ที่จะเอาตำรวจที่ไม่มีคุณวุฒิมาประจำ แล้วก็มาบอกว่าพอไม่มีคุณวุฒิก็เลยไม่ได้เงิน เดี๋ยวเขาจะมาฟ้องร้องอีก ไม่ต้องบรรจุเลย ใครที่มีอยู่แล้ว แล้วอยากได้เงินเพิ่มก็ต้องไปเรียนคุณวุฒิเพิ่ม แล้วคุณก็เป็นการแก้ปัญหาชั่วคราวในการเลื่อนตำแหน่ง อนาคตจะต้องไม่มีมาบรรจุ ปล่อยให้ว่างไปเลย ไม่ใช่ไปเอาใครมาทำก็ได้ มันก็จะแก้ปัญหาไม่ได้ ก็คือยอมให้สเปคแข็งเลย พวกอบรม 18 ชั่วโมง ตัดทิ้งไปเถอะ ไม่มีประโยชน์เลย ประสบการณ์ทำงานมาหลายปีเนี่ย ผมยืนยันว่าทำงานไม่ได้ แม้กระทั่งเราทำหลักสูตรประมวลผลให้เรียน 1 ปี ก็ยังทำงานไม่ได้ เพราะการที่เราจะให้คุณวุฒิเนี่ยมันง่ายกว่ามหาวิทยาลัย

เพราะงั้นตรงนี้เราไม่ต้องมารับภาระอบรมอะไรพวกนี้ เอาคนที่เขามีคุณวุฒิมาดีกว่า แล้วก็อบรมเพิ่ม แต่ก็คือว่าตรงนี้จะเป็นแนวทางการแก้ปัญหา

(2) อีกส่วนหนึ่งก็คือตำรวจชั้นประทวน ชั้นผู้น้อย พอเราไม่มีเงินให้ เขาก็ไม่อยู่ เขาหนีไปอยู่หน่วยอื่นที่มีเงินประจำตำแหน่งเข้ามา เพราะฉะนั้นเด็กที่เข้ามาจากสายคุณวุฒิที่เป็นพวกช่างที่มีความรู้ความสามารถ รับมาไม่กี่ปีพอเขาครบเขาก็ย้ายออก ก็เลยทำให้บุคลากรของเราไม่เพียงพอ ผมก็เลยเสนอ ตร. ว่าควรจะต้องมีอีก 1 สายขึ้นมาใน ตร. ไม่ใช่มีป้องกันปราบปรามและก็สืบสวน แต่จะต้องมีอีก 1 สายหนึ่ง คือสนับสนุนงานป้องกันปราบปราม แต่เพื่อที่จะให้พวกเราสามารถเอาเงินตรงนี้ให้กับเจ้าหน้าที่ที่เป็นหน่วยงานด้าน IT ได้ อย่าไปเทียบว่า IT กับตำรวจ เหมือนกับ IT หน่วยงานอื่นที่ต้องให้ทุกคนทั่วประเทศ ไม่ใช่นะ เราเป็นหน่วยงานด้าน IT ที่ช่วยในเรื่องของงานป้องกันและปราบปรามโดยเฉพาะ เพราะฉะนั้นคนกลุ่มนี้ควรจะต้องได้เงินประจำตำแหน่งในกลุ่มนี้ มิฉะนั้นเราจะบอกให้คนกรอกข้อมูลลงในสถิติคดีอาญา คนพวกนี้ไม่มีเงิน ต้องไปเอาสายป้องกันปราบปรามมาประจำ ซึ่งผมบอกว่าทำไมเราต้องเอาสายป้องกันปราบปรามมาเพราะเขาจะไม่ได้เงิน มันก็เลยเป็นเหมือนการแก้ไขปัญหาแบบแก้ไม่ตรงจุด เอาคนที่มีเงินประจำตำแหน่งตรงนี้มา แล้วตรงนี้ก็ไม่มี ทั้ง ๆ ที่ตรงนี้ต้องเป็นฝ่ายอำนวยการ ถ้าอย่างนั้นงานโรงพักทั้งหมดต้องได้เงินทั้งหมด เพียงแต่ว่าเราแก้ไม่ตรงจุด คือเพิ่มมาอีกหนึ่งสาย ล่าสุดที่ไปชี้แจงทาง กต. เขาบอกว่าเขาจะลองรับไปดำเนินการ ซึ่งตรงนี้เคยคุยแล้วก็เห็นด้วย แต่ว่าอาจจะต้องมีการผลักดัน งานวิจัยในครั้งนี้ควรบรรจุไฟล์เป็นคำแนะนำได้ มันก็จะรองรับกัน ทำให้แก้ปัญหาด้านนี้ได้ตรงจุดมากขึ้น

