รายงานวิจัยฉบับสมบูรณ์

เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

โดย

พลตำรวจโท ดร.ณรงค์ กุลนิเทศ และคณะ

หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์

มหาวิทยาลัยราชภัฏสวนสุนันทา

กันยายน 2556

สัญญาเลขที่ RDG5540039

รายงานวิจัยฉบับสมบูรณ์

เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

คณะผู้วิจัย	สังกัด
1. พลตำรวจโท ดร.ณรงค์ กุลนิเทศ	หลักสูตรปรัชญาดุษฎีบัณฑิต และวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา
2. พ.ต.อ.สมศักดิ์ หน่องพงษ์	ฝ่ายอำนวยการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ
3. รศ.พ.ต.อ.วรธัช วิชชุวาณิชย์	กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
4.นางสาวณิช วงศ์ส่องจ้า	หลักสูตรปรัชญาดุษฎีบัณฑิต และวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

สนับสนุนโดยสำนักงานกองทุนสนับสนุนการวิจัย (สกว.)

บทสรุปสำหรับผู้บริหาร

1. ความเป็นมาและความสำคัญของปัญหา

1) อาชญากรรมคอมพิวเตอร์

ในสังคมไทยมองเห็นประโยชน์ของเครือข่ายอินเทอร์เน็ตอย่างมากมายมหาศาล หรือมองภาพพจน์ของคนที่ใช้อินเทอร์เน็ตว่าเป็นผู้ที่มีความรู้ ความสามารถในการใช้เทคโนโลยีสื่อสาร และโดยรวม คือกลุ่มคนที่รักความก้าวหน้า ทันสมัย ทันต่อเหตุการณ์ จึงได้เลือกใช้เทคโนโลยีที่ทันสมัยเป็นเครื่องมือในการแสวงหาความรู้ ซึ่งบางคนเสียเวลา เสียค่าใช้จ่ายเพื่อที่จะเรียนรู้วิธีการใช้ หรือเรียนรู้วิธีการนำประโยชน์ของเทคโนโลยีไปเป็นเครื่องมือในการแสวงหาความรู้เพิ่มเติม การศึกษาต่อในระดับสูงขึ้นไป หรือนำไปใช้เพื่อการประกอบอาชีพเพื่อดำรงชีพ

อย่างไรก็ตาม แม้ว่าเทคโนโลยีสารสนเทศและการสื่อสารจะเป็นสิ่งที่มีประโยชน์อย่างมากมายมหาศาลแต่ก็มีโทษมากมายเช่นกัน จากข่าวในหน้าหนังสือพิมพ์ที่ปรากฏอยู่บ่อยครั้ง ว่ามีผู้นำเอาความรู้ความสามารถ และคุณสมบัติของเทคโนโลยีสื่อสารอินเทอร์เน็ตไปใช้ในทางมิชอบ จนทำให้เกิดความเสื่อมเสียชื่อเสียงหรือถึงแก่ชีวิต เพียงเพื่อได้รับผลประโยชน์ส่วนตัว ซึ่งทำความเดือดร้อนให้แก่ครอบครัวของผู้เสียหาย จนทำให้สังคมเดือดร้อน อยู่เป็นระยะ ปัญหาที่สำคัญ คือ เจ้าหน้าที่ตำรวจและประชาชน ไม่มีความรู้ทางด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์อย่างเพียงพอ การสร้างองค์ความรู้และคู่มือทางด้านอาชญากรรมคอมพิวเตอร์ จะทำให้การป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น

คำว่า “อาชญากรรมคอมพิวเตอร์” มีคำเรียกมากมายหลายคำว่า Computer crime, Computer related crime, E-crime, Information technology crime. High-tech crime, Computer misuse, Computer abuse ซึ่งล้วนแล้วแต่ใช้แทนกันได้ทั้งนั้น เพราะขึ้นอยู่กับมุมมองของนักกฎหมายแต่ละสาขา แต่ความหมายที่ครอบคลุมหมายถึง *“การกระทำใด ๆ ที่ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย โดยผู้กระทำ ได้อาศัยความรู้ด้านเทคโนโลยีคอมพิวเตอร์ ไม่มากก็น้อยในอันที่จะกระทำความผิด และให้การกระทำนั้นเป็นผลสำเร็จ ไม่ว่าลักษณะของการกระทำนั้น จะเป็นการใช้คอมพิวเตอร์แบบเครื่องมือ หรือให้คอมพิวเตอร์เป็นเป้าหมาย ซึ่งจำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถทางเทคโนโลยีคอมพิวเตอร์เข้ามาดำเนินการกับผู้กระทำความผิด ตั้งแต่กระบวนการสืบสวน สอบสวน การฟ้องร้อง ตลอดจนการพิจารณาคดีเพื่อลงโทษผู้กระทำความผิด”* การประกอบอาชญากรรมทางคอมพิวเตอร์ได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล อาชญากรรมทางคอมพิวเตอร์ จึงจัดเป็นอาชญากรรมทางเศรษฐกิจ หรืออาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ

2) เครือข่ายและปัญหาทางด้านอาชญากรรมคอมพิวเตอร์

ปัญหาอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นทั่วประเทศไทยในปัจจุบันทั้งการกระทำผิดเกี่ยวกับเว็บไซต์ที่ผิดกฎหมายในลักษณะความผิดโดยทั่วไป และเว็บไซต์ที่กระทำความผิดเกี่ยวกับการจาบจ้วงสถาบันพระมหากษัตริย์ ซึ่งเป็นการกระทำผิดตาม ป.อาญามาตรา 112 และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีปริมาณที่กระทำผิดเป็นจำนวนมาก

จากสถิติคดีอาญาของการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีประจำปี พ.ศ.2552-2555 ซึ่งรวบรวมโดย กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ (บก.ปอท. เริ่มก่อตั้งหน่วยงานเมื่อ 7 ก.ย. 2552) สถิติใน พ.ศ.2552 พบว่า มีเว็บไซต์ที่กระทำผิดโดยทั่วไป 22 คดี พ.ศ.2553 มีเว็บไซต์ที่กระทำผิดในคดีทั่วไป 35 คดี พ.ศ.2554 จำนวน 429 คดี พ.ศ.2555 (ม.ค.-ส.ค.2555) กระทำผิดในคดีทั่วไป 287 คดี แต่เมื่อพิจารณาถึงเว็บไซต์ที่จาบจ้วงสถาบันพระมหากษัตริย์ ตาม ป.อาญา มาตรา 112 พบในปี พ.ศ.2552 มีการกระทำผิด 154 คดี พ.ศ.2553 กระทำผิด 153 คดี พ.ศ.2554 กระทำผิด 186 คดี แต่ในปี พ.ศ.2555 (ม.ค.-ส.ค. 2555) มีการกระทำผิดถึง 15,338 คดี จะเห็นได้ว่า การกระทำผิดตาม ป.อาญา มาตรา 112 ในปี 2555 มีการกระทำผิดสูงกว่าปี 2554 ถึง 82.46 เท่า หรือ สูงขึ้นถึงร้อยละ 8,146.31 ซึ่งจะเห็นว่าเป็นสถิติที่สูงขึ้นอย่างมากผิดปกติ จึงเป็นเหตุผลหนึ่งที่ควรนำเรื่องนี้มาศึกษา

ภัยบนอินเตอร์เน็ต และรูปแบบในการกระทำผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ปัญหาทางด้านโครงสร้างทางกฎหมายและปัญหาด้านการสืบสวนทางด้านอาชญากรรมคอมพิวเตอร์ กฎหมายและความรู้ของพนักงานสอบสวน ยังก้าวไปไม่ทันต่อการกระทำผิด ดังกล่าว เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน **(Globalization)** และการกระทำผิดทางด้านอาชญากรรมคอมพิวเตอร์ มีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา จึงมีความจำเป็นต้องศึกษาถึงเครือข่ายทางด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

3) เขตอำนาจในการพิจารณาคดี

ตาม พ.ร.บ.คอมพิวเตอร์ 2550 ได้ระบุถึงเขตอำนาจในการพิจารณาคดี ซึ่งในกรณีที่ผู้กระทำความผิดตาม พ.ร.บ.นี้นอกราชอาณาจักร ถึงแม้ว่าผู้กระทำผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทย หรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร (ม.17)

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักร และ

(1) ผู้ใดกระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้น หรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

การกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในบางครั้งผู้กระทำความผิดอยู่นอกประเทศ เช่น คดีความผิดตาม ป.อาญา มาตรา 112 ซึ่งนับวันจะมีปริมาณคดีเพิ่มขึ้นเป็นจำนวนมาก จึงจำเป็นต้องสร้างเครือข่าย และการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เป็นการป้องกันและปราบปรามการกระทำผิดดังกล่าว

จากหลักการและเหตุผลข้างต้น หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา ร่วมกับคณาจารย์ที่มีความรู้และประสบการณ์การทำวิจัย และผู้มีความรู้ความเชี่ยวชาญทางด้านอาชญากรรมคอมพิวเตอร์ จากหน่วยงานต่างๆ เช่น กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานพิสูจน์หลักฐานตำรวจ กรมสอบสวนคดีพิเศษ สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ กองบัญชาการเทคโนโลยีและสารสนเทศ กระทรวงเทคโนโลยีและสารสนเทศ จึงมีความสนใจที่จะทำการวิจัย เพื่อศึกษาการแก้ปัญหาอาชญากรรมคอมพิวเตอร์ โดยการจัดการความรู้จากเอกสาร งานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ในแต่ละหน่วยงาน ผ่านการจัดกิจกรรมแลกเปลี่ยนเรียนรู้ เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยนำเข้ากระบวนการผลลัพธ์ รวมทั้งรูปแบบที่ดี (Best Practice) ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะทางด้านเครือข่าย และการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เพื่อนำมาพัฒนางานทางด้านดังกล่าว ทำให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้งคุ้มครองสิทธิและเสรีภาพ ด้วยความรวดเร็ว เที่ยงตรง และเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นแนวทางในการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ให้เป็นที่ยอมรับ ศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

2. วัตถุประสงค์ของการวิจัย

1) เพื่อพัฒนาหารูปแบบที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) เพื่อสร้างเครือข่ายในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

3) เพื่อสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์หลังจากมีการศึกษาวิธีการป้องกันและปราบปรามจากต่างประเทศ และนำมาประยุกต์ใช้

3. คำถามของการวิจัย

1) กระบวนการด้านอาชญากรรมคอมพิวเตอร์ในปัจจุบันมีลักษณะอย่างไร

2) ปัญหาและอุปสรรคในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ปัจจุบันมีอะไรบ้างและสามารถแก้ไขปัญหาและอุปสรรคดังกล่าวได้หรือไม่อย่างไร

3) แนวทางมาตรฐานตามขั้นตอนต่าง ๆ ด้านอาชญากรรมคอมพิวเตอร์ มีการบูรณาการภาพรวมที่ได้ผลลัพธ์เป็นแนวทาง มาตรฐาน ขั้นตอนเป็นอย่างไร

4. ขอบเขตของการวิจัย

1) ขอบเขตด้านเนื้อหาการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยภาคสนามที่ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) และใช้หลักการวิจัยเชิงปฏิบัติการมีส่วนร่วม (Participatory Action Research) ที่ผู้วิจัยได้เข้าไปมีส่วนร่วมและลงมือวิจัยด้วยตนเองเพื่อวิเคราะห์ข้อกฎหมาย และระเบียบที่เกี่ยวข้องกับการปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ และค้นหาวิธีการปฏิบัติงาน นโยบายในการบริหารจัดการ รวมทั้งปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้อง ในด้านการสร้างคู่มือการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ และสร้างการจัดการฐานความรู้ด้านอาชญากรรมคอมพิวเตอร์จากกฎหมายและระเบียบ รายงานการสืบสวน สำนวนการสอบสวน และจากการศึกษาเชิงลึกจากกลุ่มเป้าหมายที่เกี่ยวข้องประกอบกับการวิจัยเชิงปฏิบัติการ (Action Research) โดยการจัดประชุมเพื่อแลกเปลี่ยนเรียนรู้ และถอดบทเรียน ซึ่งจะทำให้องค์กรเกิดการเรียนรู้จากประสบการณ์ในการปฏิบัติงานของผู้ร่วมถอดบทเรียน และได้แนวคิดใหม่ที่เป็นประโยชน์ในการปฏิบัติงานต่อไป

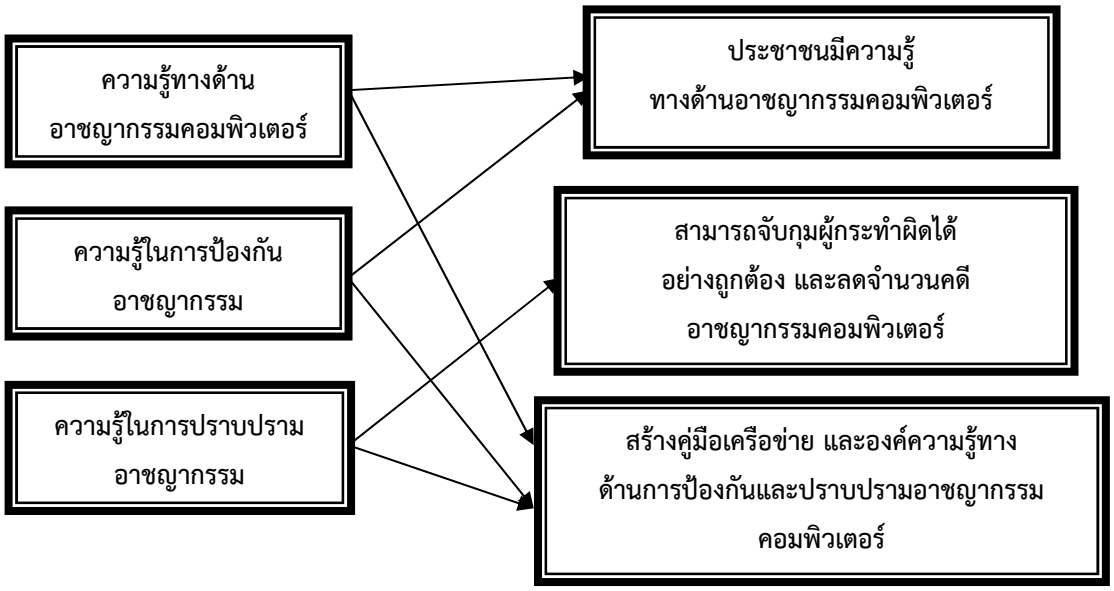
2) ขอบเขตด้านกลุ่มเป้าหมาย / พื้นที่

กลุ่มเป้าหมายในการวิจัยครั้งนี้ คือ ผู้บริหารสถานีตำรวจ เจ้าหน้าที่ตำรวจ ทั้งระดับสัญญาบัตรและชั้นประทวนหน่วยงานที่เกี่ยวข้อง และประชาชน เครือข่ายที่มีความรู้ ความชำนาญและประสบการณ์โดยศึกษาเฉพาะกลุ่มเป้าหมายที่เป็นผู้เชี่ยวชาญ และมีประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ โดยทำการคัดเลือกจากเจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้อง และประชาชน เข้าร่วมประชุมกลุ่มย่อย (Focus Group) หรือการสัมมนาแลกเปลี่ยนเรียนรู้ จะคัดเลือกจากเจ้าหน้าที่ที่มีประสบการณ์ เพื่อให้ได้กลุ่มเป้าหมายที่มีความรู้ความเชี่ยวชาญอย่างแท้จริง

3) ขอบเขตด้านระยะเวลา

การวิจัยครั้งนี้มีระยะเวลาดำเนินการ 12 เดือน

5. กรอบแนวคิดของการวิจัย



กรอบแนวคิดของการวิจัย

6. ความสำคัญของการวิจัย

วัตถุประสงค์ที่สำคัญของงานวิจัยนี้คือการได้คู่มือแนวทางมาตรฐานตามขั้นตอนต่างๆที่เป็นแนวทางสำหรับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ก่อให้เกิดผลในทางบวกด้านอาชญากรรมคอมพิวเตอร์ให้ลดลง ดังนั้นความสำคัญที่คาดว่าจะได้รับจากงานวิจัยในครั้งนี้คือ

1) ได้องค์ความรู้ที่สามารถนำไปพัฒนาต่อยอดจัดทำเป็นคู่มือแนวทางมาตรฐานในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) เพิ่มพูนทักษะเป้าหมายของเจ้าหน้าที่ตำรวจ

3) เพื่อเสนอแนะแนวทางในการปรับปรุงและพัฒนาระบบงานอาชญากรรมคอมพิวเตอร์ เพื่อนำไปใช้ประโยชน์ในการสืบสวนอาชญากรรมคอมพิวเตอร์

4) หน่วยงานที่มีหน้าที่ได้นำเอาคู่มือมาใช้เป็นรูปแบบในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ได้แก่

(1) ผู้บริหารสถานีตำรวจ และหัวหน้าหน่วยงานที่ปฏิบัติงานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

(2) ชุมชนเครือข่ายที่มีความรู้ ประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์

(3) องค์กรเอกชนที่เกี่ยวข้อง

(4) กลุ่มผู้พิพากษาและอัยการ

(5) กระทรวงเทคโนโลยีและสารสนเทศ

(6) ประชาชน

(7) กลุ่มสื่อมวลชน

7. ผลที่คาดว่าจะได้รับ

1) ได้ข้อกฎหมายและระเบียบที่ผ่านการแก้ไข ปรับปรุงให้มีความเหมาะสมต่อการนำไปใช้งานในสถานการณ์ปัจจุบัน เพื่อสร้างการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) ได้ทราบวิธีการปฏิบัติงาน นโยบายในการบริหารจัดการ รวมทั้งปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้อง ในการปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

3) ได้คู่มือการจัดการความรู้ด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

4) ได้เครือข่ายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

5) ได้เว็บไซต์ที่เป็นการจัดการทางด้านอาชญากรรมคอมพิวเตอร์

8. กระบวนการผลักดันผลงานดังกล่าวออกสู่การใช้ประโยชน์

1) การประชุมเพื่อทำการแลกเปลี่ยนเรียนรู้ ประชุมร่วมกันระหว่างทีมถอดบทเรียน โดยเชิญผู้เชี่ยวชาญในด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และเจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้อง เครือข่ายที่มีประสบการณ์และความเชี่ยวชาญ และประชาชน เพื่อปรับปรุง และเสนอแนะงานวิจัยให้มีความสมบูรณ์มากยิ่งขึ้น โดยจัดขึ้น ณ กรุงเทพมหานคร จำนวน 4 ครั้ง มีรายละเอียดดังนี้

ครั้งที่ 1 จัดที่กรุงเทพมหานคร (ระเบียบและข้อกฎหมายต่างๆ ที่เกี่ยวข้อง)
ครั้งที่ 2 จัดที่กรุงเทพมหานคร (ค้นหาปัญหา และอุปสรรคต่าง ๆ)
ครั้งที่ 3 จัดที่กรุงเทพมหานคร (สร้างคู่มือการจัดการความรู้)
ครั้งที่ 4 จัดที่กรุงเทพมหานคร (มอบคู่มือการจัดการความรู้)

2) การนำบทความตีพิมพ์ในวารสารต่าง ๆ เพื่อเผยแพร่ผลงานการวิจัยสู่สาธารณชน

3) การจัดทำคู่มือการจัดการความรู้ทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

4) จัดทำเว็บไซต์เพื่อเป็นฐานข้อมูลในการพัฒนางานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

9.ผลการวิจัย

1) สถานการณ์ปัจจุบันทางด้านอาชญากรรมคอมพิวเตอร์

1.1) ปัจจุบันเจ้าหน้าที่บังคับใช้กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ดังนี้

1) พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ.2550

2) พ.ร.บ.ที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่างๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำ

ขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

3) กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้ บริการอื่น ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

4) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

5) ประกาศกระทรวงเทคโนโลยีและสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

6) ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนการสอบสวนและการดำเนินคดีกับผู้กระทำความผิดว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

7) ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ออก พ.ศ.2555

8) ประมวลกฎหมายอาญา **หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ของลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6** และ **มาตรา 269/7**

9) พ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ.2547 ซึ่งให้อำนาจพนักงานเจ้าหน้าที่

10) กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ฉบับที่ 2 พ.ศ. 2555

11) กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

1.2) ลักษณะหรือรูปแบบอาชญากรรมคอมพิวเตอร์ในประเทศไทย มีดังนี้

1) การเข้าถึงระบบข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) ตัวอย่างเช่น การเจาะระบบ/รหัส (Hacking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass) เพื่อทำลายระบบคอมพิวเตอร์ หรือแก้ไขเปลี่ยนแปลงข้อมูล หรือเข้าถึงข้อมูลที่เก็บรักษาไว้ เป็นความลับ เช่น รหัสผ่าน (Passwords Hacking) หรือเป็นความลับทางการค้า (Trade Secret)

2) การใช้คอมพิวเตอร์โดยไม่ชอบ (Computer Misuse) อันทำให้โปรแกรมและข้อมูลเสียหาย ตัวอย่างเช่น การลักลอบดักข้อมูลโดยฝ่าฝืนต่อกฎหมาย การส่งไวรัสคอมพิวเตอร์และอีเมล์ขยะ

3) การใช้คอมพิวเตอร์เป็นเครื่องมือ (Computer Fraud) เช่น การสร้างโปรแกรม Salame techniques เพื่อปัดเศษเงินในบัญชีของบุคคลอื่นมารวมเก็บไว้ในบัญชีของตนเอง หรือโปรแกรม Logic Bombs เพื่อเฝ้าติดตามความเคลื่อนไหวของระบบบัญชี และระบบเงินเดือนและทำการเปลี่ยนแปลงตัวเลขในระบบดังกล่าว

4) การฉ้อโกงบัตรเครดิต (Credit Card Fraud) เช่น

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access) เช่น Hackers
- การนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต (Unauthorized Use by Insider) เช่น พนักงานในบริษัทเว็บไซต์นำข้อมูลไปใช้โดยไม่ได้รับอนุญาตเพื่อประโยชน์ของตนเอง
- การดักข้อมูล (Interception of transmission of information)
- การส่งอีเมล์และตั้งเว็บไซต์หลอก (Phishing Scam and Spoof e – commerce sites) หมายถึงการโจรกรรมข้อมูลในรูปแบบของการปลอมแปลงอีเมล์และทำการสร้างเว็บไซต์ปลอมเพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอีเมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ เช่น Username Password

1.3) ฐานความผิดที่เกี่ยวข้องกับคอมพิวเตอร์

ฐานความผิดที่ 1 (มาตรา 5, มาตรา 7)

การเจาะระบบ (Hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) ซึ่งการกระทำเช่นว่านี้เป็นการขัดขวางการใช้ระบบคอมพิวเตอร์โดยชอบของบุคคลอื่นอันอาจทำให้เกิดการเปลี่ยนแปลงแก้ไข หรือการทำงานระบบคอมพิวเตอร์ ได้โดยปกติ (มาตรา 5)

ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

รวมถึงข้อมูลคอมพิวเตอร์ ซึ่งข้อมูลนั้นเป็นการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ (มาตรา 7)

ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ฐานความผิดที่ 2 (มาตรา 6)

ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ เช่นมีการลงทะเบียน Username และ password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ แล้วนำไปเปิดเผยแก่ผู้หนึ่งผู้ใดหรือหลายคน แล้วน่าจะเกิดความเสียหายแก่ผู้อื่นได้

ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 3 (มาตรา 8)

การดักรับโดยวิธีการทางเทคนิค (technical means) เพื่อลักลอบดักฟัง (listen) ตรวจสอบ (monitoring) หรือติดตามเนื้อหาสาระของข่าวสาร(surveillance) ที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่

คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่เพราะบางกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่นการติดต่อผ่านทางโทรศัพท์เคลื่อนที่ การติดต่อโดยใช้เทคโนโลยีไร้สายประเภท wireless LAN เป็นต้น ซึ่งนอกจากการใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อบันทึกข้อมูลที่มีการส่งผ่านกันแล้ว ยังรวมถึงกรณีการใช้ซอฟต์แวร์ หรือรหัสผ่านต่างๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านถึงกันด้วย ทั้งนี้ ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 4 (มาตรา 9)

กระทำการอันเป็นการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ เว้นแต่ การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์ (traffic data) เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ ตัวอย่างเช่น การสื่อสารผ่านระบบ Anonymous remailer system หรือการเปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร อาทิ การเข้ารหัสข้อมูล (encryption) เป็นต้น

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 5 (มาตรา 10, มาตรา 12)

กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ หากผู้กระทำได้กระทำไปโดยมีอำนาจหรือสิทธิโดยชอบย่อมไม่เป็นความผิดเพราะไม่เข้าองค์ประกอบความผิดที่ว่า “โดยมิชอบ”ดังเช่น การทดสอบหรือรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์โดยบุคคลผู้ได้รับมอบอำนาจจากผู้เป็นเจ้าของระบบคอมพิวเตอร์ (owner) หรือผู้ปฏิบัติการ (operator) หรือการปรับแก้ระบบปฏิบัติการ (operating system) ของคอมพิวเตอร์โดยผู้ปฏิบัติการ (operator) ก่อนติดตั้งซอฟต์แวร์ใหม่ๆ ตัวอย่างเช่น การติดตั้งซอฟต์แวร์เพื่อการเชื่อมต่ออินเทอร์เน็ตซึ่งจะมีผลให้ระบบคอมพิวเตอร์ทำงานไม่เป็นปกติทั้งก่อนและหลังการติดตั้งโปรแกรม

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ถ้าเกิดความเสียหายแก่ประชาชนในทันที หรือภายหลัง ไม่ว่าจะเกิดขึ้นพร้อมกันของมาตรา 9 และ มาตรา 10 หรือไม่ (มาตรา 12(1))

ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท (โทษหนักขึ้น)

การกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ (มาตรา 9) หรือระบบคอมพิวเตอร์ (มาตรา 10) ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ (มาตรา 12(2))

ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท (โทษหนักขึ้นอีก) ถ้ามีใครตาย (มาตรา 12 วรรคท้าย) ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี (หนักที่สุด)

ฐานความผิดที่ 6 (มาตรา 11)

การทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข เช่นส่ง E-mail มากจนล้นระบบคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยากในการใช้ระบบคอมพิวเตอร์ของเขา ภาษาอังกฤษเรียกว่า “spamming” โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล

ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

แต่การปกปิดหรือปลอมแปลงนี้ต้องเป็นเรื่องของ “แหล่งที่มาของการส่งข้อมูล” ซึ่งตรวจสอบได้โดย “ข้อมูลจราจรทางคอมพิวเตอร์” ได้แก่การปกปิดหรือปลอมแปลง IP address และหมายถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบถึงแหล่งที่มาของการส่งข้อมูลและส่งผลให้ไม่อาจตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น จึงไม่ใช่เรื่องการปกปิดหรือปลอมแปลงโดยการไม่ใช้ชื่อจริง หรือการเปลี่ยนแปลงใช้ชื่อหรือใช้นามแฝง หรือใช้ email-address ที่ผิดไปหรือเปลี่ยนแปลงไปซึ่งยังตรวจสอบแหล่งที่มาของการส่งข้อมูลได้อยู่

ฐานความผิดที่ 7 (มาตรา 13)

จำหน่าย เผยแพร่ ชุดคำสั่งเพื่อนำไปใช้เป็นเครื่องมือในการทำความผิด ฐานความผิดที่ 1–6

ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 8 (มาตรา 14)

การนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์

1) ปลอม ไม่ว่าทั้งหมด หรือบางส่วน ที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน

2) เท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตระหนกแก่ประชาชน

3) ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4) ใดๆ ที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่ ส่งต่อ โดยรู้อยู่แล้วว่าเป็นข้อมูลฯ ตาม (1) (2) (3) หรือ (4)

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 9 (มาตรา 15)

ผู้ให้บริการใดจงใจสนับสนุน หรือ ยินยอมให้มีการกระทำตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (ผิดเหมือนกับเป็นผู้กระทำเอง)

ฐานความผิดที่ 10 (มาตรา 16)

นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (แต่ยอมความกันได้) และไม่มีความผิด ถ้ากระทำโดยสุจริต

(1.พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

2.คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550)

1.4) ปัญหาอุปสรรคของข้อกฎหมายและระเบียบที่เกี่ยวข้องเกี่ยวกับงานด้านอาชญากรรมคอมพิวเตอร์ และข้อเสนอแนะต่อการแก้ไขปัญหาในสถานการณ์ปัจจุบัน

ระบบงานด้านอาชญากรรมคอมพิวเตอร์ เป็นนวัตกรรมใหม่เพื่อการพิสูจน์หลักฐานทางคอมพิวเตอร์ในการกระทำผิด โดยองค์ความรู้ทางเทคโนโลยีคอมพิวเตอร์ รวมกับการใช้ในแนวทางการสืบสวนสอบสวน และการสร้างความน่าเชื่อถือของพยานหลักฐานที่ได้ ซึ่งถือได้ว่าจะทำให้มีน้ำหนักมากที่สุด

1) ให้ความรู้แก่พนักงานสอบสวน และผู้เกี่ยวข้องของสถานีตำรวจทุกแห่ง ทั้งในพื้นที่กองบัญชาการตำรวจนครบาล กองบัญชาการตำรวจภูธรภาคต่าง ๆ และหน่วยงานสนับสนุน ในการรับแจ้งความดำเนินคดีด้านอาชญากรรมคอมพิวเตอร์ เขตกอำนาจการสอบสวน เพราะการกระทำความผิดของคนร้ายนั้นสามารถกระทำความผิดได้ทั่วประเทศ ไม่ต้องปรากฏตัวในสถานที่เกิดเหตุ การตรวจสถานที่เกิดเหตุ การเก็บรวบรวมพยานหลักฐานในการตรวจสถานที่เกิดเหตุ เพราะวัตถุพยานอาจถูกทำลายโดยไม่ได้ตั้งใจ หรือทำให้คุณค่าของวัตถุพยานในสถานที่เกิดเหตุลดน้อยลง รวมทั้งไปเพิ่มวัตถุพยานในสถานที่เกิดเหตุ ซึ่งจะทำให้การสืบสวนสอบสวนประสบความสำเร็จในการคลี่คลายคดี ทั้งนี้เพื่อเกิดประโยชน์ในด้านการสืบสวนสอบสวนผู้กระทำความผิดและการไปเป็นพยานศาล สามารถให้ข้อมูลที่ชัดเจนต่ออัยการและผู้พิพากษาในการพิจารณาคดี

2) ควรมีระเบียบกำหนดให้เจ้าหน้าที่ที่ปฏิบัติด้านคดีอาชญากรรมคอมพิวเตอร์ เช่น พนักงานสอบสวน ผู้ช่วยพนักงานสอบสวน ตลอดจนเจ้าหน้าที่อื่นๆ ที่มีส่วนเกี่ยวข้องกับงานด้านอาชญากรรมคอมพิวเตอร์ ต้องผ่านการฝึกอบรมความรู้ทางอาชญากรรมคอมพิวเตอร์ เกี่ยวกับวัตถุพยาน การป้องกันและรักษาสถานที่เกิดเหตุ ความสำคัญของวัตถุพยานและสถานที่เกิดเหตุ เป็นต้น ทั้งนี้เพื่อประโยชน์และเกิดประสิทธิภาพสูงสุดในการใช้พยานหลักฐานทางคอมพิวเตอร์ในการคลี่คลายคดี

3) การจัดเก็บข้อมูลการตรวจพิสูจน์ ควรมีการประสานงานกันในเรื่องของพฤติการณ์แห่งคดีระหว่างพนักงานสอบสวนและเจ้าหน้าที่ตรวจพิสูจน์เพื่อประโยชน์แห่งรูปคดี โดยในปัจจุบันการดำเนินงานด้านการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ ยังขาดแนวทาง รูปแบบและมาตรฐานที่ชัดเจน โดยเฉพาะแนวทางการปฏิบัติงานสำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่ปฏิบัติงานด้านการรวบรวมพยานหลักฐานทาง

คอมพิวเตอร์ ตลอดจนเจ้าหน้าที่ผู้ดำเนินการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ ด้วยเหตุนี้จึงเกิดคำถามและข้อสงสัยที่เกี่ยวกับกระบวนการดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ด้วยเหตุที่ว่าข้อมูลคอมพิวเตอร์และหลักฐานทางอิเล็กทรอนิกส์นั้น ไม่สามารถอธิบายให้เข้าใจได้ง่ายด้วยวิธีการเดิมที่ใช้ในกระบวนการยุติธรรมโดยปกติ หากแต่จำเป็นต้องอาศัยหลักการและวิธีการที่แตกต่างไปจากการนำเสนอพยานหลักฐานแบบอื่นๆ จึงทำให้หลายฝ่ายตั้งคำถามและข้อสงสัยเกี่ยวกับกระบวนการสืบสวนและสอบสวนอาชญากรรมคอมพิวเตอร์ เนื่องจากหากกระบวนการรวบรวมพยานหลักฐาน และการตรวจพิสูจน์ที่เจ้าหน้าที่ได้ปฏิบัตินั้นไม่เป็นไปตาม มาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ.2477 แล้วนั้นจะทำให้พยานหลักฐานที่ได้ทำการรวบรวม ตลอดจนข้อมูลที่ได้จากการตรวจพิสูจน์นั้น อาจถูกปฏิเสธในการรับฟังเป็นพยานหลักฐานในชั้นศาลได้ ด้วยเหตุที่ว่าเป็นการได้มาซึ่งพยานหลักฐานโดยมิชอบด้วยกฎหมาย ดังนั้นกระบวนปฏิบัติงานที่ดีจึงต้องเป็นไปตามข้อกำหนดทางกฎหมายและยังมีกระบวนการปฏิบัติในเชิงเทคนิคที่เหมาะสม ซึ่งในการพัฒนามาตรฐานการปฏิบัติงานสาหรับการรวบรวมพยานหลักฐานและการตรวจพิสูจน์หลักฐานคอมพิวเตอร์นั้น ควรมีขั้นตอนการดำเนินงานแบ่งออกเป็นสองขั้น ได้แก่ จัดทำมาตรฐานการเก็บรวบรวมพยานหลักฐานคอมพิวเตอร์ และแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รายละเอียดของทั้งสองขั้นตอนมีดังนี้

1) การจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ การจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ มีขั้นตอนการดำเนินงานดังนี้

1.1 การรวบรวมและศึกษาเอกสารที่เกี่ยวข้องกับกระบวนการรวบรวมพยานหลักฐานคอมพิวเตอร์ โดยได้ทำการค้นคว้า ศึกษาข้อมูลจาก เอกสารวิชาการ เอกสารประกอบการฝึกอบรม และหนังสือ ประกอบกับหลักการปฏิบัติงานของหน่วยงานบังคับใช้กฎหมายในต่างประเทศ อีกทั้งรายงานการวิจัย วิทยานิพนธ์ วารสารและสิ่งพิมพ์ ตลอดจนกฎหมายของประเทศไทยที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานคอมพิวเตอร์

1.2 การวิเคราะห์ข้อมูล และการจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ สำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้อง โดยการนำรูปแบบหลักการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของหน่วยงานผู้บังคับใช้กฎหมายในต่างประเทศ มาทำการวิเคราะห์และสังเคราะห์เพื่อจัดทำเป็นมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ให้ผู้เชี่ยวชาญที่มีประสบการณ์ ทำการพิจารณาปรับปรุง แก้ไข ให้เหมาะสมกับการปฏิบัติงาน

1.3 ดำเนินการปรับปรุงมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ ตามข้อเสนอแนะและความก้าวหน้าทางเทคโนโลยีเพื่อให้มีความสมบูรณ์อย่างต่อเนื่อง

2) จัดทำแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ การจัดทำแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ มีขั้นตอนการดำเนินงาน ดังนี้

2.1 การดำเนินตามมาตรฐานการปฏิบัติงานการรวบรวมพยานหลักฐานคอมพิวเตอร์เพียงอย่างเดียวนั้น ไม่สามารถทำให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายสามารถหาตัวผู้กระทำความผิดมาลงโทษได้ หากแต่ยังต้องอาศัยผลลัพธ์จากการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เพื่อแสดงถึงหลักฐานและข้อเท็จจริงของอาชญากรรมต่างๆ ที่เกิดขึ้น ด้วยเหตุนี้เองที่ทำให้มีความจำเป็นในการพัฒนาแนวทางปฏิบัติงาน สำหรับการตรวจพิสูจน์พยานหลักฐานคอมพิวเตอร์ขึ้น เพื่อเป็นคู่มืออ้างอิงสำหรับเจ้าหน้าที่ ผู้ซึ่งจะต้องค้นหาหลักฐานทางคอมพิวเตอร์ด้วยเทคนิคและวิธีการที่น่าเชื่อถือ ตลอดจนยังคงต้องสามารถยืนยันความถูกต้องได้ เพื่อให้สามารถนำเสนอหลักฐานนั้นต่อศาลโดยปราศจากข้อสงสัยใดๆ

2.2 การวิเคราะห์ข้อมูล และจัดทำการจัดทำแนวทางการปฏิบัติงานสำหรับตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ สำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้อง โดยการนำข้อมูลและเอกสารวิชาการ เอกสารประกอบการอบรมในหลักสูตรการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ มาทำการวิเคราะห์เพื่อจัดทาเป็นมาตรฐานการปฏิบัติงานสาหรับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ เพื่อให้ผู้เชี่ยวชาญที่มีประสบการณ์ ทำการพิจารณาปรับปรุง แก้ไข ให้เหมาะสมกับการปฏิบัติงาน

2.3 ดำเนินการปรับปรุงมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ ตามข้อเสนอแนะและความก้าวหน้าทางเทคโนโลยีเพื่อให้มีความสมบูรณ์อย่างต่อเนื่อง

ข้อเสนอแนะ

1. ถ้ากล่าวถึงบทบาทและความสำคัญของข้อมูลของคอมพิวเตอร์ ระบบและเครือข่ายคอมพิวเตอร์ในยุคปัจจุบันที่ทุกกิจกรรมของเรามีการใช้สิ่งเหล่านี้ตลอด ดังนั้นกฎหมายจะต้องให้ความคุ้มครองสิ่งต่างๆ เหล่านี้ด้วย โดยะต้องให้ความคุ้มครองในเรื่องความลับ ความครบถ้วนและความสามารถในการใช้ประโยชน์ได้ ซึ่งเป็นคุณลักษณะ (properties) ของสิ่งเหล่านี้ได้ครบถ้วน รวมทั้งการให้ความคุ้มครองสิทธิในทรัพย์สินจากการกระทำความผิดรูปใหม่ด้วย

2. ในกรณีของการบัญญัติให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิด ดังที่ได้กล่าวมาแล้วกฎหมายของประเทศต่างๆบัญญัติองค์ประกอบของความผิดในเรื่องนี้ไว้ไม่เหมือนกัน เช่น บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเพียงอย่างเดียวเป็นความผิด บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์จะเป็นความผิดเมื่อมีองค์ประกอบอย่างอื่นด้วย เช่น ผู้กระทำมีเจตนาที่จะกระทำความผิดอย่างอื่นภายหลังจากการเข้าถึงคอมพิวเตอร์ หรือผู้กระทำได้ไปซึ่งข้อมูล หรือการกระทำต่างๆ เช่น แก้ไขเปลี่ยนแปลงหรือทำให้ข้อมูลเสียหาย หรือเป็นการเข้าถึงคอมพิวเตอร์ที่มีการติดตั้งระบบรักษาความปลอดภัย เป็นต้น

เนื่องจากการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นการทำให้เกิดความเสียหายต่อสิทธิความเป็นส่วนตัว และความลับของข้อมูล และเมื่อสามารถเข้าถึงคอมพิวเตอร์ได้แล้ว ผู้กระทำการดังกล่าวก็สามารถจะก่อให้เกิดความเสียหายอย่างใดๆ ได้อีกอาศัยเหตุผลดังกล่าว จึงสมควรกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดอาญาทันทีที่มีการเข้าถึงคอมพิวเตอร์

3. เมื่อพิจารณาถึงประสบการณ์ของประเทศสหรัฐอเมริกาในการแก้ไขปัญหาเรื่องการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆ แล้ว จะเห็นว่า แม้ว่าสหรัฐอเมริกาจะมีกฎหมายที่ใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์หลายฉบับ แต่ในทางปฏิบัติในสหรัฐอเมริกากลับมิได้มีการเตรียมความพร้อมในเรื่องการจัดหาทรัพยากรต่างๆ ที่จำเป็นต่อการบังคับใช้กฎหมายให้มีประสิทธิภาพ เช่น เงินงบประมาณ บุคลากร และอุปกรณ์ต่างๆ เป็นต้น จนถึงกับมีการวิพากษ์วิจารณ์กันว่า “กฎหมายให้ความคุ้มครองประเทศสหรัฐอเมริกาจากปัญหาเรื่องอาชญากรรมทางคอมพิวเตอร์ในทางทฤษฎีมากกว่าทางปฏิบัติ” ในที่สุดทำให้ต้องมีการแก้ไขในเรื่องนี้มาแล้ว ส่วนประเทศไทยนอกจากควรจะต้องกำหนดฐานความผิดทางอาญาสำหรับการกระทำความผิดต่อคอมพิวเตอร์แล้ว ทุกฝ่ายที่เกี่ยวข้องกับเรื่องนี้ควรจะต้องจัดเตรียมงบประมาณ บุคลากร อุปกรณ์ เครื่องมือ ทรัพยากร การฝึกอบรมความรู้ และสิ่งอื่นๆ ที่จำเป็นต่อการบังคับใช้กฎหมายให้พร้อมด้วย เพื่อเจ้าหน้าที่สามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ

4. การป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ควรจะต้องอาศัยทั้งมาตรการทางกฎหมายและมาตรการอย่างอื่นควบคู่กันไปเสมอ ในส่วนของมาตรการทางกฎหมาย นอกจากจะต้องมีการแก้ไขปรับปรุงกฎหมายอาญาสารบัญญัติ เพื่อกำหนดฐานความผิดให้ครอบคลุมถึงการกระทำความผิดรูปแบบใหม่ที่อยู่นอกขอบเขตของกฎหมายที่ใช้บังคับอยู่เดิมแล้ว ยังต้องปรับปรุงกฎหมายอาญาวิธีสบัญญัติ เพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพและเป็นธรรมด้วย และที่สำคัญ คือ ลักษณะของการกระทำความผิดต่อคอมคอมพิวเตอร์ที่มักจะเป็นกระทำความผิดข้ามประเทศ ดังนั้นจึงต้องให้มีการร่วมมือกับประเทศต่างๆ เพื่อให้การดำเนินกับผู้กระทำความผิดเป็นไปอย่างมีประสิทธิภาพ และรวดเร็ว

5. ภาครัฐควรกำหนดนโยบายระดับชาติให้ชันเจน ทั้งในเรื่องนโยบายด้านการรักษาความมั่นคงคอมพิวเตอร์และเครือข่าย และการปราบปรามอาชญากรรมทางคอมพิวเตอร์ รวมทั้งผลักดันกฎหมายและมาตรการต่างๆ ที่จะช่วยงานป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ให้สัมฤทธิ์ผลในทางปฏิบัติอย่างเร่งด่วน เช่น การจัดตั้งองค์กรที่รับผิดชอบในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในระดับชาติ เพื่อกำหนดนโยบายระดับสูงลงสู่ระดับปฏิบัติ

6. การสร้างเครือข่ายป้องกันและปราบปรามโดยนำภาคเอกชนที่มีบทบาท เข้ามารวมมืออย่างใกล้ชิดในเรื่องต่างๆ ได้แก่ การค้นคว้าวิจัยและรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์รวมทั้งการประสานนโยบายและการปฏิบัติร่วมกับองค์กรต่างๆ ที่เกี่ยวข้องทั้งในและต่างประเทศ

7. มาตรการอื่นๆ ที่ควรจะนำมากำหนดในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ ได้แก่

7.1 ด้านการพัฒนาบุคลากร

1) ควรมีการกำหนดผู้รับผิดชอบในการจัดทำหลักสูตรการฝึกอบรมต่างๆ เพื่อเตรียมความพร้อมของของบุคลากรในกระบวนการยุติธรรมทุดระดับ ตั้งแต่ระดับผู้ปฏิบัติการไปจนถึงระดับผู้บริหารของสำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อัยการและศาล

2) ควรมีการจัดการฝึกอบรมและให้ความรู้ (Training and Education) ทางเทคนิคการรักษาความปลอดภัยและเทคนิคการสืบหาร่องรอยการกระทำผิด (forensic) ตลอดจนประเด็นกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

3) ภาครัฐและเอกชน ควรส่งเสริมให้มีการเรียนการสอนด้านเทคโนโลยีการรักษาความปลอดภัยของระบบคอมพิวเตอร์ รวมถึงมีการสอบวัดมาตรฐานบุคลากรที่ทำงานด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ตลอดจนการสนับสนุนการพัฒนาวิชาการด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ด้วย

7.2 การบริหารและการจัดการองค์กร

1) ควรมีการจัดทำฐานข้อมูลเพื่อรวบรวมเว็บไซต์ที่มีพฤติกรรมการให้บริการแก่ผู้ใช้งานอินเตอร์เน็ตในทางที่ไม่เหมาะสม เพื่อประโยชน์ในการศึกษา และเป็นข้อมูลสนับสนุนให้แก่หน่วยงานที่เกี่ยวข้อง

7.3 ด้านเทคโนโลยี

1) หน่วยงานทั้งภาครัฐและเอกชนที่มีการใช้งานระบบเครือข่ายคอมพิวเตอร์ ควรมีการส่งเสริมให้มีการติดตั้งเทคโนโลยีต่างๆ ที่ใช้ในการป้องกันรักษาระบบเครือข่ายคอมพิวเตอร์ของตนเองให้มีความปลอดภัย รวมทั้งกำหนดให้มีการตรวจสอบประเมินความเสี่ยงของระบบคอมพิวเตอร์อย่างต่อเนื่อง อาทิ การติดตั้งระบบการตรวจสอบไวรัส (Scan virus) ระบบการตรวจจับการบุกรุก (Intrusion Detection) หรือการติดตั้งกำแพงไฟ (Firewall) เป็นต้น

7.4 ด้านมาตรการทางสังคม

1) ควรมีการกำหนดแผนการรณรงค์ประชาสัมพันธ์ ให้มีการพัฒนาและสร้างเสริมจริยธรรม เพื่อสร้างแนวปฏิบัติดีหรือวัฒนธรรมการใช้เทคโนโลยีที่ถูกต้องให้แก่คนในสังคมรวมทั้งสร้างวัฒนธรรมของความมั่นคง (Culture of Security) ในการใช้โครงสร้างพื้นฐานสารสนเทศหรือข่ายคอมพิวเตอร์ และการใช้งานอินเทอร์เน็ต โดยเริ่มจากสถาบันการศึกษา ครอบครัว และชุมชน

อย่างไรก็ตาม ปัจจุบันหน่วยงานภาครัฐและองค์กรเอกชนต่างๆ ได้มีความตื่นตัวต่อปัญหาอาชญากรรมทางคอมพิวเตอร์กันมากขึ้น แต่ปัญหาอาชญากรรมดังกล่าวนั้น ไม่สามารถแก้ไขได้โดยองค์กรใดองค์กรหนึ่ง จำเป็นต้องได้รับการร่วมมือจากทุกฝ่ายในสังคมเพราะจริงๆ แล้วปัญหาอาชญากรรมทางคอมพิวเตอร์สุดท้ายก็ขึ้นอยู่กับจริยธรรมทำของผู้ใช้งาน (User) ซึ่งต้องได้รับความร่วมมือจากสังคมในการปลูกฝังวัฒนธรรมการใช้งานที่ถูกต้อง จึงจะสามารถแก้ไขปัญหาได้อย่างแท้จริง

2) ข้อมูลคดีอาชญากรรมคอมพิวเตอร์ที่ประสบความสำเร็จ (Best Practice) แนวทาง ขั้นตอน เทคนิค วิธีการสืบสวนสอบสวนปฏิบัติงาน

"แก๊งคอลล์เซ็นเตอร์" หรือการใช้ระบบโทรศัพท์ข้ามประเทศ ล่อหลอกให้เหยื่อโอนเงินผ่านตู้เอทีเอ็ม ซึ่งกำลังระบาดอย่างหนักในปัจจุบัน โดยผู้ตกเป็นเหยื่อไม่จำเป็นว่าจะเป็นเพศไหน วัยไหน ฐานะ หรือสาขาอาชีพ เพราะแม้แต่แพทย์ ผู้พิพากษา หรือตำรวจ ก็ยังเคย**"พลาด"** โอนเงินให้กับแก๊งเหล่านี้มาแล้วจึงขอเจาะ

ข้อมูลเกี่ยวกับ **"แก๊งคอลล์เซ็นเตอร์"** เพื่อเป็นเครื่องเตือนใจให้กับเราๆ ท่านๆ ป้องกันการตกเป็นเหยื่อให้ต้องเสียทั้งเงิน เจ็บทั้งใจ ทั้งนี้สภาพปัญหาแก๊ง Call Center มีพฤติกรรมการหลอกลวงเหยื่อโอนเงินผ่านตู้เอทีเอ็มเข้าบัญชีที่เปิดไว้ ซึ่งก่อให้เกิดความเดือดร้อนกับประชาชนในทุกกลุ่มระดับอาชีพและการศึกษา เช่น เกิดการกระทำความผิดมากในช่วงช่วงระยะเวลาการชำระและคืนภาษีประจำปี และเนื่องจากสถาบันการเงินได้ส่งเสริมให้ลูกค้าผู้รับบริการได้จัดการการเงินโดยสามารถทำธุรกรรมทางอิเล็กทรอนิกส์ได้ ยิ่งส่งผลให้แก๊ง Call Center มีพฤติกรรมหลอกลวงประชาชน โดยทำให้ประชาชนเกิดความกลัว หรือ ทำให้เกิดความโลภ และตกเป็นเหยื่อโอนเงินผ่านเข้าบัญชีของแก๊ง Call Center

วีโอไอพี คือ อะไร

วีโอไอพี (VoIP) ย่อมาจาก วอยซ์โอเวอร์ไอพี (Voice over Internet Protocol) (หรือชื่ออื่น IP Telephony, Internet telephony, หรือ Digital Phone) เป็นการสื่อสารทางเสียงผ่านโครงข่าย **อินเทอร์เน็ต** หรือโครงข่ายอื่น ๆ ที่ใช้**อินเทอร์เน็ตโพรโทคอล** สัญญาณเสียงจะถูกตัดแบ่งเป็นแพ็คเก็ตวิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์แบบดั้งเดิม เปรียบได้กับการให้รถยนต์วิ่งแทรกกันได้ตามช่องว่างที่มีอยู่ของถนน แทนการให้รถยนต์คันเดียวจองถนนวิ่งแบบผูกขาด ข้อดีของวีโอไอพีก็คือการสามารถใช้โครงข่ายได้อย่างมีประสิทธิภาพ ทำให้สามารถให้บริการได้ในอัตราค่าบริการที่ถูกลงมาก ในการใช้บริการวีโอไอพี ผู้ใช้บริการจะต้องเชื่อมต่อกับอินเทอร์เน็ตก่อน หลังจากนั้น สามารถใช้โปรแกรมคอมพิวเตอร์ที่เรียกว่า ซอฟท์โฟน และไมโครโฟนกับหูฟัง เพื่อพูดคุยกับปลายทางได้ ในปัจจุบัน มีอุปกรณ์ที่เรียกว่า **อะนาล็อกเทเลโฟนอะแด็ปเตอร์** เข้ามาแทนการใช้คอมพิวเตอร์ต่อกับอินเทอร์เน็ต และใช้เครื่องโทรศัพท์อะนาล็อกที่ใช้งานตามบ้านหรือสำนักงานทั่วไปในการโทรศัพท์แบบวีโอไอพีได้ ทำให้ได้รับความสะดวกและความรู้สึกไม่แตกต่างจากการใช้โทรศัพท์แบบดั้งเดิม การใช้งานวีโอไอพีสามารถใช้งานได้ทั้งในการโทรศัพท์ถึงปลายทางที่เป็นวีโอไอพีเช่นเดียวกัน ซึ่งส่วนใหญ่จะไม่มีการเก็บค่าบริการ แต่ทั้งสองข้างจะต้องออนไลน์พร้อมกัน หรือจะโทรไปยังปลายทางที่เป็นหมายเลขโทรศัพท์ปกติ ทั้งโทรศัพท์ประจำที่หรือโทรศัพท์เคลื่อนที่ก็ได้ ในกรณีนี้ จะต้องมีการสมัครเป็นสมาชิกของบริการและชำระค่าบริการล่วงหน้า แต่ค่าบริการจะถูกกว่าการโทรศัพท์ปกติมาก จุดด้อยของวีโอไอพี คือ ในบางกรณีคุณภาพเสียงอาจจะไม่ดีเท่าโทรศัพท์ปกติ และอาจจะมีการดีเลย์หรือการที่สัญญาณเสียงเดินทางมาช้า ทำให้พูดสวนกันไม่ได้ถนัด ต้องรอให้แต่ละฝ่ายพูดให้จบก่อนจึงจะพูดได้ แต่ปัญหานี้ได้รับการปรับปรุงขึ้นมาอย่างต่อเนื่องจนแทบจะไม่มีความแตกต่างอีกต่อไป ข้อเสียอีกประการหนึ่งก็คือ โทรศัพท์วีโอไอพี จะใช้งานไม่ได้เมื่อไฟฟ้าดับ หรืออินเทอร์เน็ตเกิดขัดข้อง

วีโอไอพี หรือที่เรียกกันย่อ ๆ ว่า “วอยซ์” ได้รับความนิยมมากขึ้น เนื่องจากคุณภาพที่ได้รับปรับปรุงและค่าใช้จ่ายที่ถูก จนในที่สุดอาจจะกลายเป็นบริการฟรี เช่น เดียวกับการใช้งานอินเทอร์เน็ตอื่น ๆ เช่น การสืบค้นเว็บไซต์ การใช้อีเมลล์ เพราะอันที่จริงก็ไม่มีความแตกต่างกันมากนัก ผู้ใช้บริการเพียงแต่จ่ายค่าเชื่อมต่ออินเทอร์เน็ตเท่านั้น เนื่องจากในปัจจุบัน วีโอไอพี ไม่มีหมายเลขของตัวเอง ได้มีความพยายามที่จะสร้างเลขหมายโทรศัพท์สำหรับวีโอไอพีที่ใช้งานได้ทั่วโลก เรียกว่า “อีนัม” (enum) ซึ่งถ้าได้มีการยอมรับ

แพร่หลาย เราก็จะมีหมายเลขนี้ติดตัวเราไปได้ทุกที่ทั่วโลก เพียงแต่เข้าอินเทอร์เน็ตได้ก็สามารถติดต่อกันได้โดยกดหมายเลขอีนัมคล้าย ๆ กับโทรศัพท์ในปัจจุบัน ถ้าโครงข่ายไว-ไฟ หรือ ไวแม็กซ์ มีการขยายครอบคลุมมากขึ้น ก็เป็นไปได้ว่าจะมีอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตผ่านไว-ไฟ หรือ ไวแม็กซ์ ที่สามารถใช้วีโอไอพีได้ ซึ่งจะมีความสามารถสูงกว่าโทรศัพท์เคลื่อนที่ในปัจจุบันเป็นอย่างมาก เนื่องจากมีแบนด์วิดธ์ที่กว้าง การใช้วีดีโอโฟน จะกลายเป็นมาตรฐานทั่วไป ในปัจจุบัน ก็เริ่มมีการวางตลาดเครื่องโทรศัพท์มือถือที่ใช้เป็นโทรศัพท์ไว-ไฟในตัวบ้างแล้ว

2.1) รูปแบบและวิธีการของผู้กระทำความผิด

ปัจจุบันแก๊งคอลเซ็นเตอร์ในรูปแบบอาชญากรข้ามชาติ ยังไม่คงหมดไปง่ายๆ ในยุคการจับจ่ายใช้สอยผ่านเครื่องมือทางธุรกรรมการเงินคือบัตรเครดิต ที่เป็นไปด้วยความสะดวก รวมไปถึงการติดต่อสื่อสารระหว่างประเทศบวกกับช่องทางอินเตอร์เน็ทที่สามารถติดต่อหรือหาข้อมูลได้อย่างรวดเร็ว ที่แก๊งอาชญากรข้ามชาติได้ใช้เป็นช่องทางแอบอ้างและหลอกเหยื่อให้โอนเงินในรูปแบบต่าง ๆ **เพื่อมิให้ตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์ ถ้าเจอเหตุการณ์ลักษณะดังกล่าวจึงควรจะตั้งสติ ถ้ามีการโทรแอบอ้างมาจึงควรที่จะโทรกลับไปเช็คหน่วยงานที่แก๊งคอลเซ็นเตอร์ได้แอบอ้างไว้ ที่สำคัญควรตรวจสอบความเคลื่อนไหวของบัญชียอดเงินรวมไปถึงยอดหนี้ค้างชำระของตนเองเสมอเชื่อว่าแก๊งมิจฉาในคราบอาชญากรรมคอลเซ็นเตอร์ข้ามชาติที่มาในรูปแบบหลากหลายก็ไม่สามารถทำอะไรเราได้อย่างแน่นอน**

พฤติการณ์ของแก๊งคนร้าย

- เกือบทั้งหมดเป็นชาวจีนแผ่นดินใหญ่ และไต้หวัน ส่วนคนไทยหรือคนชาติอื่นที่เข้าร่วมขบวนการ เป็นเพียงพนักงานรับโทรศัพท์กับผู้เปิดบัญชีรับเงินที่ได้จากการล่อลวงเท่านั้น

- การตั้งคอลล์เซ็นเตอร์มี 2 รูปแบบ คือ

1) **ตั้งศูนย์ในประเทศไทย** (เพื่อโทร.กลับไปล่อลวงชาวจีนแผ่นดินใหญ่หรือไต้หวัน) โดยเช่าบ้านหรูตามหมู่บ้านในกรุงเทพฯหรือเมืองท่องเที่ยวสำคัญๆ เช่น เชียงใหม่ ภูเก็ต จากนั้นว่าจ้างชาวจีนแผ่นดินใหญ่หรือไต้หวันเข้ามาพักที่บ้าน โดยจะมีอุปกรณ์ต่างๆ ให้พร้อม และติดตั้งระบบโทรศัพท์ข้ามประเทศผ่านอินเตอร์เน็ต หรือ **VOIP (**Voice over Internet Protocol) โทร.กลับไปหลอกเหยื่อชาวจีนหรือไต้หวัน

2) **ตั้งศูนย์นอกประเทศไทย** ที่ตำรวจเคยจับกุมได้เกือบทั้งหมดอยู่ที่ประเทศจีน โดยศูนย์จะอยู่ตามห้องพักหรือแฟลตต่าง ๆ มีนายทุนจ้างคนไทยทำหน้าที่เป็นคอลล์เซ็นเตอร์โทร.กลับมาหลอกเหยื่อชาวไทย

- **คอลล์เซ็นเตอร์ทั้ง 2 แบบ** จะมีการว่าจ้างคนในประเทศนั้น ๆ (ประเทศที่โทร.ไปล่อลวง) ไปเปิดบัญชีธนาคารรอเอาไว้ เช่น หลอกเหยื่อคนไทยก็จะจ้างคนไทยไปเปิดบัญชีธนาคารเอาไว้ จากนั้นจะมี **“ม้าวิ่ง”** คือชาวจีนหรือไต้หวัน ทำหน้าที่ตระเวนกดเงินตามตู้เอทีเอ็ม ต่าง ๆ เพื่อกดเงินออกจากบัญชีที่เปิดรอไว้ดังกล่าว เมื่อได้เงินมาก็จะส่งเงินต่อไปยังกลุ่มขบวนการด้วยวิธีการต่าง ๆ เช่น รวบรวมเป็นเงินสดหิ้วออกนอกประเทศ หรือนำไปโอนผ่านบัญชีธนาคาร หรือใช้ระบบโพยก๊วน

- **"ม้าวิ่ง"** จะเดินทางเข้าออกประเทศมาแล้วหลายครั้ง หลังทำงานเสร็จก็เดินทางกลับ แต่ยังไม่แน่ชัดว่าแต่ละกลุ่มที่เข้ามานั้นอยู่ในประเทศนานเท่าไร

- ผู้ต้องหาส่วนใหญ่ที่จับกุมได้ จะเป็นคนที่ทำหน้าที่คอลล์เซ็นเตอร์, คนไทยที่ถูกจ้างให้เปิดบัญชี และ "ม้าวิ่ง" ที่กดเงินตามตู้เอทีเอ็ม แต่ยังไม่เคยสาวไปถึงนายทุนใหญ่ที่อยู่เบื้องหลังได้เลยแม้แต่ครั้งเดียว

- วิธีการหลอก จะมีการเขียนสคริปต์ให้คนที่ถูกจ้างมาเป็นคอลล์เซ็นเตอร์ใช้พูดตามบทที่เขียนขึ้น ซึ่งที่พบมีทั้งภาษาไทยและภาษาจีน ส่วนเนื้อหาในสคริปต์จะมีใจความที่ทำให้เหยื่อเกิดความโลภหรือความหวาดกลัว เช่น ในช่วงที่ประชาชนต้องทำเรื่องเสียภาษี แก๊งคนร้ายก็จะฉวยโอกาสสมอ้างเป็นเจ้าหน้าที่สรรพากรหลอกว่ามีเงินภาษีคืน ให้ไปทำธุรกรรมทางตู้เอทีเอ็ม จะได้สะดวก ได้เงินคืนทันที ไม่ต้องเสียเวลามาทำเรื่อง หรืออ้างว่าถูกรางวัลจากการสุ่มเบอร์

- ส่วนการหลอกด้วยความหวาดกลัวนั้น มักจะอ้างเป็นเจ้าหน้าที่ธนาคาร เจ้าหน้าที่รัฐ เช่น ปปง. ดีเอสไอ กรมสรรพากร เจ้าหน้าที่ศาล เนื้อหาหลักๆ จะพุ่งเป้าไปที่บัญชีธนาคารของเหยื่อมีปัญหาต่าง ๆ นานา

- หลังทำให้เหยื่อเกิดความโลภหรือหวาดกลัวแล้ว ผู้ที่ทำหน้าที่คอลล์เซ็นเตอร์ก็จะหว่านล้อมด้วยคำพูดแบบหวังดีคือต้องการช่วยเหลือ แต่แท้ที่จริงแล้วประสงค์ร้าย โดยพูดอย่างไรก็ได้ให้เหยื่อไปที่ตู้เอทีเอ็มเพื่อกดโอนเงินไปเข้าบัญชีที่แก๊งคนร้ายเปิดรอไว้แล้ว

กลุ่มแก๊งที่พบบ่อย

กลุ่มแก๊ง "คอลล์เซ็นเตอร์" ที่ปฏิบัติการหลอกลวงเหยื่อเอาไว้อย่างน่าสนใจ โดยแบ่งออกเป็น 2 กลุ่มใหญ่ๆ คือ

1) แก๊งคืนเงินภาษี

คนร้ายจะหลอกเหยื่อว่าได้รับภาษีตกค้างคืนเนื่องจากมีการปรับลดหรือเหตุผลอื่นๆ หากต้องการเงินภาษีดังกล่าวต้องรีบดำเนินการภายในวันนี้เท่านั้น (แน่นอนว่าเหยื่ออยากได้เงินแต่ไม่มีเวลา) คนร้ายจะดำเนินการต่อไปดังนี้

- แนะนำให้ไปที่ตู้เอทีเอ็มที่คนร้ายถนัด

- ทำอย่างไรก็ได้ให้ผู้เสียหายเลือกเมนูภาษาอังกฤษ และพูดโต้ตอบอย่างรวดเร็วให้ผู้เสียหายสับสนจนต้องรีบทำการที่คนร้ายบอก

- หลอกให้อ่านตัวเลขและโอนเงินของเหยื่อ กว่าเหยื่อจะรู้ตัวว่าถูกหลอกก็ต่อเมื่อโอนเงินไปแล้ว

- คนร้ายวางหู ในช่วงนี้เหยื่อจะมีเวลาคิดและรู้ว่าถูกหลอก แต่สายเสียแล้ว

2) แก๊งหนี้บัตรเครดิต

คนร้ายจะหลอกเหยื่อว่ามีหนี้บัตรเครดิตจากธนาคารต่างๆ ไม่ว่าเหยื่อจะมีบัตรเครดิตหรือบัญชีของธนาคารนั้นๆ หรือไม่ แน่นอนว่าเหยื่อจะต้องตกใจ จากนั้นคนร้ายจะดำเนินการต่อไปดังนี้

- เริ่มหลอกเหยื่อโดยใช้หมายเลขที่ไม่มีในสารบบ เช่น มีเครื่องหมายบวกอยู่ด้านหน้า หรือเป็นหมายเลขที่ไม่โชว์เบอร์

- คนร้ายจะใช้เสียงพูดที่บันทึกเสียงสุภาพสตรีหรือสุภาพบุรุษเลียนแบบทางธนาคาร

- คนร้ายจะพูดหลอกลวงเหยื่อ เช่น ท่านมีหนี้ค้างบัตรเครดิตของธนาคาร...100,000 บาท ฟังซ้ำกด 1 ภาษาอังกฤษกด 2 ติดต่อเจ้าหน้าที่กด 9

- เมื่อเหยื่อกด 9 จะมีคนร้ายอีกหนึ่งคนพูดจาไพเราะว่าเขาเป็นเจ้าหน้าที่ เพิ่งได้รับโอนสายจากคอลล์ เซ็นเตอร์ ไม่ทราบรายละเอียด กรุณาแจ้งชื่อ สกุล เลขบัตรประชาชน อายุ ที่อยู่ เบอร์ที่ทำงาน เลขบัญชีและเลขบัตรเครดิตหากท่านมี จากนั้นจะหว่านล้อมอย่างรวดเร็วถึงวิธีการระงับหนี้แบบเร่งด่วนโดยโอนสายไปยังคนร้ายอีกคน

- คนร้ายคนที่สามจะดำเนินการหลอกเหยื่อโดยแนะนำตนเองว่าเป็นเจ้าหน้าที่ฝ่ายกฎหมายและเร่งรัดหรือประนอมหนี้ธนาคาร ซึ่งพูดจารวดเร็วหว่านล้อมให้รีบระงับหนี้โดยทำธุรกรรมทางโทรศัพท์ หากต้องการให้กดตามที่คนร้ายบอก หรือรีบไปที่ตู้เอทีเอ็ม จากนั้นคนร้ายจะให้เลือกเมนูภาษาอังกฤษ และหลอกให้ผู้เสียหายปฏิบัติตามจนเสร็จสิ้นและวางหูไป ช่วงนี้ผู้เสียหายถึงมีเวลาคิดจึงรู้ว่าถูกหลอก

รูปแบบหนึ่งของ แก๊งคอลล์เซ็นเตอร์ ที่ทำการหลอก ข่มขู่ หาข้อมูล จากประชาชนทั่วไปโดยการสุ่มโทร ผสมกับหลากหลายรูปแบบในการหลอกลวง อาทิ โทรมาจากธนาคารพาณิชย์แอบอ้างว่าติดค้างหนี้อยู่ให้ไปที่ตู้ ATM เพื่อโอนเงินมาชำระหนี้ โทรมาจากศาลอาญาว่าไปทำความผิดเกี่ยวกับธุรกรรมทางการเงินและจะถูกออกหมาย จับถ้าไม่โอนเงินมาตามที่แอบอ้าง หรือโทรมาจากเจ้าหน้าที่สรรพากรอ้างว่ายังไม่ได้ชำระหนี้และข่มขู่เอาข้อมูล จากบัตรประชาชน เพื่อที่สามารถตรวจสอบข้อมูลต่างๆของคนอื่น เช่นข้อมูลทางการเงิน ข้อมูลบัตรเครดิต ฯลฯ ได้มากมาย หรือกระทั่งอ้างว่าเป็นเจ้าหน้าที่กรมสรรพากรหลอกว่าจะโอนภาษีเงินได้เข้า บัญชีให้และหลอกให้ผู้เสียหายไปกดเงินที่ตู้ ATM เมื่อเหยื่อหลงเชื่อจึงให้โอนเข้าบัญชีของแก๊งคอลล์เซ็นเตอร์ที่เป็นขบวนการมีทั้งคนไทยและชาวต่างประเทศ ฯลฯ ซึ่งการสูญเสียเงินและทรัพย์สินจะเกิดขึ้นอย่างแน่นอนถ้าไม่รู้เท่าทันมิจฉาชีพ รูปแบบของ แก๊งคอลล์เซ็นเตอร์ ที่ปัจจุบันมีเครือข่ายโยงใยกับกลุ่มบุคคลต่างชาติในแถบเอเชียเป็นส่วนใหญ่

ตัวอย่างคดีที่มีการจับกุมได้ มีแผนประทุษกรรมว่ากลุ่มผู้ต้องหาได้ใช้บ้านเช่าในหมู่บ้านหรูและตั้งสำนักงานคอลล์เซ็นเตอร์ เพื่อให้สมาชิกในแก๊งใช้โทรศัพท์มือถือโทรสุ่มหาผู้เสียหายผ่านเครื่องขยายช่องสัญญาณอินเทอร์เน็ต จากนั้นระบบจะรันสุ่มต่อสายให้โทรหาเบอร์ผู้เสียหาย โดยแก๊งผู้ต้องหาจะแบ่งหน้าที่ทำงานกันเป็นทีม ทีมแรกจะทำหน้าที่โทรเข้าไปหาผู้เสียหาย พร้อมหลอกว่าเป็นเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมาย ได้ตรวจสอบมีเงินจากขบวนการอาชญากรรม โอนไปยังบัญชีผู้เสียหาย ทำให้ผู้เสียหายตกใจกลัว จากนั้นจะบอกว่าเจ้าหน้าที่จะขอตรวจสอบบัญชีการเงิน ขอให้ผู้เสียหายบอกชื่อ สกุล อายุ วัน เกิด ที่อยู่ บัญชีธนาคาร เพื่อขอตรวจสอบ เมื่อผู้เสียหายปฏิเสธว่าไม่เกี่ยวข้องกับขบวนการอาชญากรรม แก๊งผู้ต้องหาจะทำทีโอนสายให้คุยกับอีกทีมที่ปลอมตัวเจ้าหน้าที่ของหน่วยงานต่างๆ ถ้าผู้เสียหายหลงเชื่อ แก๊งผู้ต้องหาจะหลอกให้ผู้เสียหายไปที่ทำธุรกรรมโอนเงินที่ตู้เอทีเอ็ม กดรหัสและเปลี่ยนเมนูเป็นภาษาอังกฤษ และบอกให้ทำ

ตามขั้นตอนต่าง ๆ ในที่สุดเหยื่อจะถูกหลอกให้กดโอนเงินเข้าบัญชีของแก๊งผู้ต้องหา หรืออีกวิธีแก๊งผู้ต้องหาจะอ้างว่าเป็นเจ้าหน้าที่ธนาคาร หลอกเหยื่อว่าเป็นหนี้บัตรเครดิตจำนวนมาก เมื่อเหยื่อปฏิเสธ ก็จะสอบถามข้อมูลส่วนตัว พร้อมหลอกให้ไปกดโอนเงินที่ตู้เอทีเอ็ม โดยอ้างว่าจะขอตรวจสอบบัญชีธนาคาร หรืออีกวิธีผู้ต้องหาจะแจ้งว่า เป็นเจ้าหน้าที่กรมสรรพากร โทร.บอกผู้เสียหายว่า ได้รับคืนภาษี ขอให้ผู้เสียหายไปทำตามขั้นตอนที่ตู้เอทีเอ็มเพื่อขอรับเงินภาษีคืน จนเหยื่อพลาดท่าหลงเชื่อโอนเงินเข้าบัญชีผู้ต้องหาเป็นจำนวนมาก โดยแก๊งคอลล์เซ็นเตอร์ทำให้ผู้เสียหายสูญมูลค่าไม่ต่ำกว่า 100 ล้านบาท และจากการตรวจสอบเส้นทางทางการเงิน พบว่า แก๊งผู้คอลล์เซ็นเตอร์นั้น ได้โอนเงินของผู้เสียหายเข้าไปในบัญชีธนาคารของแก๊งคอลล์เซ็นเตอร์ที่ร่วมทำกันเป็นขบวนการในประเทศจีน และไต้หวัน ซึ่งกลุ่มผู้กระทำความผิดนี้จัดว่าเป็นขบวนการอาชญากรรมข้ามชาติรายใหญ่ที่มีเครือข่ายมากมาย พวกนี้จะเข้ามาใช้ประเทศไทยเพื่อใช้เป็นฐานตั้งคอลล์เซ็นเตอร์ สุ่มโทรหลอกเหยื่อในหลายประเทศในภูมิภาคเอเชีย

2.2) กลุ่มผู้กระทำความผิด (อาชญากรรม และองค์กรอาชญากรรม)

สรุปผลการจับกุมแก๊ง Call Center ที่ตั้งในสาธารณรัฐประชาชนจีน

1) การจับกุมแก๊ง Call Center ร่วมกับเจ้าหน้าที่ของสาธารณรัฐประชาชนจีนที่โทรศัพท์หลอกลวงคนไทย

1.1 เมื่อ พ.ศ. 2551 ที่เมืองซัวเถา สาธารณรัฐประชาชนจีน จับกุมผู้ต้องหาชาวไทย จำนวน 42 คน และนำกลับมาเพื่อดำเนินคดีฉ้อโกงประชาชนในประเทศไทย โดยศาลมีคำพิพากษาแล้วบางส่วน และบางส่วนผู้ต้องหายังอยู่ในกระบวนการทางศาล

1.2 เมื่อวันที่ 8 เมษายน 2553 ที่เมืองฉางอัน เขตตงก่วน มณฑลกวางตุ้ง จับกุมผู้ต้องหาชาวไทยจำนวน 13 คน ซึ่งขณะนี้อยู่ระหว่างการดำเนินคดีที่สาธารณรัฐประชาชนจีน และยังนำตัวกลับประเทศไทย

กรณีตั้งศูนย์ Call center ในต่างประเทศ คนร้ายจ้างคนไทยเดินทางไปทำงานรับโทรศัพท์ โดยเข้ามาเช่าที่พักอาศัยในสาธารณรัฐประชาชนจีน และมีพฤติกรรมหลอกลวงเหยื่อที่มีสัญชาติไทยที่อยู่ในประเทศไทย โดยโทรศัพท์จากสาธารณรัฐประชาชนจีนเพื่อไปหลอกเหยื่อชาวไทย ที่อยู่ในประเทศไทยให้โอนเงินเข้าบัญชีที่ประเทศไทย และผู้ร้ายจะกดเงินจากตู้เอทีเอ็มในประเทศไทย

โดยกลุ่มคนร้ายมีเทคโนโลยีอันทันสมัยได้ทำการหลอกลวงให้ผู้เสียหายโอนเงินผ่านระบบบัตรอิเล็กทรอนิกส์ โดยกลุ่มคนร้ายฉ้อโกงประชาชนด้วยวิธีการต่างๆ อาทิเช่น แจ้งว่าเป็นผู้ถูกรางวัลของสลากกินแบ่งรัฐบาล ได้รับเงินภาษีเงินส่วนบุคคลคืนจากราชการ เป็นหนี้จากการใช้บัตรเครดิต หรือถูกกลุ่มมิจฉาชีพนำบัตรเครดิตของผู้เสียหายไปใช้ ทำให้ผู้เสียหายหลงเชื่อตกเป็นเหยื่อ เกิดความเสียต่อประชาชนเป็นจำนวนมาก คณะทำงานสืบสวนปราบปรามฯ ได้ดำเนินการสืบสวนจนทราบว่ากลุ่มคนร้ายมีศูนย์ Call Center อยู่ในประเทศจีน จึงได้ร่วมกับสถานเอกอัครราชทูตสาธารณรัฐประชาชนจีนประจำประเทศไทย ร่วมสืบสวนติดตามจับกุมคนร้ายที่ฉ้อโกงประชาชนไทยด้วยวิธีการต่าง ๆ ในประเทศจีน ณ มณฑลกวางตุ้ง ประเทศจีน ตั้งแต่เดือนพฤศจิกายน 2550

จนทราบว่า กลุ่มคนร้ายทำเป็นรูปขบวนการ แบ่งหน้าที่กันทำการหลอกลวงฉ้อโกงประชาชนมานานประมาณ 8 ปี มีผู้เสียหายจำนวนมากในหลายประเทศในเขตเอเชียตะวันออกเฉียงใต้ อาทิ ไทย,มาเลเซีย ,ไต้หวัน และจีน เป็นต้น จนกระทั่งต่อมา คณะทำงานสืบสวนปราบปราม ฯ ร่วมกับตำรวจจีน ทำการตรวจค้นอาคารโย่ว หยี ต้า ซ่า เมืองซัวเถา ประเทศจีน ซึ่งคนร้ายใช้เป็นที่ตั้ง Call Center ที่ใช้หลอกผู้เสียหายชาวไทย ผลการตรวจค้นจับกุมได้ผู้ต้องหาที่เป็นคนไทย จำนวน 42 คน (เป็นชาย 24 คน หญิง 18 คน) และยังมีผู้ต้องหาเป็นคนจีน ไต้หวัน เกาหลี และมาเลเซีย อีกจำนวนมาก ซึ่งทางตำรวจจีนได้ขอดำเนินคดีกับผู้ต้องหาทั้งหมด ตามกฎหมายจีนก่อน ต่อมาคณะทำงานสืบสวนปราบปรามฯ ได้ดำเนินการประสานกับทางตำรวจจีนมาโดยตลอดเพื่อขอรับตัวผู้ต้องหาชาวไทยทั้งหมดจำนวน 42 คน กลับมาดำเนินคดีในประเทศไทย ทางตำรวจจีนได้แจ้งให้เจ้าหน้าที่ตำรวจไทยไปรับผู้ต้องหาซึ่งเป็นชาวไทยทั้งหมดจำนวน 40 คนกลับมาดำเนินคดีในประเทศไทย

3) องค์ความรู้เกี่ยวกับแนวทางการพัฒนาประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และคดีที่ประสบความสำเร็จ (Best Practice) เนื่องจากเครือข่ายการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

แนวคิด **การจัดการความรู้** หมายถึง การรวบรวมองค์ความรู้ด้านกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง ขั้นตอน แนวทางการปฏิบัติงานด้านนิติวิทยาศาสตร์ที่มีอยู่อย่างกระจัดกระจายในรูปของหนังสือ ตำรา เอกสารทางราชการ สำนวนการสอบสวนและรายงานการสืบสวน รวมทั้งความรู้ที่มีอยู่ในตัวผู้ปฏิบัติงาน มาพัฒนาให้เป็นระบบสร้างเกณฑ์ในหมวดต่างๆ การวัด การวิเคราะห์ และการจัดการความรู้ การมุ่งเน้นทรัพยากรบุคคล การจัดการกระบวนการ และผลลัพธ์การดำเนินการ

แนวทาง เพื่อให้มีความรู้ความเข้าใจ สร้างเสริมสำนึกรับผิดชอบในวิชาชีพตามหลักจริยธรรมที่พึงปฏิบัติ และป้องกันการทุจริตประพฤติมิชอบของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย มุ่งหล่อหลอมจิตใจ อุปนิสัย และเสริมสร้างบุคลิกภาพ ตลอดจนพฤติกรรมที่เหมาะสม เพียบพร้อมไปด้วยคุณธรรม ความซื่อสัตย์สุจริต ความเสียสละความสำนึกในหน้าที่ และการบริการประชาชน เป็นที่ศรัทธาและเชื่อถือของประชาชน

การจัดการความรู้อย่างเป็นรูปธรรม และมีประสิทธิภาพด้วยการจัดการความรู้ด้านการรวบรวมข้อมูลการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ โดยมีแผนบริหารจัดการองค์ความรู้ในระยะเร่งด่วน ระยะสั้นและระยะยาว

วิธีการจัดการความรู้มาสร้างการเปลี่ยนแปลงเพื่อพัฒนาองค์ความรู้ด้านการปฏิบัติงานการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจ ฝ่ายปกครอง และประชาชน

มีการปฏิบัติการและกิจกรรม มีวิธีการรวบรวมข้อมูลหลาย ๆ รูปแบบ เช่น การเข้าร่วมเรียนรู้กับเจ้าหน้าที่ตำรวจที่เป็นผู้มีความรู้ความเชี่ยวชาญ และมีประสบการณ์ด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

1) ขยายหน่วยด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ออกไปยังส่วนภูมิภาค เพื่อรองรับปัญหาอาชญากรรมคอมพิวเตอร์

2) ปรับอัตรากำลังพลให้เหมาะสมกับปริมาณงาน รวมถึงการจัดฝึกอบรมทางด้านเทคโนโลยีสารสนเทศเพิ่มเติม อย่างสม่ำเสมอ

3) เผยแพร่ความรู้ทางหนังสือจากคู่มือด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ซึ่งสามารถนำความรู้ไปใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

4) เผยแพร่ทาง CD แก่ผู้มีหน้าที่ในการปฏิบัติงานด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์เพื่อเป็นคู่มือในการปฏิบัติงานอย่างเป็นมาตรฐานเดียวกันอย่างเป็นรูปธรรม และมีประสิทธิภาพ

10. สรุปผลการศึกษา

1) สภาพปัญหาอาชญากรรมคอมพิวเตอร์ในสังคมไทยปัจจุบัน

ปัจจุบันเทคโนโลยีคอมพิวเตอร์ เปรียบเสมือนวิถีชีวิตของมนุษย์นับวันจะยิ่งทวีความสำคัญเพิ่มมากขึ้นเรื่อยๆ และยังมีอิทธิพลมากพอที่จะเปลี่ยนแปลงวิถีชีวิตมนุษย์ไปในทิศทางต่างๆ ได้ทำให้สถานการณ์เกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มมากขึ้น เนื่องจากการขยายตัวของผู้ใช้งานคอมพิวเตอร์ในประเทศไทยเพิ่มสูงขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้งานคอมพิวเตอร์ในสังคมไทย ยังขาดความรู้ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีสารสนเทศอย่างแท้จริง อีกทั้งสังคมไทยยังขาดการเอาใจใส่ในประเด็นการปลูกฝังจริยธรรม คุณธรรม จรรยาบรรณเกี่ยวกับการใช้งานอินเตอร์เน็ตหรือสังคมออนไลน์ในทางที่เหมาะสม ทำให้ผู้ใช้ (Users) บางส่วนขาดจริยธรรมนำเทคโนโลยีไปใช้ในทางที่มิชอบ ประกอบกับผู้ใช้อินเตอร์เน็ตไม่ตระหนักถึงความสำคัญด้านความปลอดภัยคอมพิวเตอร์และเครือข่าย ละเลยการป้องกันตนเองและไม่รู้สึกถึงความรับผิดชอบของตนเองต่อการใช้เครือข่ายร่วมกัน ในขณะที่อินเตอร์เน็ตขยายตัวไปอย่างรวดเร็ว อาชญากรรมคอมพิวเตอร์ก็มีแนวโน้มเพิ่มขึ้น แต่จำนวนบุคลากรด้านความปลอดภัยคอมพิวเตอร์และเครือข่ายกลับมีจำนวนจำกัด ซึ่งไม่เพียงพอต่อการดูแลระบบทั้งภาครัฐและภาคเอกชน ทำให้ระบบเครือข่ายในประเทศไทยขาดการควบคุมดูแลด้านความมั่นคงปลอดภัยของผู้ใช้งาน

ปัญหาทางด้านกฎหมาย ความแตกต่างกันของอาชญากรรมคอมพิวเตอร์และอาชญากรรมพื้นฐานทำให้เกิดปัญหา ไม่ว่าจะเป็นประเด็นของการตีความ การกำหนดฐานความผิด การประเมินความเสียหายจากการกระทำความผิด เขตอำนาจศาล ผู้รับผิดชอบ ความแตกต่างทางกฎหมาย และการสืบสวนตลอดจนการรวบรวมพยานหลักฐาน เพื่อพิสูจน์ความผิดของอาชญากรรมคอมพิวเตอร์เป็นประเด็นหรือช่องโหว่ที่กระทบต่อการปฏิบัติในการดำเนินคดีทุกขั้นตอน ไม่ว่าจะเป็นการสืบสวน สอบสวน การเก็บและรวบรวมพยานหลักฐาน การตรวจพิสูจน์พยานหลักฐานต่างๆ การพิจารณาและการพิพากษาคดี ซึ่งเมื่อกฎหมายอาชญากรรมทางคอมพิวเตอร์มีผลบังคับใช้ ก็จะส่งผลในทางปฏิบัติตามมา เนื่องจากปัญหาด้านความรู้ ความเข้าใจ เกี่ยวกับเทคโนโลยีและอาชญากรรมคอมพิวเตอร์ของบุคลากรในสายกระบวนการยุติธรรม ไม่ว่าจะเป็นตำรวจ อัยการ ศาล ล้วนแล้วแต่เป็นจุดอ่อนในกระบวนการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์เป็นอย่างยิ่ง ดังนั้น สิ่งที่ควรจะคำนึงมากที่สุดในเวลานี้ คือ ทำอย่างไรเราถึงจะได้ประยุกต์ใช้หรือประมาณการณ์ที่จะ

นำไปใช้ได้อย่างถูกต้องและถูกวิธี เพื่อไม่ให้คอมพิวเตอร์และอินเตอร์เน็ตกลายเป็นภัยหรืออันตรายต่อมนุษย์และสังคม

กระบวนการจัดการปัญหาคดีทางด้านอาชญากรรมคอมพิวเตอร์ในประเทศไทยยังไม่มีรูปธรรมที่ชัดเจนมากนัก ประการสำคัญ คือ ความรู้ ความเข้าใจในเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต การประยุกต์ใช้กฎหมายต่างๆ และการรักษาความน่าเชื่อถือของพยานหลักฐานที่ได้ ในการใช้ลงโทษคนร้าย หน่วยงานที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ มีการทำงานในลักษณะต่างหน่วยต่างทำ และเนื่องจากพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายซึ่งบังคับใช้ได้ไม่นานไม่เอื้อต่อการปฏิบัติงานจริงในบางประเด็น เช่น การดำเนินงานหลายๆ อย่าง ได้ให้อำนาจเฉพาะพนักงานเจ้าหน้าที่ในการดำเนินงานเท่านั้น ทำให้เจ้าหน้าที่ตำรวจโดยเฉพาะพนักงานสอบสวนหลายพื้นที่เกิดปัญหาในการขอข้อมูลจากผู้ให้บริการทางอินเทอร์เน็ต ว่าเป็นอำนาจของผู้ใดกันแน่ จะต้องมีการฝึกอบรมความรู้ทางเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต และการประยุกต์ใช้กฎหมายต่างๆ แก่เจ้าหน้าที่ที่เกี่ยวข้องตลอดเวลา เพื่อให้ทันต่อการพัฒนาทางเทคโนโลยีที่มีการพัฒนาที่รวดเร็วอย่างมาก รวมถึงรูปแบบและวิธีการกระทำความผิดของคนร้ายที่จะพัฒนาเปลี่ยนแปลงไปตามการพัฒนาทางเทคโนโลยีที่เกิดขึ้น

จากการที่ปัจจุบันสภาพสังคมของเรากลายเป็นสังคมออนไลน์ที่ทุกคนสามารถติดตามข้อมูลข่าวสารผ่านระบบอินเทอร์เน็ตได้แบบรวดเร็วทันที (Online Real Time) ดังนั้น การที่เราจะมีผู้ให้บริการเว็บไซต์ต่างๆ มารวมตัวกันในการแลกเปลี่ยนข้อมูลข่าวสารที่ตัวผู้ให้บริการเว็บไซต์แต่ละเว็บไซต์ได้ทำการเก็บรวบรวมปัญหาต่างๆ ที่เกิดขึ้นกับเว็บไซต์ของตนเอง โดยรวมตัวกันเป็นเครือข่ายชุมชนออนไลน์ จึงเป็นช่องทางหนึ่งที่สำคัญในการช่วยเหลือการทำงานของทางราชการ ในการสืบสวน สอบสวน ป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพราะจะมีข้อมูลข่าวสารที่เป็นประโยชน์ต่อผู้ใช้งาน (Users) ในการป้องกันการตกเป็นเหยื่อของอาชญากรทางเทคโนโลยี ดังนั้นในการแก้ไขปัญหาดังกล่าว เราต้องมีการร่วมกันระหว่างหน่วยงานภาครัฐ และหน่วยงานภาคเอกชน โดยควรมีการรวมกลุ่มกันของผู้ประกอบการเว็บไซต์ต่างๆ เพื่อรวมตัวกันเป็นชุมชนออนไลน์ในการเผยแพร่ข้อมูลข่าวสารที่เป็นประโยชน์ต่อสังคมออนไลน์

2) ประโยชน์ของเครือข่ายชุมชนออนไลน์

1) ร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง และวิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการป้องกันปัญหาดังกล่าว

2) ร่วมแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็บไซต์ (Black List)

3) จัดเวทีให้มีการร่วมงานประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแรกเปลี่ยนข้อคิดเห็นและกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

3) กฎ 4 ประการในการรักษาความน่าเชื่อถือของพยานหลักฐานทางคอมพิวเตอร์

1) ต้องไม่กระทำให้เกิดการเปลี่ยนแปลงใด ๆ ในพยานหลักฐาน

2) กรณีที่มีความจำเป็นไม่สามารถหลีกเลี่ยงการเปลี่ยนแปลงของพยานหลักฐานได้ ต้องสามารถอธิบายได้ และพยายามให้เกิดการเปลี่ยนแปลงน้อยที่สุดเท่าที่จะเป็นไปได้

3) บันทึกรายละเอียดต่าง ๆ ทุกขั้นตอนที่กระทำกับพยานหลักฐานทางอิเล็กทรอนิกส์ และหากใช้เครื่องมืออื่นที่ได้รับมาตรฐานเช่นเดียวกันจะต้องได้รับผลลัพธ์แบบเดียวกัน

4) ผู้ที่เป็นเจ้าของคดี ต้องทำให้แน่ใจว่าได้ปฏิบัติถูกต้องตามกฎหมายและกฎในการรักษาความน่าเชื่อถือของพยานหลักฐาน

4) การวิจัยเพื่อจัดทำคู่มือเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

กระบวนการของการจัดทำคู่มือเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ตำรวจและหน่วยงานต่างๆ ที่เกี่ยวข้อง เครื่องมือที่ใช้ในการวิจัยนี้ คือ การประชุมเพื่อแลกเปลี่ยนความรู้ (Storytelling) เพื่อรวบรวมความรู้ที่ฝังลึกอยู่ในตัวบุคคล เช่น ประสบการณ์ พรสวรรค์ หรือสัญชาตญาณ และความรู้ชัดแจ้ง เช่น จากทฤษฎี ข้อกฎหมาย ระเบียบและวิธีการปฏิบัติงาน ขั้นตอนการพิสูจน์หลักฐาน รวมทั้งรวบรวมปัญหา อุปสรรค และข้อเสนอแนะ แนวทางการปรับปรุงและพัฒนาระบบงานด้านการจัดการเกี่ยวกับคดีทางด้านอาชญากรรมคอมพิวเตอร์ ให้มีประสิทธิภาพมากยิ่งขึ้น โดยเชิญกลุ่มเป้าหมายเข้าร่วมประชุมแลกเปลี่ยนความรู้และแสดงความคิดเห็น ประกอบไปด้วย ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ของสำนักงานตำรวจแห่งชาติ, กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม, กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์, เจ้าหน้าที่ฝ่ายสืบสวน, พนักงานสอบสวน, พนักงานอัยการ, ผู้พิพากษา, ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยบนระบบเครือข่ายและด้านอาชญากรรมคอมพิวเตอร์จากหน่วยงานเอกชน และสื่อมวลชนต่างๆ ที่เกี่ยวข้องกับงานด้านอาชญากรรมคอมพิวเตอร์ มาประชุมเพื่อแลกเปลี่ยนความรู้ ประสบการณ์ และแสดงความคิดเห็นร่วมกับคณะผู้วิจัยโดยได้สรุปในเชิงเสนอแนะดังนี้

11. ข้อเสนอแนะแนวทางในการแก้ไขปัญหาและอุปสรรค

1) พนักงานสอบสวน ยังขาดความรู้ความเข้าใจในเรื่องของระบบคอมพิวเตอร์ และระบบอินเทอร์เน็ต เมื่อผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที เพราะไม่รู้กระบวนการในการทำงานที่เกิดขึ้น ซึ่งเป็นปัญหาใหญ่ที่จะต้องมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต และกฎหมายที่เกี่ยวข้องแก่พนักงานสอบสวนทั่วประเทศ โดยเฉพาะประเด็นการตั้งคำถามของพนักงานสอบสวน เป็นเพราะขาดความรู้ทำให้ตั้งคำถามอย่างไม่มีทิศทาง และรวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติหน้าที่ด้วย

2) พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐาน ในหลายกรณีไม่มีความน่าเชื่อถือ เนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of custody) ซึ่งเป็นการพิสูจน์ความเชื่อมโยง

ของพยานหลักฐานกับการกระทำความผิด กระบวนการส่งต่อวัตถุพยานจะต้องมีการบันทึกรายละเอียดของวัตถุพยานซึ่งเริ่มตั้งแต่การตรวจพบ และเก็บวัตถุพยานในสถานที่เกิดเหตุรวมถึงผู้จัดส่ง – ผู้รับ ผู้ตรวจพิสูจน์ตลอดทั้งกระบวนการสืบสวนสอบสวน ดังนั้นจึงต้องมีการบันทึกเป็นหลักฐานตามลำดับเวลา เพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้นๆ หากขาดการต่อเนื่องของการครอบครองวัตถุพยาน เมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือในชั้นศาล