(3) อีกส่วนหนึ่งที่หลายคนพูดกันก็คือ การให้ความดีความชอบการแต่งตั้งมีปัญหา อันนี้ผมเห็นด้วยว่านอกจากเงินแล้ว ความก้าวหน้าในชีวิตราชการ ไม่มีการพัฒนาเท่าที่ควร โดยเฉพาะเรื่องขั้นเงินเดือน เราก็จะเจอให้เขียนประเมิน ก็เขียนกันไป พอถึงเวลาอยากให้ใครก็หยิบยกคนนั้นขึ้นมา มันไม่ตอบสนองในความเป็นจริง บางคนไปช่วยราชการแต่ได้ขั้น คนที่อยู่ก็มองหน้ากันว่าต่อไปตัวเองอยากได้ขั้นไม่ต้องทำงาน ไปชงกาแฟดีกว่า นี่คือวิธีการที่ผิด เพราะฉะนั้นผมคิดว่าหลายประเทศเขาแก้ปัญหาตรงนี้ได้อย่างไร ผมศึกษาหลายประเทศ เคยคุยกับเพื่อนก็บอกว่าประเทศเขาใช้วิธีการประเมินแบบ 360 องศา หมายความว่าผู้บังคับบัญชา เพื่อนร่วมงาน ลูกน้องประเมินกันหมด แต่น้ำหนักไม่เท่ากัน ผู้บังคับบัญชามีแต้มเยอะกว่า เพราะฉะนั้นผู้บังคับบัญชาให้ใครก็อาจจะคูณด้วยจำนวนตัวเลขที่เยอะหน่อย เพื่อนร่วมงานแต้มเท่ากัน ผู้ใต้บังคับบัญชาคูณ 0.5 อย่างนี้เป็นต้น ก็จะทำให้ในระดับตัวเองทุกคนมองใครจะได้ที่ 1 ที่ 2 เขาจะไม่มานั่งเสียเวลา ไปเช้าหรือเปล่า เงินเดือนอะไรอย่างไร ไม่ต้องมานั่งคิด เขาจะ Ranking เลยว่ามีที่ให้กี่ที่ แล้วคุณคิดว่าใครที่จะได้ เช่น มีที่ว่าง 3 ที่ใครจะได้ ก็ให้ทุกคนประเมินมาเลย 1 2 3 แล้วเอาทุกอย่างมารวมกันออกมาเป็นผลลัพธ์ มันจะเป็นสิ่งที่ตรงกับความต้องการของคนในหน่วยงานมากที่สุด โดยผู้บังคับบัญชาจะไม่สามารถลงมาแทรกแซงได้ มิเช่นนั้นถ้าผู้บังคับบัญชาแทรกแซงได้ก็คือขอคนนี้มา ผู้การก็ต้องให้โดยจำใจ เพราะเราไม่มีระบบในการที่จะเป็นกลไกในการตรวจสอบตรงนี้ ถ้าทำระบบตรงนี้ได้ ไม่เฉพาะแค่ตำรวจ หน่วยงานภาครัฐทั่วประเทศ สามารถทำเป็นตัว Application ประเมิน 360 องศา ให้คนมาลงทะเบียนแล้วก็ประเมินกันในหน่วยงานหรือองค์กร เราสามารถใช้เทคโนโลยีที่จะตรวจสอบย้อนหลัง เพราะฉะนั้นใครที่ไม่เคยทำงานเลยก็

จะถูกประเมินง่าย ว่าคนนี้ไม่เคยมาทำงานที่หน่วยเลย แล้วถ้ายังดันทุรังอีกก็จะไปโดนเรื่องของการผิดวินัย อันนี้ผมว่าจะเป็นวิธีการที่สามารถแก้ปัญหาโดยภาพรวมได้ทั้งหมด

(4) ตอนนี้ผมมีแนวความคิดที่จะทำอยู่ 2 เรื่อง คือ จัดอบรมประจำปีที่เราทำกันอยู่กับหน่วยงานต่าง ๆ เรากำลังมองในเรื่องของการเรียนในระบบ e-learning ประเด็นแรกคือ ผมจะใช้แฟลตฟอร์มในการให้ความรู้พื้นฐานเบื้องต้น เป็นเชิงให้ความรู้ประชาชน ให้ความรู้ตำรวจในเบื้องต้นว่า เวลามีคดีควรจะต้องทำอย่างไรบ้าง ประชาชนรู้ก็ไม่เสียหาย ส่วนในเรื่องของการสืบสวนทางอิเล็คโทรนิค เราก็จะต้องให้เขามาเทรนนิ่งกับเรา แต่ก่อนที่ใครจะมาเป็น ต้องไปเรียนรู้หลักสูตรพื้นฐาน แล้วก็สอบให้ผ่านเกณฑ์ให้ได้ก่อน ถ้าคุณไม่มีความรู้เบื้องต้นที่จะสอบผ่านเกณฑ์ก็จะไม่อนุญาตให้เข้ามาอบรม มิเช่นนั้นเราจะเป็นคนที่ไม่มีความรู้อะไรเลยมาก็ไม่รู้เรื่อง เพราะไม่มีพื้นฐาน เราไม่ต้องเสียเวลามาปูพื้นฐานให้คนกลุ่มนี้ เราก็จะให้เขาไปเรียนรู้เอง ซึ่งเชื่อว่าเขาทำได้ หลังจากเขาเรียนรู้เสร็จ ประเมินผ่าน 80% คุณถึงจะมีสิทธิที่จะเข้ามาเรียน

(5) สุดท้ายที่ผมอยากจะสรุปนอกจากที่เรามองในเรื่องของโครงสร้างหน่วยงาน ผมอยากหยิบยกคำ ๆ หนึ่งว่า เราควรจะต้องสร้างระบบ eco system สำหรับเจ้าหน้าที่ที่จะสามารถวิเคราะห์และทำงานได้ ถ้าสภาพแวดล้อมมันเอื้ออำนวยในการทำ มันจะเป็นภาพใหญ่ที่เราจะแก้ปัญหาได้ตรงจุด แต่ถ้าสภาพแวดล้อมไม่เอื้ออำนวยเจ้าหน้าที่ยังคงอยู่ทำอะไรทุกอย่างไปผมว่าก็ล้มเหลว แล้วระบบ eco system มีอะไรบ้าง ก็อาจจะใส่ตั้งแต่โครงสร้าง ก็คิดว่าจะเป็นภาพที่นำเสนอให้สามารถพัฒนาต่อไปได้

8) อดีตผู้ทรงคุณวุฒิ สำนักงานตำรวจแห่งชาติและอดีตรองผู้บัญชาการตำรวจนครบาล ได้ให้ข้อคิดเห็นเพิ่มเติม ดังนี้