3) สำนักงานศาล และสำนักงานอัยการสูงสุด ควรมีการจัดตั้งหน่วยงานเฉพาะขึ้นมาดูแลรับผิดชอบคดีทางด้านอาชญากรรมคอมพิวเตอร์เป็นการเฉพาะ เพราะสำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ ได้มีการจัดตั้งหน่วยงานเฉพาะเพื่อดูแลรับผิดชอบคดีทางด้านอาชญากรรมคอมพิวเตอร์แล้ว เนื่องจากเป็นคดีที่ต้องทำความเข้าใจในเรื่องของเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต ที่มีความซับซ้อนและเข้าใจยากในบางกรณีเพราะเป็นเรื่องเทคนิคเฉพาะ อีกทั้งมีคดีทางด้านอาชญากรรมคอมพิวเตอร์เกิดขึ้นจำนวนมาก และมีแนวโน้มว่าเพิ่มมากขึ้นทุกปี

4) บทบาทของสื่อมวลชนในบางกรณีมีผลกระทบต่อการปฏิบัติงาน และการนำเสนอรายละเอียดในทางคดีที่นำไปเผยแพร่ต่อสาธารณชน บางครั้งสื่อมวลชนมีการนำเสนอข้อมูลส่วนที่สำคัญในการนำวิธีการหรือผลลัพธ์ในการทำงานของเจ้าหน้าที่ไปเปิดเผย คนร้ายจึงไม่ทิ้งร่องรอยในการกระทำความผิดไว้หรือมีการใช้เทคโนโลยีที่ซับซ้อนมากขึ้นในการอำพรางหรือหลบซ่อนตัวเอง ทำให้เจ้าหน้าที่ปฏิบัติงานยากลำบากขึ้น ซึ่งเป็นจุดอ่อนต่อการปฏิบัติงานของเจ้าหน้าที่

5) เห็นควรสรรหาบุคลากรเพื่อมาปฏิบัติหน้าที่ทางด้านคดีอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นเพื่อรองรับปัญหาทางด้านคดีอาชญากรรมคอมพิวเตอร์ที่เพิ่มมากขึ้น

6) จัดซื้อวัสดุอุปกรณ์ในการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับคดีทางด้านอาชญากรรมทางคอมพิวเตอร์ที่มีความทันสมัย ใช้เวลาในการตรวจพิสูจน์น้อย เคลื่อนย้ายได้ง่าย และให้ผลการตรวจพิสูจน์ที่ถูกต้อง แน่นอน เพื่อลดระยะเวลาและปริมาณงาน เช่น ซอฟต์แวร์การกู้ข้อมูลที่ถูกลบไปแล้ว เป็นต้น

บทคัดย่อ

โครงการวิจัยเรื่อง “เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์” มีวัตถุประสงค์เพื่อพัฒนาหารูปแบบที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์สร้างเครือข่ายในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ สร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ หลังจากมีการศึกษาวิธีการป้องกันและปราบปรามจากต่างประเทศ และนำมาประยุกต์ใช้ กลุ่มเป้าหมาย คือ เจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้อง และประชาชนเครือข่ายที่มีความรู้ ความชำนาญและประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ การประชุมเพื่อแลกเปลี่ยนเรียนรู้ (Storytelling) โดยใช้กระบวนการ “การจัดการความรู้” โดยการรวบรวมองค์ความรู้ที่มีอยู่ในองค์กร ซึ่งกระจัดกระจายอยู่ในตัวบุคคล และเอกสารมาพัฒนาให้เป็นระบบ ผลการวิจัย พบว่า

1.สภาพการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ สรุปประเด็นหลักสำคัญ ได้แก่ 1) ปัจจุบันเจ้าหน้าที่ใช้กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประมวลกฎหมายอาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ และ พ.ร.บ.ลิขสิทธิ์ พ.ศ.2537 เป็นต้น 2) หน่วยงานที่รับผิดชอบดำเนินการคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ได้แก่ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสำนักงานตำรวจจะเป็นด่านแรกในการดำเนินการ สืบสวน สอบสวน ป้องกัน และปราบปรามอาชญากรรมทางคอมพิวเตอร์

2. รูปแบบของคดีที่ต้องให้ความสำคัญและนำส่งวัตถุพยานของกลางตรวจพิสูจน์ทางคอมพิวเตอร์ ได้แก่ 1) คดีลักทรัพย์ เช่น นำเครื่องคอมพิวเตอร์ที่สงสัยว่าเป็นเครื่องที่ถูกโจรกรรมไปตรวจหาข้อมูลเพื่อเปรียบเทียบกับข้อมูลการใช้งานที่ผู้เสียหายมีอยู่ 2) คดีเกี่ยวกับชีวิต เช่น ในที่เกิดเหตุที่พบศพถูกฆ่าแล้วเผามีบัตรประจำตัวประชาชนถูกเผาเหลือแต่ส่วนที่เป็นแถบแม่เหล็กตกอยู่สามารถนำส่งตรวจเพื่อสืบค้นข้อมูลที่มีอยู่ในแถบแม่เหล็กได้ 3) คดีระเบิด เช่น การใช้โทรศัพท์เป็นตัวจุดชนวนระเบิด หลังจากมีการระเบิดแล้วพบ sim โทรศัพท์ตกในที่เกิดเหตุ สามารถนำส่งตรวจหาข้อมูลที่มีอยู่ในซิมการ์ดได้ 4) คดีละเมิด เช่น การนำภาพผู้เสียหายไปตัดต่อดัดแปลงให้เสียหาย 5) คดีผู้ก่อการร้าย เช่น กรณีมีการใช้เครื่องคอมพิวเตอร์เชื่อมต่ออินเตอร์เน็ตเพื่อส่งข้อมูลที่ใช้ในการก่อการร้าย 6) คดีเกี่ยวกับการปลอมแปลง เช่น มีการแก้ไข และเปลี่ยนแปลงข้อมูลของผู้เสียหาย และ 7) คดียาเสพติด เช่น ตรวจหาข้อมูลที่สามารถเชื่อมโยงไปถึงตัวคนร้ายได้ เช่น มีของกลางที่เป็นโทรศัพท์, กล้องถ่ายภาพ, บัตรที่มีการบันทึกข้อมูลระบบดิจิตอล

3. ปัญหาข้อขัดข้องในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ได้แก่ 1) ปัญหาที่เกิดก่อนการตรวจพิสูจน์ เช่น ความรู้ความสามารถเรื่องคอมพิวเตอร์ของพนักงานสอบสวนในการสอบสวนคดี 2) ปัญหาที่เกิดระหว่างการตรวจพิสูจน์ เช่น ข้อจำกัดของระบบคอมพิวเตอร์ หรือ Software และ 3) ปัญหาที่เกิดหลังการตรวจพิสูจน์ เช่น ผลการตรวจไม่เป็นประโยชน์ต่อรูปคดี

4. การจัดทำเครือข่ายทางด้านอาชญากรรมคอมพิวเตอร์ คือ การร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง วิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการป้องกันปัญหาทางด้านอาชญากรรมคอมพิวเตอร์ รวมทั้งแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็บไซต์ (Black List) ร่วมกันจัดเวทีประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแลกเปลี่ยนข้อคิดเห็น และกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

Abstract

The research topic of Network and Knowledge management in Cyber Crime. There is an objective to develop suitable model for the prevention and suppression of cyber crime and establish a network Knowledge and create the handbook of prevention and suppression of cyber crime after study and apply research foreign. The target groups are police, other related agencies and network people who have knowledge and experience in the prevention and suppression of cyber crime. Tools used in the study are the meeting for knowledge exchanging (Storytelling) by using the process “Knowledge Management” by Gathering of knowledge, which is scattered in the individual and document to develop system. The results showed that:

1. Situation of the cyber crime: 1) Present, Polices use law such as Computer Related Crime Act. B.E. 2550, the penal code category 4: faults on electronic cards and Copyright Act. B.E. 2537 etc. Responsible agency such as Royal Thai Police, Department of Special Investigation, Ministry of Information and Communication Technology but Royal Thai Police is the first stage of investigation, prevention and suppression of cyber crime.

2. The importance of the model case and evidence identification in Cyber Crime such as 1) Theft Case for example, Computer suspected to be stolen for detects data to compare with the data victim. 2) Life Case for example, In crime scene, found body were killed and burned with a magnetic strip ID card can check to detect data contained in the magnetic strip. 3) Explode Case for example, Using Mobile phone is a detonated a bomb after the bomb exploded found sim card in crime scene can check to detect data contained in sim card. 4) Infringe Case for example, Modified photo montage victim. 5) Terrorism Case for example, Using Computer connected internet for send data. 6) Falsification Case for example, Edit and change data of the victim. And 7) Narcotic Case, for example Detection of data can link to the offender, such as Mobile phone, Camera, Digital card.

3. Problems in the operation of the Cyber Crime such as 1) Problem before identification for example, Knowledge and Capabilities of the police. 2) Problem between identification for example, Limitation of computer systems or Software. And 3) Problem after identification for example, Results not beneficial to the case.

4. The preparation of the network cyber crime. Sharing data about the scam form. Prevention methods manually from this cyber crime. And other data useful to prevent the crime. Including sharing data about the list of offenders on the Website (Black List). Jointly organized the seminar online community network to share ideas to reduce the Cyber crimes. Time continuously.

คำนำ

เอกสารร่างรายงานวิจัยฉบับสมบูรณ์ “เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์” ได้รับการสนับสนุนจากสำนักงานกองทุนสนับสนุนการวิจัย (สกว.) มีระยะเวลาศึกษาตั้งแต่กันยายน พ.ศ. 2555 – กันยายน พ.ศ. 2556 มีวัตถุประสงค์สำคัญเพื่อพัฒนาหารูปแบบที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ สร้างเครือข่ายในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ และสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์หลังจากมีการศึกษาวิธีการป้องกันและปราบปรามจากต่างประเทศ และนำมาประยุกต์ใช้

สาระสำคัญในรายงานจำแนกออกเป็น 5 บท ได้แก่ บทที่ 1 กล่าวถึงความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการวิจัย คำถามในการวิจัย ขอบเขตในการวิจัย ขั้นตอนการดำเนินงานวิจัย วิธีดำเนินการวิจัย กรอบแนวความคิดของการวิจัย ผลที่จะได้รับจากการวิจัย และกระบวนการผลักดันผลงานดังกล่าวออกสู่การใช้ประโยชน์ สำหรับเนื้อหาในบทที่ 2 เป็นการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง ซึ่งได้แก่ แนวคิดทฤษฎีที่เกี่ยวข้อง กฎหมายที่เกี่ยวข้อง รวมทั้งงานวิจัยที่เกี่ยวข้อง บทที่ 3 เสนอรายงานผลการดำเนินงาน ซึ่งได้แก่ สถานการณ์ปัจจุบันทางด้านอาชญากรรมคอมพิวเตอร์ ข้อมูลเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ ข้อมูลคดีอาชญากรรมคอมพิวเตอร์ที่ประสบความสำเร็จ (Best Practice) แนวทาง ขั้นตอน เทคนิค วิธีการสืบสวนสอบสวนปฏิบัติงาน องค์ความรู้เกี่ยวกับแนวทางการพัฒนาประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และขั้นตอนการดำเนินการจัดการความรู้ ทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ สำหรับบทที่ 4ผลที่ได้จากการดำเนินการเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ และบทที่ 5 ซึ่งเป็นเนื้อหาเกี่ยวกับการสรุปผลการศึกษาและข้อเสนอแนะ

คณะผู้ศึกษาวิจัยขอขอบพระคุณทุกท่านที่ให้การสนับสนุนกระบวนการศึกษา และหวังว่ารายงานการศึกษาวิจัยฉบับนี้จะเป็นประโยชน์ต่อการปฏิบัติงานตามเจตนารมณ์ และวัตถุประสงค์ของการวิจัยในการในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

คณะผู้ศึกษาวิจัย
กันยายน 2556

กิตติกรรมประกาศ

การดำเนินโครงการวิจัย “เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์” สำเร็จลงได้ด้วยดีเนื่องจากได้รับความอนุเคราะห์จาก ดร.สีลาภรณ์ บัวสาย ผู้อำนวยการฝ่ายชุมชนและสังคม สำนักงานกองทุนสนับสนุนการวิจัย (สกว.) ที่ให้โอกาสแก่หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา ในการดำเนินโครงการวิจัยในครั้งนี้

คณะผู้วิจัยขอขอบคุณ ผู้เข้าร่วมประชุมจากหน่วยงานต่างๆ ได้แก่ สำนักงานอัยการสูงสุด กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มงานคณาจารย์ คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติ และกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี ตลอดจนหน่วยงานที่เกี่ยวข้องที่ไม่ได้เอ่ยนามมา ณ ที่นี้ ที่เป็นผู้ให้ข้อมูลสำคัญในการดำเนินกิจกรรมแลกเปลี่ยนเรียนรู้ในครั้งนี้ และทำให้การดำเนินโครงการสำเร็จลุล่วงไปได้ด้วยดี

สุดท้ายนี้ คณะผู้วิจัย ขอขอบคุณ รองศาตราจารย์ ดร.ฤเดช เกิดวิชัย อธิการบดี มหาวิทยาลัยราชภัฏสวนสุนันทา และรองศาตราจารย์ ดร.ช่วงโชติ พันธุเวช อดีตอธิการบดี มหาวิทยาลัยราชภัฏสวนสุนันทา และ **พลตำรวจเอกญาณพล ยั่งยืน** รองอธิบดีกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ที่ให้ความอนุเคราะห์เป็นที่ปรึกษาโครงการ จนทำให้โครงการวิจัยบรรลุเป้าหมายและวัตถุประสงค์จนเสร็จสมบูรณ์ได้ด้วยดี

คณะผู้ศึกษาวิจัย
กันยายน 2556

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตาราง

สารบัญภาพ

บทที่ 1
บทนำ

ในการศึกษาโครงการเรื่องเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์นั้น คณะผู้วิจัยได้ศึกษาเกี่ยวกับ

1) ความเป็นมาและความสำคัญของปัญหา
2) วัตถุประสงค์ของการวิจัย
3) คำถามของการวิจัย
4) ขอบเขตของการวิจัย
5) กรอบแนวความคิดของการวิจัย
6) ความสำคัญของการวิจัย
7) ผลที่คาดว่าจะได้รับ
8) กระบวนการผลักดันผลงานดังกล่าวออกสู่การใช้ประโยชน์
9) นิยามศัพท์เฉพาะ

1.1 ความเป็นมาและความสำคัญของปัญหา

1) อาชญากรรมคอมพิวเตอร์

ในสังคมไทยมองเห็นประโยชน์ของเครือข่ายอินเทอร์เน็ตอย่างมากมายมหาศาล หรือมองภาพพจน์ของคนที่ใช้อินเทอร์เน็ตว่าเป็นผู้ที่มีความรู้ ความสามารถในการใช้เทคโนโลยีสื่อสาร และโดยรวม คือกลุ่มคนที่รักความก้าวหน้า ทันสมัย ทันต่อเหตุการณ์ จึงได้เลือกใช้เทคโนโลยีที่ทันสมัยเป็นเครื่องมือในการแสวงหาความรู้ ซึ่งบางคนเสียเวลา เสียค่าใช้จ่ายเพื่อที่จะเรียนรู้วิธีการใช้ หรือเรียนรู้วิธีการนำประโยชน์ของเทคโนโลยีไปเป็นเครื่องมือในการแสวงหาความรู้เพิ่มเติม การศึกษาต่อในระดับสูงขึ้นไป หรือนำไปใช้เพื่อการประกอบอาชีพเพื่อดำรงชีพ

อย่างไรก็ตาม แม้ว่าเทคโนโลยีสารสนเทศและการสื่อสารจะเป็นสิ่งที่มีประโยชน์อย่างมากมายมหาศาลแต่ก็มีโทษมากมายเช่นกัน จากข่าวในหน้าหนังสือพิมพ์ที่ปรากฏอยู่บ่อยครั้ง ว่ามีผู้นำเอาความรู้ความสามารถ และคุณสมบัติของเทคโนโลยีสื่อสารอินเทอร์เน็ตไปใช้ในทางมิชอบ จนทำให้เกิดความเสื่อมเสียชื่อเสียงหรือถึงแก่ชีวิต เพียงเพื่อได้รับผลประโยชน์ส่วนตัว ซึ่งทำความเดือดร้อนให้แก่ครอบครัวของผู้เสียหายจนทำให้สังคมเดือดร้อน อยู่เป็นระยะ ปัญหาที่สำคัญ คือ เจ้าหน้าที่ตำรวจและประชาชน ไม่มีความรู้ทางด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์อย่างเพียงพอ การสร้างองค์ความรู้และคู่มือทางด้านอาชญากรรมคอมพิวเตอร์ จะทำให้การป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์มีประสิทธิภาพมากยิ่งขึ้น

คำว่า “อาชญากรรมคอมพิวเตอร์” มีคำเรียกมากมายหลายคำว่า Computer crime, Computer related crime, E-crime, Information technology crime. High-tech crime, Computer misuse, Computer abuse ซึ่งล้วนแล้วแต่ใช้แทนกันได้ทั้งนั้น เพราะขึ้นอยู่กับมุมมองของนักกฎหมายแต่ละสาขา แต่ความหมายที่ครอบคลุมหมายถึง *“การกระทำใด ๆ ที่ฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย โดยผู้กระทำ ได้อาศัยความรู้ด้านเทคโนโลยีคอมพิวเตอร์ ไม่มากก็น้อยในอันที่จะกระทำความผิด และให้การกระทำนั้นเป็นผลสำเร็จ ไม่ว่าลักษณะของการกระทำนั้น จะเป็นการใช้คอมพิวเตอร์แบบเครื่องมือ หรือให้คอมพิวเตอร์เป็นเป้าหมาย ซึ่งจำเป็นต้องอาศัยบุคลากรที่มีความรู้ความสามารถทางเทคโนโลยีคอมพิวเตอร์เข้ามาดำเนินการกับผู้กระทำความผิด ตั้งแต่กระบวนการสืบสวน สอบสวน การฟ้องร้อง ตลอดจนการพิจารณาคดีเพื่อลงโทษผู้กระทำความผิด”* การประกอบอาชญากรรมทางคอมพิวเตอร์ได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล อาชญากรรมทางคอมพิวเตอร์ จึงจัดเป็นอาชญากรรมทางเศรษฐกิจ หรืออาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ

2) เครือข่ายและปัญหาทางด้านอาชญากรรมคอมพิวเตอร์

ปัญหาอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นทั่วประเทศไทยในปัจจุบันทั้งการกระทำผิดเกี่ยวกับเว็บไซต์ที่ผิดกฎหมายในลักษณะความผิดโดยทั่วไป และเว็บไซต์ที่กระทำความผิดเกี่ยวกับการจาบจ้วงสถาบันพระมหากษัตริย์ ซึ่งเป็นการกระทำผิดตาม ป.อาญามาตรา 112 และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีปริมาณที่กระทำผิดเป็นจำนวนมาก

จากสถิติคดีอาญาของการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีประจำปี พ.ศ.2552-2555 ซึ่งรวบรวมโดย กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ (บก.ปอท. เริ่มก่อตั้งหน่วยงานเมื่อ 7 ก.ย. 2552) สถิติใน พ.ศ.2552 พบว่า มีเว็บไซต์ที่กระทำผิดโดยทั่วไป 22 คดี พ.ศ.2553 มีเว็บไซต์ที่กระทำผิดในคดีทั่วไป 35 คดี พ.ศ.2554 จำนวน 429 คดี พ.ศ.2555 (ม.ค.-ส.ค.2555) กระทำผิดในคดีทั่วไป 287 คดี แต่เมื่อพิจารณาถึงเว็บไซต์ที่จาบจ้วงสถาบันพระมหากษัตริย์ ตาม ป.อาญา มาตรา 112 พบในปี พ.ศ.2552 มีการกระทำผิด 154 คดี พ.ศ.2553 กระทำผิด 153 คดี พ.ศ.2554 กระทำผิด 186 คดี แต่ในปี พ.ศ.2555 (ม.ค.-ส.ค. 2555) มีการกระทำผิดถึง 15,338 คดี จะเห็นได้ว่า การกระทำผิดตาม ป.อาญา มาตรา 112 ในปี 2555 มีการกระทำผิดสูงกว่าปี 2554 ถึง 82.46 เท่า หรือ สูงขึ้นถึงร้อยละ 8,146.31 ซึ่งจะเห็นว่าเป็นสถิติที่สูงขึ้นอย่างมากผิดปกติ (ตาราง 1-1) จึงเป็นเหตุผลหนึ่งที่ควรนำเรื่องนี้มาศึกษา

ตาราง 1-1 สถิติคดีอาญาของการกระทำผิดเกี่ยวกับการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ประจำปี พ.ศ.2552-2555

ลำดับ	หน่วยงานที่ตรวจพบ	จำนวนเว็บไซต์							
		2552		2553		2554		2555	
		ทั่วไป	เว็บหมิ่น	ทั่วไป	เว็บหมิ่น	ทั่วไป	เว็บหมิ่น	ทั่วไป	เว็บหมิ่น
1	บก.ปอท.	22	154	35	104	429	186	287	74
2	สันติบาล	-	-	-	-	-	-	-	-
3	กระทรวงมหาดไทย	-	-	-	49	-	-	-	-
4	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร	-	-	-	-	-	-	-	2,499
5	คณะกรรมการอำนวยการกำหนดนโยบายป้องกันและปราบปรามการนำเสนอข้อมูลข่าวสารที่ผิดกฎหมาย	-	-	-	-	-	29 (ช่วง 10-15 ม.ค.55) (ช่วง 16-22 ม.ค.55) (ช่วง 23-24 ม.ค.55) (ช่วง 26 ม.ค.55) (ช่วง 7 ก.พ.-29 มิ.ย.55) (ช่วง 19 ก.พ.-28 ส.ค.55)	-	-	51 79 34 125 11,376 1,100
6	อื่น ๆ	-	-	-	-	-	-	-	-
รวมทั้งสิ้น		**22**	**154**	**35**	**153**	**429**	**186**	**287**	**15,338**

ที่มา : กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.), 2555

หมายเหตุ 1) สถิติ 2555 รวบรวม มกราคม-สิงหาคม 2555

2) บก.ปอท.บช.ก. เริ่มตั้งหน่วยงานเมื่อ 7 ก.ย. 2552

ภัยบนอินเตอร์เน็ต และรูปแบบในการกระทำผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ปัญหาทางด้านโครงสร้างทางกฎหมายและปัญหาด้านการสืบสวนทางด้านอาชญากรรมคอมพิวเตอร์ กฎหมายและความรู้ของพนักงานสอบสวน ยังก้าวไปไม่ทันต่อการกระทำผิด ดังกล่าว เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน **(Globalization)** และการกระทำผิดทางด้านอาชญากรรมคอมพิวเตอร์ มีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลา จึงมีความจำเป็นต้องศึกษาถึงเครือข่ายทางด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

3) เขตอำนาจในการพิจารณาคดี

ตาม พ.ร.บ.คอมพิวเตอร์ 2550 ได้ระบุถึงเขตอำนาจในการพิจารณาคดี ซึ่งในกรณีที่ผู้กระทำความผิดตาม พ.ร.บ.นี้นอกราชอาณาจักร ถึงแม้ว่าผู้กระทำผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทย หรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร (ม.17)

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักร และ

(1) ผู้ใดกระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้น หรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

การกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในบางครั้งผู้กระทำความผิดอยู่นอกประเทศ เช่น คดีความผิดตาม ป.อาญา มาตรา 112 ซึ่งนับวันจะมีปริมาณคดีเพิ่มขึ้นเป็นจำนวนมาก จึงจำเป็นต้องสร้างเครือข่าย และการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เป็นการป้องกันและปราบปรามการกระทำผิดดังกล่าว

จากหลักการและเหตุผลข้างต้น หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา ร่วมกับคณาจารย์ที่มีความรู้และประสบการณ์การทำวิจัย และผู้มีความรู้ความเชี่ยวชาญทางด้านอาชญากรรมคอมพิวเตอร์ จากหน่วยงานต่างๆ เช่น กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานพิสูจน์หลักฐานตำรวจ กรมสอบสวนคดีพิเศษ สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ กองบัญชาการเทคโนโลยีและสารสนเทศ กระทรวงเทคโนโลยีและสารสนเทศ จึงมีความสนใจที่จะทำการวิจัย เพื่อศึกษาการแก้ปัญหาอาชญากรรมคอมพิวเตอร์ โดยการจัดการความรู้จากเอกสาร งานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ในแต่ละหน่วยงาน ผ่านการจัดกิจกรรมแลกเปลี่ยนเรียนรู้ เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยนำเข้ากระบวนการผลลัพธ์ รวมทั้งรูปแบบที่ดี (Best Practice) ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะทางด้านเครือข่าย และการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เพื่อนำมาพัฒนางานทางด้านดังกล่าว ทำให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้งคุ้มครองสิทธิและเสรีภาพ ด้วยความรวดเร็ว เที่ยงตรง และเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นแนวทางในการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ให้เป็นที่ยอมรับ ศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1) เพื่อพัฒนาหารูปแบบที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) เพื่อสร้างเครือข่ายในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

3) เพื่อสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์หลังจากมีการศึกษาวิธีการป้องกันและปราบปรามจากต่างประเทศ และนำมาประยุกต์ใช้

1.3 คำถามของการวิจัย

1) กระบวนการด้านอาชญากรรมคอมพิวเตอร์ในปัจจุบันมีลักษณะอย่างไร

2) ปัญหาและอุปสรรคในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ปัจจุบันมีอะไรบ้าง และสามารถแก้ไขปัญหาและอุปสรรคดังกล่าวได้หรือไม่อย่างไร

3) แนวทางมาตรฐานตามขั้นตอนต่าง ๆ ด้านอาชญากรรมคอมพิวเตอร์ มีการบูรณาการภาพรวมที่ได้ผลลัพธ์เป็นแนวทาง มาตรฐาน ขั้นตอนเป็นอย่างไร

1.4 ขอบเขตของการวิจัย

1) ขอบเขตด้านเนื้อหาการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยภาคสนามที่ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) และใช้หลักการวิจัยเชิงปฏิบัติการมีส่วนร่วม (Participatory Action Research) ที่ผู้วิจัยได้เข้าไปมีส่วนร่วมและลงมือวิจัยด้วยตนเองเพื่อวิเคราะห์ข้อกฎหมาย และระเบียบที่เกี่ยวข้องกับการปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ และค้นหาวิธีการปฏิบัติงาน นโยบายในการบริหารจัดการ รวมทั้งปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้อง ในด้านการสร้างคู่มือการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ และสร้างการจัดการฐานความรู้ด้านอาชญากรรมคอมพิวเตอร์จากกฎหมายและระเบียบ รายงานการสืบสวน สำนวนการสอบสวน และจากการศึกษาเชิงลึกจากกลุ่มเป้าหมายที่เกี่ยวข้องประกอบกับการวิจัยเชิงปฏิบัติการ (Action Research) โดยการจัดประชุมเพื่อแลกเปลี่ยนเรียนรู้ และถอดบทเรียน ซึ่งจะทำให้องค์กรเกิดการเรียนรู้จากประสบการณ์ในการปฏิบัติงานของผู้ร่วมถอดบทเรียน และได้แนวคิดใหม่ที่เป็นประโยชน์ในการปฏิบัติงานต่อไป

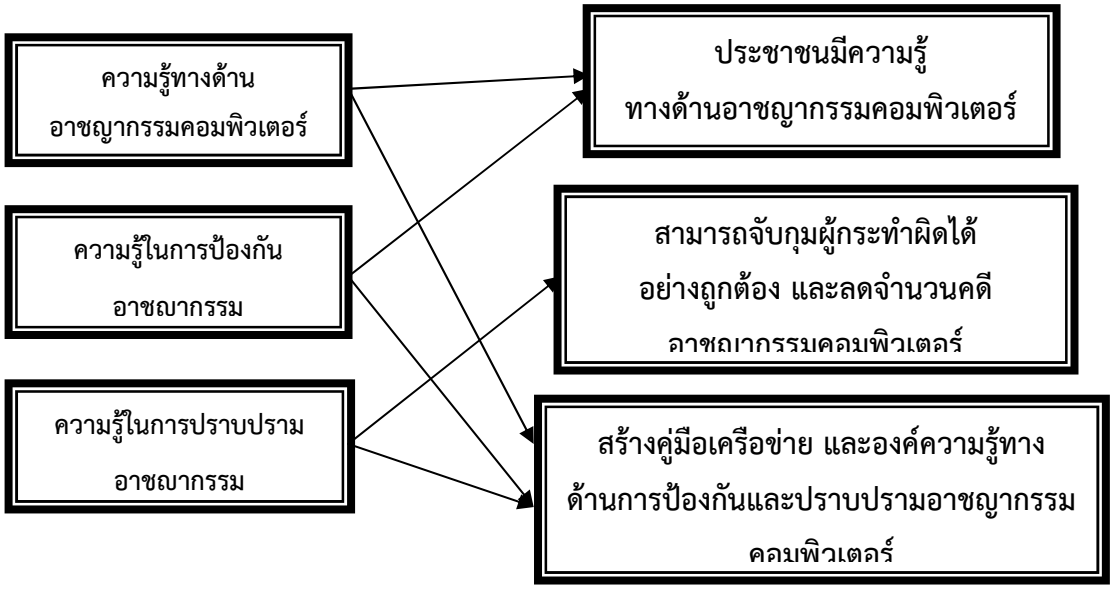
2) ขอบเขตด้านกลุ่มเป้าหมาย / พื้นที่

กลุ่มเป้าหมายในการวิจัยครั้งนี้ คือ ผู้บริหารสถานีตำรวจ เจ้าหน้าที่ตำรวจ ทั้งระดับสัญญาบัตรและชั้นประทวนหน่วยงานที่เกี่ยวข้อง และประชาชน เครือข่ายที่มีความรู้ ความชำนาญและประสบการณ์โดยศึกษาเฉพาะกลุ่มเป้าหมายที่เป็นผู้เชี่ยวชาญ และมีประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ โดยทำการคัดเลือกจากเจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้อง และประชาชน เข้าร่วมประชุมกลุ่มย่อย (Focus Group) หรือการสัมมนาแลกเปลี่ยนเรียนรู้ จะคัดเลือกจากเจ้าหน้าที่ที่มีประสบการณ์ เพื่อให้ได้กลุ่มเป้าหมายที่มีความรู้ความเชี่ยวชาญอย่างแท้จริง

3) ขอบเขตด้านระยะเวลา

การวิจัยครั้งนี้มีระยะเวลาดำเนินการ 12 เดือน

1.5 กรอบแนวคิดของการวิจัย



ภาพ 1-1 กรอบแนวคิดของการวิจัย

1.6 ความสำคัญของการวิจัย

วัตถุประสงค์ที่สำคัญของงานวิจัยนี้คือการได้คู่มือแนวทางมาตรฐานตามขั้นตอนต่างๆที่เป็นแนวทางสำหรับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ก่อให้เกิดผลในทางบวกด้านอาชญากรรมคอมพิวเตอร์ให้ลดลง ดังนั้นความสำคัญที่คาดว่าจะได้รับจากงานวิจัยในครั้งนี้คือ

1) ได้องค์ความรู้ที่สามารถนำไปพัฒนาต่อยอดจัดทำเป็นคู่มือแนวทางมาตรฐานในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) เพิ่มพูนทักษะเป้าหมายของเจ้าหน้าที่ตำรวจ

3) เพื่อเสนอแนะแนวทางในการปรับปรุงและพัฒนาระบบงานอาชญากรรมคอมพิวเตอร์ เพื่อนำไปใช้ประโยชน์ในการสืบสวนอาชญากรรมคอมพิวเตอร์

4) หน่วยงานที่มีหน้าที่ได้นำเอาคู่มือมาใช้เป็นรูปแบบในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ได้แก่

(1) ผู้บริหารสถานีตำรวจ และหัวหน้าหน่วยงานที่ปฏิบัติงานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

(2) ชุมชนเครือข่ายที่มีความรู้ ประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์

(3) องค์กรเอกชนที่เกี่ยวข้อง

(4) กลุ่มผู้พิพากษาและอัยการ

(5) กระทรวงเทคโนโลยีและสารสนเทศ

(6) ประชาชน

(7) กลุ่มสื่อมวลชน

1.7 ผลที่คาดว่าจะได้รับ

1) ได้ข้อกฎหมายและระเบียบที่ผ่านการแก้ไข ปรับปรุงให้มีความเหมาะสมต่อการนำไปใช้งานในสถานการณ์ปัจจุบัน เพื่อสร้างการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) ได้ทราบวิธีการปฏิบัติงาน นโยบายในการบริหารจัดการ รวมทั้งปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้อง ในการปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

3) ได้คู่มือการจัดการความรู้ด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

4) ได้เครือข่ายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

5) ได้เว็บไซต์ที่เป็นการจัดการทางด้านอาชญากรรมคอมพิวเตอร์

1.8 กระบวนการผลักดันผลงานดังกล่าวออกสู่การใช้ประโยชน์

1) การประชุมเพื่อทำการแลกเปลี่ยนเรียนรู้ ประชุมร่วมกันระหว่างทีมถอดบทเรียน โดยเชิญผู้เชี่ยวชาญในด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และเจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้อง เครือข่ายที่มีประสบการณ์และความเชี่ยวชาญ และประชาชน เพื่อปรับปรุง และเสนอแนะงานวิจัยให้มีความสมบูรณ์มากยิ่งขึ้น โดยจัดขึ้น ณ กรุงเทพมหานคร จำนวน 4 ครั้ง มีรายละเอียดดังนี้

ครั้งที่ 1 จัดที่กรุงเทพมหานคร (ระเบียบและข้อกฎหมายต่างๆ ที่เกี่ยวข้อง)
ครั้งที่ 2 จัดที่กรุงเทพมหานคร (ค้นหาปัญหา และอุปสรรคต่าง ๆ)
ครั้งที่ 3 จัดที่กรุงเทพมหานคร (สร้างคู่มือการจัดการความรู้)
ครั้งที่ 4 จัดที่กรุงเทพมหานคร (มอบคู่มือการจัดการความรู้)

2) การนำบทความตีพิมพ์ในวารสารต่าง ๆ เพื่อเผยแพร่ผลงานการวิจัยสู่สาธารณชน

3) การจัดทำคู่มือการจัดการความรู้ทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

4) จัดทำเว็บไซต์เพื่อเป็นฐานข้อมูลในการพัฒนางานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

1.9 นิยามศัพท์เฉพาะ

เครือข่าย หมายถึง กลุ่มของผู้ใช้คอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่างๆ ที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่าย สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ร่วมกันในเครือข่ายได้ ตัวอย่างของกลุ่มเครือข่ายที่เราคุ้นเคย ได้แก่ เครือข่ายของโทรศัพท์ ดาวเทียม วิทยุ หรือเครือข่ายคอมพิวเตอร์ โดยช่องทางที่ใช้ในการติดต่อสื่อสารกัน เรียกว่า ช่องสัญญาณ (Communication channel) กลุ่มของเครือข่ายเป็นผู้ที่มีความรู้ความชำนาญเกี่ยวกับอาชญากรรมคอมพิวเตอร์

การจัดการความรู้ หมายถึง การรวบรวมองค์ความรู้ด้านกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง ขั้นตอน แนวทางการปฏิบัติงานทางด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ที่มีอยู่อย่างกระจัดกระจายในรูปของหนังสือ ตำรา เอกสารทางราชการ สำนวนการสอบสวนและรายงาน การสืบสวน รวมทั้งความรู้ที่มีอยู่ในตัวผู้ปฏิบัติงาน มาพัฒนาให้เป็นระบบเพื่อให้เจ้าหน้าที่ตำรวจของสำนักงานตำรวจแห่งชาติและเจ้าหน้าที่หน่วยงานอื่นที่เกี่ยวข้อง สามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพ

อาชญากรรมคอมพิวเตอร์ หมายถึง อาชญากรรมอินเตอร์เน็ต แต่กระทำต่อหรือใช้คอมพิวเตอร์ส่วนบุคคลเป็นเครื่องมือ กลับมีการอาศัยระบบเครือข่ายคอมพิวเตอร์ เพื่อช่วยให้การกระทำความผิดขยายวงกว้างขึ้น สะดวกรวดเร็ว สลับซับซ้อนมากยิ่งขึ้น และที่สำคัญติดตามหาตัวกระทำความผิดได้ยากลำบากยิ่งขึ้น

บทที่ 2
ทบทวนวรรณกรรม

ในการศึกษาโครงการวิจัยเรื่อง เครือข่ายและการจัดการความรู้ด้านอาชญากรรมคอมพิวเตอร์ คณะผู้วิจัยได้ดำเนินการศึกษาเกี่ยวกับ

1) แนวคิดและทฤษฎีที่เกี่ยวข้อง

1.1) แนวคิดการจัดการความรู้

1.2) แนวคิดและทฤษฎีอาชญากรรมคอมพิวเตอร์

2) งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีที่เกี่ยวข้อง

1) แนวคิดการจัดการความรู้

ปัจจุบันเป็นสังคมแห่งการเรียนรู้ แหล่งความรู้มีอยู่มากมาย และกระจัดกระจายอยู่ในหลายรูปแบบ ความรู้เป็นผลผลิตของสารสนเทศ ซึ่งประกอบด้วย ข้อเท็จจริง ความคิดเห็น ทฤษฎี หลักการและกรอบแนวคิดต่างๆ รวมถึงทักษะ และประสบการณ์ของแต่ละบุคคล ซึ่งเราใช้เพื่อการตัดสินใจ การดำเนินชีวิตของมนุษย์ ชีวิตส่วนตัว หรือการทำงานในองค์กรต้องใช้ความรู้เป็นเครื่องมือช่วยในการตัดสินใจในเรื่องต่าง ๆ ดังนั้น จึงเกิดแนวคิดว่าเราจะทำอย่างไรเราจึงจะสามารถใช้ความรู้ที่เรามีอยู่ให้เกิดประโยชน์สูงสุด Knowledge Management เกิดจากข้อมูลข่าวสารต่าง ๆ ที่เกิดขึ้นอย่างมากมาย ทำให้องค์กรต่าง ๆ มีข้อมูลจัดเก็บอยู่จำนวนมาก และเกิดความต้องการที่จะจัดให้อยู่อย่างเป็นระเบียบ เข้าถึงง่าย ทันต่อการนำไปใช้งาน (ไพบูลย์ ปะวะเสนะ, 2547)

1.1) ความเป็นมาของการคิดจัดการความรู้

สารสนเทศกระจัดกระจาย และการจัดเก็บอยู่ในแหล่งเก็บที่หลากหลาย ที่สำคัญยิ่งไปกว่านั้น คือ มีข้อมูลมากมาย แต่ความรู้มีน้อย ในยามที่ต้องการข้อมูลเพื่อการตัดสินใจ การรวบรวมข้อมูลทำได้ไม่เต็มประสิทธิภาพและไม่ครบถ้วน อีกทั้งใช้เวลาในการค้นหานาน การจัดการความรู้อย่างมีระบบจะช่วยให้ปัญหาดังกล่าวบรรเทาลง หรือหมดไป ยิ่งไปกว่านั้นการก้าวเข้าสู่สังคมภูมิปัญญาและความรอบรู้ เป็นแรงผลักดันทำให้องค์กรต้องการพัฒนาไปเป็นองค์กรแห่งการเรียนรู้ (Learning Enterprise) เพื่อสร้างคุณค่าจากภูมิปัญญาและความรอบรู้ที่มีอยู่เปลี่ยนสินทรัพย์ทางปัญญาให้เป็นทุน ด้วยการจัดการความรอบรู้ และภูมิปัญญาซึ่งมีผลให้เกิดการเปลี่ยนรูปแบบการทำงานเป็นแบบผู้ปฏิบัติที่มีความรู้ (Knowledge Worker) ด้วย (ยืน ภู่วรวรรณ, 2546)

ขั้นแรกที่จะนำไปสู่การจัดการความรู้ คือ การจัดเก็บข้อมูลไว้ในคลังข้อมูล (Data warehouse) ที่มีการวิเคราะห์ประมวลผล คัดกรองข้อมูล (Data Mining) เพื่อให้ได้ความรู้ที่น่าสนใจ ได้แก่ กฎ ระบบหรือลักษณะที่เกิดขึ้นประจำ รูปแบบ ความแปลกแยก หรือสิ่งผิดปกติจากข้อมูลที่เก็บไว้ในฐานข้อมูลขนาดใหญ่ในการแข่งขันทางด้านธุรกิจนำการจัดการความรู้เข้ามาใช้ โดยมีเหตุผลดังนี้

1) บริษัทต่าง ๆ กลายเป็นองค์กรแห่งความรู้ มีการใช้ความรู้ในการทำงานมากขึ้นรวมถึงการแข่งขันทางด้านธุรกิจ

2) การเปลี่ยนแปลงของตลาดการแข่งขันทำให้ต้องมีการพัฒนาองค์กรพัฒนาการบริหารจัดการภายในองค์กร

3) การจัดการความรู้ทำให้บุคคลเกิดการเปลี่ยนแปลงไปในทางที่ดีขึ้น

4) ความรู้ทำให้องค์กรอยู่รอด

5) ความซับซ้อนขององค์กรในปัจจุบันจึงต้องมีการจัดการความรู้

6) ความรู้ช่วยในการตัดสินใจ

7) ความต้องการในการใช้ความรู้ร่วมกัน

8) ความรู้เฉพาะบุคคลเป็นสิ่งที่มีความสัมพันธ์กับองค์กร

9) การเติบโตของบริษัทและธุรกิจ

1.2) ความหมายของการจัดการความรู้

นักวิชาการและบุคลากรด้านการจัดการความรู้หลายท่านและหลายสถาบันได้เห็นความสำคัญและทำการศึกษารูปแบบ แนวทางในการพัฒนาการจัดการความรู้ ไว้ดังนี้

Hedeo Yamazaki (อ้างถึงใน วรภัทร์ ภู่เจริญ, 2548) ได้แสดงปิรามิดของความรู้โดยเริ่มจากฐานล่าง คือ ข้อมูล ทำการสังเคราะห์จนได้สารสนเทศ แล้วคิดเปรียบเทียบเชื่อมโยงจนได้ความรู้ และนำไปใช้จนเก่งกลายเป็นปัญญา ซึ่งจะผ่าน 3 กระบวนการ คือ การแสวงหาความรู้ การตีความ ขยายความเข้าใจ การนำความรู้ไปประยุกต์ใช้

วรภัทร์ ภู่เจริญ (2548) กล่าวถึงวงจรความรู้ว่ามีขั้นตอนของวงจร คือ

1) Identify ระบุค้นหากำหนดความรู้และแหล่งความรู้

2) Capture คือการเก็บสะสม รวบรวมความรู้ต่าง ๆ

3) Select ประเมินคุณค่าดูว่าขัดแย้งกันเองหรือไม่ จริงหรือเท็จ

4) Store จัดเก็บในฐานข้อมูลความรู้ขององค์กร

5) Apply นำไปประยุกต์ใช้แก้ปัญหา วิจัย อบรม

6) Create สร้างความรู้ใหม่ๆ ทดลองวิจัย

7) Sell นำไปขาย สร้างสินค้าใหม่ บริการใหม่ ๆ

Laudon (2000) กล่าวถึง Knowledge Management ว่า การบริหารจัดการความรู้ในองค์กรมีความสำคัญเป็นพิเศษในองค์การที่มีลักษณะการบริหารงานแบบแบนราบและแบบเครือข่าย ซึ่งในการจัดการในระดับต่างๆ จะมีการจัดการแยกแยะความจริงในส่วนที่จะสามารถนำมาช่วยสมาชิกในทีม ในการพัฒนางานในหน้าที่ รวมทั้งการแบ่งปันข้อมูล เพื่อพัฒนางานในส่วนงานอื่นๆ ที่เกี่ยวข้องกันด้วย

Stair (2001) กล่าวว่า การบริหารการจัดการความรู้ เป็นกระบวนการรวบรวมจัดการความรู้ความชำนาญ ไม่ว่าความรู้นั้นจะอยู่ในคอมพิวเตอร์ ในกระดาษ หรือตัวบุคคล โดยมีจุดมุ่งหมายเพื่อจัดการให้บุคลากรได้รับความรู้ และแลกเปลี่ยนความรู้ ทำให้เกิดการเปลี่ยนแปลงพฤติกรรมจากเดิม โดยให้เกิดประสบการณ์และความชำนาญเพิ่มขึ้น

Tiwana (2000) ให้ความหมายการบริหารจัดการความรู้ว่า หมายถึง การจัดการความรู้ในองค์กร สำหรับงานด้านธุรกิจ

วีรวุธ มาฆะศิรานนท์ (2542) กล่าวถึง การบริหารจัดการความรู้ว่า การบริหารจัดการความรู้เป็นกระบวนการบริหารรูปแบบใหม่ ที่เน้นในด้านการพัฒนากระบวนงานควบคู่ไปกับการพัฒนากระบวนการเรียนรู้ โดยทุกกระบวนงานจะต้องสัมพันธ์กับความคิดสร้างสรรค์ที่เป็นผลมาจากการขยายวงและการประสานความรอบรู้ รวมถึงการฉลาดคิดไปตลอดทั่วทั้งองค์กรอยู่ตลอดเวลา ซึ่งเท่ากับว่าองค์กรที่มีการบริหารจัดการความรู้นี้อย่างเป็นระบบ ก็จะเกิดเป็นโอกาสอันสำคัญต่อการพัฒนาให้เป็นองค์กรที่เปี่ยมไปด้วยการทำงานอย่างฉลาดคิดและสร้างสรรค์ในที่สุด ทำให้องค์กรนั้นสามารถเผชิญกับการแข่งขันและการเปลี่ยนในทุก ๆ รูปแบบ และสามารถฟันฝ่าอุปสรรคทั้งมวลได้เป็นอย่างดี

ศรันย์ ชูเกียรติ (2541) กล่าวถึง การจัดองค์ความรู้ในองค์กร หมายถึง การจัดการและรักษาระดับในการจัดเก็บองค์ความรู้ในองค์กรให้เป็นระบบเป็นระเบียบ ตลอดจนสามารถนำไปใช้ประโยชน์ได้จริงในทางปฏิบัติ

จากแนวคิดดังกล่าว สรุปได้ว่า การจัดความรู้ (Knowledge Management) หมายถึง กระบวนการความรู้ที่เน้นการแลกเปลี่ยนความรู้ของคนในองค์กรใดองค์กรหนึ่ง โดยต้องอาศัยการแลกเปลี่ยนเรียนรู้ มีการปฏิสัมพันธ์ต่อกันของคนภายในองค์กรเดียวกัน เมื่อรวบรวมแล้วก็มีการนำความรู้ที่ได้มาสังเคราะห์ และการจำแนกหรือจัดระบบใหม่เพื่อสร้างเป็นองค์ความรู้ใหม่ที่สามารถนำไปพัฒนาปรับปรุงองค์การ ในการบริหารจัดการและนำความรู้เผยแพร่ต่อสาธารณชนต่อไป