ผมมองว่าข้อมูลน่าจะครบถ้วนสมบูรณ์แล้ว แต่ดูในเรื่องของคดีที่ได้นำเสนอ คดีเรื่องหมิ่นประมาททางเทคโนโลยี ก็คงต้องไล่เรียงให้ครบถ้วน เพื่อที่จะเป็นรูปแบบที่ส่งไปให้กับพนักงานสอบสวนแล้วเขาสามารถที่จะทำได้ทุกคดี เพราะฉะนั้นก็คงจะต้องไปไล่เรียงทั้งสองด้าน คือ ทั้งด้านของ ปอท. และ สน. ว่าเขามาแจ้งในเรื่องอะไรบ้าง ก็เอามาเป็นองค์ความรู้ในแต่ละเรื่องว่าจะต้องทำอย่างไร ใส่เข้าไปด้วยว่าในเรื่องของกฎหมาย ผิดกฎข้อหาอะไรบ้าง ใส่ให้ครบ ที่สำคัญที่สุดคือการเก็บพยานหลักฐานในแต่ละเรื่องจะต้องเก็บอะไรบ้าง ก็บอกเขาว่าต้องเก็บจากตรงนั้นตรงนี้ วงเล็บบอกเขาว่าคือตรงไหน ก็คิดว่าถ้าได้คู่มือก็จะช่วยได้ในระดับหนึ่ง เพราะจากที่ฟังดูอีก 2 ปีข้างหน้าอาจจะจับต้องได้จริง ๆ ตอนนี้ยังจับต้องไม่ได้ก็ต้องมีคู่มือลงไปก่อน ถ้าเขาดูแล้วทำได้ผมว่าเป็นอานิสงส์สูงสุดสำหรับพวกเรา

9) ผู้เชี่ยวชาญเฉพาะด้านคดีพิเศษ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ได้ให้ข้อคิดเห็นเพิ่มเติม ดังนี้

ที่คุยกันเรื่องที่สำคัญคือเรื่องของการจัดโครงสร้างหน่วยงาน สิ่งหนึ่งที่สำคัญเลย มีปัญหาในทุกเรื่องคือเรื่องของงบประมาณ ส่วนใหญ่แล้วเรื่องพวกนี้จะใช้เงินสูง เพราะฉะนั้นตรงนี้ต้องเป็นงบประมาณที่เพียงพอและต่อเนื่อง ส่วนอีกเรื่องไม่ค่อยมีใครพูดถึงมากนัก เวลาเราหาพยานหลักฐานเรามุ่งเน้นที่จะหาพยานหลักฐานให้ครบ ส่วนใหญ่ที่เรามองเป็นเรื่ององค์ประกอบภายนอกจริง ๆ แล้วพยานหลักฐานถ้าเราสามารถวิเคราะห์แล้วเชื่อมโยงได้ องค์ประกอบที่อยู่ภายในจริง ๆ ว่าเขามีส่วนร่วมหรือมีส่วนรู้เห็นอะไรด้วย

ไหม เจตนามันมีมากกว่านั้น แต่สมัยนี้ไม่ค่อยมีใครใช้ ถามว่าที่ทำแบบนี้มันเห็นผลไหม ส่วนมากผมคุยกับใครก็จะพูดถึงแค่องค์ประกอบภายนอก ภายในคือเรื่องสำคัญมาก เพราะมันอยู่ที่เจตนา ส่วนอีกเรื่องที่สำคัญ คือเรื่องของเชิงป้องกัน อาชญากรรมไซเบอร์ส่วนใหญ่ถ้าเราทำไม่สำเร็จ เราไม่สามารถตอบอะไรได้ ถ้าเราทำสำเร็จเราจะสามารถปิดช่องโหว่ได้ เราสามารถระมัดระวังในการก่อเหตุได้ ส่วนใหญ่จะไม่ค่อยเห็น ถามว่าคดีนี้เกิดอะไรขึ้นก็บอกแต่ว่ามันหายไปแล้ว จริง ๆ ที่กรมมีในเรื่องของการทดสอบระบบ ทดสอบอีเมล อันนี้แค่ปลอมอีเมลแต่ไม่เหมือนกันแค่ตัวเดียว แต่จริง ๆ มันมีมากกว่านี้อีกที่ปลอมอีเมลเหมือนกัน 100% แต่ตรงนี้ผมก็ report ไม่ได้ แต่ถ้าเราทำได้ดีที่สุดมันจะสามารถปิดช่องโหว่ตรงนี้ได้ อย่างเรื่องเงินเราสามารถแก้ปัญหาได้อย่างเวลาที่ติดต่อสื่อสารควรใช้ช่องทางเดิม เช่นเขาบอกเปลี่ยน account มีการถามเขาอีกก็มันโดนแฮกไปแล้ว มันต้องเป็นช่องทางอื่น เช่นเบอร์ เวลาติดต่อเราก็ควรติดต่อช่องทางเดิม คุยกับคนเดิม อะไรแบบนี้ ก็เป็นตัวอย่างในเชิงป้องกัน

10) ผู้กำกับการสถานีตำรวจภูธรหน่องม่วง จังหวัดลพบุรี ได้ให้ข้อคิดเห็นเพิ่มเติม ดังนี้

ต้องมีกฎหมายคุ้มครองเจ้าหน้าที่ด้วย เจ้าหน้าที่ที่ต้องทะลุทะลวงข้อมูล เอานู่นเอานี่ ถ้าเรามีคนมาแจ้งความ พอแจ้งความเสร็จ เข้าสู่ทะเบียนราษฎร์ พอเข้าสู่ทะเบียนราษฎร์เสร็จ ลูกน้องถูกฟ้องว่าไปเข้าทะเบียนราษฎร์ของเขาได้อย่างไร แล้วทีนี้ก็ตั้งกรรมการ พอจะเข้าทะเบียนราษฎร์ทีก็เป็นแบบนี้ กฎหมายจะคุ้มครองเจ้าหน้าที่อย่างไร การแก้ไขหมิ่นประมาทรู้สึกว่าจะให้ตาม ป.อาญา

11) ผศ.ดร.ศรีปริญญา ธูปกระจ่าง นักวิจัยโครงการ ได้ให้ความคิดเห็นว่า

จากประสบการณ์หลาย ๆ ด้านมีความคิดเห็น เคยเป็นผู้เสียหายที่ถูกดึงกระเป๋าไป ซึ่งมีโทรศัพท์อยู่ในกระเป๋า ซึ่งแจ้งความไป 3 วันถึงจะได้กระเป๋ามา เห็นชัดว่ามีแรงโน้มน้าว เขามีองค์ความรู้และเครือข่ายมากพอ ที่จะดึงข้อมูล ถึงแม้จะไม่มีงบเงินที่สนับสนุน นอกจากนั้นแล้วอยากจะนำเรียนท่านหัวหน้าโครงการว่าตำรวจไม่ได้ทำงานเพียงฝ่ายเดียว ยังมีภาคีที่คอยช่วยเหลือ ถ้าไปค้นคว้าก็จะเห็น สถาบันการศึกษา สิ่งที่เราต้องมีคือ เด็กรุ่นหลัง เพราะเด็กรุ่นหลังเก่งไอทีมากเขาสามารถที่จะทำได้เลย ถ้าเราได้บูรณาการให้คนกลุ่มนี้เป็นอาสาสมัคร ถ้ามองถึงอาชญากรรมคอมพิวเตอร์ ถ้ามีชุดของอาสาสมัครซึ่งได้ให้ดูเรื่องอาชญากรรมจี้ ชิงปล้นอะไรเหล่านี้ สิ่งหนึ่งที่อยากจะให้เราเป็นส่วนหนึ่งให้กับเขา อย่างในกรณีที่ตัวเองเป็นหนึ่งในผู้เสียหาย จริง ๆ แล้วการทำงานของตำรวจก็มีความสนใจในเรื่องนี้ ประกอบกับเทคโนโลยีในปัจจุบันอาจจะกระทำความผิดกันมาก บางทีเราเองก็ไม่ทัน ก็เข้าใจตำรวจที่ทำหน้าที่ทุกอย่าง แล้วถ้าไม่มีเขาในกรณีที่ว่าไม่รับคดี เหมือนกับว่าปัดคดีแต่จริง ๆ แล้วความรับผิดชอบเขาสูง