1.3) การจัดการความรู้ในประเทศไทย

วิจารณ์ พานิช (2547) แห่งสถาบันส่งเสริมการจัดการความรู้เพื่อสังคมได้ดำเนินการเผยแพร่แนวคิดด้านการจัดการความรู้ได้กล่าวว่า ความเป็นองค์กรเรียนรู้ (Learning Organization) และการจัดการความรู้ (Knowledge Management) เป็นเสมือน 2 หน้าของเหรียญเดียวกัน คืออาจมองว่าเป็นเรื่องเดียวกันก็ได้ มองว่าเป็นคนละเรื่องแต่เกี่ยวข้องกันส่งเสริมเกื้อกูลซึ่งกันและกันได้ในการดำเนินการจัดการความรู้ต้องนำหลักการและวิธีการขององค์กรเรียนรู้มาประยุกต์ใช้ และในการพัฒนาองค์กรให้เป็นองค์กรเรียนรู้ ก็ต้อง

นำเอาวิธีการจัดการความรู้มาประยุกต์ใช้องค์กรเรียนรู้ คือ องค์กรที่มีความสามารถสูงต่อการรับรู้การเรียนรู้ ซึ่งหมายความว่ามีความไวในการเปิดรับจับกระแสของสภาพแวดล้อมขององค์กรตลอดเวลามีความสามารถในการรับรู้การเปลี่ยนแปลงทั้งที่เป็นการเปลี่ยนแปลงของสภาพแวดล้อมภายนอกและที่เป็นการเปลี่ยนแปลงภายในองค์กรและเอาใจใส่ข้อมูลนั้นนำมาใช้ปรับตัวหรือเปลี่ยนแปลงองค์กรเอง องค์กรเรียนรู้มีการรับรู้และเรียนรู้ในทุกส่วนขององค์กรไม่ใช่รับรู้และเรียนรู้เฉพาะในกลุ่มผู้บริหารระดับสูงแต่รับรู้และเรียนรู้ในทุกกลุ่มและทุกระดับของพนักงาน เมื่อมีการรับรู้และเรียนรู้ ก็หมายความว่า มีการสร้างความรู้ขึ้นเองภายในองค์กร ได้เป็นการโยงเข้าหากระบวนการจัดการความรู้องค์กรเรียนรู้มีผลผลิตอย่างน้อย 4 ประการ ได้แก่ 1) ผลสัมฤทธิ์ของงานสูง เช่น ผลงานตอบสนองหรือตรงตามความต้องการของลูกค้า (Responsiveness) เป็นผลงานหรือกระบวนการทำงานที่มีนวัตกรรม (Innovation) มีการสร้างขีดความสามารถขององค์กร และของพนักงาน Competency มีการทำงานอย่างมีประสิทธิภาพ (Efficiency) ซึ่งหมายความว่า Output สูง โดยที่ input ต่ำ 2) เกิดการพัฒนาคนซึ่งหมายถึงพนักงานเกิดการเรียนรู้ เพิ่มพูนความรู้และประสบการณ์จากการทำงานและเกิดทักษะในการเรียนรู้ที่เรียกว่าเป็นบุคคลเรียนรู้ (Learning Person) 3) มีการพัฒนาความรู้ทำให้ความรู้เพิ่มพูนขึ้นในองค์กรและในพนักงาน และ 4) องค์กรมีศักยภาพสูงขึ้นโดยเฉพาะอย่างยิ่งศักยภาพในการรับรู้และเรียนรู้อันนำไปสู่ศักยภาพในการปรับตัวหรือการเปลี่ยนแปลงตนเอง ซึ่งหมายถึง การเป็นองค์กรเรียนรู้

ส่วนการจัดการความรู้ วิจารณ์ พานิช (2547) กล่าวว่าการจัดการความรู้เป็นเครื่องมือที่ช่วยให้ดำเนินการบรรลุวัตถุประสงค์ตามเป้าหมาย ซึ่งมักเป็นเป้าหมายที่ยากซับซ้อน และมักใช้เป็นเครื่องมือเพื่อบรรลุผลสัมฤทธิ์ของงานในลักษณะที่สูงส่ง การจัดการความรู้เป็นเครื่องมือ (Means) ไม่ใช่เป้าหมาย (End) การจัดการความรู้ไม่ใช่การเอาความรู้มาจัดระบบ หรือจัดการเพื่อให้ผู้อื่นนำไปใช้ แต่เป็นการดำเนินการเพื่อให้การปฏิบัติงานมีการประยุกต์ใช้ความรู้อย่างเข้มข้นและทำให้งานมีผลสัมฤทธิ์สูง โดยที่ความรู้ที่นำมาประยุกต์ใช้นั้นได้มาจากหลากหลายทาง ได้แก่ การได้มาจากภายนอกองค์กร การนำเอามาจากองค์ความรู้ภายในองค์กร โดยที่อาจเป็นความรู้ฝังลึก (Tacit knowledge) เป็นประสบการณ์ที่สั่งสมยาวนานเป็นภูมิปัญญา เป็นความรู้ขององค์การ และความรู้ชัดแจ้ง (Explicit knowledge) เป็นความรู้ที่อยู่ในรูปแบบที่เป็นเอกสารหรือวิชาการ อยู่ในตำราคู่มือปฏิบัติงานทั้งที่เป็นความรู้จากภายนอกและความรู้ของกลุ่มผู้ร่วมงาน ความรู้ดังกล่าวต้องนำมาปรับใช้ให้เหมาะสมต่อกาลเทศะ หรือบริบทขององค์กรและเมื่อมีการประยุกต์ใช้ความรู้ในการทำงานก็มีการนำประสบการณ์จากการทำงานของพนักงานมาร่วมกันกลั่นกรองเป็นความรู้ใหม่ในกระบวนการจัดการความรู้ มีการสร้างความรู้ทั้งที่เป็นการสร้างความรู้ก่อนการปฏิบัติงาน สร้างความรู้ระหว่างปฏิบัติงาน และสร้างความรู้หลังจากงานสำเร็จหรือเสร็จสิ้น ต้องมีกระบวนการดำเนินการให้มีการแลกเปลี่ยนเรียนรู้ระหว่างพนักงานอย่างเข้มข้น ทำให้ความรู้ของบุคคล ถูกปรับไปเป็นความรู้ขององค์กรมีการจัดเก็บความรู้ขององค์กรให้อยู่ในสภาพที่ค้นหามาใช้งานได้ง่ายที่เรียกว่า “การจัดการความรู้แบบฉับพลัน” (Just in Time Knowledge Management)

การจัดการความรู้เป็นกระบวนการ (Process) ที่ดำเนินการร่วมกันโดยผู้ปฏิบัติงานในองค์กรหรือหน่วยงานย่อยขององค์กร เพื่อสร้างและใช้ความรู้ในการทำงานให้เกิดผลสัมฤทธิ์ดีขึ้นกว่าเดิม การจัดการ

ความรู้ในความหมายนี้เป็นกิจกรรมของผู้ปฏิบัติงานไม่ใช่กิจกรรมของนักวิชาการหรือนักทฤษฎี แต่นักวิชาการหรือนักทฤษฎีอาจเป็นประโยชน์ในฐานะแหล่งความรู้ (Resource person) หรือผู้อำนวยความสะดวกในการจัดการความรู้ การจัดการความรู้เป็นกระบวนการที่เป็นวงจรต่อเนื่อง เกิดการพัฒนางานอย่างต่อเนื่องสม่ำเสมอเป้าหมาย คือ การพัฒนาคน โดยมีความรู้เป็นเครื่องมือมีกระบวนการจัดการความรู้เป็นเครื่องมือในการจัดการความรู้ ความรู้ที่เราคุ้นเคยกันเป็นอย่างดีคือ ความรู้ยุคที่ 1 เป็นความรู้ที่สร้างขึ้นโดยนักวิชาการมีความเป็นวิทยาศาสตร์เน้นความเป็นเหตุผล พิสูจน์ได้โดยวิธีการทางวิทยาศาสตร์หรือวิชาการมีการจำแนกแยกแยะเป็นความรู้เฉพาะสาขาวิชาการเป็นความรู้ที่เน้นความลึก ความเป็นวิชาการเฉพาะด้าน (Specialization) เน้นความรู้ที่อยู่ในรูปแบบที่เป็นเอกสาร หรือวิชาการอยู่ในตำรา คู่มือปฏิบัติงาน ส่วนความรู้ที่เน้นในเรื่องการจัดการความรู้เป็นความรู้ยุคที่ 2 ซึ่งเป็นความรู้ที่ผูกพันอยู่กับงานหรือกิจกรรมของบุคคลและองค์กร เป็นความรู้ที่ใช้ในงาน และสร้างขึ้นโดยผู้ปฏิบัติงานหรือกลุ่มผู้ปฏิบัติงานเอง โดยอาจสร้างขึ้นจากการเลือกเอาความรู้เชิงทฤษฎีหรือความรู้จากภายนอกมาปรับแต่ง เพื่อการใช้งานหรือสร้างขึ้นโดยตรงจากประสบการณ์ในการทำงาน ความรู้นี้มีลักษณะบูรณาการและมีความจำเพาะต่อบริบทของงานกลุ่มผู้ปฏิบัติงาน หน่วยงานและองค์กรนั้นๆ ความรู้ในยุคที่ 2 เน้นความรู้เป็นประสบการณ์ที่สั่งสมมายาวนานเป็นภูมิปัญญา

โดยการจัดการความรู้มีเป้าหมาย 3 ประการ ได้แก่ 1) เพื่อพัฒนางานให้มีคุณภาพและผลสัมฤทธิ์ยิ่งขึ้น 2) เพื่อการพัฒนาคนคือพัฒนาผู้ปฏิบัติงานในที่นี้คือพนักงานทุกระดับ แต่ที่ได้ประโยชน์มากที่สุด คือ พนักงานชั้นผู้น้อย และระดับกลาง และ 3) เพื่อการพัฒนาฐานความรู้ขององค์กรหรือหน่วยงานเป็นการเพิ่มพูนทุนความรู้หรือทุนปัญญาขององค์กรซึ่งช่วยทำให้องค์กรมีศักยภาพในการฟันฝ่าความยากลำบากหรือความไม่แน่นอนในอนาคตได้ดีขึ้น

การนิยามคำว่า “ความรู้” มีความหมายหลายนัย และหลายมิติ เช่น ความรู้คือ สิ่งที่เมื่อนำไปใช้ไม่หมดหรือสึกหรอ แต่ยิ่งงอกเงยหรืองอกงามขึ้น ความรู้ คือ สารสนเทศที่นำไปสู่การปฏิบัติ ความรู้เป็นสิ่งที่คาดเดาไม่ได้ ความรู้เกิดขึ้น ณ จุดที่ต้องการใช้ความรู้นั้นความรู้เป็นสิ่งที่ขึ้นกับบริบทและกระตุ้นให้เกิดขึ้นโดยความต้องการ เป็นต้น

ในยุคแรกๆ ของการพัฒนาศาสตร์ด้านการจัดการความรู้มองว่าความรู้มาจากการจัดระบบและตีความสารสนเทศ (Information) ตามบริบทและสารสนเทศก็มาจาการประมวลข้อมูล (Data) ความรู้ไม่มีประโยชน์ถ้าไม่นำไปสู่การกระทำหรือการตัดสินใจในการจัดการสมัยใหม่ โดยเฉพาะในยุคสังคมที่ใช้ความรู้เป็นฐาน (Knowledge-based Society) มองความรู้ว่าเป็นทุนปัญญาหรือทุนความรู้สำหรับใช้สร้างคุณค่าและมูลค่า (Value) การจัดการความรู้เป็นกระบวนการนำทุนปัญญาไปสร้างคุณค่าและมูลค่า ซึ่งอาจเป็นมูลค่าทางธุรกิจหรือคุณค่าทางสังคมก็ได้

แนวคิดการจัดการความรู้ของโนนากะ และทาเคอุชิ (Nonaka & Takeuchi, 1995 อ้างถึงในวิจารณ์ พานิช, 2547) เสนอเกลียวความรู้ SECI ว่าเป็นเครื่องมืออย่างหนึ่งในการยกระดับความรู้ และนำรูปแบบต่างๆ ทำให้เกิดการแลกเปลี่ยนความรู้ฝังลึก (Tacit Knowledge) หรือประสบการณ์ Externalization

ซึ่งเป็นกระบวนการสื่อความรู้จากประสบการณ์ในการทำงานออกมาเป็นภาษาพูดหรือภาษาเขียนเท่ากับเป็นการเปลี่ยนความรู้ในคนออกมาเป็นความรู้ชัดแจ้ง (Explicit Knowledge) หรือความรู้ที่เข้ารหัส (Codified knowledge) ซึ่งเป็นความรู้ที่สามารถแลกเปลี่ยนกันได้โดยง่ายผ่านวิธีการด้านเทคโนโลยีสื่อสารและสารสนเทศ กระบวนการผนวกรวมหรือสังเคราะห์ความรู้ในกระดาษเข้าด้วยกันเรียกว่า Combination ก็จะได้ความรู้ในกระดาษที่กว้างขวางและลึกซึ้งขึ้นกระบวนการสุดท้ายในวงจร SECI คือ Internalization ซึ่งเป็นการบันทึกความรู้ในกระดาษไปเป็นความรู้ที่ฝังลึกในตัวคนหรือฝังเข้าไปในผลิตภัณฑ์ หรือกระบวนการทำงาน ซึ่งผลิตภัณฑ์หรือกระบวนการนี้ไปสัมพันธ์กับลูกค้าหรือผู้ใช้ผลิตภัณฑ์ และเกิดความพึงพอใจหรือประสบการณ์ในการใช้ผลิตภัณฑ์หรือใช้กระบวนการทำงานนั้นเป็นข้อมูลใหม่หรือเพิ่มเติมเข้ามาในกระบวนการจัดการความรู้ ยกระดับเกลียวความรู้ขึ้นไปอีกวงจร SECI ดำเนินการต่อเนื่องเรื่อยไปไม่สิ้นสุด

ดังนั้น การบริหารจัดการความรู้ เป็นระบบบริหารจัดการความรู้ให้เป็นระเบียบ ครบถ้วน ง่ายต่อการเรียกใช้จัดเก็บตามความต้องการ เก็บรักษาความรู้ให้ควบคู่กับองค์กรตลอดไป โดยนำเทคโนโลยีเข้ามาใช้ในการจัดการ

สรุปได้ว่า การจัดการความรู้ หมายถึง การบริหารจัดการเพื่อให้บุคคลที่ต้องการใช้ความรู้ได้รับความรู้ที่ต้องการในเวลาที่ต้องการ เพื่อให้บรรลุเป้าหมายการทำงาน (Right Knowledge-Right People -Right Time)

นอกจากนี้มีการศึกษาของวิจารณ์ พานิช (2548, หน้า 120-122) ซึ่งมีข้อคิดเห็นเพิ่มเติม ดังนี้

1) ระบบการให้รางวัลและการยกย่อง ระบบที่เน้นการแข่งขันระหว่างบุคคล ให้รางวัลแก่ผลงานระดับบุคคลนั้นมีผลลบต่อการจัดการความรู้ ทำให้บุคลากรไม่แลกเปลี่ยนความรู้ระหว่างกัน แต่ระบบการให้รางวัลและยกย่องที่เน้นผลงานของกลุ่มบุคลากร เน้นการยกย่องกระบวนการร่วมมือและการแลกเปลี่ยนความรู้ระหว่างกันได้นำมาสู่การสนับสนุนการจัดการความรู้

2) ความรู้และทักษะ ทั้งระดับบุคคล หรือเครือข่ายมีความสำคัญต่อการจัดการความรู้

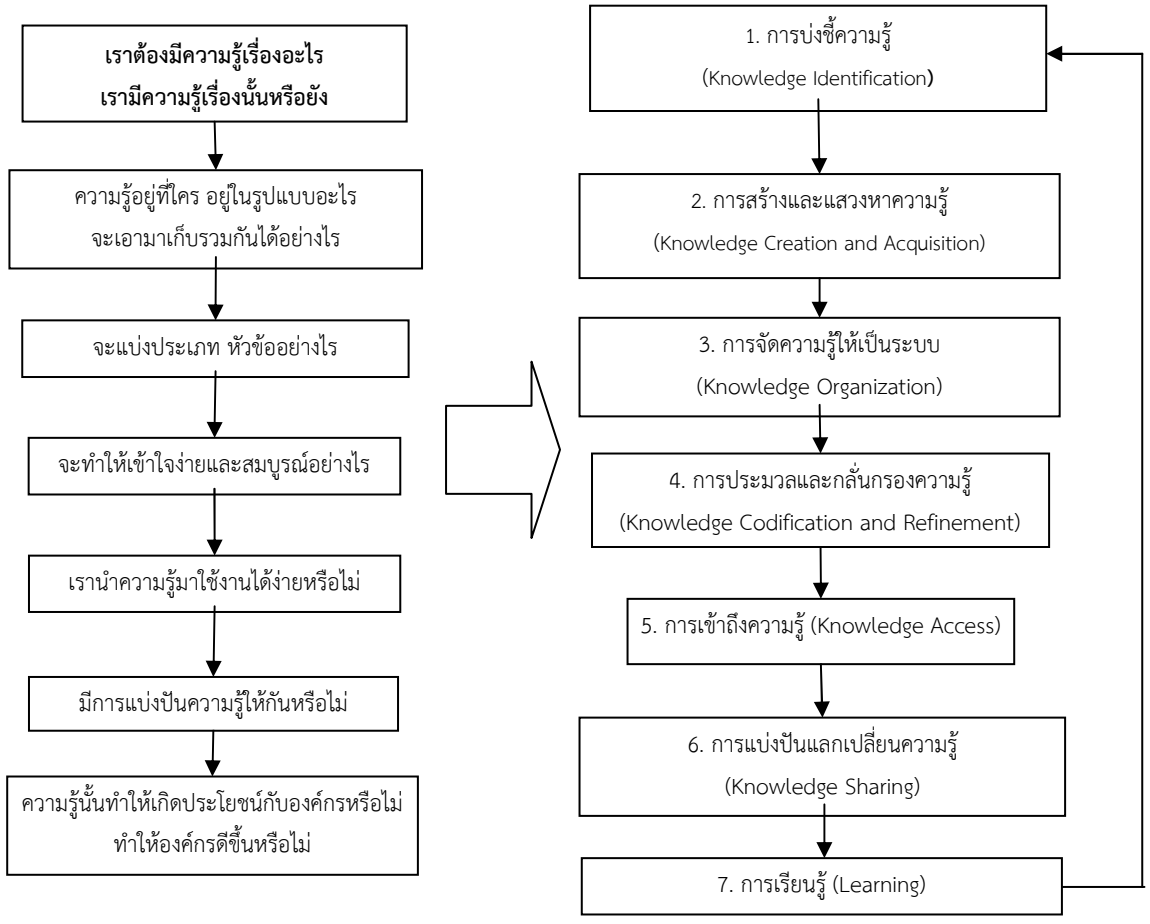
ดังนั้นจากการศึกษา พบว่า ปัจจัยแห่งความสำเร็จของการจัดการความรู้เกิดจากผู้นำต้องมีความจริงจัง ให้การสนับสนุน และทำให้เป็นตัวอย่าง โครงสร้างขององค์การเปิดโอกาสในการแสวงหาความรู้ เปิดสู่สภาพแวดล้อมภายนอก วัฒนธรรมองค์การสร้างวัฒนธรรมการเรียนรู้ สนับสนุนความคิดสร้างสรรค์ใช้ข้อมูลหลักฐานและเหตุผลช่วยส่งเสริมกิจกรรมการจัดการความรู้ ใช้เทคโนโลยีสารสนเทศเข้ามาช่วยในการจัดการการเข้าถึงแหล่งความรู้ ช่วยอำนวยความสะดวกในการค้นหาข้อมูล ช่วยในการสื่อสารแลกเปลี่ยนข้อมูลและความรู้ การถ่ายทอดข้อมูลภายใต้การจัดการอย่างเหมาะสมให้เกิดความมุ่งมั่นร่วมกัน และมีวิสัยทัศน์ร่วมกันของบุคคลในองค์กร มีการประเมินผลทำให้เข้าใจกระบวนการจัดการความรู้ขั้นตอนต่างๆ ผลลัพธ์จากกิจกรรมการจัดการความรู้ รวมทั้งผลกระทบที่เกิดขึ้น มีระบบการให้รางวัลและการยกย่อง เน้นการยกย่องกระบวนการร่วมมือและการแลกเปลี่ยนความรู้ระหว่างกันได้นำมาสู่การสนับสนุนการจัดการความรู้ และมีความรู้และทักษะทั้งระดับบุคคลหรือเครือข่ายมีความสำคัญต่อการจัดการความรู้

1.4) กระบวนการการจัดการความรู้

จากรายละเอียดข้างต้นพอสรุปได้ว่าการจัดการความรู้ หมายถึง การรวบรวมองค์ความรู้ที่มีอยู่ในองค์กร ซึ่งกระจัดกระจายอยู่ในตัวบุคคลหรือเอกสาร มาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้ และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพ อันจะส่งผลให้องค์กรมีความสามารถในเชิงแข่งขันสูงสุด โดยที่ความรู้มี 2 ประเภท คือ

1) ความรู้ที่ฝังอยู่ในคน (Tacit Knowledge) เป็นความรู้ที่ได้จากประสบการณ์ พรสวรรค์ หรือสัญชาตญาณของแต่ละบุคคลในการทำความเข้าใจในสิ่งต่างๆ เป็นความรู้ที่ไม่สามารถถ่ายทอดออกมาเป็นคำพูดหรือลายลักษณ์อักษรได้โดยง่าย เช่น ทักษะในการทำงาน งานฝีมือหรือการคิดเชิงวิเคราะห์ บางครั้งจึงเรียกว่าเป็นความรู้แบบนามธรรม

2) ความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่สามารถรวบรวม ถ่ายทอดได้ โดยผ่านวิธีต่างๆ เช่น การบันทึกเป็นลายลักษณ์อักษร ทฤษฎี คู่มือต่างๆ และบางครั้งเรียกว่าเป็นความรู้แบบรูปธรรม



ภาพ 2-1 กระบวนการจัดการความรู้ (Knowledge Management Process)

กระบวนการจัดการความรู้ (Knowledge Management Process) เป็นกระบวนการแบบหนึ่งที่จะช่วยให้องค์กรเข้าใจถึงขั้นตอนที่ทำให้เกิดกระบวนการจัดการความรู้ หรือพัฒนาการของความรู้ที่จะเกิดขึ้นภายในองค์กร ประกอบด้วย 7 ขั้นตอน ดังนี้

1) การบ่งชี้ความรู้ เช่น พิจารณาว่าวิสัยทัศน์/พันธกิจ/เป้าหมาย คืออะไร และเพื่อให้บรรลุเป้าหมายเราจำเป็นต้องรู้อะไร ขณะนี้เรามีความรู้อะไรบ้าง อยู่ในรูปแบบใด อยู่ที่ใคร

2) การสร้างและแสวงหาความรู้ เช่น การสร้างความรู้ใหม่ แสวงหาความรู้จากภายนอก รักษาความรู้เก่า กำจัดความรู้ที่ใช้ไม่ได้แล้ว

3) การจัดความรู้ให้เป็นระบบ เป็นการวางโครงสร้างความรู้ เพื่อเตรียมพร้อมสำหรับการเก็บความรู้อย่างเป็นระบบในอนาคต

4) การประมวลและกลั่นกรองความรู้ เช่น ปรับปรุงรูปแบบเอกสารให้เป็นมาตรฐานใช้ภาษาเดียวกัน ปรับปรุงเนื้อหาให้สมบูรณ์

5) การเข้าถึงความรู้ เป็นการทำให้ผู้ใช้ความรู้นั้นเข้าถึงความรู้ที่ต้องการได้ง่ายและสะดวก เช่น ระบบเทคโนโลยีสารสนเทศ (IT) Web board บอร์ดประชาสัมพันธ์ เป็นต้น

6) การแบ่งปันแลกเปลี่ยนความรู้ทำได้หลายวิธีการ โดยกรณีเป็น Explicit Knowledge อาจจัดทำเป็นเอกสาร ฐานความรู้ เทคโนโลยีสารสนเทศ หรือกรณีเป็น Tacit Knowledge อาจจัดทำเป็นระบบ ทีมข้ามสายงาน กิจกรรมกลุ่มคุณภาพและนวัตกรรม ชุมชนแห่งการเรียนรู้ ระบบพี่เลี้ยง สับเปลี่ยนงาน การยืมตัว เวทีแลกเปลี่ยนความรู้ เป็นต้น

7) การเรียนรู้ควรทำให้การเรียนรู้เป็นส่วนหนึ่งของงาน เช่นเกิดระบบการเรียนรู้จากการสร้างองค์ความรู้ นำความรู้ไปใช้เกิดการเรียนรู้และประสบการณ์ใหม่ และหมุนเวียนต่อไปอย่างต่อเนื่อง

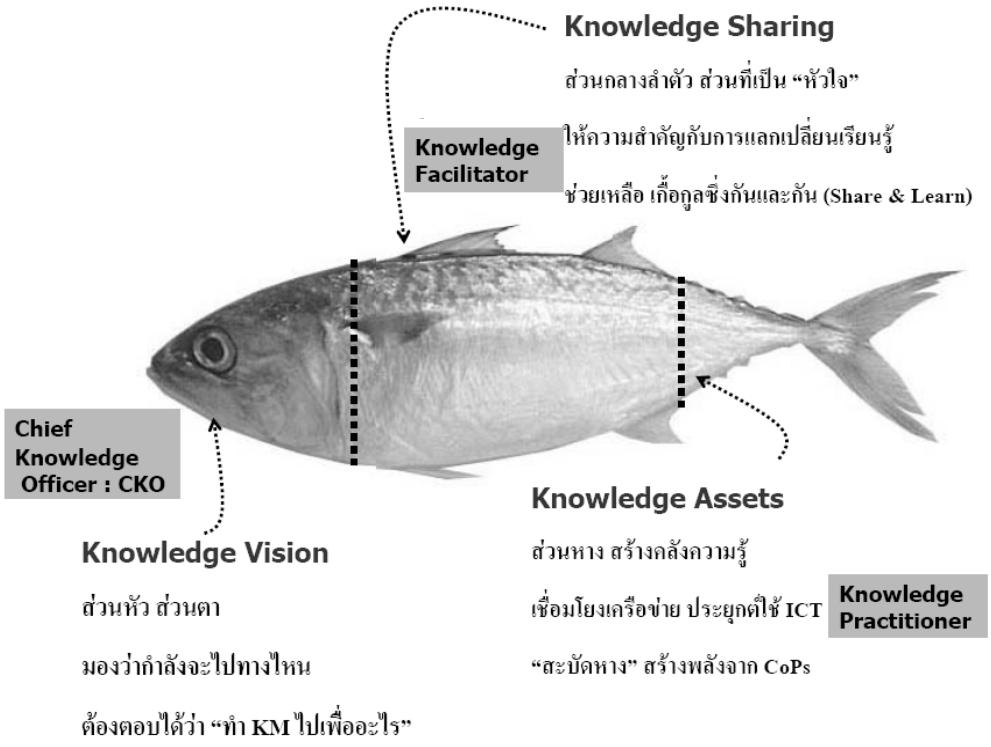
1.5) เครื่องมือในการจัดการความรู้

การจัดการความรู้ประกอบด้วย กระบวนการหลักๆ ได้แก่ การค้นหาความรู้ การสร้างและแสวงหาความรู้ใหม่ การจัดความรู้ให้เป็นระบบ การประมวลผลและกลั่นกรองความรู้ การแบ่งปันแลกเปลี่ยนความรู้ สุดท้ายคือ การเรียนรู้ และเพื่อให้มีการนำความรู้ไปใช้ให้เกิดประโยชน์สูงสุดต่อองค์กร เครื่องมือหลากหลายประเภทถูกสร้างขึ้นมาเพื่อนำไปใช้ในการถ่ายทอดและแลกเปลี่ยนความรู้ ซึ่งอาจแบ่งเป็น 2 กลุ่มใหญ่ ๆ คือ

1) เครื่องมือที่ช่วยในการ “เข้าถึง”ความรู้ ซึ่งเหมาะสำหรับความรู้ประเภท Explicit

2) เครื่องมือที่ช่วยในการ “ถ่ายทอด”ความรู้ ซึ่งเหมาะสำหรับความรู้ประเภท Tacit ซึ่งต้องอาศัยการถ่ายทอด โดยปฏิสัมพันธ์ระหว่างบุคคลเป็นหลักในบรรดาเครื่องมือดังกล่าวที่มีผู้นิยมใช้กันมากประเภทหนึ่งคือ ชุมชนแห่งการเรียนรู้ หรือชุมชนนักปฏิบัติ (Community of Practice : CoP) และการเล่าเรื่อง (storytelling)

รูปแบบการจัดการความรู้ได้จำลองแบบมาจากรูปปลาทู เพื่อกำหนดบทบาทและหน้าที่ของแต่ละส่วนซึ่งมีความเกี่ยวข้องกันออกเป็น 3 ส่วนและให้ความหมายของแต่ละส่วนให้ชัดเจน ผู้ปฏิบัติสามารถเข้าใจและศึกษารายละเอียดได้ด้วยตนเอง



ภาพ 2-2 Model ปลาทู
ที่มา: ประพนธ์ ผาสุกยืด (2550)

จากโมเดลปลาทู สามารถอธิบายการจัดการความรู้ ได้ดังนี้

Chief Knowledge Officer: CKO เป็นส่วนหัวของปลา หมายถึง เป้าหมายหลักของการจัดการความรู้ เพื่อบรรจุวิสัยทัศน์ขององค์กร (kv) โดยมีคุณเอื้อ (ceo) เป็นบุคคลสำคัญในการส่งเสริม

Knowledge Sharing: KS เป็นส่วนกลางของตัวปลา ส่วนที่เป็นหัวใจสำคัญของการแลกเปลี่ยนความรู้ บุคคลสำคัญที่จะทำให้เกิดการแลกเปลี่ยนเรียนรู้คือคุณอำนวย (Knowledge Facilitator) เป็นผู้จุดประกายและอำนวยความสะดวก โดยมีคุณกิจเป็น ผู้แสดงการแลกเปลี่ยนเรียนรู้

Knowledge Assets: KA เป็นส่วนหางปลา เป็นส่วนคลังความรู้ที่เป็นรูปธรรมที่เกิดจากการกำหนดทิศทางในส่วนหัว และการแลกเปลี่ยนความรู้ ในด้านจัดการ โดยมีคุณลิขิตเป็นผู้บันทึกและตีความและคุณประสานช่วยอำนวยการประสานงานต่างๆ

1.6) บุคคลสำคัญที่ดำเนินการจัดการความรู้

1) ผู้บริหารสูงสุด (CEO) สำหรับวงการจัดการความรู้ ถ้าผู้บริหารสูงสุดเป็นแชมป์เปียน (เห็นคุณค่า และดำเนินการผลักดัน KM) เรื่องที่ว่ายากทั้งหลายก็ง่ายขึ้น ผู้บริหารสูงสุดควรเป็นผู้ริเริ่มกิจกรรมจัดการความรู้ โดยกำหนดตัวบุคคลที่จะทำหน้าที่“คุณเอื้อ (ระบบ)” ของ KM ซึ่งควรเป็นผู้บริหารระดับสูง เช่น รองอธิบดี รองผู้อำนวยการใหญ่ ผู้บัญชาการ ผู้บังคับการ เป็นต้น

2) คุณเอื้อ (Chief Knowledge Officer, CKO) ถ้าการริเริ่มมาจากผู้บริหารสูงสุด “คุณเอื้อ” ก็สบายไปเปลาะหนึ่ง แต่ถ้าการริเริ่มที่แท้จริงไม่ได้มาจากผู้บริหารสูงสุด บทบาทแรกของ “คุณเอื้อ” ก็คือ นำเป้าหมาย/หัวปลา ไปขายผู้บริหารสูงสุด ให้ผู้บริหารสูงสุดกลายเป็นเจ้าของ “หัวปลา” ให้ได้ บทบาทต่อไปของ “คุณเอื้อ” คือ การหา “คุณอำนวย” และร่วมกับ “คุณอำนวย” จัดให้มีการกำหนด “เป้าหมาย/หัวปลา” ในระดับย่อยๆ ของ “คุณกิจ/ผู้ปฏิบัติงาน” คอยเชื่อมโยง “หัวปลา” เข้ากับวิสัยทัศน์ พันธกิจ เป้าหมายและยุทธศาสตร์ขององค์กร จัดบรรยากาศแนวราบ และการบริหารงานแบบเอื้ออำนาจ (Empowerment) ร่วม Share ทักษะในการเรียนรู้และแลกเปลี่ยนเรียนรู้ เพื่อประโยชน์ในการดำเนินการจัดการความรู้โดยตรง และเพื่อแสดงให้ “คุณกิจ” เห็นคุณค่าของทักษะดังกล่าว, จัดสรรทรัพยากรสำหรับใช้ในกิจกรรมจัดการความรู้ พร้อมคอยเชื่อมโยงการจัดการความรู้เข้ากับกิจกรรมสร้างสรรค์อื่นๆ ทั้งภายในและนอกองค์กร ติดตามความเคลื่อนไหวของการดำเนินการให้คำแนะนำบางเรื่อง และแสดงท่าทีชื่นชมในความสำเร็จ อาจจัดให้มีการยกย่องในผลสำเร็จ และให้รางวัลที่อาจไม่เน้นสิ่งของแต่เน้นการสร้างความภาคภูมิใจในความสำเร็จ

3) คุณอำนวย (Knowledge Facilitator , KF) เป็นผู้คอยอำนวยความสะดวกในการจัดการความรู้ ความสำคัญของ “คุณอำนวย” อยู่ที่การเป็นนักจุดประกายความคิดและการเป็นนักเชื่อมโยง โดยต้องเชื่อมโยงระหว่างผู้ปฏิบัติ (“คุณกิจ”) กับผู้บริหาร (“คุณเอื้อ”), เชื่อมโยงระหว่าง “คุณกิจ”ต่างกลุ่มภายในองค์กร, และเชื่อมโยงการจัดการความรู้ภายในองค์กรกับภายนอกองค์กร โดยหน้าที่ที่ “คุณอำนวย” ควรทำคือร่วมกับ “คุณเอื้อ” จัดให้มีการกำหนด “หัวปลา” ของ “คุณกิจ” อาจจัด “มหกรรมหัวปลา” เพื่อสร้างความเป็นเจ้าของ “หัวปลา” จัดตลาดนัดความรู้ เพื่อให้ คุณกิจ นำความสำเร็จมาแลกเปลี่ยนเรียนรู้ ถอดความรู้ออกมาจากวิธีทำงานที่นำไปสู่ความสำเร็จนั้น เพื่อการบรรลุ “หัวปลา” จัดการดูงาน หรือกิจกรรม “เชิญเพื่อนมาช่วย” (Peer Assist) เพื่อให้บรรลุ “หัวปลา” ได้ง่าย หรือเร็วขึ้น โดยที่ผู้นั้นจะอยู่ภายในหรือนอกองค์กรก็ได้ เรียนรู้วิธีทำงานจากเขา เชิญเขามาเล่าหรือสาธิต - จัดพื้นที่เสมือนสำหรับการแลกเปลี่ยนเรียนรู้ และสำหรับเก็บรวบรวมขุมความรู้ที่ได้ เช่น ใช้เทคโนโลยีการสื่อสารและสารสนเทศซึ่งรวมทั้งเว็บไซต์ เว็บบอร์ด เว็บบล็อก อินทราเน็ต จดหมายข่าว เป็นต้น ส่งเสริมให้เกิดชุมชนแนวปฏิบัติ (CoP-Community of Practice) ในเรื่องที่เป็นความรู้ หรือเป็นหัวใจในการบรรลุเป้าหมายหลักขององค์กร เชื่อมโยงการดำเนินการจัดการความรู้ขององค์กรกับกิจกรรมจัดการความรู้ภายนอก เพื่อสร้างความคึกคักและเพื่อแลกเปลี่ยนเรียนรู้กับภายนอก

4) คุณกิจ (Knowledge Practitioner, KP) “คุณกิจ” หรือผู้ปฏิบัติงาน เป็นพระเอกหรือนางเอกตัวจริงของการจัดการความรู้ เพราะเป็นผู้ดำเนินกิจกรรมจัดการความรู้ประมาณร้อยละ

90-95 ของทั้งหมด “คุณกิจ” เป็นเจ้าของ “หัวปลา” โดยแท้จริง และเป็นผู้ที่มีความรู้ (Explicit Knowledge) และเป็นผู้ที่ต้องมาแลกเปลี่ยนเรียนรู้ ใช้ หา สร้าง แปลง ความรู้เพื่อการปฏิบัติให้บรรลุถึง “เป้าหมาย/หัวปลา” ที่ตั้งไว้

5) คุณประสาน (Network Manager) และคุณลิขิต เป็นผู้ที่คอยประสานเชื่อมโยงเครือข่ายการจัดการความรู้ระหว่างหน่วยงาน ให้เกิดการแลกเปลี่ยนเรียนรู้ในวงที่กว้างขึ้น เกิดพลังร่วมมือทางเครือข่ายในการเรียนรู้และยกระดับความรู้แบบทวีคูณ

1.7) กิจกรรมแลกเปลี่ยนเรียนรู้ในองค์กร

กิจกรรมแลกเปลี่ยนเรียนรู้กันเองในองค์กรไม่ใช่เกิดขึ้นง่ายๆ ผู้บริหารองค์กรจึงต้องจัดให้มีคนมาจัดการให้เกิดบรรยากาศเหล่านี้ การแลกเปลี่ยนเรียนรู้จึงน่าจะเกิดผลดีอย่างน้อย 9 ประการ คือ

1) เกิดการเทียบเคียงความรู้ (bench marking) กัน
2) เป็นการแลกเปลี่ยน แบ่งปัน best practices กัน
3) กระตุ้นให้คนในองค์กรเกิดความกระตือรือร้น
4) บุคลากรสร้างกัลยาณมิตรที่ดีต่อกัน
5) ส่งเสริมการมีส่วนร่วม (การร่วมคิดร่วมทำ)
6) แต่ละคนต่างทำตามพันธะสัญญาที่มีต่อกัน
7) สร้างความเสียสละ และดูแลซึ่งกันและกัน
8) รู้จักปรับตัวและยืดหยุ่น
9) สร้างวัฒนธรรมนำไปสู่องค์กรแห่งการเรียนรู้ (learning organization)

กิจกรรมแลกเปลี่ยนเรียนรู้ที่มีพลังของกระบวนการ KM มีหลายกิจกรรม แต่กิจกรรมหนึ่งที่ใช้แล้วได้ผลและควรทดลองนำไปปรับใช้คือ กิจกรรมเรื่องเล่าเร้าพลัง (Storytelling) ที่สามารถดำเนินการผ่านชุมชนผู้ปฏิบัติ (Community of Practices: CoPs) ในแต่ละเรื่องแต่ละประเด็นที่เรากำหนดเป้าหมายร่วมกันไว้ ซึ่งมีกติกาหรือข้อตกลงในการดำเนินการ

1.8) กิจกรรมเรื่องเล่าเร้าพลัง (storytelling)

การเล่าเรื่องเป็นเครื่องมือของการจัดการความรู้ มีเป้าหมายคือให้มีความรู้จากการปฏิบัติ ปลดปล่อยความเชื่อ ความคิด และการปฏิบัติออกมาเป็นคำพูด และหน้าตาท่าทาง (Non-verbal communication) การปลดปล่อยความรู้จากการปฏิบัตินี้ ผู้ปลดปล่อยจะอยู่ในสภาพที่มีทั้งจิตใต้สำนึกและจิตสำนึก (subconscious & conscious) โดยมีเป้าหมายให้เกิดการสื่อสาร ทั้งโดยใช้จิตสำนึกและจิตใต้สำนึก ดังนั้นถ้าฝึกปฏิบัติจนมีความชำนาญ การเล่าเรื่องจะปลดปล่อยความรู้ออกมาอย่างทรงพลังอย่างไม่น่าเชื่อ ซึ่งเป็นความรู้ที่ฝังลึกอยู่ภายใน โดยใช้วิธีการดังนี้

1) เป็นวิธีการเรียนรู้จากผลสำเร็จที่ปลายทาง นั่นคือความสำเร็จจากการปฏิบัติจริงของผู้อื่นซึ่งเป็นวิธีการปฏิบัติที่ดีที่สุดของเขา (best practices) แล้วมาเล่าให้ฟัง โดยให้สมาชิกแต่ละคน (กลุ่มหนึ่ง

ควรอยู่ระหว่าง 8–10 คน) ผลัดกันเล่าเรื่องความสำเร็จที่ภูมิใจ ประทับใจ ของตนหรือของหน่วยงานของตน ให้เล่าเพียงประเด็นเดียวต่อหนึ่งเรื่อง เล่าแบบได้ใจความและเล่าสั้น ๆ ใช้เวลาประมาณคนละ 2 – 3 นาที

2) เป็นการแลกเปลี่ยนเรียนรู้กันในชุมชนผู้ปฏิบัติ (CoPs) ในเรื่องใดเรื่องหนึ่งโดยเฉพาะ เช่น CoP การใช้ ICT เพื่อการบริหาร CoP การวิจัยเพื่อพัฒนาการปฏิบัติงาน เป็นต้น โดยมี ผู้อำนวยความสะดวก (facilitator) ในการเล่าเรื่อง (อาจเรียกว่า คุณอำนวย)

3) กฎของผู้เล่า ต้องเล่าให้น่าสนใจ เล่าตามความเป็นจริง เล่าเฉพาะเหตุการณ์ บรรยากาศ ตัวละคร ความคิดของผู้เล่าในขณะเกิดเหตุการณ์ ไม่ตีความระหว่างเล่า เล่าให้เห็นบุคคล พฤติกรรม การปฏิบัติ ความสัมพันธ์ที่ไม่เยิ่นเย้อ

4) กฎของผู้ฟัง ใช้กฎสุนทรียสนทนา (Dialogue) คือ

(1) ฟังโดยไม่พูดแทรก ไม่เสนอข้อแนะนำใดๆ ไม่วิจารณ์ ไม่แย้ง แต่เมื่อเขาเล่าจบสามารถซักถามใน ลักษณะขอข้อมูลเพิ่มเติมได้

(2) ฟังด้วยความตั้งใจ ไม่ต้องพะวงหรือเตรียมตัวในการพูดของตนเองในการพูดรอบต่อๆ ไป ให้ตั้งใจฟังอย่างเดียว พอถึงรอบที่เราต้องพูดก็ให้พูดความจริงออกมาจากใจ

(3) ฟังด้วยความเข้าใจ คือการจับประเด็นจากขุมความรู้ที่เล่าให้ได้ ดังนั้นการเล่าและการฟังจึงอยู่ภายใต้บรรยากาศที่ดีเป็นมิตร ชื่นชม ไม่ตัดสินว่าผิดหรือถูก ไม่คาดหวังกับผลลัพธ์มากจนลืมเปิดใจรับฟังผู้อื่น

(4) กำหนดให้มีผู้บันทึกขุมความรู้จากเรื่องเล่า (อาจเรียกว่า คุณลิขิต) ซึ่งจะบันทึกประเด็นหรือวิธีการปฏิบัติของผู้เล่าแต่ละคนจนครบทุกคน

(5) เมื่อเล่าครบทุกคนแล้ว ผู้บันทึกจะอ่านขุมความรู้ของทุกคนให้สมาชิกฟัง แล้วสมาชิกจะช่วยกันสังเคราะห์ขุมความรู้เหล่านั้นเป็นแก่นความรู้ เพื่อการเทียบเคียงวิธีการปฏิบัติ (Benchmarking) กับประสบการณ์เดิมตามบริบทของแต่ละคน แล้วสร้างเป็นองค์ความรู้ของตนเอง พร้อมทั้งนำไปสู่การปฏิบัติตน ปฏิบัติงานให้ก้าวหน้าต่อไป แล้วจะเกิดเป็น Tacit knowledge นำมาแลกเปลี่ยนเรียนรู้กันใหม่ ต่อยอดความรู้ให้เพิ่มพูนมากยิ่งๆขึ้นไปโดยไม่มีวันจบสิ้น

1.9) ชุมชนนักปฏิบัติ (Community of Practice, CoP)

เป็นวิธีการหนึ่งที่สำคัญในการจัดการความรู้ขององค์กร และจะนำไปสู่การเป็นองค์กรแห่งการเรียนรู้ ด้วยการสร้างเป็นชุมชนขึ้นมา เพื่อทำการแลกเปลี่ยนแบ่งปันความรู้ รวมทั้งประสบการณ์ของผู้ที่สนใจในเรื่องเดียวกัน มีวัตถุประสงค์ หรืออุดมการณ์ร่วมกันผ่านทั้งรูปแบบที่เป็นทางการและไม่เป็นทางการ โดยอาจจะมีการพบปะกันจริง หรือพบปะกันแบบเสมือนผ่านทางเครือข่ายอินทราเน็ตหรืออินเตอร์เน็ต ซึ่งจะเป็นการทำให้เกิดการทำงานที่มีการประสานร่วมมือกันปรึกษาหารือกัน มีลักษณะเป็นการทำงานแบบเชื่อมโยงกันเป็นเครือข่ายที่มีการแบ่งปันความรู้ร่วมกัน หากองค์การสามารถเชื่อมโยงชุมชนนักปฏิบัติหลายๆ ชุมชนเข้าด้วยกัน ก็จะเป็นเครือข่ายการทำงานที่มีการปฏิบัติงานร่วมกันจากหลายๆ ฟังก์ชั่นงาน ทำให้

บุคลากรไม่เพียงแต่มีความรู้ ความสามารถเฉพาะด้านใดด้านหนึ่งเท่านั้น แต่อาจจะมีความรู้ ความสามารถที่หลากหลายมากขึ้น เมื่อได้มีการแบ่งปันความรู้ร่วมกันผ่านชุมชนนักปฏิบัติ

รูปแบบของชุมชนนักปฏิบัติ ลักษณะรูปแบบในการทำชุมชนนักปฏิบัติ มีด้วยกันหลายรูปแบบ แตกต่างกันไป แล้วแต่ว่าแต่ละชุมชนจะเลือกใช้แบบใดแบบหนึ่ง หรืออาจจะผสมผสานกันก็ได้ โดยมีรูปแบบดังต่อไปนี้

1) แบบกลุ่มเล็ก มี 5-6 กลุ่ม กลุ่มละ 6-7 คน ซึ่งมีข้อดี คือ สามารถแลกเปลี่ยนประสบการณ์กันได้อย่างทั่วถึง

2) แบบเป็นทางการ (Public) ที่เปิดเผย มีการจัดทำเป็นโครงการ KM ของ สถาบันการจัดการความรู้เพื่อสังคม (สคส.) ดำเนินการโดย KM Team ขององค์กร เนื่องจากเป็น โครงการนำร่องจัดเป็นครั้งแรก จึงต้องทำแบบเป็นทางการ

3) แบบไม่เป็นทางการ เป็นลักษณะที่ต้องการพบปะ แลกเปลี่ยนประสบการณ์กันเมื่อไรก็ได้ตามความเหมาะสม และต้องการของสมาชิก เช่น สภากาแฟ หรือพบปะพูดคุยกันในโต๊ะอาหาร เป็นต้น

4) แบบบนลงล่าง (Top Down) เพราะเป็นนโยบายขององค์กร ซึ่งต่อไปในอนาคตเมื่อทุกคนมีความรู้ความเข้าใจ เรื่อง KM ดีแล้ว แต่ละฝ่ายงานจะมีการทำ CoP แบบรากหญ้า (Grass Root) ที่เริ่มต้นรวมตัวกันจากสมาชิกภายในฝ่าย

5) แบบคละฝ่าย เนื่องจากหัวข้อเรื่องการทำ CoP เป็นหัวข้อใหญ่ มีลักษณะงานที่เกี่ยวข้องกันหลายฝ่าย คือ งานบริการด้านฝึกอบรม จำเป็นต้องแลกเปลี่ยนเรียนรู้กับฝ่ายต่าง ๆ ที่เกี่ยวข้องกับงานฝึกอบรม

6) แบบเน้นการแลกเปลี่ยนความรู้ระหว่างคนกับคน แบบซึ่งหน้า (Face to Face) ไม่ใช่การแลกเปลี่ยนความรู้โดยผ่านสื่อ Intranet หรือ Internet

7) แบบที่มีการแลกเปลี่ยนความรู้ระหว่างคนในองค์กร และคนนอกองค์กร เนื่องจากมีเจ้าหน้าที่ผู้ปฏิบัติงานจากหน่วยงานภายนอกมาร่วมกิจกรรมด้วย

เราสามารถเลือกใช้แต่ละแบบได้ตามความเหมาะสมของแต่ละสถานการณ์หรือแต่ละหน่วยงาน

1.10) การทบทวนหลังกิจกรรม (AAR - After Action Review)

1) การทบทวนหลังกิจกรรม (AAR - After Action Review) เป็นเครื่องมือจัดการ ความรู้ที่ใช้ง่ายที่สุด แต่ทรงพลังที่สุด

2) ใช้เครื่องมือนี้เพื่อทำให้เกิดการมีส่วนร่วมของสมาชิกทุกคน และทำให้สมาชิกทุกคนมีสติตื่นตัวอยู่กับงานและการเรียนรู้

3) AAR เป็นเครื่องมือที่ทำให้ KM อยู่ในงานประจำ

4) ทุกคนที่ร่วมกิจกรรม เข้าร่วมทำ AAR โดยนั่งล้อมวงเป็นวงกลมหรือรูปตัว ยู

5) สร้างบรรยากาศที่เป็นอิสระ เท่าเทียมกัน

6) ให้ทุกคนพูดออกมาจากใจ ไม่มีถูก-ผิด เน้นการตีความ การนำเสนอแบบมองต่างมุม การสร้างคุณค่า/มูลค่า เพิ่ม จากความแตกต่างหลากหลาย

7) มี “คุณลิขิต” คอยจดบันทึกประเด็น สำหรับนำไปใช้ต่อ

8) ทุกคนตอบคำถาม 5 ข้อ (อาจเพิ่ม–ลด ข้อ หรือปรับเปลี่ยนแต่ละข้อตามความเหมาะสม

(1) ในการ ทำงาน/ประชุม ครั้งนี้ ตนเองมีความมุ่งหมาย/วัตถุประสงค์อย่างไรบ้าง

(2) วัตถุประสงค์ข้อใด ที่บรรลุมากเกินความคาดหมาย เพราะเหตุใด

(3) วัตถุประสงค์ข้อใด บรรลุน้อย หรือไม่บรรลุเลย เพราะเหตุใด

(4) หากจะทำงาน/ประชุม เช่นนี้อีก มีคำแนะนำให้ปรับปรุงอะไรบ้าง

(5) ตนเองจะกลับไปทำอะไรบ้าง

“คุณอำนวย” ของกิจกรรม AAR ควรสรุปประเด็นสำคัญๆ ของแต่ละข้อ รวมทั้งสรุปภาพรวม สำหรับนำไปใช้ดำเนินการต่อไป เป็นกิจกรรมที่เราต้องทำหลังจากทำกิจกรรมการเล่าเรื่อง หรือชุมชนนักปฏิบัติแล้วเพื่อเราจะได้ทราบว่าเราได้หรือไม่ได้อะไรจากกิจกรรมนั้นบ้าง เพื่อใช้เป็นข้อมูลในการทำกิจกรรมครั้งต่อๆ ไป

เนื่องจากกิจกรรมในกระบวนการ KM มีมากมาย เราจึงสามารถพิจารณาประยุกต์ใช้ได้ตามความเหมาะสมของแต่ละบริบท อย่างไรก็ตามการทำ KM ขององค์กรต่าง ๆ ในปัจจุบันยังมีปัญหาอุปสรรคอีกหลายประการ ปัญหาสำคัญที่สุด คือ เรื่อง วัฒนธรรมองค์กรที่ยังเป็นแนวตั้งมากกว่าแนวราบสืบทอดกันมายาวนาน บุคลากรก็ยังสาละวนกับการจัดการงานประจำแต่ละวันให้เสร็จสิ้นไปอย่างหัว ไม่วาง หางไม่เว้น พอมีเรื่องใหม่เข้ามาก็เกรงว่าไปเพิ่มงานประจำให้มากขึ้นอีก จึงปฏิเสธหรือไม่ก็ทำอย่างไม่เต็มใจ การแก้ไขคงต้องใช้เวลาอีกยาวนาน ซึ่งต้องอาศัยผู้บริหาร (CKO) และผู้อำนวยความสะดวก (คุณอำนวย) ที่เป็นแบบอย่างและมีความแน่วแน่ในการหากลยุทธ์มาปรับเปลี่ยนวัฒนธรรมองค์กรให้เป็นแนวราบอย่างต่อเนื่องมากขึ้น โดยอาจใช้กระบวนการ KM แทรกซึมลงไปในกิจกรรมพัฒนาคน พัฒนางานในสภาพการณ์ปกติ (ธเนศ ขำเกิด, 2549)

2) แนวคิดและทฤษฎีอาชญากรรมคอมพิวเตอร์

2.1) ประวัติอาชญากรรมคอมพิวเตอร์ (ญาณพล ยั่งยืน, 2555)

คงปฏิเสธไม่ได้ว่า “อาชญากรรมคอมพิวเตอร์” เรื่อยมาจนถึง “อาชญากรรมไซเบอร์ หรืออาชญากรรมอินเทอร์เน็ต” เหล่านี้ล้วนแล้วแต่เป็นผลพวงด้านลบที่เกิดขึ้น พัฒนาการ และขยายตัวมาพร้อมๆ หรือไล่ๆ กับวิวัฒนาการ และความก้าวหน้าทางเทคโนโลยีในยุคข้อมูลข่าวสาร

นวัตกรรมใหม่อย่างคอมพิวเตอร์ และการเชื่อมต่อระหว่างกันจนเกิดเป็นเครือข่ายขนาดเล็กและใหญ่ ในช่วงปลายทศวรรษที่ 60 (ปีค.ศ.1969) กำเนิดอินเทอร์เน็ต) ในขณะที่ด้านหนึ่งถูกใช้เป็นเครื่องมือในการกระทำความผิด อีกด้านหนึ่งก็ถูกเล็งให้กลายเป็นเป้าหมายแห่งการกระทำความผิดในฐานะที่เป็นอุปกรณ์ หรือช่องทางสำคัญ ในการเก็บรักษาและ/หรือ รับ-ส่ง ข้อมูลข่าวสาร ทรัพย์สินที่ปัจจุบันดูเหมือนจะมีค่ามากกว่าทรัพย์ประเภทที่มีรูปร่างบางอย่างเสียอีก

วิวัฒนาการของอาชญากรรมคอมพิวเตอร์ (Computer Crime) จากอดีตเรื่อยมาจนถึงยุคของอาชญากรรมเครือข่าย (Cyber Crime) หรืออาชญากรรมอินเทอร์เน็ต (Internet Crime) ในปัจจุบันที่กำลังกลายเป็นปัญหาสำคัญ และแก้ไม่ตกของประเทศทั้งหลาย ในอันที่จะหาวิธีในการป้องกัน และปราบปรามการกระทำความผิดเหล่านี้ ทั้งนี้เพื่อให้ทราบที่มา และเห็นถึงความเปลี่ยนแปลงเป้าหมายการกระทำความผิดจากสิ่งที่กฎหมายประสงค์จะคุ้มครอง (Rechtsgut) ไปสู่อีกสิ่งหนึ่ง ซึ่งเกิดขึ้นในช่วงระยะเวลาเพียงไม่กี่สิบปีเท่านั้น จนหลายๆ ประเทศ รวมทั้งประเทศไทยเองจำเป็นต้องเร่งบัญญัติกฎหมายใหม่ขึ้นมารองรับ รวมทั้งเพื่อเป็นประโยชน์ต่อการวิเคราะห์หาแนวโน้มขอบเขตความเสียหายอื่น ๆ ที่อาจขยายตัวต่อไปตามวิวัฒนาการทางเทคโนโลยีในอนาคตด้วย

1) การกระทำความผิดต่อสิทธิความเป็นส่วนตัวและข้อมูลส่วนบุคคล แม้ในที่สุดแล้วจนถึงปัจจุบัน จะยังไม่มีใครสามารถให้คำนิยาม คำว่า “อาชญากรรมคอมพิวเตอร์” ที่ชัดเจน ครอบคลุม และเป็นเอกภาพจนเป็นที่ยอมรับกันในระหว่างประเทศได้ แต่หากกล่าวถึงความหมายโดยทั่ว ๆ ไปที่ทำให้คนในสังคมเริ่มเข้าใจ และตระหนักรู้ถึงความเสียหายที่เกิดขึ้นจากอาชญากรรมประเภทนี้แล้ว ความหมายโดยในดังกล่าวได้เริ่มขึ้นเมื่อไม่กี่สิบปีที่ผ่านมานี้เอง ในช่วงระยะเวลาที่ข้อมูลชีวิตของมนุษย์จำนวนหนึ่งถูกควบคุม หรือตกอยู่ภายใต้การทำงานของเทคโนโลยีคอมพิวเตอร์

ทศวรรษที่ 60 (ช่วงปี ค.ศ. 1960-1970) นับเป็นช่วงเวลาแรก ๆ ที่เริ่มมีความพยายามการชี้ให้เห็นถึง ภยันตรายจากการกระทำความผิดทางคอมพิวเตอร์ ทั้งนี้ด้วยในสมัยนั้น หลายประเทศในแถบตะวันตกใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลส่วนบุคคลของประชาชนในรัฐเข้าด้วยกัน และด้วยเหตุที่มีการนำข้อมูลต่างๆ เหล่านี้ไปรวบรวมไว้ภายใต้การจัดการของรัฐนี้เอง นักวิชาการจำนวนหนึ่งจึงเริ่มอภิปรายถกเถียงถึงประเด็นปัญหาที่ประชาชนอาจถูกตรวจสอบ เฝ้ามอง หรือควบคุมจากรัฐได้ โดยข้อถกเถียงทั้งหลายได้รับอิทธิพลมาจากหนังสือของ George Orwell ชื่อ “1984” อันเป็นหนังสือด้านการเมืองการปกครอง แต่มีเนื้อหาส่วนหนึ่งที่ Orwell กล่าวถึงพัฒนาการทางเทคโนโลยีข้อมูลข่าวสาร พร้อมๆ กับชี้ให้เห็นว่า แม้ในช่วงเวลาเริ่มต้น กระบวนทัศน์ (Paradigm) ของมนุษย์ที่มีต่อ

คอมพิวเตอร์ คือ อุปกรณ์หรือเครื่องมือทรงพลัง ที่มีประโยชน์ต่อระบบการจัดการข้อมูลอย่างสูง ที่จะทำให้การทำงานต่างๆ ของมนุษย์สะดวก และรวดเร็วขึ้น แต่ในอนาคต การใช้เทคโนโลยี และเครื่องมือชนิดนี้ โดยเฉพาะอย่างยิ่งโดยรัฐ จะเริ่มล้ำเส้น และเกินขอบเขตความเป็นส่วนตัวของประชาชน หรือ จะถูกใช้เป็นเครื่องมือในควบคุมตรวจสอบพฤติกรรมพลเมืองโดยผู้ปกครองรัฐมากขึ้นเรื่อยๆ

และด้วยเหตุที่ยุคสมัยนั้น คุณประโยชน์หลักๆ ของเครื่องคอมพิวเตอร์ ยังจำกัดอยู่เพียงแค่การเก็บบันทึก ประมวลผล หรือเชื่อมต่อข้อมูลต่าง ๆ ของประชาชนในประเทศเท่านั้น ความเข้าใจที่มีต่อการกระทำความผิดโดยมีคอมพิวเตอร์เข้าไปเกี่ยวข้องในยุคสมัยแรกๆ จึงยังไม่ได้มีความหมายทำนองเดียวกับ “อาชญากรรมคอมพิวเตอร์” ที่เราเข้าใจกันในปัจจุบัน แต่หมายถึง การกระทำความผิดใดๆ ที่เป็นอันตรายต่อข้อมูลข่าวสาร และระดับความลับ หรือความเป็นส่วนตัวที่มนุษย์แต่ละคนอาจไม่ได้ต้องการเปิดเผยให้ผู้อื่นได้รับรู้

ดังนั้น สิ่งสำคัญที่คนเริ่มให้ความสนใจ และเรียกร้องให้รัฐต้องให้ความคุ้มครองเป็นพิเศษ คือ ข้อมูลส่วนบุคคลนั่นเอง และข้อมูลข่าวสารที่มีความสำคัญ ที่รัฐควรต้องให้การคุ้มครองอย่างมาก ก็คือ ความลับในทางวิชาชีพต่างๆ โดยเฉพาะอย่างยิ่ง ข้อมูลทางการแพทย์ ความลับของราชการ ข้อมูลทางการเงิน การธนาคาร หรือข้อมูลทางด้านคดีความ เป็นต้น

แต่เพราะในช่วงระยะหลังๆ ที่ผ่านมา จากการเก็บสถิติการกระทำความผิดที่เกิดขึ้นในหลายๆ ประเทศ พบว่า การกระทำความผิดต่อ “ข้อมูลข่าวสาร” ที่ได้รับความคุ้มครองตามกฎหมายอัน มีผลกระทบต่อประโยชน์ของปัจเจกชนมีจำนวนไม่มาก เราจึงไม่ค่อยได้ยินว่า ข้อมูลส่วนบุคคลเป็นเป้าหมายสำคัญที่รัฐต้องเฝ้าระวังป้องกันเป็นพิเศษ จากการกระทำความผิดทางคอมพิวเตอร์

อย่างไรก็ตาม คดีการกระทำความผิดต่อข้อมูลข่าวสารที่เกิดขึ้น มักมีระดับของภยันตรายที่แตกต่างกันไป ขึ้นอยู่กับว่าข้อมูลที่ถูกละเมิดนั้น เป็นของใครหรือหน่วยงานใด เช่น การจารกรรมข้อมูลข่าวสารที่เกี่ยวกับระบบความปลอดภัยของรัฐ อันตรายที่เกิดขึ้นอาจกว้างกว่าการขโมยข้อมูลส่วนบุคคลบางอย่าง เพื่อผู้กระทำความผิดจะนำไปใช้ในการข่มขู่ หรือรีดไถจากเจ้าของข้อมูล คดีสำคัญ ๆ เกี่ยวกับการกระทำความผิดต่อข้อมูลที่เคยเกิดขึ้นมาแล้ว เช่น การขโมยข้อมูลการรักษาผู้ป่วยโรคเอดส์ในประเทศแอฟริกาใต้ ซึ่งต่อมาข้อมูลนั้น ถูกส่งต่อไปยังผู้จ้างวานของผู้ป่วยจนเขาได้รับความเสียหาย หรือคดีที่บริษัท IBM ถูกฟ้องร้องเมื่อปี 1986 ว่าระบบความปลอดภัย (RACF) อาจโดนพนักงานของบริษัทตรวจสอบโดยเจ้าของไม่อนุญาต เป็นต้น

2) *อาชญากรรมเศรษฐกิจ แม้ในปัจจุบัน อาชญากรรมคอมพิวเตอร์ ที่เกิดขึ้นในหลาย ๆ กรณี เป็นความผิดในกลุ่มอื่น ที่มีผลกระทบต่อชีวิต ระบบรักษาความปลอดภัย หรือเป็นอันตรายต่อสังคม* ซึ่งอาจไม่ได้เกี่ยวพันกับปัญหาในทางเศรษฐกิจเลยก็ตาม แต่ในยุคสมัยหนึ่ง “อาชญากรรม” หรือ “การกระทำความผิด” อันมีคอมพิวเตอร์เข้าไปเกี่ยวข้องนี้ ได้เคยถูกขึ้นบัญชีให้อยู่ในกลุ่มของอาชญากรรมทางเศรษฐกิจ หรือ ที่รู้จักกันในนาม White Collar Crimes อาชญากรรมเชิ้ตขาว หรืออาชญากรรมเสื้อคอปก ที่ผู้กระทำความผิดเป็นกลุ่มคนทำงานดีแต่งตัวดี หรือมีความรู้ความสามารถเท่านั้น

ความหมายของอาชญากรรมทางเศรษฐกิจ ค่อนข้างกว้าง ครอบคลุมความผิดหลายอย่าง เป็นการกระทำที่สร้างความเสียหาย ทั้งแก่เศรษฐกิจของปัจเจกชน แลประเทศชาติสังคมส่วนรวมมีลักษณะของการทำลายความเชื่อถือ ความมั่นคงทางเศรษฐกิจ ตัวอย่างอาชญากรรมเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา การปั่นหุ้น ความผิดเกี่ยวกับภาษีอากร ธุรกิจต่าง ๆ สถาบันการเงิน เกี่ยวกับการค้าหรือธุรกิจเงินนอกระบบ เป็นต้น ในช่วงทศวรรษที่ 70 (ช่วงปี ค.ศ.1970-1980) การอภิปรายเพื่อแก้ไขปัญหาการกระทำความผิดทางคอมพิวเตอร์ ไม่ได้จำกัดขอบเขตให้อยู่ที่ประเด็น การกระทำความผิดต่อข้อมูลข่าวสารส่วนบุคคลอีกต่อไป แต่รัฐเริ่มหันมาให้ความสนใจในประเด็นปัญหาอาชญากรรมทางเศรษฐกิจมากขึ้น ทั้งนี้เนื่องจากพบว่าสถิติการกระทำความผิดทางคอมพิวเตอร์ที่เกิดขึ้น ได้ส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศ โดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจการเงิน เพิ่มจำนวนสูงขึ้นจนน่าวิตก

หลังจากปี ค.ศ.1969 ที่เทคโนโลยีอินเทอร์เน็ตเกิดขึ้นครั้งแรก และได้รับการพัฒนาเรื่อยมาจนอินเทอร์เน็ตได้กลายเป็นส่วนสำคัญในการทำงานในหน่วยงานของรัฐ รวมทั้งผู้ประกอบธุรกิจรายใหญ่ๆ ของประเทศ ในขณะที่เทคโนโลยีชนิดนี้สร้างความสะดวก และความเป็นอิสระในการแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ประกอบธุรกิจทั้งหลาย โดยไม่จำเป็นต้องเดินทางไปพบกันโดยตรง แต่ในอีกด้านหนึ่งมันก็กลายเป็นประโยชน์ สำหรับผู้กระทำความผิดที่ต้องการจารกรรม หรือลักลอบทำซ้ำข้อมูลเหล่านั้นไปใช้ประโยชน์ทางธุรกิจของตน หรือสร้างความเสียหายทางด้านการเงินต่อธุรกิจของผู้อื่น

จากที่สมัยเดิมอาชญากรรมเศรษฐกิจไม่ได้มีเครื่องมือพิเศษเพื่อเพิ่มศักยภาพในการกระทำความผิด และมักเป็นแค่เพียงการปลอมแปลง หรือการกระทำต่อเอกสารบัญชีการเงิน การธนาคาร และเอกสารอื่นๆ เท่านั้น อาชญากรรมเศรษฐกิจรูปแบบใหม่ที่มีเทคโนโลยีคอมพิวเตอร์ และเครือข่ายอินเทอร์เน็ตเข้ามาเกี่ยวข้อง จนสามารถขยายขอบเขตไปสู่ความเสียหายต่อเศรษฐกิจในด้านอื่นๆ ด้วย ก็เริ่มปรากฏตัวขึ้นในยุคนี้เอง มีการจำแนกอาชญากรรมคอมพิวเตอร์ ออกเป็นสองกลุ่มใหญ่ คือ กลุ่มความผิดที่ผู้กระทำอาศัยคอมพิวเตอร์เป็นเครื่องมือ และกลุ่มความผิดที่ระบบคอมพิวเตอร์และข้อมูลที่อยู่ในคอมพิวเตอร์เป็นเป้าหมายของผู้กระทำความผิด

ความผิดสำคัญๆ ที่เกิดขึ้นบ่อยครั้ง และได้รับความสนใจจากนักกฎหมาย และนักวิชาการด้านอื่นๆ ด้วย เช่น การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation) การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage) หรือการกรรโชก รีดไถทางคอมพิวเตอร์ การเข้าไปในระบบโดยปราศจากอำนาจ (Computer hacking) และการละเมิดลิขสิทธิ์ซอร์ฟแวร์ รวมทั้งการลักลอบขโมยผลิตภัณฑ์ที่มีลิขสิทธิ์ต่างๆ เช่น เพลงหรือภาพยนตร์

2.2) ลักษณะของอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ต

ลักษณะของอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ตนี้ เป็นการแบ่งโดยดูจาก “บทบาท” ของเครื่องคอมพิวเตอร์ที่เข้าไปเกี่ยวพันกับความผิดที่เกิดขึ้นเป็นหลัก โดยแบ่งออกได้เป็น 3 ลักษณะใหญ่ ๆ ด้วยกันคือ

1) *คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (Computers as incidental to crime)* การกระทำความผิดในลักษณะนี้ “บทบาท” ของคอมพิวเตอร์ จะไม่มีความสำคัญมากนัก กล่าวคือ คอมพิวเตอร์ไม่ใช่สาระสำคัญในกระทำความผิด แม้ผู้กระทำความผิดไม่มีคอมพิวเตอร์ ความผิดที่ได้กระทำเหล่านั้นก็สามารถสำเร็จลงได้เหมือนกัน ดังนั้น คอมพิวเตอร์จึงเป็นเพียงอุปกรณ์เสริม หรือช่วยอำนวยความสะดวกให้กับการกระทำความผิดในรูปแบบเดิม ๆ เท่านั้น เช่น ใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับการค้ายาเสพติด ใช้คอมพิวเตอร์ในการติดต่อสื่อสารในองค์กรอาชญากรรม หรือใช้คอมพิวเตอร์ในการเก็บสะสมภาพลามกเด็ก เป็นต้น ซึ่งจะเห็นได้ว่า ความผิดต่างๆ เหล่านี้ไม่ว่าจะเป็น การค้ายา องค์กรอาชญากรรม หรือครอบครองภาพลามกเด็ก ล้วนแล้วแต่เป็นความผิดตามกฎหมายอาญาปกติ แม้ผู้กระทำไม่ได้ใช้คอมพิวเตอร์เพื่ออำนวยความสะดวกก็ตาม (เป็นที่น่าสังเกตว่า สำหรับการมีภาพลามกอนาจารเด็กไว้ในครอบครอง แม้ไม่ได้นำไปเผยแพร่ต่อสาธารณะนั้น ตามกฎหมายไทยยังไม่ถือเป็นความผิดฐานใดๆ แต่ตามกฎหมายของนานาประเทศ รวมทั้งประเทศเยอรมัน แม้เพียงครอบครองเป็นเจ้าของโดยไม่ต้องเผยแพร่ต่อ ก็ถือเป็นความผิดตามกฎหมายแล้ว)

ดังนั้น ลักษณะของอาชญากรรมในข้อนี้ จึงยังไม่ถือเป็นปัญหาใหม่ ที่ต้อง “บัญญัติกฎหมายใหม่” ขึ้นมารองรับในส่วนนี้ จึงมีเพียงปัญหาในการแสวงหาพยานหลักฐานและตัวผู้กระทำผิดมาเพื่อพิสูจน์ความผิดเท่านั้น ที่จำต้องมีการปรับปรุงแก้ไขกฎหมายที่มีอยู่ เพื่อให้การสืบสวนสอบสวนมีประสิทธิภาพ และเหมาะสมกับเทคโนโลยีที่ก้าวหน้าต่อไป

2) *คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (Computers as a tool in the commission of a crime)* คอมพิวเตอร์เข้ามามีบทบาทหรือเป็นส่วนสำคัญที่จะทำให้การกระทำความผิดสำเร็จลงได้ ความผิดในกลุ่มนี้ส่วนใหญ่มักเป็นเรื่องของอาชญากรรมอินเทอร์เน็ต ยกตัวอย่าง เช่น การเผยแพร่ภาพลามกอนาจารหรือข้อความที่มีเนื้อหาเป็นภัยต่อสังคม หรือความมั่นคงผ่านทางเครือข่ายการพนันบนเครือข่าย การหมิ่นประมาทผู้อื่นด้วยการโฆษณาโดยอาศัยเครือข่ายอินเทอร์เน็ต การละเมิดทรัพย์สินทางปัญญาด้วยการดาวน์โหลด หรือทำซ้ำผลงานอันมีลิขสิทธิ์ต่างๆ การลักลอบหรือขโมยใช้บริการสารสนเทศ การฟอกเงินทางอิเล็กทรอนิกส์ หรือการโอนเงินที่ได้มาจากการกระทำความผิดผ่านทางอินเทอร์เน็ตเพื่อให้เกิดความยากลำบากต่อการตามหาต้นตอของเงินเหล่านั้น การฉ้อโกงผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น ซึ่งจะเห็นได้ว่า ความผิดเหล่านี้ แม้หลายๆ ฐานจะมีบัญญัติไว้ในกฎหมายอาญาปกติแล้วก็ตาม แต่ความผิดจะสำเร็จได้ผู้กระทำต้องอาศัยคอมพิวเตอร์เป็นเครื่องมือสำคัญ ซึ่งเป็นผลให้การกระทำความผิดเกิดขึ้นรวดเร็ว ตรวจสอบยาก และความเสียหายแผ่ขยายไปในวงกว้าง

ดังนั้น แม้ไม่จำเป็นต้องออกกฎหมายกำหนดฐานความผิดขึ้นใหม่ (กฎหมายสารบัญญัติ) แต่ด้วยความสลับซับซ้อนของความผิด ความยากลำบากในการผู้กระทำความผิด จึงจำเป็นต้องมีการปรับปรุงกฎหมายในส่วนของมาตรการในทางปฏิบัติ (กฎหมายวิธีสบัญญัติ) เพื่อให้สอดรับกับความผิดมากขึ้น

นอกจากนี้ในปัจจุบัน ยังปรากฏว่าวิธีการและรูปแบบของการกระทำความผิดในบางประเภท โดยเฉพาะอย่างยิ่งการละเมิดทรัพย์สินทางปัญญา ได้ถูกพัฒนาให้แตกต่างไปจากรูปแบบการกระทำความผิดเดิมๆ จนเกิดปัญหาโต้แย้งที่ยังหาข้อยุติไม่ได้ว่า การกระทำแบบนี้จะถือเป็นความผิดหรือไม่ เช่น การทำ Hyperlink Inline link หรือ Deepling Framing และ Caching หรือ Proxy Caching เป็นต้น ดังนั้น รัฐอาจจำเป็นต้องแก้ไขกฎหมายเพิ่มเติม หรือบัญญัติกฎหมายใหม่ขึ้นมาโดยเฉพาะเพื่อใช้กับ ความผิดบางฐานในกลุ่มนี้เช่นกัน (Hyperlink คือ การเชื่อมต่อเอกสารอิเล็กทรอนิกส์หนึ่ง กับเอกสารอิเล็กทรอนิกส์อื่น บนเครือข่ายอินเทอร์เน็ต ด้วยปุ่ม ข้อความ สัญลักษณ์ หรือรูปภาพ ในทางอินเทอร์เน็ต หมายถึง เส้นทางที่อ้อมไปสู่ข้อมูลที่พึงประสงค์ของผู้ใช้ และด้วยคุณสมบัติในการเชื่อมโยงนี้เอง ไฮเปอร์ลิงค์จึงกลายเป็นส่วนประกอบสำคัญของระบบ WWW จนเป็นที่มาของการขนานนามเทคโนโลยีอินเทอร์เน็ตว่า Information Superhighway แต่เดิมไฮเปอร์ลิงค์มีขึ้นเพื่ออำนวยความสะดวกในการใช้งานอินเทอร์เน็ต แต่ปัจจุบันอาจทำเพื่อลดค่าใช้จ่ายในการจัดทำเว็บไซต์ของตนเอง เพื่อหารายได้จากการโฆษณา หรือแม้แต่การดึงลูกค้ามาใช้บริการเว็บไซต์ของตนเอง Inlinelink หรือ Deeplink ต่างจากการทำไฮเปอร์ลิงค์ธรรมดา คือ แทนที่จะเชื่อมโยงไปยังหน้าเว็บไซต์ของผู้อื่นก่อน กลับเชื่อมโยงไปยังเนื้อหาในเว็บไซต์ของเขาโดยตรง ผลของการเชื่อมโยงในลักษณะนี้ ก็คือ ผู้ใช้บริการอาจไม่เห็นโฆษณา หรือไม่ทราบว่าใครเป็นเจ้าของเว็บไซต์ที่ถูกเชื่อมเหล่านั้น, คือการ “ล้อมกรอบ” พัฒนามาจากการทำไฮเปอร์ลิงค์ แต่แตกต่างกัน คือ แทนที่หน้าจอจะแทนที่ใหม่ทั้งหมดด้วยเว็บไซต์ที่ถูกลิงค์ กลับปรากฏว่าเว็บไซต์นั้นอยู่ใน “กรอบ” ของเว็บไซต์เดิม รหัส URL ก็ยังอยู่ในเว็บไซต์เดิมที่ทำเฟรมมิ่ง ผลคือ ผู้ใช้งานอินเทอร์เน็ตอาจเชื่อว่างานที่ปรากฏอยู่ในจอภาพมีต้นกำเนิดจากเว็บไซต์เดียวกัน ซึ่งน่าจะก่อให้เกิดความเสียหายต่อเจ้าของเว็บไซต์ที่ถูกดึงเข้าไปในกรอบ ตัวอย่างเช่น www.norsorpor.com, Caching หรือ Proxy Caching คือ การเก็บข้อมูลสำรองไว้เรียกใช้ เพื่อเพิ่มความเร็วในการทำงาน ซึ่งอาจถือเป็นการ “ทำซ้ำ” รูปแบบหนึ่ง เช่น ทำซ้ำแหล่งที่อยู่ ทำซ้ำแหล่งที่อยู่ ทำซ้ำเวบเพจในครั้งแรกที่เปิดเข้าไป ทั้งนี้เพื่อที่การเข้าใช้ในภายหลังจะได้รวดเร็วขึ้น การทำแบบนี้สามารถเกิดขึ้นได้ทั้งในคอมพิวเตอร์ส่วนตัว และบนเครื่องแม่ข่าย (Server) ที่เรียกว่า Proxy Caching ปกติแล้วข้อมูลที่ถูกทำซ้ำแบบ Caching นี้ จะถูกส่งผ่านแบบง่าย ๆ และถูกทิ้งไปทันทีที่การใช้คอมพิวเตอร์สิ้นสุดลง ตัวอย่างเช่น เว็บ yahoo ในเยอรมันทำซ้ำอีเมล์ของผู้ใช้อินเทอร์เน็ต จากแม่ข่ายในอเมริกา เพื่อให้ผู้ใช้อินเทอร์เน็ตในเยอรมันสามารถเรียกดูเมล์จาก yahoo ได้รวดเร็ว แทนที่จะต้องเรียกมาจากแม่ข่ายในอเมริกาโดยตรง เป็นต้น)

3) *คอมพิวเตอร์ในฐานะที่เป็นเป้าหมาย หรือวัตถุแห่งการกระทำความผิด (Computers as the target of the crime)* อาชญากรรมในลักษณะนี้ถือเป็นความผิดประเภทที่มีปัญหาทางด้านกฎหมายมากที่สุดในปัจจุบันเนื่องจากมีรูปแบบการกระทำความผิดแบบใหม่ทั้งหมดไม่ว่าจะเป็น วิธีการ หรือวัตถุที่ถูกกระทำต่อจนไม่อาจตีความกฎหมายเดิมที่มีอยู่ให้ครอบคลุมได้ และจำเป็นต้องบัญญัติกฎหมายใหม่เพื่อกำหนดฐาน

ความผิดใหม่ขึ้นมา เนื่องจากผู้กระทำความผิดมีเป้าหมายอยู่ที่ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์เป็นสำคัญทั้งนี้อาจเป็นการเข้าถึง ทำลาย เปลี่ยนแปลง หรือกระทำด้วยประการใดๆ เพื่อให้ระบบ และข้อมูลดังกล่าวได้รับความเสียหาย เปลี่ยนแปลงไปจากเดิม โดยตนเองอาจได้รับประโยชน์จากการกระทำดังกล่าวด้วยหรือไม่ก็ตาม ปัจจุบันอาจแบ่งการกระทำความผิดในกลุ่มนี้ออกได้เป็น 6 ประเภทที่สำคัญ คือ

3.1) *การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized access to information system)* การเข้าถึง ในที่นี้อาจเป็นการเข้าถึงระบบ ข้อมูล หรือ เครือข่ายประเภทต่าง ๆ โดยที่ผู้กระทำนั้นไม่มีอำนาจทั้งตามกฎหมาย สัญญา หรือข้อตกลงใดๆ ที่จะเข้าถึงได้ ผู้กระทำอาจมีมูลเหตุจูงใจแตกต่างกันไป เช่น เพื่อทดลองวิชาเอาชนะระบบป้องกันความปลอดภัยต่างๆ เพื่อจารกรรมข้อมูล แอบใช้บริการสารสนเทศฟรี หรือเพื่อสร้างความเสียหายให้กับเจ้าของระบบ หรือข้อมูลเหล่านั้น วิธีการที่ใช้กระทำมีทั้งวิธีการง่ายๆ เช่น การแอบดูรหัสผ่านโดยตรงไปจนถึงวิธีการที่มีขั้นตอน และเครื่องมือพิเศษที่ยุ่งยากซับซ้อน เช่น ใช้โปรแกรมดักรหัส หรือเครื่องมือสืบค้นรหัสผ่าน อาชญากรในกลุ่มการกระทำความผิดนี้ จึงมีตั้งแต่นักเรียนนักศึกษา มือสมัครเล่น พวกก่อกวนระบบ ไปจนถึงมืออาชีพที่กระทำเพื่อผลประโยชน์อย่างใดอย่างหนึ่งโดยเฉพาะ เช่น ตัวอย่างคดีที่เกิดขึ้นในปี พ.ศ.2528 ณ มลรัฐ New Jersey มีเด็กนักเรียนชาย 7 คน ได้ทำการเจาะระบบเข้าไปที่คอมพิวเตอร์ของหน่วยงานแพนทากอน ปี พ.ศ.2528 แพนทากอน รายงานว่าระบบคอมพิวเตอร์ของหน่วยงานถูกโจมตีถึง 250,000 ครั้ง และ 65% คือการพยายามเข้าถึงระบบเท่านั้น ในประเทศไทยเองก็เคยมีอาจารย์มหาวิทยาลัยโดนเจาะระบบเพื่อขโมยข้อสอบ และเฉลยซึ่งเก็บไว้ในคอมพิวเตอร์ส่วนตัวที่มหาวิทยาลัยผ่านทางระบบ LAN เป็นต้น และมีรายงานว่าบริษัทโทรศัพท์ถือเป็นเป้าหมายยอดนิยมที่สุดสำหรับนักเจาะระบบ ทั้งนี้เพราะมีจุดอ่อนค่อนข้างมาก และผู้เจาะได้ประโยชน์จากการใช้บริการฟรี

ตัวอย่างฐานความผิดที่สำคัญ และเป็นที่รู้จักที่สุดในความผิดกลุ่มนี้ คือ การเจาะระบบ (Hacking and Cracking) หมายถึง การเข้าไปในระบบคอมพิวเตอร์โดยไม่มีอำนาจ ซึ่งอาจเป็นกรณีการเข้าถึงในระดับกายภาพ คือ กรณีผู้กระทำความผิดดำเนินการโดยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านและใช้เครื่องคอมพิวเตอร์ของผู้อื่นนั้นโดยตรง หรืออาจเป็นกรณีการเข้าถึงโดยผู้กระทำความผิดอยู่ห่างโดยระยะทาง เช่น การเจาะระบบผ่านทางเครือข่ายอินเทอร์เน็ต อินทราเน็ต หรือ ระบบ LAN การเข้าถึงระบบ หรือข้อมูลคอมพิวเตอร์โดยผู้กระทำมิได้มีเหตุจูงใจ หรือต้องการทำให้เกิดความเสียหายต่อระบบ หรือข้อมูลเลย เรียกว่า Hacking ส่วนกรณีที่เข้าไปโดยมีมูลเหตุเพื่อทำลาย หรือก่อให้เกิดความเสียหายต่อระบบ หรือข้อมูลด้วยจะเรียกว่า Cracking นอกจากนี้ยังมีวิธีการอื่นๆ ที่ใช้กันอยู่ เช่น Superzapping และ Piggybacking เป็นต้น Superzapping คือ การกระทำความผิดด้วยการใช้เครื่องมือของระบบที่ทำให้สามารถเข้าไปในระบบคอมพิวเตอร์ได้ในกรณีฉุกเฉินเปรียบเสมือนกุญแจผีที่จะนำมาใช้ก็ต่อเมื่อกุญแจดอกหลักหายหรือมีปัญหา โดยมาจากคำว่า Superzap ซึ่งเป็นโปรแกรม macro-utility ที่นิยมใช้มากในศูนย์คอมพิวเตอร์ของบริษัท IBM ตัวอย่างความผิดที่พบ คือ กรณีผู้ครอบครอง หรือรู้วิธีใช้ system tool ดังกล่าว เข้าไปในระบบ แล้วเปลี่ยนแปลงเงินในกองทุน หรือเปลี่ยนข้อมูลบางอย่างเพื่อประโยชน์ต่อตนเอง Piggybacking มี 2 ลักษณะด้วยกันคือ 1) Physical (ทางกายภาพ) ผู้กระทำความผิดจะลักลอบ หรือหาวิธีเข้าไปในเขตควบคุม ซึ่งอาจ

ควบคุมด้วยประตูไฟฟ้า หรือเครื่องกล โดยรอให้บุคคลที่มีอำนาจมาใช้ประตู เมื่อประตูเปิดผู้กระทำความผิดจะฉวยโอกาสตอนประตูยังไม่ปิดสนิทเข้าไปด้วย เป็นต้น และ 2) Electronic (ทางอิเล็กทรอนิกส์) ซึ่งอาจเกิดขึ้นได้กรณีที่เมื่อมีการใช้สายการสื่อสารเดียวกันกับผู้ได้รับอนุญาต เช่น ใช้สายเคเบิลหรือผ่านโมเด็ม เป็นต้น

3.2) *การดักข้อมูลคอมพิวเตอร์ (computer interception)* คือ การดักข้อมูลหรือสิ่งต่างๆ ที่ได้มาจากการปฏิบัติการทางคอมพิวเตอร์ ซึ่งอาจเป็นตัวเนื้อหาข้อมูลจราจร หรือรหัสผ่านต่างๆ วิธีการที่ใช้มี 2 ลักษณะใหญ่ๆ คือ ด้วยการเข้าถึงระบบคอมพิวเตอร์ก่อน แล้วจึงดักข้อมูล และด้วยการใช้เครื่องมือพิเศษเพื่อใช้ในการดักข้อมูล โดยไม่ต้องเข้าไปในระบบคอมพิวเตอร์ เช่นการดักข้อมูลที่กำลังมีการส่งผ่านให้แก่กันบนเครือข่าย โดยวิธีหลังนี้จะง่ายกว่าวิธีแรก ในขณะที่การตรวจพบทำได้ยากกว่า เพราะหาร่องรอยลำบาก มูลเหตุจูงใจของการดักข้อมูล ส่วนมากมักเป็นไปเพื่อประโยชน์อย่างใดอย่างหนึ่งต่อตัวเอง หรือผู้อื่น ดังเช่นคดีที่เคยเกิดการฟ้องร้องในโครงการก่อสร้างระบบรถไฟความเร็วสูงในประเทศเกาหลีใต้ บริษัทของประเทศฝรั่งเศสซึ่งเข้าร่วมประมูลโครงการ เคยดักข้อมูลของ บริษัท Siemens ของประเทศเยอรมัน ซึ่งเป็นคู่แข่งเพื่อตรวจสอบว่าราคาที่บริษัทเยอรมันเสนออยู่ที่เท่าไหร่ และทางฝรั่งเศส จะได้เสนอราคาที่ต่ำกว่าเพื่อชนะการประมูล เป็นต้น สำหรับรูปแบบ และวิธีการที่รู้จักกันในกลุ่มนี้ คือการทำ Trap Doors หรือที่เรียกว่า “กับดัก” คือ การกระทำความผิดด้วยการเขียนโปรแกรมเลียนแบบ ให้คล้ายกับหน้าจอปกติของระบบคอมพิวเตอร์ เพื่อลวงให้มีผู้เข้ามาใช้คอมพิวเตอร์ ทำให้ผู้กระทำผิดทราบรหัสประจำตัวของผู้ใช้ (ID number) หรือทราบรหัสผ่าน (password) จากการป้อนข้อมูลของผู้ใช้ผ่านทางหน้าจอลวงให้ login prompt หลังจากได้ข้อมูลแล้ว โปรแกรมนี้จะถูกเก็บบันทึกไว้ในไฟล์ลับ แล้วกลับคืนหน้าจอที่แท้จริงมาให้ผู้ใช้ได้ใช้งานใหม่ และเมื่อได้รหัสประจำตัว หรือรหัสผ่านแล้ว ผู้กระทำความผิดก็สามารถสวมรอยเข้าไปถึงข้อมูลอื่นๆ ของเหยื่อได้ ตัวอย่างความผิดที่พบบ่อย คือ การลักใช้เวลา หรือบริการทางอิเล็กทรอนิกส์ต่างๆ เช่น แอบใช้เวลาอินเทอร์เน็ต ส่วนวิธีการอื่นๆ ที่ใช้กันอยู่ในปัจจุบัน เช่น วิธีการที่เรียกว่า Data Leakage และ Wiretapping หรือ Packet Sniffer เป็นต้น (Data Leakage คือ การกระทำที่ปราศจากอำนาจ แอบซ่อนเร้นนำข้อมูลออกไป หรือทำสำเนาข้อมูลจากระบบคอมพิวเตอร์ หรือด้วยการดักข้อมูลในระหว่างที่ผู้ใช้ทำข้อมูลรั่วไหลออกไปโดยไม่ตั้งใจ เช่น เกิดจากการฟุ้งกระจายของคลื่นอิเล็กทรอนิกส์ในขณะกำลังทำงาน ผู้กระทำผิดอาจใช้เครื่องดักสัญญาณ มาตั้งในบริเวณใกล้เคียงกับคอมพิวเตอร์ที่ทำงานอยู่ เพื่อดักข้อมูลดังกล่าว ความผิดที่เจอมักเป็นกรณีการจารกรรมข้อมูลของสายลับ ความผิดนี้อาจถือว่าอยู่ในกลุ่มการจารกรรมข้อมูลด้วย, Wiretapping หรือ Packet Sniffer คือ การกระทำความผิดด้วยการลักลอบดักฟังสัญญาณการสื่อสารโดยเจตนาที่จะรับประโยชน์จากการเข้าถึงข้อมูล โดยผ่านวงจรการสื่อสาร (communication circuit) และจากการที่ในปัจจุบันมีผู้ใช้อินเทอร์เน็ตจำนวนมาก ทำให้อาชญากรรมประเภทนี้ทำได้ง่าย และรวดเร็วมากยิ่งขึ้น ทั้งนี้เนื่องจากมีการใช้เส้นทางร่วมกันของข้อมูลจำนวนมาก (information superhighway) การกระทำลักษณะนี้จึงมีจำนวนเพิ่มมากขึ้น โปรแกรม Sniffer สามารถใช้ดักเลขประจำตัว และรหัสผ่านเข้าระบบรวมทั้งข้อมูลบัตรเครดิต และข้อมูลอีเมล์ส่วนบุคคล เพื่อนำไปใช้เข้าถึงที่อยู่อื่น ๆ ต่อไป การกระทำผิดด้วยวิธี

นี้ ปกติผู้กระทำต้องมีอุปกรณ์พิเศษช่วยในการดักรับสัญญาณ หรืออย่างน้อยที่สุดต้องมีโมเด็ม เพื่อใช้ร่วมกับเครื่องคอมพิวเตอร์)

3.3) *การจารกรรมข้อมูลคอมพิวเตอร์ (computer espionage)* ความผิดลักษณะนี้จะคล้ายๆ กับการดักข้อมูล กล่าวคือ มีการลักเอาไปซึ่งข้อมูลคอมพิวเตอร์ของผู้เสียหาย เพียงแต่วิธีการจะไม่ใช่แค่เพียงแอบดักเอา ซึ่งอาจไม่ต้องเข้าถึงระบบคอมพิวเตอร์ก่อน หรือสามารถดักเอาในระหว่างการติดต่อสื่อสาร ในการจารกรรมผู้กระทำความผิดจะต้องเข้าไปในระบบคอมพิวเตอร์ เพื่อค้นหากลุ่มข้อมูลที่ถูกเก็บไว้ในคอมพิวเตอร์ที่ตนเองต้องการ แล้วทำซ้ำออกไป ข้อมูลส่วนใหญ่ที่มักโดยจารกรรม คือ ความลับทางการค้า ข้อมูลทางเศรษฐกิจ ข้อมูลของลูกค้า ข้อมูลทางอุตสาหกรรม หรือ ทรัพย์สินทางปัญญา ตัวอย่างคดีใหญ่ ๆ ที่เกี่ยวกับการกระทำในลักษณะนี้ คือ ปี พ.ศ. 2529 มีนักเจาะระบบเข้าไปในคลังข้อมูลของประเทศสหรัฐอเมริกา แล้วจารกรรมข้อมูลความรู้ต่างๆ เพื่อนำไปขายให้กับ KGB เบอร์ลินตะวันออก เป็นต้น รูปแบบการจารกรรมข้อมูลที่เป็นที่รู้จักในปัจจุบันคือ Scavenging หรือการกระทำความผิดด้วยวิธีการที่คล้ายกับคุ้ยเขี่ยขยะ เพื่อหาของที่ยังมีประโยชน์ใช้ได้ โดยเที่ยวค้นหาไปตามสถานที่ที่เชื่อว่ามีการเก็บข้อมูล (computer storage area) รวมทั้งการหาจากถังขยะในบริเวณใกล้ๆ กับเครื่องคอมพิวเตอร์ เพราะผู้ใช้บางคนอาจจดข้อมูลสำคัญหรือพิมพ์สำเนาบางอย่างเกินจำเป็น จดหมายเลขประจำตัว หรือรหัสผ่านเป็นกระดาษ แล้วทิ้งในถังขยะโดยไม่ทำลาย เมื่อได้ข้อมูลไปแล้วก็จะนำไปสวมรอยใช้บริการต่างๆ ทางอิเล็กทรอนิกส์ต่อไป นอกจากนี้ ก็มีวิธีที่เรียกว่า Data Leakage ดังเคยกล่าวไปแล้วในกรณีการดักข้อมูลนั่นเอง สำหรับปัญหาด้านกฎหมายในเรื่องนี้ คงเป็นเช่นเดียวกับการดักข้อมูล คือ การตีความกับความผิดฐาน “ลักทรัพย์” ซึ่งในที่สุดจำเป็นต้องมีการบัญญัติกฎหมายใหม่ขึ้นมารองรับโดยเฉพาะเช่นกัน

3.4) *การก่อวินาศกรรมทางคอมพิวเตอร์ (computer sabotage)* คือ การกระทำด้วยวิธีการใดๆ เช่น การนำเข้า แก้ไข เปลี่ยนแปลง ลบ ทำลาย เพื่อรบกวน ขัดขวาง แทรกแซง ให้ระบบคอมพิวเตอร์หยุดทำงาน หรือทำความเสียหายต่อข้อมูลต่างๆ ที่อยู่ในคอมพิวเตอร์ วิธีการที่ผู้กระทำความผิดมักจะใช้ คือใช้ Crash Program หรือโปรแกรมอันตรายต่างๆ แอบแฝง หรือส่งเข้าไปแทรกแซงในระบบคอมพิวเตอร์ของผู้เสียหาย โปรแกรมอันตรายที่เป็นที่รู้แพร่หลายมากที่สุด คือ Virus ซึ่งเป็นโปรแกรมที่จะปรากฏขึ้นในแฟ้มทำงานจริง หลังจากปรากฏขึ้นแล้ว แฟ้มดังกล่าวจะทำหน้าที่ที่แตกต่างจากเดิม เช่น แสดงข้อความบางอย่างบนจอ แฟ้มหรืองานทั้งหมดหรือบางส่วนถูกเปลี่ยนแปลง หรือถูกทำลายไป ไวรัสจะมีลักษณะสำคัญ 2 ประการ คือ 1) มีความสามารถในการแพร่กระจายโดยติดตัวเองกับแฟ้มข้อมูลหรือระบบปฏิบัติการ และ 2) ไวรัสจะสามารถสร้างความเสียหายได้ก็ต่อเมื่อปรากฏขึ้นในแฟ้ม และแฟ้มดังกล่าวถูกเปิดใช้งานแล้วเท่านั้น ไวรัสตัวแรกถูกเขียนขึ้นเมื่อปี พ.ศ.2526 เพื่อเป็นแบบฝึกหัดสำหรับนักศึกษา แต่ไวรัสตัวที่ถูกเขียนขึ้นโดยมีเจตนาเพื่อกระทำความผิด เกิดขึ้นเมื่อปี พ.ศ.2529 ที่เมือง Lahore ประเทศปากีสถาน และปี พ.ศ.2533 ไวรัสเริ่มเข้ามาแพร่กระจายในอินเทอร์เน็ต จนในช่วงปี พ.ศ.2543 มีการประมาณกันว่า มีไวรัสคอมพิวเตอร์เกิดใหม่ทุกวัน ๆ ละ 10 ถึง 15 ตัว

นอกจากการก่อวินาศกรรมโดยใช้โปรแกรมไวรัสแล้ว ปัจจุบันยังมีโปรแกรมอันตรายตัวอื่นๆ ที่เริ่มเป็นที่รู้จักกันอย่างกว้างขวาง เช่น Trojan Horse, Logic Bombs หรือ Time Bombs, Jamming หรือ Flooding และ Worms เป็นต้น สำหรับปัญหาทางด้านกฎหมายในการกระทำความผิดฐานนี้ จะคล้ายคลึงกับการดักและจารกรรมข้อมูล คือ ปัญหาเรื่องการตีความคำว่า “ทรัพย์” เพียงแต่เป็นการตีความในความผิดฐาน “ทำให้เสียทรัพย์” ไม่ใช่ “ลักทรัพย์” เพราะผู้กระทำความผิดมิได้มุ่งหวังที่จะนำเอาข้อมูลคอมพิวเตอร์ไปคง เป็นแต่เพียงต้องการสร้างความเสียหายให้กับระบบ และข้อมูลของผู้เสียหายเท่านั้น อย่างไรก็ตามมีการบัญญัติการกระทำความผิดฐานนี้ไว้ในกฎหมายที่รู้จักกันในฐานความผิด Computer sabotage เป็นต้น (Trojan Horse คือ การกระทำความผิดด้วยการเขียนโปรแกรมคอมพิวเตอร์ที่น่าใช้และมีประโยชน์ โดยแอบแฝงชุดคำสั่งที่พร้อมจะทำลายข้อมูล และซอฟแวร์ตัวอื่นไปด้วย เมื่อถึงเวลา โปรแกรมที่ไม่ดีจะปรากฏตัวขึ้นเพื่อปฏิบัติการทำลายข้อมูล หรือทำให้ข้อมูลเกิดความเสียหาย ตัวอย่างที่พบมักอยู่ในรูปของซอฟต์แวร์ประเภท shareware หรือ freeware คำว่า “Trojan Horse” เป็นชื่อที่มาจากนิยายกรีกโบราณ ซึ่งเป็นเรื่องการทำสงครามระหว่างกองทัพกรีก กับเมืองโทรจัน (บางคนรู้จักในชื่อ “เมืองทรอย”) ฝ่ายกรีกซึ่งเป็นฝ่ายรุกแกล้งทำอุบายว่าแพ้แล้วหนีไปโดยทิ้งม้าไว้ที่ซ่อนทหารกรีกไว้ในนั้น ฝ่ายโทรจัน ไม่รู้กลอุบาย จึงเปิดประตูเมืองแล้วเอาม้าเข้าไปในเมือง จัดงานเฉลิมฉลองจนเมามาย พอตกกลางคืนทหารที่ซ่อนอยู่จึงออกมาเปิดประตูเมืองเพื่อให้กองทัพกรีกเข้าไป เป็นผลให้ฝ่ายโทรจันพ่ายแพ้และถูกยึดเมืองในที่สุด, Logic Bombs หรือ Time Bombs คือ การกระทำความผิด ด้วยการเขียนโปรแกรมคำสั่งอย่างมีเงื่อนไข ซึ่งโปรแกรมนั้นจะเริ่มทำงานเมื่อมีสภาวะ เวลา หรือมีสภาพการณ์ตรงตามที่ผู้สร้างโปรแกรมกำหนดเป็นเงื่อนไขเอาไว้ ซอฟต์แวร์พวกนี้จะมีความฉลาดแฝงอยู่ สามารถติดตามดูความเคลื่อนไหวของระบบบัญชี ระบบเงินเดือน แล้วทำการเปลี่ยนแปลงตัวเลขเหล่านั้นให้ตรงกับความต้องการของมัน ความสามารถอื่นๆ เช่น reformatted hard disk เป็นต้น ตัวอย่างความผิดที่พบมักเป็นการเปลี่ยนแปลงเรคคอร์ดเงินเดือนของผู้สร้างโปรแกรมนั้นๆ เอง โดยทำให้เงินเพิ่มขึ้นพร้อมๆ กันหลายๆ เรคคอร์ดเพื่อป้องกันการจับพิรุธได้ Logic Bombs มักถูกแฝงมากับโปรแกรมอื่นๆ ในรูปแบบของ Trojan Horse นั่นเอง, Jamming หรือ Flooding คือ การกระทำความผิดด้วยการทำให้คอมพิวเตอร์ตัวให้บริการอินเทอร์เน็ตเต็มไปด้วยคำขอของเว็บเพจแบบปลอมๆ มีผลทำให้เครื่อง Server นั้น ปฏิเสธผู้ใช้ปกติที่ต้องการขอใช้บริการ หรือ ดาวน์โหลดข้อมูลจริงๆ หรืออาจทำให้คอมพิวเตอร์ตัวที่ให้บริการอยู่นั้นเสียหาย วิธีการนี้เรียกอีกอย่างหนึ่งว่า การโจมตีด้วยการปฏิเสธการให้บริการ (Denial of Service (DoS) Attack) เช่น การส่งคำขอปลอมไปยังเว็บโฆษณาจำนวนมาก ทำให้เว็บนั้นโหลดข้อมูลเกิน จนไม่สามารถให้บริการต่อไปได้ Worms คือ โปรแกรมที่เพิ่มจำนวนด้วยตัวของมันเอง ความแตกต่างระหว่างไวรัสกับเวิร์ม คือ ไวรัสจะไม่เพิ่มจำนวนด้วยตัวเอง แต่จะถูกทำซ้ำเพียงเมื่อแฟ้มที่ทำงานนั้นถูกเปิดเพื่อใช้งาน ในขณะที่เวิร์มเป็นโปรแกรมเดี่ยว ๆ ที่สามารถเพิ่มจำนวน และแพร่กระจายได้เองโดยไม่ต้องอาศัยการทำงานของมนุษย์ ปกติแล้วเวิร์มรูปแบบเดิม จะไม่เปลี่ยนแปลงข้อมูลในแฟ้ม แต่จะทำลายด้วยการเพิ่มจำนวนตัวเองขึ้นหลายเท่า ทำให้พื้นที่ในคอมพิวเตอร์ของผู้เสียหายเต็ม ซึ่งการปล่อยเวิร์มในเครือข่ายอินเทอร์เน็ต ก็จะมีผลทำให้อินเทอร์เน็ตทำงานช้าลง

3.5) *การปลอมข้อมูลคอมพิวเตอร์ (computer forgery)* คือ การกระทำความผิดด้วยการปลอมข้อมูลคอมพิวเตอร์ทั้งหมดหรือบางส่วน ด้วยการแก้ไขเปลี่ยนแปลง หรือทำด้วยประการอื่นใด เพื่อให้ผู้อื่นหลงเชื่อว่าข้อมูลเหล่านั้นเป็นข้อมูลที่ถูกต้องแท้จริง ทั้งนี้นอกจากการกระทำในลักษณะนี้จะสร้างความเสียหายต่อระบบความน่าเชื่อถือในเอกสารข้อมูลต่างๆ ที่อาจมีผลกระทบต่อสังคม เศรษฐกิจโดยรวมแล้ว ในบางกรณีอาจก่อให้เกิดอันตรายต่อชีวิต และร่างกายได้อีกด้วย ดังเช่นที่เคยเกิดขึ้นกับโรงพยาบาลแห่งหนึ่ง ซึ่งมีผู้เจาะระบบเข้าไปในฐานข้อมูลผู้ป่วย แล้วทำการแก้ไขเปลี่ยนแปลงรายการยาที่รักษา จนเป็นผลให้เกิดการจ่ายยาผิดพลาดกับผู้ป่วย และเป็นอันตรายต่อชีวิต เป็นต้น ตัวอย่างรูปแบบและวิธีการการเข้าถึงระบบเพื่อปลอมแปลงข้อมูลนี้ คือการกระทำความผิดที่เรียกว่า Asynchronous Attack หรือการกระทำโดยอาศัยจุดอ่อนที่เกิดขึ้นจากการทำงานของระบบปฏิบัติการคอมพิวเตอร์ซึ่งเป็นแบบ Multi Processing คือ สามารถทำงานหลายอย่างได้พร้อมกันในเวลาเดียวกัน ซึ่งจะแยกการทำงานแต่ละอย่างออกไปและไม่ต้องเข้าคิวทำงานตามลำดับก่อนหลัง การประมวลผลข้อมูลจะเสร็จไม่พร้อมกัน งานที่เสร็จแล้วผู้ใช้อาจจะยังไม่ทราบผลทันทีจนกว่าจะเรียกข้อมูล ในขั้นตอนนี้เองจึงมีจุดอ่อนเกิดขึ้น ซึ่งผู้กระทำความผิดจะฉวยโอกาสในระหว่างเครื่องทำงาน เข้าไปแก้ไขเปลี่ยนแปลง หรือกระทำการใด ๆ ต่องานในคอมพิวเตอร์โดยผู้ใช้ไม่อาจทราบได้เลยว่ามีการกระทำผิดเกิดขึ้นแล้ว

3.6) *การฉ้อโกงทางคอมพิวเตอร์ (computer frauds)* คือ การกระทำด้วยวิธีการใดๆต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เพื่อให้ระบบนั้นทำงานหรือแสดงผลที่ผิดพลาด หรือผิดปกติไปจากเดิมหรือที่ควรจะต้องแสดง จนเป็นเหตุให้ผู้กระทำนั้นได้ประโยชน์ในทางทรัพย์สินอย่างหนึ่งอย่างใดไปโดยมิชอบด้วยกฎหมาย โดยวิธีการทำให้คอมพิวเตอร์แสดงผลผิดไปจากเดิม เช่น การสร้างโปรแกรมคอมพิวเตอร์หรือแก้ไขเปลี่ยนแปลงโปรแกรมบางอย่างเพื่อให้คอมพิวเตอร์ปฏิบัติการตามความต้องการของตนเอง ตัวอย่างการกระทำความผิดที่เป็นที่รู้จักกันในปัจจุบัน คือ Salami Techniques หรือการกระทำความผิดด้วยการปัดเศษของจำนวนเงินทศนิยมตัวที่สาม หรือปัดเศษทิ้งให้เหลือแต่จำนวนเงินที่สามารถจ่ายได้ง่าย แล้วนำเศษทศนิยมมาใส่ไว้ในบัญชีของตนเอง หรือผู้อื่น ในขณะที่ผลรวมของบัญชียังคงสมดุล (balance) ตลอดเวลา ตัวอย่างคดีที่พบมักเกิดขึ้นในวงการธนาคาร โดยผู้กระทำความผิด คือโปรแกรมเมอร์ของธนาคารนั้นๆ เอง การฉ้อโกงอีกรูปแบบหนึ่งที่พบ คือ Simulation และ Modeling วิธีการทั้งสองนี้ มีความคล้ายคลึงกัน แต่มีลักษณะแตกต่างกันที่สำคัญ โดย Simulation คือ การพยายามสร้าง หรือสมมติเหตุการณ์ที่เกิดขึ้นให้ใกล้เคียงกับความเป็นจริงที่เกิดขึ้น ในขณะที่ Modeling คือ สิ่งที่มีการออกแบบแตกต่างออกไป และพยายามสร้างของจริงขึ้นมาให้เหมือนกับแบบ หรือหุ่นจำลองที่ได้ทำขึ้น เช่น แบบบ้านจำลอง หรือแบบเครื่องบินจำลอง แม้ด้วยวิธีการทั้งสองนี้ คอมพิวเตอร์อาจถูกใช้เป็นเครื่องมือในการวางแผนการควบคุมและติดตามความเคลื่อนไหวในการประกอบอาชญากรรมได้ แต่ในทางกลับกันผู้กระทำความผิดก็สามารถสร้างแบบจำลอง เพื่อวางแผนประกอบอาชญากรรมได้เช่นกัน ตัวอย่างเช่น มีการสร้างแบบจำลองในการปฏิบัติการ หรือช่วยในการตัดสินใจในการทำกรมธรรม์ประกันภัย ด้วยการจัดทำกรมธรรม์ปลอมขึ้นมา เป็นต้น

เนื่องจากการ “ฉ้อโกงทางคอมพิวเตอร์” มีลักษณะสำคัญประการหนึ่งที่แตกต่างไปจากความผิดฐานฉ้อโกงธรรมดาตามกฎหมายอาญา คือ การฉ้อโกงคอมพิวเตอร์เป็นการหลอก หรือกระทำต่อระบบคอมพิวเตอร์ ในขณะที่การฉ้อโกงธรรมดาจะเป็นการกระทำต่อบุคคล หรือพูดง่าย ๆ คือ ผู้กระทำผิดทำการหลอกลวงคน เพื่อให้ตนเองได้ประโยชน์ในทางทรัพย์สิน ซึ่งปัจจุบันอาจใช้คอมพิวเตอร์เป็นเครื่องมือด้วยก็ได้ (บางคนจึงอาจเกิดความสับสนกับการฉ้อโกงทางคอมพิวเตอร์) เช่น การทำ Fisching หรือPhishing ที่กำลังแพร่หลาย ก็เป็นวิธีการฉ้อโกงรูปแบบใหม่ ที่ผู้กระทำผิดจะใช้วิธีส่งข้อความที่จะหลอกผู้เสียหาย (บุคคล) มาทางอีเมล์ ส่วนมากจะหลอกว่าส่งมาจากธนาคารหรือสถาบันการเงินที่บุคคลนั้นเป็นลูกค้าอยู่ และอ้างว่าเกิดปัญหาที่ทางธนาคารต้องจัดการข้อมูลใหม่ จำเป็นต้องขอรหัส หรือข้อมูลเพิ่มเติมจากลูกค้า เมื่อลูกค้าคนใดหลงเชื่อแล้วส่งข้อมูลกลับไป ข้อมูลเหล่านั้นก็จะถูกนำไปใช้ประโยชน์ หรือถอนเงินออกไปจากบัญชีด้วยวิธีการง่ายๆ แบบนี้ มีรายงานว่า คนอเมริกันที่มีบัญชีออนไลน์ (Banking-Online) ถูกหลอกให้มีการโอนเงินไปแล้วนับล้านคน โดยมีความเสียหายรวมหลายพันล้านดอลลาร์สหรัฐ อย่างไรก็ตาม ด้วยการทำ Fisching นี้ เรายังไม่เห็นว่าเป็นวิธีการที่อยู่ในกลุ่ม “ฉ้อโกงทางคอมพิวเตอร์” เพราะยังมีลักษณะของการหลอกบุคคลธรรมดาอยู่ ซึ่งหากติดตามหาตัวผู้กระทำความผิดได้ ก็สามารถเอาผิดตามกฎหมายอาญาปกติได้

การฉ้อโกงที่จะเข้าความหมายในความผิดกลุ่มนี้ คือ การที่ผู้กระทำหลอก “ระบบคอมพิวเตอร์” คือ มีคอมพิวเตอร์มีเป้าหมายของการกระทำความผิดนั่นเอง เช่นเขียนโปรแกรมปัดเศษเงินดังกล่าวมาแล้ว เมื่อเป้าหมายที่ถูกกระทำเป็นคนละอย่างกัน ในหลายๆ ประเทศจึงได้บัญญัติฐานความผิดขึ้นมาเพื่อใช้กับการฉ้อโกงทางคอมพิวเตอร์นี้โดยเฉพาะเจาะจง

2.3) ความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ต

ความเสียหายที่เกิดขึ้นจากอาชญากรรมทันสมัยเหล่านี้มีมากมาย แต่อาจจำแนกกลุ่มให้เหลือเพียง 2 กลุ่มใหญ่ คือ

1) ความเสียหายที่ประเมินค่าเป็นเงินได้ เช่น ความเสียหายจากการสูญเสียรายได้ กำไรจากการขายผลิตภัณฑ์ ค่าซ่อมแซมระบบคอมพิวเตอร์ ค่าจัดการข้อมูลที่สูญหายหรือถูกทำลายไป ค่าจัดการระบบรักษาความปลอดภัยใหม่ รวมทั้งความสูญเสียความเชื่อถือจากลูกค้า และค่าเสียโอกาสอื่น ๆ

2) ความเสียหายที่มิอาจประเมินค่าเป็นเงินได้ เช่น ความเสียหายต่อสังคม เศรษฐกิจ การเมือง ระบบอำนวยความยุติธรรม ขนบธรรมเนียมหรือศีลธรรมอันดีของประชาชน ความเสียหายต่อสิทธิความเป็นส่วนตัว รวมทั้งความเสียหายแฝงอื่นๆ เช่น ราคาสินค้าสูงขึ้น เนื่องจากเพราะผู้ประกอบการที่เกิดความเสียหายมักจะผลักภาระให้แก่ผู้บริโภค เป็นต้น

2.4) การสืบหาตัวผู้กระทำความผิดทางคอมพิวเตอร์ / อินเทอร์เน็ต

อาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ตกำลังสร้างความเสียหายอย่างมาก ปัจจุบันประเทศต่าง ๆ จึงจำต้องช่วยกันหาทางรับมือกับอาชญากรรมเหล่านี้กันอย่างเร่งด่วน เพียงแต่ในที่สุดแล้ว หลายประเทศก็ยัง

ประสบปัญหาต่างๆ ในการป้องกันและปราบปรามการกระทำความผิดชนิดนี้อยู่ดี โดยอาจแยกสภาพปัญหาออกได้เป็น 3 ส่วน ดังต่อไปนี้

1) สภาพปัญหาในส่วนของมาตรการตามกฎหมายสารบัญญัติ (กฎหมายที่กำหนดเนื้อหาสาระของฐานความผิดต่าง ๆ เช่น ไม่อาจตีความกฎหมายเก่าได้เนื่องเพราะ มีลักษณะการกระทำ เครื่องมือ และวิธีการอันเป็นองค์ประกอบความผิดที่แตกต่างออกไปจากการกระทำความผิดในรูปแบบเดิม จนที่สุดต้องบัญญัติกฎหมายขึ้นมาใหม่เพื่อรับมือกับปัญหาที่เกิดขึ้น

2) สภาพปัญหาในส่วนของมาตรการตามกฎหมายวิธีสบัญญัติ (กฎหมายที่ว่าด้วยวิธีการในทางปฏิบัติหรือใช้บังคับกฎหมายสารบัญญัติ) แบ่งย่อยออกเป็นปัญหา 3 ด้าน คือ ความยากลำบากในการระบุตัวผู้กระทำความผิดเพื่อติดตามจับกุมมาดำเนินคดี อุปสรรคในการแสวงหารวบรวม และรับฟังพยานหลักฐานอิเล็กทรอนิกส์ ที่สามารถถูกแก้ไขเปลี่ยนแปลง หรือสูญหายทำลายได้ในเวลาอันรวดเร็ว และปัญหาความรู้ความสามารถของเจ้าหน้าที่ไม่เพียงพอหรือยังไม่ทัดเทียมกับอาชญากรมืออาชีพทั้งหลาย

3) สภาพปัญหาในส่วนของมาตรการทางกฎหมาย และความร่วมมือระหว่างประเทศ เช่น ฐานความผิดตามกฎหมายของแต่ละประเทศที่แตกต่างกัน อันนำไปสู่ปัญหาการให้ความช่วยเหลือทางกฎหมายอาญา รวมทั้งปัญหาการส่งผู้ร้ายข้ามแดน ปัญหาเกี่ยวกับเขตอำนาจศาล ทั้งนี้เพราะการกระทำความผิดในลักษณะนี้ โดยเฉพาะอย่างยิ่งการกระทำผ่านเครือข่ายอินเทอร์เน็ต มักมีความเกี่ยวพันกับเขตอำนาจศาลของหลายประเทศ เช่น ผู้กระทำอยู่ในประเทศหนึ่ง แต่ผลของการกระทำเกิดขึ้นในอีกประเทศหนึ่ง เป็นต้น

2.5) แนวทางในการดำเนินการเกี่ยวกับเว็บไซต์ที่ผิดกฎหมาย

เว็บไซต์ ถือเป็นระบบการติดต่อสื่อสารจากการพัฒนาเทคโนโลยีสมัยใหม่ โดยมีลักษณะเป็นเครือข่ายเชื่อมโยงซึ่งกันและกันแบบไร้พรมแดน จากจุดนี้เองทำให้มีการใช้ประโยชน์ทางด้านข้อดีของการติดต่อสื่อสารทางอินเทอร์เน็ตมาประยุกต์ใช้กับอาชญากรรมรูปแบบใหม่ ที่กำลังเกิดขึ้น เช่น การสร้างเว็บไซต์ที่ผิดกฎหมาย การลงข้อความใส่ร้ายผู้อื่น การนำคลิปวีดีโอไปเผยแพร่ต่อสาธารณะ การหลอกลวงให้ผู้ใช้บริการหลงเชื่อเกี่ยวกับข้อมูลที่แสดงอยู่เป็นต้น

ดังนั้น การแก้ไขปัญหา ป้องกัน และปราบปราม อันสืบเนื่องมาจากการใช้เทคโนโลยีการสื่อสารเพื่อจุดประสงค์ที่จะทำลาย หรือหวังผลประโยชน์ใด ๆ ก็ตาม ปัจจุบันได้มีปัญหาที่เกิดขึ้นกับ Web site ผิดกฎหมาย ซึ่งมีแนวโน้มความรุนแรงเพิ่มขึ้น สามารถจำแนกออกเป็นดังนี้ (เชาวลิต อัตถศาสตร์, 2554)

1) การจัดทำ Web site เพื่อวัตถุประสงค์ในการกระทำความผิดโดยตรง เช่น การสร้าง web site เพื่อจำหน่ายสินค้าที่ผิดกฎหมาย สร้างช่องทางสำหรับการติดต่อ แลกเปลี่ยน แจ้งข้อมูลที่มีจุดประสงค์ในทางที่ไม่ดี รวมไปถึงการหลอกลวงผู้ที่เข้ามาใช้บริการให้หลงเชื่อว่าเป็นผู้ให้บริการจริง

2) การใช้ Web site ผู้อื่นกระทำผิดต่อบุคคลที่สามให้เกิดความเสียหาย เช่น การนำรูปภาพผู้อื่นไปเผยแพร่ในทางที่ผิด การส่งข้อความ หรือประกาศข้อความที่ให้ผู้อื่นเสื่อมเสีย

ชนิดของ Web site ที่มีอยู่ในปัจจุบัน ได้แก่

1) *เว็บไซต์ส่วนตัว (Personal website)* เป็นเว็บที่สร้างขึ้นเพื่อเผยแพร่ข้อมูลส่วนตัว เช่น ข้อมูลเกี่ยวกับส่วนตัว การศึกษา การงาน ความสนใจ เป็นต้น

2) *เว็บไซต์เพื่อธุรกิจการค้า (Promotional website)* เว็บไซต์นี้มีจุดประสงค์เพื่อการค้าขาย สินค้า การโฆษณาสินค้า การส่งเสริมการขาย ในเว็บไซต์จะมีข้อมูลของสินค้าราคาและการบริการต่างๆ ซึ่งในปัจจุบันตลาดประเภทนี้กำลังใช้กันมากขึ้น

3) *เว็บไซต์ที่เสนอข่าวประจำวัน (Current website)* เป็นเว็บที่เสนอข้อมูลประเภทข่าว ซึ่งจะเปลี่ยนไปเป็นประจำวัน เช่น เว็บไซต์ของหนังสือพิมพ์ไทยรัฐ เดลินิวส์ เป็นต้น

4) *เว็บไซต์ส่งเสริมการบริการเป็นสื่อกลางของข้อมูล (Share Information website)* เป็นเว็บที่มีจุดประสงค์ที่จะใช้เป็นการแลกเปลี่ยนข้อมูลตามกลุ่มสนใจ เช่น แบ่งตามอาชีพ ตามงานอดิเรก เป็นต้น

5) *เว็บไซต์ที่สร้างขึ้นเพื่อชักชวน หรือโฆษณาชวนเชื่อ (Persuasive website)* เป็นเว็บที่เชิญชวนหรือชักนำให้เห็นคล้อยตามในเรื่องที่ผู้สร้างต้องการ

6) *เว็บไซต์เพื่อการสอน (Instructional website)* เป็นเว็บที่สร้างขึ้นเป็นการสอนโดยเฉพาะเป็นรายวิชา (Course) อาจแยกย่อยเป็นหัวเรื่องเรื่องย่อย ๆ ก็ได้ สำหรับเว็บไซต์ประเภทนี้จะจำกัดผู้ใช้เฉพาะราย

7) *เว็บไซต์ที่จำกัดเฉพาะสมาชิก (Regisrational website)* เป็นเว็บไซต์ที่บริการเฉพาะสมาชิกเท่านั้น ผู้ที่จะใช้ต้องลงทะเบียนตามราคาที่กำหนดโดยบัตรเครดิต หรือผ่านธนาคาร ผู้ให้บริการจึงจะให้หมายเลขสมาชิกและรหัสผ่าน แต่การขายสินค้าหรือบริการใด ๆ ของเว็บไซต์เหล่านี้ จะเชิญชวนผู้ที่สนใจโดยมีตัวอย่างสินค้าหรือบริการให้ศึกษาบางส่วนจนพอใจด้วย

2.6) หลักการสืบสวน Web Site

1) ก่อนเกิดเหตุ

- การ Monitor เพื่อตรวจสอบดูความผิดปกติจากสถานการณ์ต่าง ๆ ที่เกิดขึ้น เช่น ด้านการเมือง การเกิดปัญหาทางด้านวิกฤติเศรษฐกิจ และความเปลี่ยนแปลงจากการนำเทคโนโลยีมาใช้งาน ตัวอย่าง Game Online ตลอดจนภัยด้านความมั่นคงที่เกิดจาก Web site ต่างประเทศ โดยจำแนกออกตามประเภทของ web เป็นต้น

2) ขณะเกิดเหตุ

- การเก็บหลักฐานพยานในที่เกิดเหตุ หรือ บน Web site สามารถจำแนกเป็นดังนี้

2.1) เก็บหลักฐานเกี่ยวกับการใช้งาน การติดต่อสื่อสาร เช่น URL, Link, รูปแบบของ web site, Banner, Web stat, Source, Graphic properties, Content Signature ฯลฯ

2.2) เก็บพฤติกรรม พฤติการณ์ รายละเอียด Web site ที่ผิดกฎหมาย ว่ามีลักษณะ รูปแบบอย่างไร คือ เป็นเว็บไซต์ที่ทำผิดกฎหมายโดยตรง เว็บไซต์ที่หลอกลวง หรือเว็บไซต์ที่เป็นทางผ่านให้ผู้อื่นเข้ามากระทำความผิด

2.3) ข้อมูลการติดต่อสื่อสารระหว่าง Webmaster กับ User หรือ ผู้ที่โพสกระทู้ เพื่อที่จะเก็บหมายเลข IP Address วันเวลา เพื่อใช้ในการที่จะตรวจสอบกับ ISP

3) หลังเกิดเหตุ

- การตรวจสอบ IP Address ของ Server โดยใช้โปรแกรมตรวจสอบ
- แสวงหาแหล่งที่ตั้งของ Server
- ตรวจสอบเกี่ยวกับผู้ให้บริการ และผู้เช่าพื้นที่หรือเช่าช่วง ตลอดจนผู้ดูแลเว็บไซต์
- ตรวจสอบ URL และข้อความ รูปภาพที่แสดงในการกระทำผิด

เครื่องมือในการตรวจสอบ

- DNStools
  - Domaintools.com
  - Dnsstuff.com
  - All-networktools.com
  - Robtex.com
  - Etc.
- Google
- Teleport
- Archive.org
- Etc.

กฎหมายที่เกี่ยวข้อง

- พ.ร.บ.ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
  - สารบัญญัติ โดยเฉพาะ ม.14

  หน้าที่ของผู้ให้บริการในการเก็บข้อมูลจราจรคอมพิวเตอร์
  - อำนาจของพนักงานเจ้าหน้าที่
  - การปิดกั้น website

2.7) มาตรการเสริมอื่นๆ ในการป้องกันและปราบปรามกระทำความผิด (จตุชัย แพงจันทร์, 2547)

วิวัฒนาการทางคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตได้นำไปสู่การขยายตัวของเครือข่ายทางสังคมอันเป็นคุณประโยชน์อย่างยิ่ง ปรากฏการณ์นี้เกิดจากกฎเกณฑ์สำคัญ 3 ข้อ คือ

1) ยิ่งคอมพิวเตอร์มีประสิทธิภาพสูงขึ้น ราคายิ่งถูกลง (Moore's Law) เมื่อราคาถูกลงทำให้มีผู้สามารถใช้อินเทอร์เน็ตมากขึ้น

2) ประโยชน์ของอินเทอร์เน็ตจะเพิ่มขึ้นเท่ากับจำนวนผู้ใช้ยกกำลังสอง (Metcalfe's Law) [xi] ตัวอย่างเช่น ถ้ามีผู้ใช้อินเทอร์เน็ตคนเดียว ประโยชน์ก็มีค่าเท่ากับศูนย์ เพราะใช้ติดต่อสื่อสารกับคนอื่นไม่ได้ แต่ถ้ามีผู้ใช้อินเทอร์เน็ตเพิ่มเป็น 10 คน ประโยชน์ของอินเทอร์เน็ตก็จะเพิ่มขึ้นเท่ากับ 10 x 10 หรือ 100 เท่า [xii]

ยิ่งไปกว่านี้ ผู้คนทั้งโลกก็ได้อาศัยการติดต่อสื่อสารผ่านอินเทอร์เน็ตในการสร้างเครือข่ายทางสังคมใหม่ๆ เพิ่มขึ้นอย่างมากมาย พวกเขาสามารถช่วยเหลือร่วมมือกัน สร้างสรรค์ประโยชน์ให้กันและกันได้มากขึ้นอีกเป็นทวีคูณ

3) ทุนทางสังคมหรือประโยชน์ที่เกิดจากเครือข่ายสังคมใหม่ ๆ เหล่านี้ เพิ่มขึ้นในอัตราเร่งที่เท่ากับสองยกกำลังจำนวนผู้ใช้อินเทอร์เน็ต (Reed's Law) คือ ถ้ามีผู้ใช้เพิ่มขึ้น 10 คน ประโยชน์ที่ได้รับจากเครือข่ายทางสังคมจะเพิ่มขึ้นถึง 2 ยกกำลัง 10 หรือ 1,024 เท่าทีเดียว

นอกจากมาตรการทางกฎหมาย ที่หลาย ๆ ประเทศทั่วโลก รวมทั้งประเทศไทย เรากำลังพยายามพัฒนา และปรับปรุงเพื่อรองรับกับการกระทำความผิดรูปแบบใหม่ ๆ แล้ว มาตรการเสริมอื่น ๆ ที่จำเป็นต้องทำควบคู่ไปกับการบังคับใช้กฎหมาย เช่น

1) การให้ความรู้กับประชาชนผู้ใช้คอมพิวเตอร์ และอินเทอร์เน็ตในการติดตั้งระบบรักษาความปลอดภัย และอุปกรณ์กลั่นกรองข้อมูลต่าง ๆ

2) ผู้ให้บริการอินเทอร์เน็ตต้องให้ความร่วมมือกับเจ้าหน้าที่ และร่วมกันตรวจสอบการกระทำความผิดต่างๆ ที่เกิดขึ้นบนอินเทอร์เน็ต เพื่อดำเนินการที่เหมาะสม หรือแจ้งแหล่งกระทำความผิดไปยังเจ้าหน้าที่รัฐ

3) พัฒนาซอฟต์แวร์ที่สามารถรักษาความปลอดภัยได้ดี หรือกลั่นกรองเนื้อหาและข้อมูลที่ไม่เหมาะสมได้อย่างมีประสิทธิภาพ

2.8) ข้อดี/ข้อเสียของการควบคุมอาชญากรรมคอมพิวเตอร์/อินเทอร์เน็ตด้วยมาตรการทางกฎหมาย

ข้อดี : ก่อให้เกิดมาตรฐานที่ชัดเจนในกำหนดว่าการกระทำในลักษณะใดเป็นความผิดและต้องห้ามมิให้กระทำ, หากใช้บังคับได้จริงย่อมลดการกระทำความผิดลงได้เนื่องจากผู้กระทำความผิดเกรงกลัวโทษ ผู้ได้เสียหายได้รับเยียวยาที่เป็นรูปธรรมและสามารถเรียกร้องตามกฎหมายได้ เป็นต้น

ข้อเสีย : เป็นอุปสรรคต่อการพัฒนาเทคโนโลยีอินเทอร์เน็ต, อาจขัดต่อหลักความเป็นอิสระในการแสดงความคิดเห็นของประชาชน และผู้ใช้บริการอาจต้องจ่ายค่าใช้ในราคาแพง เนื่องจากถูกผลักภาระค่าใช้จ่ายจากผู้ให้บริการอินเทอร์เน็ต เป็นต้น

2.2 งานวิจัยที่เกี่ยวข้อง

สินเลิศ สุขุม (2543) ได้ทำการศึกษาวิจัยเรื่อง ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ โดยเก็บรวบรวมข้อมูลและประเมินผลอย่างเป็นระบบ จากแบบสอบถามจำนวน 100 ชุด และจากการสัมภาษณ์เจ้าหน้าที่ตำรวจในกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจของการปฏิบัติงาน จำนวน 10 คน แล้วนำมาวิเคราะห์หาค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และการทดสอบค่าไคสแควร์ ซึ่งการทดสอบพบความแตกต่างอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ผลการวิจัยพบว่า ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ได้แก่ ปัจจัยในด้านระยะเวลาในการทำงานเกี่ยวข้องกับคอมพิวเตอร์ และความสามารถเกี่ยวกับการใช้คอมพิวเตอร์

นัยนรัตน์ งานแสง (2547) ได้ทำการศึกษาวิจัยเรื่อง อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมอินเทอร์เน็ต มีจุดมุ่งหมายเพื่อศึกษาถึงสภาพปัญหาอาชญากรรมบนอินเทอร์เน็ตในปัจจุบัน ตลอดจนความเสียหายที่เกิดขึ้น รวมทั้งประเภทและรูปแบบของอาชญากรรมบนอินเทอร์เน็ตในประเทศไทย เพื่อแสวงหาแนวทางแก้ไขและการจัดการกับปัญหา โดยเป็นการศึกษาเชิงพรรณนา จากแนวคิดทฤษฎีต่างๆ และผลงานวิจัยที่เกี่ยวข้องมาใช้เป็นกรอบในการวิเคราะห์ข้อมูลที่ได้รับจากแบบสอบถามและการสัมภาษณ์บุคลากรผู้เชี่ยวชาญที่เกี่ยวข้อง ผลการศึกษาพบว่า ปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มขึ้นเนื่องจากการขยายตัวของประชากรอินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้อินเทอร์เน็ตในสังคมไทย ยังขาดความรู้ความเข้าใจ และการปลูกฝังด้านจริยธรรมและวัฒนธรรมการใช้งานเทคโนโลยีเชิงสร้างสรรค์ ทำให้เกิดปัญหาการนำเทคโนโลยีไปใช้ในทางมิชอบตามมาส่วนบุคลากรที่มีความรู้ความสามารถด้านการรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายของประเทศไทยมีจำนวนจำกัด รวมทั้งภาครัฐไม่มีนโยบายและองค์กรเกี่ยวกับการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์โดยตรง ประกอบกับปัญหาทางด้านกฎหมาย ซึ่งปัจจุบันยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ออกมาบังคับใช้ ทำให้เกิดปัญหาในการดำเนินคดีกับผู้กระทำผิด ไม่ว่าจะเป็นประเด็นการตีความการกำหนดฐานความผิดการประเมินความเสียหาย เขตอำนาจศาล ผู้รับผิดชอบ ความแตกต่างทางกฎหมายและการสืบสวนตลอดการรวบรวมพยานหลักฐานส่งผลกระทบต่อการดำเนินคดีในทุกขั้นตอน ไม่ว่าจะเป็นการสืบสวนสอบสวน การพิจารณา และการพิพากษาคดี นอกจากนี้ เมื่อกฎหมายอาชญากรรมทางคอมพิวเตอร์มีผลบังคับใช้ จะทำให้เกิดปัญหาในทางปฏิบัติตามมา เนื่องจากบุคลากรในกระบวนยุติธรรม ไม่ว่าจะเป็นตำรวจ อัยการ ศาล ยังไม่มีความรู้ความเข้าใจและพื้นฐานเกี่ยวกับเทคโนโลยีและอาชญากรรมคอมพิวเตอร์สำหรับประเภทและรูปแบบของอาชญากรรมบนอินเทอร์เน็ตในประเทศไทยนั้นยังไม่มีการรวบรวมอย่างชัดเจน แต่จากการศึกษาพบการกระทำผิดแบ่งเป็น 2 ลักษณะ คือ การใช้อินเทอร์เน็ตในการอำนวยความสะดวกแก่การประกอบอาชญากรรมพื้นฐาน และการใช้อินเทอร์เน็ตกระทำผิดต่อเครือข่ายคอมพิวเตอร์และข้อมูล ซึ่งข้อมูล

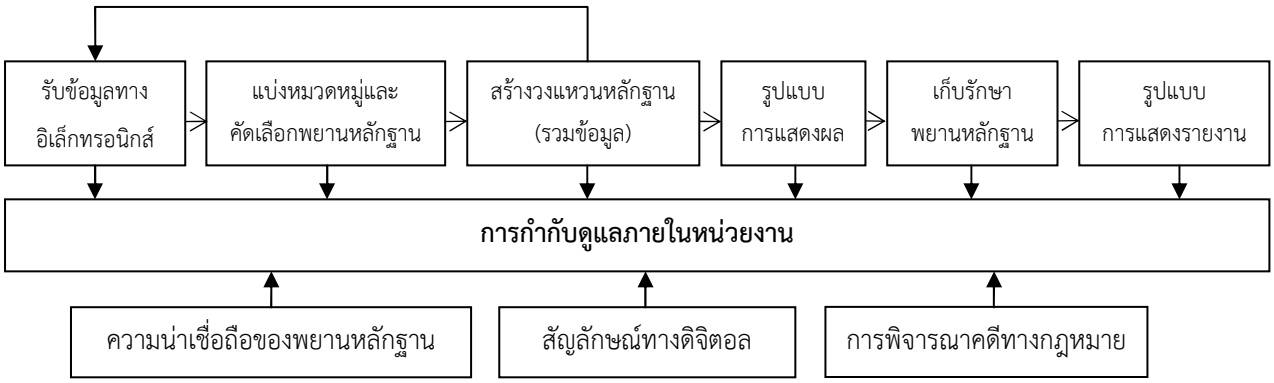
จากการสัมภาษณ์ พบว่า ผู้กระทำความผิดส่วนใหญ่เป็นเด็กและเยาวชนที่ต้องการทดลองความสามารถหรือลองวิชา นอกจากนี้ ยังพบว่า ผู้กระทำผิดบางส่วนต้องการเพียงแค่ชื่อเสียง และบางส่วนมุ่งหวังผลประโยชน์ โดยผลกระทบและความเสียหายจากอาชญากรรมบนอินเทอร์เน็ตในประเทศไทยนั้นยังไม่ปรากฏชัดเจน เนื่องจากปัญหาด้านการรายงานเหตุการณ์ และหลักเกณฑ์ในการประเมินความเสียหาย ซึ่งไม่สามารถประเมินค่าเป็นเงินได้ แต่สิ่งจะละเลยไปไม่ได้คือ ผลกระทบและความเสียหายต่อสังคมในภาพรวมรวมถึงผลกระทบต่อจริยธรรมและพฤติกรรมของเด็กและเยาวชน สรุปผลการศึกษา ปัจจัยภายในของผู้กระทำผิด คือ จริยธรรมของผู้ใช้อินเทอร์เน็ตเป็นปัจจัยสำคัญที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต ในส่วนของปัจจัยภายนอก คือ มาตรการทางกฎหมายและมาตรการป้องกันนั้นเป็นเพียงปัจจัยปลายเหตุเท่านั้น สำหรับข้อเสนอแนะ และแนวทางแก้ไขปัญหาอาชญากรรมบนอินเทอร์เน็ตในประเทศไทยนั้น จำเป็นต้องอาศัยมาตรการทางสังคมควบคู่ไปกับมาตรการทางกฎหมาย มาตรการทางสังคม คือ การปลูกฝังจริยธรรม แนวปฏิบัติที่ดี และวัฒนธรรมการใช้เทคโนโลยีที่ถูกต้อง และเสริมสร้างความตื่นตัวด้านความมั่นคง ซึ่งทุกฝ่ายต้องรับผิดชอบร่วมกัน ไม่ว่าจะเป็นสถาบันการศึกษา ต้องอบรมสั่งสอนเด็กและเยาวชนเกี่ยวกับการใช้งานเทคโนโลยีอย่างถูกต้องและเหมาะสม ผู้ปกครองควรฝังจริยธรรมการใช้เทคโนโลยี กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ควรออกกฎระเบียบที่เอื้อต่อการบังคับใช้ ทางตำรวจ ศาล อัยการ นักกฎหมายต้องมีการฝึกอบรมเตรียมพร้อม ส่วนกลุ่มนักวิจัยพัฒนาต้องทำระบบที่ปลอดภัย หน่วยให้บริการด้านอินเทอร์เน็ต ก่อนให้บริการต้องตรวจสอบวัดระบบความปลอดภัยก่อน เป็นต้น จะเห็นได้ว่าอาชญากรรมบนอินเทอร์เน็ตเป็นปัญหาที่ทุกคนต้องร่วมมือกันแก้ไข

นารี กิตติสมบูรณ์สุข (2548) ได้ทำการศึกษาวิจัยเรื่อง การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ พบว่า อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่งที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้ และผลกระทบที่เกิดกับกฎหมายอาญาของประเทศต่างๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ เพื่อค้นหาวิธีการป้องกันและปราบปราม สำหรับประเทศไทยเป็นประเทศหนึ่งที่เห็นความสำคัญของปัญหาดังกล่าวจึงมีการร่างกฎหมายอาชญากรรมคอมพิวเตอร์ขึ้นเป็นกฎหมายเฉพาะ อย่างไรก็ตามสิ่งที่ควรคำนึงควบคู่ไป คือ การมีกฎหมายบังคับใช้ กล่าวคือ ต้องมีการปรับปรุงกฎหมายวิธีสบัญญัติให้มีประสิทธิภาพด้วย โดยเฉพาะปัญหาการรวบรวมพยานหลักฐานและการรับฟังพยานหลักฐานคอมพิวเตอร์ที่เป็นข้อมูลส่วนบุคคล รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2540 มาตรา 19 ได้บัญญัติรับรองสิทธิและเสรีภาพของประชาชนไว้เป็นหลักฐาน ซึ่งในทางปฏิบัติรัฐสามารถบัญญัติกฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ในบางกรณี ดังนั้นจึงมีบทบัญญัติที่ให้อำนาจรัฐตรากฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพของประชาชนได้ภายในขอบเขตที่รัฐธรรมนูญกำหนด เช่น ในมาตรา 37 บัญญัติรับรองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคล ซึ่งเป็นสิทธิส่วนบุคคล และรัฐธรรมนูญก็มีบทบัญญัติให้อำนาจรัฐกระทำการใดๆ ก็ได้หากเป็นกรณีที่กระทำไปเพื่อประโยชน์สาธารณะ ดังนั้นรัฐอาจอาศัยข้อยกเว้นดังกล่าวบัญญัติ

กฎหมายขึ้นมาจำกัดสิทธิและเสรีภาพในข้อมูลข่าวสารบุคคลเกินความจำเป็น หรือตามอำเภอใจ โดยอ้าง “ประโยชน์สาธารณะ” เช่น รัฐอาจบัญญัติกฎหมายอนุญาตให้เจ้าหน้าที่ของรัฐเข้าตรวจสอบข้อมูลส่วนบุคคลของบุคคลใดบุคคลหนึ่งได้ตลอดเวลา ตามแต่จะเห็นสมควร โดยเฉพาะข้อมูลข่าวสารส่วนบุคคลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ เป็นต้น การกระทำดังกล่าวถือเป็นการกระทำที่กระทบกระเทือนต่อสาระสำคัญแห่งสิทธิและเสรีภาพในข้อมูลข่าวสารส่วนบุคคล ซึ่งจะมีผลตามบทบัญญัติในมาตรา 6 ที่ถือว่าเป็นบทบัญญัติดังกล่าวขัดหรือแย้งกับรัฐธรรมนูญ ซึ่งถือเป็นกฎหมายสูงสุดของประเทศ ทำให้บทบัญญัติดังกล่าวไม่สามารถใช้บังคับได้ ทั้งๆที่การเข้าสู่ข้อมูลส่วนบุคคลนี้ เป็นมาตรการใหม่ที่รัฐสามารถนำมาใช้แสวงหาพยานหลักฐานเพื่อมาดำเนินคดีกับอาชญากรที่ก่ออาชญากรรมที่การแสวงหาพยานหลักฐานรูปแบบดั้งเดิมไม่สามารถแก้ปัญหาได้ เช่น อาชญากรรมคอมพิวเตอร์ ดังนั้น จึงควรมีการบัญญัติกฎหมายขึ้นมาให้อำนาจ และควบคุมการใช้อำนาจของเจ้าหน้าที่ของรัฐในการเข้าสู่ข้อมูลข่าวสารส่วนบุคคลได้ ภายในขอบเขตที่ไม่เป็นการกระทบกระเทือนต่อสาระสำคัญแห่งสิทธิในข้อมูลข่าวสารส่วนบุคคล พยานหลักฐานที่เป็นข้อมูลส่วนบุคคลโดยทั่วไปนอกจากจะได้รับความคุ้มครองตามประมวลกฎหมายอาญาแล้วยังได้รับความคุ้มครองตามรัฐธรรมนูญในส่วนของสิทธิส่วนบุคคล และสำหรับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ซึ่งมีลักษณะแตกต่างไปจากพยานหลักฐานทั่วๆไป กล่าวคือพยานหลักฐานประเภทนี้เป็นสิ่งที่ไม่มีรูปร่าง มองไม่เห็นด้วยตาเปล่า และอยู่ในรูปของคลื่นแม่เหล็กไฟฟ้า อาจถูกแก้ไขเปลี่ยนแปลง ลบ ทำงายได้ง่าย เจ้าหน้าที่ในกระบวนการยุติธรรมทั้งหลายจึงต้องประสบปัญหาในการดำเนินคดีกับผู้กระทำความผิด โดยเฉพาะพนักงานสอบสวนที่มีหน้าที่ในการรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดของจำเลยและนำเสนอต่อศาล ผู้วิจัยได้ทำการศึกษาวิจัยปัญหาการรวบรวมพยานหลักฐานและพิสูจน์พยานหลักฐานที่เป็นอิเล็กทรอนิกส์และเป็นข้อมูลส่วนบุคคล ภายในกรอบของ 3 หัวข้อใหญ่ ได้แก่ ลักษณะของพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ สิทธิส่วนบุคคล กระบวนการค้น และกระบวนการนำเสนอพยานหลักฐานต่อศาล ภายใต้สมมติฐานว่าการรวบรวมพยานหลักฐานที่เป็นการละเมิดสิทธิบุคคลที่ได้รับการคุ้มครองตามรัฐธรรมนูญและกฎหมายอาญาเจ้าหน้าที่ของรัฐสามารถกระทำได้เพียงใด ปัจจุบันมีกฎหมายฉบับใดให้อำนาจกระทำได้อย่างไร และควรจะกระทำอย่างไรเพื่อที่จะนำตัวผู้กระทำความผิดมาลงโทษให้ได้ ซึ่งผลจากการศึกษาและวิเคราะห์ปัญหาทั้งประเทศไทยและต่างประเทศ ตลอดจนศึกษาแนวทางแก้ไขปัญหาของต่างประเทศโดยเฉพาะของประเทศสหรัฐอเมริกา อังกฤษ และญี่ปุ่น พบว่าการที่จะให้เจ้าหน้าที่ของรัฐเข้าถึงหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ได้เร็ว และไม่เป็นการละเมิดสิทธิในข้อมูลข่าวสาร จะต้องมีกฎหมายให้อำนาจในการปฏิบัติงานได้ ควรต้องมีองค์กรที่เป็นกลางเป็นผู้ให้อำนาจในการตรวจสอบการใช้อำนาจ และควรมีหลักกฎหมายลักษณะพยานหลักฐานเกี่ยวกับพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ที่ชัดเจนกว่านี้

Guofu Ma และคณะ (2554) ได้ทำการศึกษาวิจัยเรื่อง รูปแบบพื้นฐานวงแหวนหลักฐานและห่วงโซ่หลักฐานของงานทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์ พบว่า การพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการพิจารณาคดีทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์อยู่บ่อยครั้ง ซึ่งส่วนใหญ่เป็นงานด้านทางวิทยาศาสตร์ และงานด้าน

คอมพิวเตอร์ และยังไม่สามารถทำให้มีความเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก ซึ่งส่วนใหญ่จะศึกษาเฉพาะด้านเทคนิคของหลักฐานทางคอมพิวเตอร์เท่านั้น ในการศึกษานี้จึงศึกษาคุณลักษณะทั่วไปของพยานหลักฐาน วัตถุประสงค์ ความเกี่ยวข้อง และความถูกต้องของกฎหมาย เพื่อเป็นบรรทัดฐานในการสร้างแบบจำลองของนิติวิทยาศาสตร์คอมพิวเตอร์บนพื้นฐานของวงแหวนและห่วงโซ่ของหลักฐาน ดังแสดงในภาพ 2-3



ภาพ 2-3 รูปแบบพื้นฐานวงแหวนหลักฐานและห่วงโซ่หลักฐานของงานนิติวิทยาศาสตร์คอมพิวเตอร์

Matthew Tart (2555) ได้ทำการศึกษาวิจัยเรื่อง หลักการและวิธีการสำรวจสำหรับการวิเคราะห์ตำแหน่งเสาโทรศัพท์ย้อนหลัง พบว่า โทรศัพท์มือถือมีข้อมูลที่สำคัญและสามารถนำไปใช้ในการสืบคดี หรือเป็นพยานหลักฐานที่ใช้ในชั้นศาล ซึ่งยังมีข้อมูลอื่นๆที่มีความเกี่ยวข้อกับโทรศัพท์มือถือที่ทำให้ได้ข้อมูลในการสืบสวนมากขึ้นไปอีก เช่น ข้อมูลการโทรเข้าออกซึ่งมีการเชื่อมโยงกับซิมการ์ดและระบบของผู้ให้บริการเครือข่ายโทรศัพท์มือถือซึ่งใช้ในการคิดค่าบริการโทรศัพท์มือถือด้วย นอกจากนี้การวิเคราะห์ ตำแหน่งเสาสัญญาณโทรศัพท์ย้อนหลัง ร่วมกับข้อมูลอื่นๆจากการสำรวจหรือข้อมูลทางภูมิศาสตร์ สามารถระบุตำแหน่งของโทรศัพท์มือถือในช่วงเวลาที่มีการใช้งานโทรศัพท์มือถือได้ รายงานนี้นำเสนอภาพรวมของ หลักการของเครื่องโทรศัพท์มือถือ และสัญญาณโทรศัพท์มือถือกระทำต่อกัน รวมไปถึงวิธีการเก็บข้อมูลในรูปแบบต่างและการแปลผล และข้อดีข้อเสียของแต่ละวิธีการ ในรายงานนี้กล่าวถึงเฉพาะการวิเคราะห์จากสัญญาณโทรศัพท์ 2จี เท่านั้น และมีปัจจัยแต่ละพื้นที่มีความแตกต่างในด้านภูมิศาสตร์ และ ผู้ให้บริการเครือข่ายโทรศัพท์มือถือแต่ในส่วนของหลักการสามารถใช้ได้กับเครือข่ายโทรศัพท์มือถือทั้ง 2จี (GSM) และ 3จี (UTMS) และไม่ได้กล่าวถึงการวิเคราะห์ตำแหน่งเสาสัญญาณโทรศัพท์ตามเวลาจริง

บทที่ 3

รายงานผลการดำเนินงาน

คณะผู้วิจัยได้ดำเนินการวางแผนปฏิบัติการตลอดโครงการ และรายงานผลการดำเนินงานในการวิจัย ดังนี้

1) สถานการณ์ปัจจุบันทางด้านอาชญากรรมคอมพิวเตอร์

2) ข้อมูลเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์

3) ข้อมูลคดีอาชญากรรมคอมพิวเตอร์ที่ประสบความสำเร็จ (Best Practice) แนวทาง ขั้นตอน เทคนิค วิธีการสืบสวนสอบสวนปฏิบัติงาน

4) องค์ความรู้เกี่ยวกับแนวทางการพัฒนาประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

5) ขั้นตอนการดำเนินการจัดการความรู้ ทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

3.1 สถานการณ์ปัจจุบันทางด้านอาชญากรรมคอมพิวเตอร์

3.1.1 ปัจจุบันเจ้าหน้าที่บังคับใช้กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ดังนี้

1) พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ.2550

2) พ.ร.บ.ที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่างๆ ซึ่งแต่เดิมอาจจะจัดทำขึ้นในรูปแบบของหนังสือให้เท่าเทียมกับนิติสัมพันธ์รูปแบบใหม่ที่จัดทำขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ รวมตลอดทั้งการลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์ และการรับฟังพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

3) กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

เพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดา อันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการ เกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ตลอดจนการให้ บริการอื่น ที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

4) กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ

5) ประกาศกระทรวงเทคโนโลยีและสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

6) ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนการสอบสวนและการดำเนินคดีกับผู้กระทำความผิดว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

7) ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ออก พ.ศ.2555

8) ประมวลกฎหมายอาญา **หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ของลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6** และ **มาตรา 269/7**

9) พ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ.2547 ซึ่งให้อำนาจพนักงานเจ้าหน้าที่

10) กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ฉบับที่ 2 พ.ศ. 2555

11) กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

3.1.2 ลักษณะหรือรูปแบบอาชญากรรมคอมพิวเตอร์ในประเทศไทย มีดังนี้

1) การเข้าถึงระบบข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) ตัวอย่างเช่น การเจาะระบบ/รหัส (Hacking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass) เพื่อทำลายระบบคอมพิวเตอร์ หรือแก้ไขเปลี่ยนแปลงข้อมูล หรือเข้าถึงข้อมูลที่เก็บรักษาไว้ เป็นความลับ เช่น รหัสผ่าน (Passwords Hacking) หรือเป็นความลับทางการค้า (Trade Secret)

2) การใช้คอมพิวเตอร์โดยไม่ชอบ (Computer Misuse) อันทำให้โปรแกรมและข้อมูลเสียหาย ตัวอย่างเช่น การลักลอบดักข้อมูลโดยฝ่าฝืนต่อกฎหมาย การส่งไวรัสคอมพิวเตอร์และอีเมล์ขยะ

3) การใช้คอมพิวเตอร์เป็นเครื่องมือ (Computer Fraud) เช่น การสร้างโปรแกรม Salame techniques เพื่อปัดเศษเงินในบัญชีของบุคคลอื่นมารวมเก็บไว้ในบัญชีของตนเอง หรือโปรแกรม Logic Bombs เพื่อเฝ้าติดตามความเคลื่อนไหวของระบบบัญชี และระบบเงินเดือนและทำการเปลี่ยนแปลงตัวเลขในระบบดังกล่าว

4) การฉ้อโกงบัตรเครดิต (Credit Card Fraud) เช่น

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access) เช่น Hackers
- การนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต (Unauthorized Use by Insider) เช่น พนักงานในบริษัทเว็บไซต์นำข้อมูลไปใช้โดยไม่ได้รับอนุญาตเพื่อประโยชน์ของตนเอง
- การดักข้อมูล (Interception of transmission of information)
- การส่งอีเมล์และตั้งเว็บไซต์หลอก (Phishing Scam and Spoof e – commerce sites) หมายถึงการโจรกรรมข้อมูลในรูปแบบของการปลอมแปลงอีเมล์และทำการสร้างเว็บไซต์ปลอมเพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอีเมล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ เช่น Username Password

3.1.3 ฐานความผิดที่เกี่ยวข้องกับคอมพิวเตอร์

ฐานความผิดที่ 1 (มาตรา 5, มาตรา 7)

การเจาะระบบ (Hacking or cracking) หรือการบุกรุกทางคอมพิวเตอร์ (computer trespass) ซึ่งการกระทำเช่นว่านี้เป็นการขัดขวางการใช้ระบบคอมพิวเตอร์โดยชอบของบุคคลอื่นอันอาจทำให้เกิดการเปลี่ยนแปลงแก้ไข หรือการทำงานระบบคอมพิวเตอร์ ได้โดยปกติ (มาตรา 5)

ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

รวมถึงข้อมูลคอมพิวเตอร์ ซึ่งข้อมูลนั้นเป็นการเก็บหรือส่งด้วยวิธีการทางคอมพิวเตอร์หรือวิธีการทางอิเล็กทรอนิกส์ (มาตรา 7)

ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

ฐานความผิดที่ 2 (มาตรา 6)

ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ เช่นมีการลงทะเบียน Username และ password หรือมีวิธีการอื่นใดที่จัดขึ้นเป็นการเฉพาะ แล้วนำไปเปิดเผยแก่ผู้หนึ่งผู้ใดหรือหลายคน แล้วน่าจะเกิดความเสียหายแก่ผู้อื่นได้

ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 3 (มาตรา 8)

การดักรับโดยวิธีการทางเทคนิค (technical means) เพื่อลักลอบดักฟัง (listen) ตรวจสอบ (monitoring) หรือติดตามเนื้อหาสาระของข่าวสาร(surveillance) ที่สื่อสารถึงกันระหว่างบุคคล หรือเป็นการกระทำเพื่อให้ได้มาซึ่งเนื้อหาของข้อมูลโดยตรงหรือโดยการเข้าถึงและใช้ระบบคอมพิวเตอร์ หรือการทำให้ได้มาซึ่งเนื้อหาของข้อมูลโดยทางอ้อมด้วยการแอบบันทึกข้อมูลสื่อสารถึงกันด้วยอุปกรณ์อิเล็กทรอนิกส์ โดยไม่คำนึงว่าอุปกรณ์อิเล็กทรอนิกส์ที่ใช้บันทึกข้อมูลดังกล่าวจะต้องเชื่อมต่อเข้ากับสายสัญญาณสำหรับส่งผ่านข้อมูลหรือไม่เพราะบางกรณีอาจใช้อุปกรณ์เช่นว่านั้นเพื่อบันทึกการสื่อสารข้อมูลที่ได้ส่งผ่านด้วยวิธีการแบบไร้สายก็ได้ เช่นการติดต่อผ่านทางโทรศัพท์เคลื่อนที่ การติดต่อโดยใช้เทคโนโลยีไร้สายประเภท wireless LAN เป็นต้น ซึ่งนอกจาการใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อบันทึกข้อมูลที่มีการส่งผ่านกันแล้ว ยังรวมถึงกรณีการใช้ซอฟต์แวร์ หรือรหัสผ่านต่างๆ เพื่อทำการแอบบันทึกข้อมูลที่ส่งผ่านถึงกันด้วย ทั้งนี้ ข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์มิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 4 (มาตรา 9)

กระทำการอันเป็นการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่น โดยมิชอบ เว้นแต่ การเปลี่ยนแปลงข้อมูลจราจรทางคอมพิวเตอร์ (traffic data) เพื่อประโยชน์ในการสื่อสารแบบไม่ระบุชื่อ ตัวอย่างเช่น การสื่อสารผ่านระบบ Anonymous remailer system หรือการ

เปลี่ยนแปลงข้อมูลเพื่อการรักษาความลับและความปลอดภัยของการสื่อสาร อาทิ การเข้ารหัสข้อมูล (encryption) เป็นต้น

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 5 (มาตรา 10, มาตรา 12)

กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวน จนไม่สามารถทำงานตามปกติได้ หากผู้กระทำได้กระทำไปโดยมีอำนาจหรือสิทธิโดยชอบย่อมไม่เป็นความผิดเพราะไม่เข้าองค์ประกอบความผิดที่ว่า “โดยมิชอบ”ดังเช่น การทดสอบหรือรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์โดยบุคคลผู้ได้รับมอบอำนาจจากผู้เป็นเจ้าของระบบคอมพิวเตอร์ (owner) หรือผู้ปฏิบัติการ (operator) หรือการปรับแก้ระบบปฏิบัติการ (operating system) ของคอมพิวเตอร์โดยผู้ปฏิบัติการ (operator) ก่อนติดตั้งซอฟต์แวร์ใหม่ๆ ตัวอย่างเช่น การติดตั้งซอฟต์แวร์เพื่อการเชื่อมต่ออินเทอร์เน็ตซึ่งจะมีผลให้ระบบคอมพิวเตอร์ทำงานไม่เป็นปกติทั้งก่อนและหลังการติดตั้งโปรแกรม

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ถ้าเกิดความเสียหายแก่ประชาชนในทันที หรือภายหลัง ไม่ว่าจะเกิดขึ้นพร้อมกันของมาตรา 9 และ มาตรา 10 หรือไม่ (มาตรา 12(1))

ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท (โทษหนักขึ้น)

การกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ (มาตรา 9) หรือระบบคอมพิวเตอร์ (มาตรา 10) ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ (มาตรา 12(2))

ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท (โทษหนักขึ้นอีก) ถ้ามีใครตาย (มาตรา 12 วรรคท้าย) ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี (หนักที่สุด)

ฐานความผิดที่ 6 (มาตรา 11)

การทำให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข เช่นส่ง E-mail มากจนล้นระบบคอมพิวเตอร์ของบุคคลอื่นจนทำให้เกิดความยุ่งยากในการใช้ระบบคอมพิวเตอร์ของเขา ภาษาอังกฤษเรียกว่า “spamming” โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูล

ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

แต่การปกปิดหรือปลอมแปลงนี้ต้องเป็นเรื่องของ “แหล่งที่มาของการส่งข้อมูล” ซึ่งตรวจสอบได้โดย “ข้อมูลจราจรทางคอมพิวเตอร์” ได้แก่การปกปิดหรือปลอมแปลง IP address และหมายถึงการกระทำที่ทำให้ไม่สามารถตรวจสอบถึงแหล่งที่มาของการส่งข้อมูลและส่งผลให้ไม่อาจตรวจสอบได้ทางระบบข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น จึงไม่ใช่เรื่องการปกปิดหรือปลอมแปลงโดยการไม่ใช้ชื่อจริง หรือการ

เปลี่ยนแปลงใช้ชื่อหรือใช้นามแฝง หรือใช้ email-address ที่ผิดไปหรือเปลี่ยนแปลงไปซึ่งยังตรวจสอบแหล่งที่มาของการส่งข้อมูลได้อยู่

ฐานความผิดที่ 7 (มาตรา 13)

จำหน่าย เผยแพร่ ชุดคำสั่งเพื่อนำไปใช้เป็นเครื่องมือในการทำความผิด ฐานความผิดที่ 1–6

ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 8 (มาตรา 14)

การนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์

1) ปลอม ไม่ว่าทั้งหมด หรือบางส่วน ที่น่าจะเกิดความเสียหายแก่ผู้อื่น หรือประชาชน

2) เท็จ ที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตระหนกแก่ประชาชน

3) ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4) ใดๆ ที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้

(5) เผยแพร่ ส่งต่อ โดยรู้อยู่แล้วว่าเป็นข้อมูลฯ ตาม (1) (2) (3) หรือ (4)

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ฐานความผิดที่ 9 (มาตรา 15)

ผู้ให้บริการใดจงใจสนับสนุน หรือ ยินยอมให้มีการกระทำตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

ต้องระวางโทษจำคุกไม่เกินห้าปี หรือ ปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (ผิดเหมือนกับเป็นผู้กระทำเอง)

ฐานความผิดที่ 10 (มาตรา 16)

นำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (แต่ยอมความกันได้) และไม่มีความผิด ถ้ากระทำโดยสุจริต

(1.พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

2.คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550)

3.1.4 ปัญหาอุปสรรคของข้อกฎหมายและระเบียบที่เกี่ยวข้องเกี่ยวกับงานด้านอาชญากรรมคอมพิวเตอร์ และข้อเสนอแนะต่อการแก้ไขปัญหาในสถานการณ์ปัจจุบัน

ระบบงานด้านอาชญากรรมคอมพิวเตอร์ เป็นนวัตกรรมใหม่เพื่อการพิสูจน์หลักฐานทางคอมพิวเตอร์ในการกระทำผิด โดยองค์ความรู้ทางเทคโนโลยีคอมพิวเตอร์ รวมกับการใช้ในแนวทางการสืบสวนสอบสวน และการสร้างความน่าเชื่อถือของพยานหลักฐานที่ได้ ซึ่งถือได้ว่าจะทำให้มีน้ำหนักมากที่สุด

1) ให้ความรู้แก่พนักงานสอบสวน และผู้เกี่ยวข้องของสถานีตำรวจทุกแห่ง ทั้งในพื้นที่กองบัญชาการตำรวจนครบาล กองบัญชาการตำรวจภูธรภาคต่าง ๆ และหน่วยงานสนับสนุน ในการรับแจ้งความดำเนินคดีด้านอาชญากรรมคอมพิวเตอร์ เขตกอำนาจการสอบสวน เพราะการกระทำความผิดของคนร้ายนั้นสามารถกระทำความผิดได้ทั่วประเทศ ไม่ต้องปรากฏตัวในสถานที่เกิดเหตุ การตรวจสถานที่เกิดเหตุ การเก็บรวบรวมพยานหลักฐานในการตรวจสถานที่เกิดเหตุ เพราะวัตถุพยานอาจถูกทำลายโดยไม่ได้ตั้งใจ หรือทำให้คุณค่าของวัตถุพยานในสถานที่เกิดเหตุลดน้อยลง รวมทั้งไปเพิ่มวัตถุพยานในสถานที่เกิดเหตุ ซึ่งจะทำให้การสืบสวนสอบสวนประสบความสำเร็จในการคลี่คลายคดี ทั้งนี้เพื่อเกิดประโยชน์ในด้านการสืบสวนสอบสวนผู้กระทำความผิดและการไปเป็นพยานศาล สามารถให้ข้อมูลที่ชัดเจนต่ออัยการและผู้พิพากษาในการพิจารณาคดี

2) ควรมีระเบียบกำหนดให้เจ้าหน้าที่ที่ปฏิบัติด้านคดีอาชญากรรมคอมพิวเตอร์ เช่น พนักงานสอบสวน ผู้ช่วยพนักงานสอบสวน ตลอดจนเจ้าหน้าที่อื่นๆ ที่มีส่วนเกี่ยวข้องกับงานด้านอาชญากรรมคอมพิวเตอร์ ต้องผ่านการฝึกอบรมความรู้ทางอาชญากรรมคอมพิวเตอร์ เกี่ยวกับวัตถุพยาน การป้องกันและรักษาสถานที่เกิดเหตุ ความสำคัญของวัตถุพยานและสถานที่เกิดเหตุ เป็นต้น ทั้งนี้เพื่อประโยชน์และเกิดประสิทธิภาพสูงสุดในการใช้พยานหลักฐานทางคอมพิวเตอร์ในการคลี่คลายคดี

3) การจัดเก็บข้อมูลการตรวจพิสูจน์ ควรมีการประสานงานกันในเรื่องของพฤติการณ์แห่งคดีระหว่างพนักงานสอบสวนและเจ้าหน้าที่ตรวจพิสูจน์เพื่อประโยชน์แห่งรูปคดี โดยในปัจจุบันการดำเนินงานด้านการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ ยังขาดแนวทาง รูปแบบและมาตรฐานที่ชัดเจน โดยเฉพาะแนวทางการปฏิบัติงานสำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่ปฏิบัติงานด้านการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ ตลอดจนเจ้าหน้าที่ผู้ดำเนินการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ ด้วยเหตุนี้จึงเกิดคำถามและข้อสงสัยที่เกี่ยวกับกระบวนการดำเนินคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ด้วยเหตุที่ว่าข้อมูลคอมพิวเตอร์และหลักฐานทางอิเล็กทรอนิกส์นั้น ไม่สามารถอธิบายให้เข้าใจได้ง่ายด้วยวิธีการเดิมที่ใช้ในกระบวนการยุติธรรมโดยปกติ หากแต่จำเป็นต้องอาศัยหลักการและวิธีการที่แตกต่างไปจากการนำเสนอพยานหลักฐานแบบอื่นๆ จึงทำให้หลายฝ่ายตั้งคำถามและข้อสงสัยเกี่ยวกับกระบวนการสืบสวนและสอบสวนอาชญากรรมคอมพิวเตอร์ เนื่องจากหากกระบวนการรวบรวมพยานหลักฐาน และการตรวจพิสูจน์ที่เจ้าหน้าที่ได้ปฏิบัตินั้นไม่เป็นไปตาม มาตรา 226 แห่งประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ.2477 แล้วนั้นจะทำให้พยานหลักฐานที่ได้ทำการรวบรวม ตลอดจนข้อมูลที่ได้จากการตรวจพิสูจน์นั้น อาจถูกปฏิเสธในการรับฟังเป็นพยานหลักฐานในชั้นศาลได้ ด้วยเหตุที่ว่าเป็นการได้มาซึ่งพยานหลักฐานโดยมิชอบด้วยกฎหมาย ดังนั้น

กระบวนปฏิบัติงานที่ดีจึงต้องเป็นไปตามข้อกำหนดทางกฎหมายและยังมีกระบวนการปฏิบัติในเชิงเทคนิคที่เหมาะสม ซึ่งในการพัฒนามาตรฐานการปฏิบัติงานสาหรับการรวบรวมพยานหลักฐานและการตรวจพิสูจน์หลักฐานคอมพิวเตอร์นั้น ควรมีขั้นตอนการดำเนินงานแบ่งออกเป็นสองขั้น ได้แก่ จัดทำมาตรฐานการเก็บรวบรวมพยานหลักฐานคอมพิวเตอร์ และแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ รายละเอียดของทั้งสองขั้นตอนมีดังนี้

1) การจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ การจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ มีขั้นตอนการดำเนินงานดังนี้

1.1 การรวบรวมและศึกษาเอกสารที่เกี่ยวข้องกับกระบวนการรวบรวมพยานหลักฐานคอมพิวเตอร์ โดยได้ทำการค้นคว้า ศึกษาข้อมูลจาก เอกสารวิชาการ เอกสารประกอบการฝึกอบรม และหนังสือ ประกอบกับหลักการปฏิบัติงานของหน่วยงานบังคับใช้กฎหมายในต่างประเทศ อีกทั้งรายงานการวิจัย วิทยานิพนธ์ วารสารและสิ่งพิมพ์ ตลอดจนกฎหมายของประเทศไทยที่เกี่ยวข้องกับการรวบรวมพยานหลักฐานคอมพิวเตอร์

1.2 การวิเคราะห์ข้อมูล และการจัดทำมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ สำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้อง โดยการนำรูปแบบหลักการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์ของหน่วยงานผู้บังคับใช้กฎหมายในต่างประเทศ มาทำการวิเคราะห์และสังเคราะห์เพื่อจัดทำเป็นมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ให้ผู้เชี่ยวชาญที่มีประสบการณ์ ทำการพิจารณาปรับปรุง แก้ไข ให้เหมาะสมกับการปฏิบัติงาน

1.3 ดำเนินการปรับปรุงมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานทางคอมพิวเตอร์ ตามข้อเสนอแนะและความก้าวหน้าทางเทคโนโลยีเพื่อให้มีความสมบูรณ์อย่างต่อเนื่อง

2) จัดทำแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ การจัดทำแนวทางการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ มีขั้นตอนการดำเนินงาน ดังนี้

2.1 การดำเนินตามมาตรฐานการปฏิบัติงานการรวบรวมพยานหลักฐานคอมพิวเตอร์เพียงอย่างเดียวนั้น ไม่สามารถทำให้เจ้าหน้าที่ผู้บังคับใช้กฎหมายสามารถหาตัวผู้กระทำความผิดมาลงโทษได้ หากแต่ยังต้องอาศัยผลลัพธ์จากการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์เพื่อแสดงถึงหลักฐานและข้อเท็จจริงของอาชญากรรมต่างๆ ที่เกิดขึ้น ด้วยเหตุนี้เองที่ทำให้มีความจำเป็นในการพัฒนาแนวทางปฏิบัติงาน สำหรับการตรวจพิสูจน์พยานหลักฐานคอมพิวเตอร์ขึ้น เพื่อเป็นคู่มืออ้างอิงสำหรับเจ้าหน้าที่ ผู้ซึ่งจะต้องค้นหาหลักฐานทางคอมพิวเตอร์ด้วยเทคนิคและวิธีการที่น่าเชื่อถือ ตลอดจนยังคงต้องสามารถยืนยันความถูกต้องได้เพื่อให้สามารถนำเสนอหลักฐานนั้นต่อศาลโดยปราศจากข้อสงสัยใดๆ

2.2 การวิเคราะห์ข้อมูล และจัดทำการจัดทำแนวทางการปฏิบัติงานสำหรับตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ สำหรับเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เกี่ยวข้อง โดยการนำข้อมูลและเอกสารวิชาการ เอกสารประกอบการอบรมในหลักสูตรการตรวจพิสูจน์หลักฐานคอมพิวเตอร์ มาทำการวิเคราะห์เพื่อ

จัดทาเป็นมาตรฐานการปฏิบัติงานสาหรับการตรวจพิสูจน์หลักฐานทางคอมพิวเตอร์ เพื่อให้ผู้เชี่ยวชาญที่มีประสบการณ์ ทำการพิจารณาปรับปรุง แก้ไข ให้เหมาะสมกับการปฏิบัติงาน

2.3 ดำเนินการปรับปรุงมาตรฐานการปฏิบัติงานสำหรับการรวบรวมพยานหลักฐานคอมพิวเตอร์ ตามข้อเสนอแนะและความก้าวหน้าทางเทคโนโลยีเพื่อให้มีความสมบูรณ์อย่างต่อเนื่อง

ข้อเสนอแนะ

1. ถ้ากล่าวถึงบทบาทและความสำคัญของข้อมูลของคอมพิวเตอร์ ระบบและเครือข่ายคอมพิวเตอร์ในยุคปัจจุบันที่ทุกกิจกรรมของเรามีการใช้สิ่งเหล่านี้ตลอด ดังนั้นกฎหมายจะต้องให้ความคุ้มครองสิ่งต่างๆ เหล่านี้ด้วย โดยะต้องให้ความคุ้มครองในเรื่องความลับ ความครบถ้วนและความสามารถในการใช้ประโยชน์ได้ ซึ่งเป็นคุณลักษณะ (properties) ของสิ่งเหล่านี้ได้ครบถ้วน รวมทั้งการให้ความคุ้มครองสิทธิในทรัพย์สินจากการกระทำความผิดรูปใหม่ด้วย

2. ในกรณีของการบัญญัติให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิด ดังที่ได้กล่าวมาแล้วกฎหมายของประเทศต่างๆบัญญัติองค์ประกอบของความผิดในเรื่องนี้ไว้ไม่เหมือนกัน เช่น บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเพียงอย่างเดียวเป็นความผิด บางประเทศกำหนดให้การเข้าถึงคอมพิวเตอร์จะเป็นความผิดเมื่อมีองค์ประกอบอย่างอื่นด้วย เช่น ผู้กระทำมีเจตนาที่จะกระทำความผิดอย่างอื่นภายหลังจากการเข้าถึงคอมพิวเตอร์ หรือผู้กระทำได้ไปซึ่งข้อมูล หรือการกระทำต่างๆ เช่น แก้ไขเปลี่ยนแปลงหรือทำให้ข้อมูลเสียหาย หรือเป็นการเข้าถึงคอมพิวเตอร์ที่มีการติดตั้งระบบรักษาความปลอดภัย เป็นต้น

เนื่องจากการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นการทำให้เกิดความเสียหายต่อสิทธิความเป็นส่วนตัว และความลับของข้อมูล และเมื่อสามารถเข้าถึงคอมพิวเตอร์ได้แล้ว ผู้กระทำการดังกล่าวก็สามารถจะก่อให้เกิดความเสียหายอย่างใดๆ ได้อีกอาศัยเหตุผลดังกล่าว จึงสมควรกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดอาญาทันทีที่มีการเข้าถึงคอมพิวเตอร์

3. เมื่อพิจารณาถึงประสบการณ์ของประเทศสหรัฐอเมริกาในการแก้ไขปัญหาเรื่องการกระทำความผิดต่อคอมพิวเตอร์รูปแบบต่างๆ แล้ว จะเห็นว่า แม้ว่าสหรัฐอเมริกาจะมีกฎหมายที่ใช้ดำเนินคดีกับการกระทำความผิดต่อคอมพิวเตอร์หลายฉบับ แต่ในทางปฏิบัติในสหรัฐอเมริกากลับมิได้มีการเตรียมความพร้อมในเรื่องการจัดหาทรัพยากรต่างๆ ที่จำเป็นต่อการบังคับใช้กฎหมายให้มีประสิทธิภาพ เช่น เงินงบประมาณ บุคลากร และอุปกรณ์ต่างๆ เป็นต้น จนถึงกับมีการวิพากษ์วิจารณ์กันว่า “กฎหมายให้ความคุ้มครองประเทศสหรัฐอเมริกาจากปัญหาเรื่องอาชญากรรมทางคอมพิวเตอร์ในทางทฤษฎีมากกว่าทางปฏิบัติ” ในที่สุดทำให้ต้องมีการแก้ไขในเรื่องนี้มาแล้ว ส่วนประเทศไทยนอกจากควรจะต้องกำหนดฐานความผิดทางอาญาสำหรับการกระทำความผิดต่อคอมพิวเตอร์แล้ว ทุกฝ่ายที่เกี่ยวข้องกับเรื่องนี้ควรจะต้องจัดเตรียมงบประมาณ บุคลากร อุปกรณ์ เครื่องมือ ทรัพยากร การฝึกอบรมความรู้ และสิ่งอื่นๆ ที่จำเป็นต่อการบังคับใช้กฎหมายให้พร้อมด้วย เพื่อเจ้าหน้าที่สามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ

4. การป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ควรจะต้องอาศัยทั้งมาตรการทางกฎหมายและมาตรการอย่างอื่นควบคู่กันไปเสมอ ในส่วนของมาตรการทางกฎหมาย นอกจากจะต้องมีการแก้ไขปรับปรุงกฎหมายอาญาสารบัญญัติ เพื่อกำหนดฐานความผิดให้ครอบคลุมถึงการกระทำความผิดรูปแบบใหม่ที่อยู่นอกขอบเขตของกฎหมายที่ใช้บังคับอยู่เดิมแล้ว ยังต้องปรับปรุงกฎหมายอาญาวิธีสบัญญัติ เพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพและเป็นธรรมด้วย และที่สำคัญ คือ ลักษณะของการกระทำความผิดต่อคอมคอมพิวเตอร์ที่มักจะเป็นกระทำความผิดข้ามประเทศ ดังนั้นจึงต้องให้มีการร่วมมือกับประเทศต่างๆ เพื่อให้การดำเนินกับผู้กระทำความผิดเป็นไปอย่างมีประสิทธิภาพ และรวดเร็ว

5. ภาครัฐควรกำหนดนโยบายระดับชาติให้ชันเจน ทั้งในเรื่องนโยบายด้านการรักษาความมั่นคงคอมพิวเตอร์และเครือข่าย และการปราบปรามอาชญากรรมทางคอมพิวเตอร์ รวมทั้งผลักดันกฎหมายและมาตรการต่างๆ ที่จะช่วยงานป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ให้สัมฤทธิ์ผลในทางปฏิบัติอย่างเร่งด่วน เช่น การจัดตั้งองค์กรที่รับผิดชอบในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในระดับชาติ เพื่อกำหนดนโยบายระดับสูงลงสู่ระดับปฏิบัติ

6. การสร้างเครือข่ายป้องกันและปราบปรามโดยนำภาคเอกชนที่มีบทบาท เข้ามารวมมืออย่างใกล้ชิดในเรื่องต่างๆ ได้แก่ การค้นคว้าวิจัยและรักษาความปลอดภัยบนเครือข่ายคอมพิวเตอร์รวมทั้งการประสานนโยบายและการปฏิบัติร่วมกับองค์กรต่างๆ ที่เกี่ยวข้องทั้งในและต่างประเทศ

7. มาตรการอื่นๆ ที่ควรจะนำมากำหนดในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ ได้แก่

7.1 ด้านการพัฒนาบุคลากร

1) ควรมีการกำหนดผู้รับผิดชอบในการจัดทำหลักสูตรการฝึกอบรมต่างๆ เพื่อเตรียมความพร้อมของของบุคลากรในกระบวนการยุติธรรมทุดระดับ ตั้งแต่ระดับผู้ปฏิบัติการไปจนถึงระดับผู้บริหารของสำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อัยการและศาล

2) ควรมีการจัดการฝึกอบรมและให้ความรู้ (Training and Education) ทางเทคนิคการรักษาความปลอดภัยและเทคนิคการสืบหาร่องรอยการกระทำผิด (forensic) ตลอดจนประเด็นกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

3) ภาครัฐและเอกชน ควรส่งเสริมให้มีการเรียนการสอนด้านเทคโนโลยีการรักษาความปลอดภัยของระบบคอมพิวเตอร์ รวมถึงมีการสอบวัดมาตรฐานบุคลากรที่ทำงานด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ตลอดจนการสนับสนุนการพัฒนาวิชาการด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ด้วย

7.2 การบริหารและการจัดการองค์กร

1) ควรมีการจัดทำฐานข้อมูลเพื่อรวบรวมเว็บไซต์ที่มีพฤติกรรมการให้บริการแก่ผู้ใช้งานอินเตอร์เน็ตในทางที่ไม่เหมาะสม เพื่อประโยชน์ในการศึกษา และเป็นข้อมูลสนับสนุนให้แก่หน่วยงานที่เกี่ยวข้อง

7.3 ด้านเทคโนโลยี

1) หน่วยงานทั้งภาครัฐและเอกชนที่มีการใช้งานระบบเครือข่ายคอมพิวเตอร์ ควรมีการส่งเสริมให้มีการติดตั้งเทคโนโลยีต่างๆ ที่ใช้ในการป้องกันรักษาระบบเครือข่ายคอมพิวเตอร์ของตนเองให้มีความปลอดภัย รวมทั้งกำหนดให้มีการตรวจสอบประเมินความเสี่ยงของระบบคอมพิวเตอร์อย่างต่อเนื่อง อาทิ การติดตั้งระบบการตรวจสอบไวรัส (Scan virus) ระบบการตรวจจับการบุกรุก (Intrusion Detection) หรือการติดตั้งกำแพงไฟ (Firewall) เป็นต้น

7.4 ด้านมาตรการทางสังคม

1) ควรมีการกำหนดแผนการรณรงค์ประชาสัมพันธ์ ให้มีการพัฒนาและสร้างเสริมจริยธรรม เพื่อสร้างแนวปฏิบัติดีหรือวัฒนธรรมการใช้เทคโนโลยีที่ถูกต้องให้แก่คนในสังคมรวมทั้งสร้างวัฒนธรรมของความมั่นคง (Culture of Security) ในการใช้โครงสร้างพื้นฐานสารสนเทศหรือข่ายคอมพิวเตอร์ และการใช้งานอินเทอร์เน็ต โดยเริ่มจากสถาบันการศึกษา ครอบครัว และชุมชน

อย่างไรก็ตาม ปัจจุบันหน่วยงานภาครัฐและองค์กรเอกชนต่างๆ ได้มีความตื่นตัวต่อปัญหาอาชญากรรมทางคอมพิวเตอร์กันมากขึ้น แต่ปัญหาอาชญากรรมดังกล่าวนั้น ไม่สามารถแก้ไขได้โดยองค์กรใดองค์กรหนึ่ง จำเป็นต้องได้รับการร่วมมือจากทุกฝ่ายในสังคมเพราะจริงๆ แล้วปัญหาอาชญากรรมทางคอมพิวเตอร์สุดท้ายก็ขึ้นอยู่กับจริยธรรมทำของผู้ใช้งาน (User) ซึ่งต้องได้รับความร่วมมือจากสังคมในการปลูกฝังวัฒนธรรมการใช้งานที่ถูกต้อง จึงจะสามารถแก้ไขปัญหาได้อย่างแท้จริง

3.2 ข้อมูลเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์

ตาราง 3-1 สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี พ.ศ.2552-2554 ของ บก.ปอท.

สถิติคดีอาญา	รับคำร้องทุกข์	รับเรื่องส่งพนักงานสอบสวนท้องที่	รับเลขคดีอาญา	คดีเสร็จสิ้น	คดีคงค้าง	หมายเหตุ
ปี 2552 ตั้งแต่ 7 ก.ย. - 30 ธ.ค.2552	47	14	22	22	-	-
ปี 2553 ตั้งแต่ 1 ม.ค.- 30 ธ.ค.53	285	74	75	72	3	ค้างคดีที่ 38,56,64
ปี 2554 ตั้งแต่ 1 ม.ค.–31 ธ.ค.54	759	62	429	416	13	ค้างคดีที่ 7,11,27,35, 37,52,53, 54,55,56,71 72,429

ตาราง 3-2 สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี พ.ศ. 2555 ของ บก.ปอท.

สถิติคดีอาญา	รับคำร้องทุกข์	รับเรื่องส่งพนักงานสอบสวนท้องที่	รับเลขคดีอาญา	คดีเสร็จสิ้น	คดีคงค้าง	หมายเหตุ
เดือนมกราคม						
กก.1	65	-	60	60	0	
กก.2	46	1	33	31	2	ค้างคดีที่ 1/55, 2/55
กก.3	63	24	36	36	0	
เดือนกุมภาพันธ์						
กก.1	108	1	99	98	1	
กก.2	12	8	2	2	0	
กก.3	19	10	-	-	-	
เดือนมีนาคม						
กก.1	6	-	3	2	1	ค้างคดีที่ 160/55
กก.2	21	1	6	6	0	
กก.3	18	20	-	-	-	
เดือนเมษายน						
กก.1	5	-	1	1	0	ค้างคดีที่ 163/55
กก.2	6	-	-	-	-	
กก.3	10	11	1	1	0	

ตาราง 3-2 (ต่อ)

สถิติคดีอาญา	รับคำร้องทุกข์	รับเรื่องส่งพนักงานสอบสวนท้องที่	รับเลขคดีอาญา	คดีเสร็จสิ้น	คดีคงค้าง	หมายเหตุ
เดือนพฤษภาคม						
กก.1	14	-	5	4	1	**ค้างคดีที่ 168/55**
กก.2	24	1	2	1	1	**ค้างคดีที่ 42/55**
กก.3	19	6	1	1	0	
เดือนมิถุนายน						
กก.1	7	-	3	2	1	
กก.2	16	-	1	1	0	
กก.3	39	6	20	20	0	
เดือนกรกฎาคม						
กก.1	12	1	5	5	0	
กก.2	26	7	2	2	0	
กก.3	27	6	3	3	0	
เดือนสิงหาคม						
กก.1	7	-	4	4	0	
กก.2	23	-	-	-	-	
กก.3	22	4	1	1	0	
เดือนกันยายน						
กก.1	7	-	1	1	0	
กก.2	31	2	1	1	0	
กก.3	25	6	-	-	-	
เดือนตุลาคม						
กก.1	13	-	5	4	1	
กก.2	24	3	1	1	0	
กก.3	32	9	1	1	0	
เดือนพฤศจิกายน						
กก.1	7	-	4	3	1	**ค้างคดีที่ 187/55**
กก.2	36	16	2	-	2	**ค้างคดีที่ 49/55, 50/55**
กก.3	36	10	-	-	-	
เดือนธันวาคม						
กก.1	7	-	4	2	2	**ค้างคดีที่ 191/55 192/55**
กก.2	19	-	2	-	2	**ค้างคดีที่ 51/55**
กก.3	25	5	-	-	-	

ตาราง 3-3 สรุปสำนวนคดีอาญา ปี พ.ศ. 2554

เดือน	ประเภทคดี												
	หมิ่นสถาบัน	หมิ่นประมาท	การพนัน		บัตรอิเล็กทรอนิกส์	พ.ร.บ. ยา	ตั๋วปลอม	ฉ้อโกง		ลามกอนาจาร	แผ่นโปรแกรม
			ฟุตบอล (ออนไลน์)	หวย (ออนไลน์)				เจาะระบบ (Hacker)	ซื้อสินค้า (ออนไลน์)	อีเมล์ (หลอกลวง)		
มกราคม	-	-	-	-	-	-	1	2	4	1	-	-
กุมภาพันธ์	-	1	2	-	-	-	-	6	-	-	1	-
มีนาคม	-	-	4	-	-	1	-	1	1	-	1	-
เมษายน	-	2	-		-	-	-	1	1	1	-	-
พฤษภาคม	-	2	3	-	-	-	-		-	2	-	-
มิถุนายน	-	6	3	-	-	1	-		-	5	3	-
กรกฎาคม	-	2	2	-	-	-	-	1	-	-	13	3
สิงหาคม	-	1	-	-	-	-	-	-	-	1	256	1
กันยายน	1	-	-	-	-	-	-	-	-	-	88	-
ตุลาคม	-	1	-	-	-	-	-	1	-	-	-	-
พฤศจิกายน	-	-	-	-	-	-	-	1	-	-	-	-
ธันวาคม	-	-	-	-	-	-	-	-	-	1	-	-
รวม	1	15	14	0	-	2	1	13	6	11	362	4

ตาราง 3-4 สรุปสำนวนคดีอาญา กก.1 บก.ปอท. ปี พ.ศ. 2555

เดือน	ประเภทคดี											
	หมิ่นพระบรมเดชานุภาพ	เข้าถึงโดยมิชอบซึ่งระบบและข้อมูลคอมฯ	การพนัน		ทำให้เสียหาย ทำลาย แก้ไขข้อมูลคอมฯ	นำเข้าสู่ระบบซึ่งข้อมูลที่มีลักษณะลามก	นำเข้าสู่ระบบซึ่งข้อมูลปลอมหรือข้อมูลอันเป็นเท็จ	นำเข้าข้อมูลเท็จเสียหายต่อความมั่นคง	จำหน่ายชุดคำสั่งที่ใช้กระทำผิด	ผู้ให้บริการไม่เก็บข้อมูลการจราจร	จำหน่ายซีดีลามก	จำหน่ายสินค้าหนีภาษี
			ฟุตบอล (ออนไลน์)	หวย (ออนไลน์)								
มกราคม	-	-	1	-	-	58	-	-	-	-	1	-
กุมภาพันธ์	-	1	1	-	1	94	1	-	-	๑		-
มีนาคม	-	1	-	-	1	-	-	-	-	-	1	-
เมษายน	-	-	-		1	-	-	-	-	-	-	-
พฤษภาคม	-	1	2	-	-	-	-	-	2	-	-	-
มิถุนายน	-	1	2	-	-		-	-	-	-	-	-
กรกฎาคม	-	-	2	-	-	-	-	-	2	-	-	1
สิงหาคม	-	-	4	-	-	-	-	-	-	-	-	-
กันยายน	-	-	1	-	-	-	-	-	-	-	-	-
ตุลาคม	-	-	3	1	-	-	-	-	-	-	-	-
พฤศจิกายน	-	-	2	1	1	-	-	-	-	-	-	-
ธันวาคม	-	-	4	-	-	-	-	-	-	-	-	-
รวม	0	4	22	2	4	152	1	0	4	1	2	1

ตาราง 3-5 สรุปสำนวนคดีอาญา กก.2 บก.ปอท. ปี พ.ศ. 2555

เดือน	ประเภทคดี											
	หมิ่นพระบรมเดชานุภาพ	เข้าถึงโดยมิชอบซึ่งระบบและข้อมูลคอมฯ	การพนัน		ทำให้เสียหาย ทำลาย แก้ไขข้อมูลคอมฯ	นำเข้าสู่ระบบซึ่งข้อมูลที่มีลักษณะลามก	นำเข้าสู่ระบบซึ่งข้อมูลปลอมหรือข้อมูลอันเป็นเท็จ	นำเข้าข้อมูลเท็จเสียหายต่อความมั่นคง	จำหน่ายชุดคำสั่งที่ใช้กระทำผิด	ผู้ให้บริการไม่เก็บข้อมูลการจราจร	จำหน่ายซีดีลามก	จำหน่ายสินค้าหนีภาษี
			ฟุตบอล (ออนไลน์)	หวย (ออนไลน์)								
มกราคม	-	-	-	-	-	30	-	-	-	3	-	-
กุมภาพันธ์	-	-	-	-	-	-	-	-	-	2	-	-
มีนาคม	-	-	-	-	-	-	-	2	-	3	1	-
เมษายน	-	-	-		-	-	-	-	-	-	-	-
พฤษภาคม	-	-	1	-	-	-	-	-	-	1	-	-
มิถุนายน	-	-	-	-	-		-	-	-	1	-	-
กรกฎาคม	-	-	2	-	-	-	-	-	-	-	-	-
สิงหาคม	-	-	-	-	-	-	-	-	-	-	-	-
กันยายน	-	-	-	-	-	-	-	-	-	1	-	-
ตุลาคม	-	-	1	-	-	-	-	-	-	-	-	-
พฤศจิกายน	-	1	-	-	-	1	-	-	-	-	-	-
ธันวาคม	-	-	-	-	-	-	2	-	-	-	-	-
รวม	**0**	**1**	**4**	**0**	**0**	**31**	**2**	**2**	**0**	**11**	**1**	**0**

ตาราง 3-6 สรุปสำนวนคดีอาญา กก.3 บก.ปอท. ปี พ.ศ. 2555

เดือน	ประเภทคดี											
	หมิ่นพระบรมเดชานุภาพ	เข้าถึงโดยมิชอบซึ่งระบบและข้อมูลคอมฯ	การพนัน		ทำให้เสียหาย ทำลาย แก้ไข ข้อมูลคอมฯ	นำเข้าสู่ระบบซึ่งข้อมูลที่มีลักษณะลามก	นำเข้าสู่ระบบซึ่งข้อมูลปลอมหรือข้อมูลอันเป็นเท็จ	นำเข้าข้อมูลเท็จเสียหายต่อความมั่นคง	จำหน่ายชุดคำสั่งที่ใช้กระทำผิด	ผู้ให้บริการไม่เก็บข้อมูลการจราจร	จำหน่ายซีดีลามก	จำหน่ายสินค้าหนีภาษี
			ฟุตบอล (ออนไลน์)	หวย (ออนไลน์)								
มกราคม	-	-	-	-	-	36	-	-	-	-	-	-
กุมภาพันธ์	-	-	-	-	-	-	-	-	-	-		-
มีนาคม	-	-	-	-	-	-	-	-	-	-	-	-
เมษายน	-	-	-		-	-	-	-	-	1	-	-
พฤษภาคม	-	-	-	-	-	-	-	-	1	-	-	-
มิถุนายน	20	-	-	-	-	-	-	-	-	-	-	-
กรกฎาคม	-	-	-	-	-	-	2	1	-	-	-	-
สิงหาคม	-	-	-	-	-	-	1	-	-	-	-	-
กันยายน	-	-	-	-	-	-	-	-	-	-	-	-
ตุลาคม	-	-	1	-	-	-	-	-	-	-	-	-
พฤศจิกายน	-	-	-	-	-	-	-	-	-	-	-	-
ธันวาคม	-	-	-	-	-	-	-	-	-	-	-	-
รวม	20	0	1	0	0	36	3	1	1	1	0	0

ตาราง 3-7 ข้อมูลสถิติด้านการสอบสวนละปราบปรามจับกุมคดีเว็บไซต์หมิ่นสถาบันฯ จาก ตร. ของ บก. ปอท.

หน่วยงาน	รับผิดชอบ	เสร็จสิ้น	อยู่ระหว่างดำเนินการ	จับกุมผู้กระทำผิดได้	หมายเหตุ
กก.1	5,469	4,616	853	-	
กก.2	5,665	4,368	1,297	-	
กก.3	4,962	3,992	970	-	
รวม	**16,096**	**12,976**	**3,120**	-	

ตาราง 3-8 ข้อมูลสถิติด้านการสอบสวนละปราบปรามจับกุมคดีเว็บไซต์หมิ่นสถาบันฯ จาก ICT ของ บก. ปอท.

หน่วยงาน	รับผิดชอบ	เสร็จสิ้น	อยู่ระหว่างดำเนินการ	จับกุมผู้กระทำผิดได้	หมายเหตุ
กก.1	4,814	-	4,814	-	
กก.2	7,134	-	7,134	-	
กก.3	3,481	3,458	23	-	
รวม	**15,429**	**3,458**	**11,971**	-	

ตาราง 3-9 ข้อมูล (URL) ที่ได้รับจากคณะอนุกรรมการตรวจสอบและพิจารณาข้อมูลข่าวสารที่ผิดกฎหมายฯ

	ส่งสำนวนให้อัยการสูงสุดพิจารณา	อยู่ระหว่างดำเนินการ	รวม
กก.1	4,548	922	**4,470**
กก.2	4,368	1,297	**5,665**
กก.3	3,299	1,663	**4,962**
รวม	**12,214**	**3,882**	**16,096**

ตาราง 3-10 ข้อมูล (URL) ที่ได้รับจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

	ส่งสำนวนให้อัยการสูงสุดพิจารณา	อยู่ระหว่างการสอบสวน	รวม
กก.1	-	4,814	**4,814**
กก.2	-	7,134	**7,134**
กก.3	-	3,481	**3,481**
รวม	**-**	**15,429**	**15,429**

3.3 ข้อมูลคดีอาชญากรรมคอมพิวเตอร์ที่ประสบความสำเร็จ (Best Practice) และกรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด

3.3.1 กรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด กรณีที่ 1 แก๊งคอลเซ็นเตอร์ในรูปแบบอาชญากรข้ามชาติ

"แก๊งคอลล์เซ็นเตอร์" หรือการใช้ระบบโทรศัพท์ข้ามประเทศ ล่อหลอกให้เหยื่อโอนเงินผ่านตู้เอทีเอ็ม ซึ่งกำลังระบาดอย่างหนักในปัจจุบัน โดยผู้ตกเป็นเหยื่อไม่จำเป็นว่าจะเป็นเพศไหน วัยไหน ฐานะหรือสาขาอาชีพ เพราะแม้แต่แพทย์ ผู้พิพากษา หรือตำรวจ ก็ยังเคย"พลาด" โอนเงินให้กับแก๊งเหล่านี้มาแล้ว จึงขอเจาะข้อมูลเกี่ยวกับ **"แก๊งคอลล์เซ็นเตอร์"** เพื่อเป็นเครื่องเตือนใจให้กับเราๆ ท่านๆ ป้องกันการตกเป็นเหยื่อให้ต้องเสียทั้งเงิน เจ็บทั้งใจ ทั้งนี้สภาพปัญหาแก๊ง Call Center มีพฤติกรรมการหลอกลวงเหยื่อโอนเงินผ่านตู้เอทีเอ็มเข้าบัญชีที่เปิดไว้ ซึ่งก่อให้เกิดความเดือดร้อนกับประชาชนในทุกกลุ่มระดับอาชีพและการศึกษา เช่น เกิดการกระทำความผิดมากในช่วงช่วงระยะเวลาการชำระและคืนภาษีประจำปี และเนื่องจากสถาบันการเงินได้ส่งเสริมให้ลูกค้าผู้รับบริการได้จัดการการเงินโดยสามารถทำธุรกรรมทางอิเล็กทรอนิกส์ได้ ยิ่งส่งผลให้แก๊ง Call Center มีพฤติกรรมหลอกลวงประชาชน โดยทำให้ประชาชนเกิดความกลัว หรือ ทำให้เกิดความโลภ และตกเป็นเหยื่อโอนเงินผ่านเข้าบัญชีของแก๊ง Call Center

วีโอไอพี คือ อะไร

วีโอไอพี (VoIP) ย่อมาจาก วอยซ์โอเวอร์ไอพี (Voice over Internet Protocol) (หรือชื่ออื่น IP Telephony, Internet telephony, หรือ Digital Phone) เป็นการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต หรือโครงข่ายอื่น ๆ ที่ใช้อินเทอร์เน็ตโพรโทคอล สัญญาณเสียงจะถูกตัดแบ่งเป็นแพ็คเก็ตวิ่งผ่านไปบนโครงข่ายที่ใช้สำหรับการสื่อสารข้อมูลทั่วไป แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์แบบดั้งเดิม เปรียบได้กับการให้รถยนต์วิ่งแทรกกันได้ตามช่องว่างที่มีอยู่ของถนน แทนการให้รถยนต์คันเดียวจองถนนวิ่งแบบผูกขาด ข้อดีของวีโอไอพีก็คือการสามารถใช้โครงข่ายได้อย่างมีประสิทธิภาพ ทำให้สามารถให้บริการได้ในอัตราค่าบริการที่ถูกลงมาก ในการใช้บริการวีโอไอพี ผู้ใช้บริการจะต้องเชื่อมต่อกับอินเทอร์เน็ตก่อน หลังจากนั้น สามารถใช้โปรแกรมคอมพิวเตอร์ที่เรียกว่า ซอฟท์โฟน และไมโครโฟนกับหูฟัง เพื่อพูดคุยกับปลายทางได้ ในปัจจุบัน มีอุปกรณ์ที่เรียกว่า อะนาล็อกเทเลโฟนอะแด็ปเตอร์ เข้ามาแทนการใช้คอมพิวเตอร์ต่อกับอินเทอร์เน็ต และใช้เครื่องโทรศัพท์อะนาล็อกที่ใช้งานตามบ้านหรือสำนักงานทั่วไปในการโทรศัพท์แบบวีโอไอพีได้ ทำให้ได้รับความสะดวกและความรู้สึกไม่แตกต่างจากการใช้โทรศัพท์แบบดั้งเดิม การใช้งานวีโอไอพีสามารถใช้งานได้ทั้งในการโทรศัพท์ถึงปลายทางที่เป็นวีโอไอพีเช่นเดียวกัน ซึ่งส่วนใหญ่จะไม่มีการเก็บค่าบริการ แต่ทั้งสองข้างจะต้องออนไลน์พร้อมกัน หรือจะโทรไปยังปลายทางที่เป็นหมายเลขโทรศัพท์ปกติ ทั้งโทรศัพท์ประจำที่หรือโทรศัพท์เคลื่อนที่ก็ได้ ในกรณีนี้ จะต้องมีการสมัครเป็นสมาชิกของบริการและชำระค่าบริการล่วงหน้า แต่ค่าบริการจะถูกกว่าการโทรศัพท์ปกติมาก จุดด้อยของวีโอไอพี คือ ในบางกรณีคุณภาพ

เสียงอาจจะไม่ดีเท่าโทรศัพท์ปกติ และอาจจะมีการดีเลย์หรือการที่สัญญาณเสียงเดินทางมาช้า ทำให้พูดสวนกันไม่ได้ถนัด ต้องรอให้แต่ละฝ่ายพูดให้จบก่อนจึงจะพูดได้ แต่ปัญหานี้ได้รับการปรับปรุงขึ้นมาอย่างต่อเนื่องจนแทบจะไม่มีความแตกต่างอีกต่อไป ข้อเสียอีกประการหนึ่งก็คือ โทรศัพท์วีโอไอพี จะใช้งานไม่ได้เมื่อไฟฟ้าดับ หรืออินเทอร์เน็ตเกิดขัดข้อง

วีโอไอพี หรือที่เรียกกันย่อ ๆ ว่า “วอยซ์” ได้รับความนิยมมากขึ้น เนื่องจากคุณภาพที่ได้รับปรับปรุงและค่าใช้จ่ายที่ถูก จนในที่สุดอาจจะกลายเป็นบริการฟรี เช่น เดียวกับการใช้งานอินเทอร์เน็ตอื่น ๆ เช่น การสืบค้นเว็บไซต์ การใช้อีเมลล์ เพราะอันที่จริงก็ไม่มีความแตกต่างกันมากนัก ผู้ใช้บริการเพียงแต่จ่ายค่าเชื่อมต่ออินเทอร์เน็ตเท่านั้น เนื่องจากในปัจจุบัน วีโอไอพี ไม่มีหมายเลขของตัวเอง ได้มีความพยายามที่จะสร้างเลขหมายโทรศัพท์สำหรับวีโอไอพีที่ใช้งานได้ทั่วโลก เรียกว่า “อีนัม” (enum) ซึ่งถ้าได้มีการยอมรับแพร่หลาย เราก็จะมีหมายเลขนี้ติดตัวเราไปได้ทุกที่ทั่วโลก เพียงแต่เข้าอินเทอร์เน็ตได้ก็สามารถติดต่อกันได้โดยกดหมายเลขอีนัมคล้าย ๆ กับโทรศัพท์ในปัจจุบัน ถ้าโครงข่ายไว-ไฟ หรือ ไวแม็กซ์ มีการขยายครอบคลุมมากขึ้น ก็เป็นไปได้ว่าจะมีอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตผ่านไว-ไฟ หรือ ไวแม็กซ์ ที่สามารถใช้วีโอไอพีได้ ซึ่งจะมีความสามารถสูงกว่าโทรศัพท์เคลื่อนที่ในปัจจุบันเป็นอย่างมาก เนื่องจากมีแบนด์วิดธ์ที่กว้าง การใช้วีดีโอโฟน จะกลายเป็นมาตรฐานทั่วไป ในปัจจุบัน ก็เริ่มมีการวางตลาดเครื่องโทรศัพท์มือถือที่ใช้เป็นโทรศัพท์ไว-ไฟในตัวบ้างแล้วแก๊งอาชญากรข้ามชาติได้ใช้เป็นช่องทางแอบอ้างและหลอกเหยื่อให้โอนเงินในรูปแบบต่าง ๆ เพื่อมิให้ตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์ ถ้าเจอเหตุการณ์ลักษณะดังกล่าวจึงควรจะตั้งสติ ถ้ามีการโทรแอบอ้างมาจึงควรที่จะโทรกลับไปเช็คหน่วยงานที่แก๊งคอลเซ็นเตอร์ได้แอบอ้างไว้ ที่สำคัญควรตรวจสอบความเคลื่อนไหวของบัญชียอดเงินรวมไปถึงยอดหนี้ค้างชำระของตนเองเสมอเชื่อว่าแก๊งมิจฉาในคราบอาชญากรรมคอลเซ็นเตอร์ข้ามชาติที่มาในรูปแบบหลากหลายก็ไม่สามารถทำอะไรเราได้อย่างแน่นอน

รูปแบบ และวิธีการของผู้กระทำความผิด

- เกือบทั้งหมดเป็นชาวจีนแผ่นดินใหญ่ และไต้หวัน ส่วนคนไทยหรือคนชาติอื่นที่เข้าร่วมขบวนการ เป็นเพียงพนักงานรับโทรศัพท์กับผู้เปิดบัญชีรับเงินที่ได้จากการล่อลวงเท่านั้น

- การตั้งคอลล์เซ็นเตอร์มี 2 รูปแบบ คือ

1) ตั้งศูนย์ในประเทศไทย (เพื่อโทร.กลับไปล่อลวงชาวจีนแผ่นดินใหญ่หรือไต้หวัน) โดยเช่าบ้านหรูตามหมู่บ้านในกรุงเทพฯหรือเมืองท่องเที่ยวสำคัญๆ เช่น เชียงใหม่ ภูเก็ต จากนั้นว่าจ้างชาวจีนแผ่นดินใหญ่หรือไต้หวันเข้ามาพักที่บ้าน โดยจะมีอุปกรณ์ต่างๆ ให้พร้อม และติดตั้งระบบโทรศัพท์ข้ามประเทศผ่านอินเตอร์เน็ต หรือ VOIP (Voice over Internet Protocol) โทรศัพท์กลับไปหลอกเหยื่อชาวจีนหรือไต้หวัน

2) ตั้งศูนย์นอกประเทศไทย ที่ตำรวจเคยจับกุมได้เกือบทั้งหมดอยู่ที่ประเทศจีน โดยศูนย์จะอยู่ตามห้องพักหรือแฟลตต่าง ๆ มีนายทุนจ้างคนไทยทำหน้าที่เป็นคอลล์เซ็นเตอร์โทรศัพท์กลับมาหลอกเหยื่อชาวไทย

- **คอลล์เซ็นเตอร์ทั้ง 2 แบบ** จะมีการว่าจ้างคนในประเทศนั้น ๆ (ประเทศที่โทร.ไปล่อลวง) ไปเปิดบัญชีธนาคารรอเอาไว้ เช่น หลอกเหยื่อคนไทยก็จะจ้างคนไทยไปเปิดบัญชีธนาคารเอาไว้ จากนั้นจะมี **"ม้าวิ่ง"** คือชาวจีนหรือไต้หวัน ทำหน้าที่ตระเวนกดเงินตามตู้เอทีเอ็ม ต่าง ๆ เพื่อกดเงินออกจากบัญชีที่เปิดรอไว้ดังกล่าว เมื่อได้เงินมาก็จะส่งเงินต่อไปยังกลุ่มขบวนการด้วยวิธีการต่าง ๆ เช่น รวบรวมเป็นเงินสดหิ้วออกนอกประเทศ หรือนำไปโอนผ่านบัญชีธนาคาร หรือใช้ระบบโพยก๊วน

- **"ม้าวิ่ง"** จะเดินทางเข้าออกประเทศมาแล้วหลายครั้ง หลังทำงานเสร็จก็เดินทางกลับ แต่ยังไม่แน่ชัดว่าแต่ละกลุ่มที่เข้ามานั้นอยู่ในประเทศนานเท่าไร

- ผู้ต้องหาส่วนใหญ่ที่จับกุมได้ จะเป็นคนที่ทำหน้าที่คอลล์เซ็นเตอร์, คนไทยที่ถูกจ้างให้เปิดบัญชี และ "ม้าวิ่ง" ที่กดเงินตามตู้เอทีเอ็ม แต่ยังไม่เคยสาวไปถึงนายทุนใหญ่ที่อยู่เบื้องหลังได้เลยแม้แต่ครั้งเดียว

- วิธีการหลอก จะมีการเขียนสคริปต์ให้คนที่ถูกจ้างมาเป็นคอลล์เซ็นเตอร์ใช้พูดตามบทที่เขียนขึ้น ซึ่งที่พบมีทั้งภาษาไทยและภาษาจีน ส่วนเนื้อหาในสคริปต์จะมีใจความที่ทำให้เหยื่อเกิดความโลภหรือความหวาดกลัว เช่น ในช่วงที่ประชาชนต้องทำเรื่องเสียภาษี แก๊งคนร้ายก็จะฉวยโอกาสสมอ้างเป็นเจ้าหน้าที่สรรพากรหลอกว่ามีเงินภาษีคืน ให้ไปทำธุรกรรมทางตู้เอทีเอ็ม จะได้สะดวก ได้เงินคืนทันที ไม่ต้องเสียเวลามาทำเรื่อง หรืออ้างว่าถูกรางวัลจากการสุ่มเบอร์

- ส่วนการหลอกด้วยความหวาดกลัวนั้น มักจะอ้างเป็นเจ้าหน้าที่ธนาคาร เจ้าหน้าที่รัฐ เช่น ปปง. ดีเอสไอ กรมสรรพากร เจ้าหน้าที่ศาล เนื้อหาหลักๆ จะพุ่งเป้าไปที่บัญชีธนาคารของเหยื่อมีปัญหาต่าง ๆ นานา

- หลังทำให้เหยื่อเกิดความโลภหรือหวาดกลัวแล้ว ผู้ที่ทำหน้าที่คอลล์เซ็นเตอร์ก็จะหว่านล้อมด้วยคำพูดแบบหวังดีคือต้องการช่วยเหลือ แต่แท้ที่จริงแล้วประสงค์ร้าย โดยพูดอย่างไรก็ได้ให้เหยื่อไปที่ตู้เอทีเอ็มเพื่อกดโอนเงินไปเข้าบัญชีที่แก๊งคนร้ายเปิดรอไว้แล้ว

กลุ่มผู้กระทำความผิดที่พบบ่อย

กลุ่มผู้กระทำความผิด "คอลล์เซ็นเตอร์" ที่ปฏิบัติการหลอกลวงเหยื่อเอาไว้อย่างน่าสนใจ โดยแบ่งออกเป็น 2 กลุ่มใหญ่ๆ คือ

1) กลุ่มผู้กระทำความผิดคืนเงินภาษี

คนร้ายจะหลอกเหยื่อว่าได้รับภาษีตกค้างคืนเนื่องจากมีการปรับลดหรือเหตุผลอื่นๆ หากต้องการเงินภาษีดังกล่าวต้องรีบดำเนินการภายในวันนี้เท่านั้น (แน่นอนว่าเหยื่ออยากได้เงินแต่ไม่มีเวลา) คนร้ายจะดำเนินการต่อไปดังนี้

- แนะนำให้ไปที่ตู้เอทีเอ็มที่คนร้ายถนัด

- ทำอย่างไรก็ได้ให้ผู้เสียหายเลือกเมนูภาษาอังกฤษ และพูดโต้ตอบอย่างรวดเร็วให้ผู้เสียหายสับสนจนต้องรีบทำการที่คนร้ายบอก

- หลอกให้อ่านตัวเลขและโอนเงินของเหยื่อ กว่าเหยื่อจะรู้ตัวว่าถูกหลอกก็ต่อเมื่อโอนเงินไปแล้ว

- คนร้ายวางหู ในช่วงนี้เหยื่อจะมีเวลาคิดและรู้ว่าถูกหลอก แต่สายเสียแล้ว

2) กลุ่มผู้กระทำความผิดหนี้บัตรเครดิต

คนร้ายจะหลอกเหยื่อว่ามีหนี้บัตรเครดิตจากธนาคารต่างๆ ไม่ว่าเหยื่อจะมีบัตรเครดิตหรือบัญชีของธนาคารนั้นๆ หรือไม่ แน่นอนว่าเหยื่อจะต้องตกใจ จากนั้นคนร้ายจะดำเนินการต่อไปดังนี้

- เริ่มหลอกเหยื่อโดยใช้หมายเลขที่ไม่มีในสารบบ เช่น มีเครื่องหมายบวกอยู่ด้านหน้า หรือเป็นหมายเลขที่ไม่โชว์เบอร์

- คนร้ายจะใช้เสียงพูดที่บันทึกเสียงสุภาพสตรีหรือสุภาพบุรุษเลียนแบบทางธนาคาร

- คนร้ายจะพูดหลอกลวงเหยื่อ เช่น ท่านมีหนี้ค้างบัตรเครดิตของธนาคาร...100,000 บาท ฟังซ้ำกด 1 ภาษาอังกฤษกด 2 ติดต่อเจ้าหน้าที่กด 9

- เมื่อเหยื่อกด 9 จะมีคนร้ายอีกหนึ่งคนพูดจาไพเราะว่าเขาเป็นเจ้าหน้าที่ เพิ่งได้รับโอนสายจากคอลล์ เซ็นเตอร์ ไม่ทราบรายละเอียด กรุณาแจ้งชื่อ สกุล เลขบัตรประชาชน อายุ ที่อยู่ เบอร์ที่ทำงาน เลขบัญชีและเลขบัตรเครดิตหากท่านมี จากนั้นจะหว่านล้อมอย่างรวดเร็วถึงวิธีการระงับหนี้แบบเร่งด่วนโดยโอนสายไปยังคนร้ายอีกคน

- คนร้ายคนที่สามจะดำเนินการหลอกเหยื่อโดยแนะนำตนเองว่าเป็นเจ้าหน้าที่ฝ่ายกฎหมายและเร่งรัดหรือประนอมหนี้ธนาคาร ซึ่งพูดจารวดเร็วหว่านล้อมให้รีบระงับหนี้โดยทำธุรกรรมทางโทรศัพท์ หากต้องการให้กดตามที่คนร้ายบอก หรือรีบไปที่ตู้เอทีเอ็ม จากนั้นคนร้ายจะให้เลือกเมนูภาษาอังกฤษ และหลอกให้ผู้เสียหายปฏิบัติตามจนเสร็จสิ้นและวางหูไป ช่วงนี้ผู้เสียหายถึงมีเวลาคิดจึงรู้ว่าถูกหลอก

รูปแบบหนึ่งของ แก๊งคอลล์เซ็นเตอร์ ที่ทำการหลอก ข่มขู่ หาข้อมูล จากประชาชนทั่วไปโดยการสุ่มโทร ผสมกับหลากหลายรูปแบบในการหลอกลวง อาทิ โทรมาจากธนาคารพาณิชย์แอบอ้างว่าติดค้างหนี้อยู่ให้ไปที่ตู้ ATM เพื่อโอนเงินมาชำระหนี้ โทรมาจากศาลอาญาว่าไปทำความผิดเกี่ยวกับธุรกรรมทางการเงินและจะถูกออกหมาย จับถ้าไม่โอนเงินมาตามที่แอบอ้าง หรือโทรมาจากเจ้าหน้าที่สรรพากรอ้างว่ายังไม่ได้ชำระหนี้และข่มขู่เอาข้อมูล จากบัตรประชาชน เพื่อที่สามารถตรวจสอบข้อมูลต่างๆของคนอื่น เช่นข้อมูลทางการเงิน ข้อมูลบัตรเครดิต ฯลฯ ได้มากมาย หรือกระทั่งอ้างว่าเป็นเจ้าหน้าที่กรมสรรพากรหลอกว่าจะโอนภาษีเงินได้เข้า บัญชีให้และหลอกให้ผู้เสียหายไปกดเงินที่ตู้ ATM เมื่อเหยื่อหลงเชื่อจึงให้โอนเข้าบัญชีของแก๊งคอลล์เซ็นเตอร์ที่เป็นขบวนการมีทั้งคนไทยและชาวต่างประเทศ ฯลฯ ซึ่งการสูญเสียเงินและทรัพย์สินจะเกิดขึ้นอย่างแน่นอนถ้าไม่รู้เท่าทันมิจฉาชีพ รูปแบบของ แก๊งคอลล์เซ็นเตอร์ ที่ปัจจุบันมีเครือข่ายโยงใยกับกลุ่มบุคคลต่างชาติในแถบเอเชียเป็นส่วนใหญ่

3.3.2 กรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด กรณีที่ 2 การจับกุมแก๊ง Call Center ที่ตั้งในสาธารณรัฐประชาชนจีน

รูปแบบ และวิธีการของผู้กระทำความผิด

มีแผนประทุษกรรมว่ากลุ่มผู้ต้องหาได้ใช้บ้านเช่าในหมู่บ้านหรู และตั้งสำนักงานคอลล์เซ็นเตอร์ เพื่อให้สมาชิกในแก๊งใช้โทรศัพท์มือถือโทรสุ่มหาผู้เสียหายผ่านเครื่องขยาย ช่องสัญญาณอินเทอร์เน็ต จากนั้นระบบจะรันสุ่มต่อสายให้โทรหาเบอร์ผู้เสียหาย โดยแก๊งผู้ต้องหาจะแบ่งหน้าที่ทำงานกันเป็นทีม ทีมแรกจะทำหน้าที่โทรเข้าไปหาผู้เสียหาย พร้อมหลอกว่าเป็นเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมาย ได้ตรวจสอบมีเงินจากขบวนการอาชญากรรม โอนไปยังบัญชีผู้เสียหาย ทำให้ผู้เสียหายตกใจกลัว จากนั้นจะบอกว่าเจ้าหน้าที่จะขอตรวจสอบบัญชีการเงิน ขอให้ผู้เสียหายบอกชื่อ สกุล อายุ วัน เกิด ที่อยู่ บัญชีธนาคาร เพื่อขอตรวจสอบ เมื่อผู้เสียหายปฏิเสธว่าไม่เกี่ยวข้องกับขบวนการอาชญากรรม แก๊งผู้ต้องหาจะทำทีโอนสายให้คุยกับอีกทีมที่ปลอมตัวเจ้าหน้าที่ของหน่วยงานต่างๆ ถ้าผู้เสียหายหลงเชื่อ แก๊งผู้ต้องหาจะหลอกให้ผู้เสียหายไปที่ทำธุรกรรมโอนเงินที่ตู้เอทีเอ็ม กดรหัสและเปลี่ยนเมนูเป็นภาษาอังกฤษ และบอกให้ทำตามขั้นตอนต่าง ๆ ในที่สุดเหยื่อจะถูกหลอกให้กดโอนเงินเข้าบัญชีของแก๊งผู้ต้องหา หรืออีกวิธีแก๊งผู้ต้องหาจะอ้างว่าเป็นเจ้าหน้าที่ธนาคาร หลอกเหยื่อว่าเป็นหนี้บัตรเครดิตจำนวนมาก เมื่อเหยื่อปฏิเสธ ก็จะสอบถามข้อมูลส่วนตัว พร้อมหลอกให้ไปกดโอนเงินที่ตู้เอทีเอ็ม โดยอ้างว่าจะขอตรวจสอบบัญชีธนาคาร หรืออีกวิธีผู้ต้องหาจะแจ้งว่า เป็นเจ้าหน้าที่กรมสรรพากร โทรศัพท์บอกผู้เสียหายว่า ได้รับคืนภาษี ขอให้ผู้เสียหายไปทำตามขั้นตอนที่ตู้เอทีเอ็มเพื่อขอรับเงินภาษีคืน จนเหยื่อพลาดท่าหลงเชื่อโอนเงินเข้าบัญชีผู้ต้องหาเป็นจำนวนมาก โดยแก๊งคอลล์เซ็นเตอร์ทำให้ผู้เสียหายสูญมูลค่าไม่ต่ำกว่า 100 ล้านบาท และจากการตรวจสอบเส้นทางทางการเงิน พบว่าแก๊งผู้คอลล์เซ็นเตอร์นั้น ได้โอนเงินของผู้เสียหายเข้าไปในบัญชีธนาคารของแก๊งคอลล์เซ็นเตอร์ที่ร่วมทำกันเป็นขบวนการในประเทศจีน และไต้หวัน ซึ่งกลุ่มผู้กระทำความผิดนี้จัดว่าเป็นขบวนการอาชญากรรมข้ามชาติรายใหญ่ที่มีเครือข่ายมากมาย พวกนี้จะเข้ามาใช้ประเทศไทยเพื่อใช้เป็นฐานตั้งคอลล์เซ็นเตอร์ สุ่มโทรศัพท์หลอกเหยื่อในหลายประเทศในภูมิภาคเอเชีย

สรุปผล

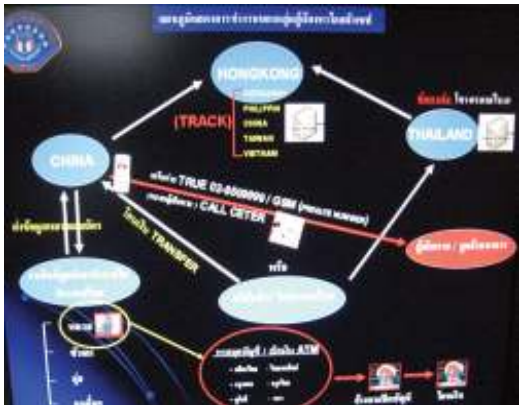
1) การจับกุมแก๊ง Call Center ร่วมกับเจ้าหน้าที่ของสาธารณรัฐประชาชนจีนที่โทรศัพท์หลอกลวงคนไทย

1.1 เมื่อ พ.ศ. 2551 ที่เมืองซัวเถา สาธารณรัฐประชาชนจีน จับกุมผู้ต้องหาชาวไทย จำนวน 42 คน และนำกลับมาเพื่อดำเนินคดีฉ้อโกงประชาชนในประเทศไทย โดยศาลมีคำพิพากษาแล้วบางส่วน และบางส่วนผู้ต้องหายังอยู่ในกระบวนการทางศาล

1.2 เมื่อวันที่ 8 เมษายน 2553 ที่เมืองฉางอัน เขตตงก่วน มณฑลกวางตุ้ง จับกุมผู้ต้องหาชาวไทยจำนวน 13 คน ซึ่งขณะนี้อยู่ระหว่างการดำเนินคดีที่สาธารณรัฐประชาชนจีน และยังนำตัวกลับประเทศไทย

กรณีตั้งศูนย์ Call center ในต่างประเทศ คนร้ายจ้างคนไทยเดินทางไปทำงานรับโทรศัพท์ โดยเข้ามาเช่าที่พักอาศัยในสาธารณรัฐประชาชนจีน และมีพฤติกรรมหลอกลวงเหยื่อที่มีสัญชาติไทยที่อยู่ในประเทศไทย โดยโทรศัพท์จากสาธารณรัฐประชาชนจีนเพื่อไปหลอกเหยื่อชาวไทย ที่อยู่ในประเทศไทยให้โอนเงินเข้าบัญชีที่ประเทศไทย และผู้ร้ายจะกดเงินจากตู้เอทีเอ็มในประเทศไทย

โดยกลุ่มคนร้ายมีเทคโนโลยีอันทันสมัยได้ทำการหลอกลวงให้ผู้เสียหายโอนเงินผ่านระบบบัตรอิเล็กทรอนิกส์ โดยกลุ่มคนร้ายฉ้อโกงประชาชนด้วยวิธีการต่างๆ อาทิเช่น แจ้งว่าเป็นผู้ถูกรางวัลของสลากกินแบ่งรัฐบาล ได้รับเงินภาษีเงินส่วนบุคคลคืนจากราชการ เป็นหนี้จากการใช้บัตรเครดิต หรือถูกกลุ่มมิจฉาชีพนำบัตรเครดิตของผู้เสียหายไปใช้ ทำให้ผู้เสียหายหลงเชื่อตกเป็นเหยื่อ เกิดความเสียต่อประชาชนเป็นจำนวนมาก คณะทำงานสืบสวนปราบปรามฯ ได้ดำเนินการสืบสวนจนทราบว่ากลุ่มคนร้ายมีศูนย์ Call Center อยู่ในประเทศจีน จึงได้ร่วมกับสถานเอกอัครราชทูตสาธารณรัฐประชาชนจีนประจำประเทศไทย ร่วมสืบสวนติดตามจับกุมคนร้ายที่ฉ้อโกงประชาชนไทยด้วยวิธีการต่าง ๆ ในประเทศจีน ณ มณฑลกวางตุ้ง ประเทศจีน ตั้งแต่เดือนพฤศจิกายน 2550



ภาพ 3-1 ภาพแสดงการทำงานของกลุ่มผู้ต้องหาโดยสังเขป

จนทราบว่า กลุ่มคนร้ายทำเป็นรูปขบวนการ แบ่งหน้าที่กันทำการหลอกลวงฉ้อโกงประชาชนมานานประมาณ 8 ปี มีผู้เสียหายจำนวนมากในหลายประเทศในเขตเอเชียตะวันออกเฉียงใต้ อาทิ ไทย,มาเลเซีย,ไต้หวัน และจีน เป็นต้น จนกระทั่งต่อมา คณะทำงานสืบสวนปราบปราม ฯ ร่วมกับตำรวจจีน ทำการตรวจค้นอาคารโย่ว หยี ต้า ซ่า เมืองซัวเถา ประเทศจีน ซึ่งคนร้ายใช้เป็นที่ตั้ง Call Center ที่ใช้หลอกผู้เสียหายชาวไทย ผลการตรวจค้นจับกุมได้ผู้ต้องหาที่เป็นคนไทย จำนวน 42 คน (เป็นชาย 24 คน หญิง 18 คน) และยังมีผู้ต้องหาเป็นคนจีน ไต้หวัน เกาหลี และมาเลเซีย อีกจำนวนมาก ซึ่งทางตำรวจจีนได้ขอดำเนินคดีกับผู้ต้องหาทั้งหมดตามกฎหมายจีนก่อน ต่อมาคณะทำงานสืบสวนปราบปรามฯ ได้ดำเนินการประสานกับทางตำรวจจีนมาโดยตลอดเพื่อขอรับตัวผู้ต้องหาชาวไทยทั้งหมดจำนวน 42 คน กลับมาดำเนินคดีในประเทศไทย ทางตำรวจจีนได้แจ้งให้เจ้าหน้าที่ตำรวจไทยไปรับผู้ต้องหาซึ่งเป็นชาวไทยทั้งหมดจำนวน 40 คนกลับมาดำเนินคดีในประเทศไทย

ภาพ 3-2 ภาพแสดงกลุ่มคนร้ายและวิธีการหลอกลวงฉ้อโกงผู้เสียหาย

3.3.3 กรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด กรณีที่ 3 คดีที่ผู้เสียหายมาแจ้งความถูกแฟนเก่านำภาพลามก อนาจารไปเผยแพร่ในเฟซบุ๊ก

รูปแบบ และวิธีการของผู้กระทำความผิด

รีดเอาทรัพย์, นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้ฯ โดยผู้กล่าวหาและผู้ต้องหาเป็นแฟนกัน ต่อมาผู้กล่าวหาต้องการเลิกคบเป็นแฟนกับผู้กล่าวหา จึงได้มีการตกลงกัน โดยผู้ต้องหาเสนอว่า ถ้าจะเลิกกับตน ก็ให้คืนเงินที่ยืมไป จำนวน 30,000 บาท คืนมา แต่ผู้กล่าวหาบอกว่าไม่ได้ยืมเงินเงินจำนวนดังกล่าว ทำให้ผู้ต้องหาโกรธจึงนำคลิปวีดีโอ ที่แอบถ่ายไว้ตอนที่มีเพศสัมพันธ์กัน ส่งมาให้ผู้กล่าวหา ทางโทรศัพท์ และข่มขู่ ผู้เสียหายกลัว

จึงได้หาเงินมาคืนให้ แต่ไม่ครบจำนวน ผู้ต้องหา จึงได้นำคลิปโพสต์ลง ในเฟซบุ๊ก ข่มขู่ผู้กล่าวหา โดยเหตุเกิดที่ แขวงบางแค เขตบางแค กรุงเทพ ศาลอาญาธนบุรี อนุมัติหมายจับ สามารถจับกุมตัวผู้ต้องหาได้ที่ปั้มน้ำมัน ริมถนนพระราม 2 จับกุมตัวได้ ได้เช็คการใช้งานโทรศัพท์ ผ่านผู้ให้บริการเครือข่าย ของผู้ต้องหา ทราบว่า กำลังจะเดินทางไปต่างจังหวัด จึงได้มีการวางแผน จับกุมได้

3.3.4 กรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด กรณีที่ 4 คดีที่ผู้เสียหายมาแจ้งความถูกหลอกลวงทางเฟสบุ๊ค ให้โอนเงินเข้าบัญชีธนาคาร

รูปแบบ และวิธีการของผู้กระทำความผิด

ร่วมกันฉ้อโกง โดยแสดงตนเป็นคนอื่น, นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอม หรือเป็นเท็จฯ โดยผู้กล่าวหารู้จักกับกลุ่มผู้ต้องหาทางเฟสบุ๊ค จากนั้นกลุ่มผู้ต้องหาจะตีสนิทหลอกเป็นแฟน และพยายามหาจุดอ่อนของผู้กล่าวหา จนพบว่า ผู้กล่าวหาต้องการให้ลูกเดินทางไปเรียนต่อต่างประเทศ กลุ่มผู้ต้องหาจึงได้วางแผนหลอกลวงว่า จะเดินทางมาทำงานในประเทศไทย โดยเข้าทำงานที่บริษัทเชลล์ออย แต่เนื่องจากการเข้าทำงานมีค่าใช้จ่ายในการเสียค่าล้างท่อน้ำมัน ได้หาเงินมาจำนวนหนึ่งแล้ว ยังขาดอยู่อีกจำนวนหนึ่ง ขอให้ผู้กล่าวหาช่วยเหลือโดยเสนอเงินก้อนโต เป็นค่าตอบแทนจากการทำงานให้ผู้เสียหายตายใจ และจะส่งลูกสาวของผู้กล่าวหา ไปเรียนต่อยังต่างประเทศ จนผู้กล่าวหาหลงเชื่อสูญเสียเงินไปหลักล้านบาท ได้ขอศาลออกหมายจับ จากการทำรายการถอนเงินที่ตู้เอทีเอ็ม และอีกส่วนหนึ่งได้เช็คราย การใช้โทรศัพท์ของผู้ต้องหา จนทราบที่อยู่ และเข้าทำการจับกุมได้ผู้ต้องหา 4 คน หลบหนี 1 คน

3.3.5 กรณีศึกษารูปแบบ และวิธีการของผู้กระทำความผิด กรณีที่ 5 คดีธนาคาร แจ้งว่ามีลูกค้าปฏิเสธการทำรายการผ่านบัตรเครดิต

รูปแบบ และวิธีการของผู้กระทำความผิด

ใช้บัตรอิเล็กทรอนิกส์ ของผู้อื่นโดยมิชอบฯ, ใช้บัตรอิเล็กทรอนิกส์ที่ผู้ออก ได้ออกให้แก่ผู้มีสิทธิ์ใช้เพื่อประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่น แทนการชำระด้วยเงินสด หรือใช้เบิกถอนเงินสด, ฉ้อโกง โดยแสดงตนเป็นคนอื่น และนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์ อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ศาลจังหวัดนนทบุรีได้ออกหมายจับตามที่พนักงานสอบสวนได้แสดงพยานหลักฐาน จากไอพีแอดเดรสที่เข้ามาทำรายการที่ธนาคาร, มีการตรวจสอบหมายเลขโทรศัพท์ ที่โทรเข้าไปที่ คอลเซ็นเตอร์ของธนาคาร

3.4 องค์ความรู้เกี่ยวกับแนวทางการพัฒนาประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และคดีที่ประสบความสำเร็จ (Best Practice) เนื่องจากเครือข่ายการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

แนวคิด **การจัดการความรู้** หมายถึง การรวบรวมองค์ความรู้ด้านกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง ขั้นตอน แนวทางการปฏิบัติงานด้านนิติวิทยาศาสตร์ที่มีอยู่อย่างกระจัดกระจายในรูปของหนังสือ ตำรา เอกสารทางราชการ สำนวนการสอบสวนและรายงานการสืบสวน รวมทั้งความรู้ที่มีอยู่ในตัวผู้ปฏิบัติงาน มาพัฒนาให้เป็นระบบสร้างเกณฑ์ในหมวดต่างๆ การวัด การวิเคราะห์ และการจัดการความรู้ การมุ่งเน้นทรัพยากรบุคคล การจัดการกระบวนการ และผลลัพธ์การดำเนินการ

แนวทาง เพื่อให้มีความรู้ความเข้าใจ สร้างเสริมสำนึกรับผิดชอบในวิชาชีพตามหลักจริยธรรมที่พึงปฏิบัติ และป้องกันการทุจริตประพฤติมิชอบของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย มุ่งหล่อหลอมจิตใจ อุปนิสัย และเสริมสร้างบุคลิกภาพ ตลอดจนพฤติกรรมที่เหมาะสม เพียบพร้อมไปด้วยคุณธรรม ความซื่อสัตย์สุจริต ความเสียสละความสำนึกในหน้าที่ และการบริการประชาชน เป็นที่ศรัทธาและเชื่อถือของประชาชน

การจัดการความรู้อย่างเป็นรูปธรรม และมีประสิทธิภาพด้วยการจัดการความรู้ด้านการรวบรวมข้อมูลการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ โดยมีแผนบริหารจัดการองค์ความรู้ในระยะเร่งด่วน ระยะสั้นและระยะยาว

วิธีการจัดการความรู้มาสร้างการเปลี่ยนแปลงเพื่อพัฒนาองค์ความรู้ด้านการปฏิบัติงานการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจ ฝ่ายปกครอง และประชาชน

มีการปฏิบัติการและกิจกรรม มีวิธีการรวบรวมข้อมูลหลาย ๆ รูปแบบ เช่น การเข้าร่วมเรียนรู้กับเจ้าหน้าที่ตำรวจที่เป็นผู้มีความรู้ความเชี่ยวชาญ และมีประสบการณ์ด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

1) ขยายหน่วยด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ออกไปยังส่วนภูมิภาค เพื่อรองรับปัญหาอาชญากรรมคอมพิวเตอร์

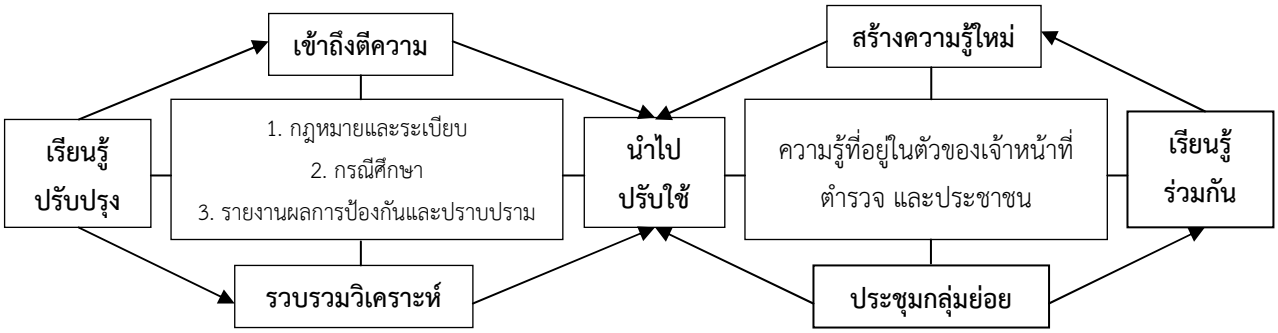
2) ปรับอัตรากำลังพลให้เหมาะสมกับปริมาณงาน รวมถึงการจัดฝึกอบรมทางด้านเทคโนโลยีสารสนเทศเพิ่มเติม อย่างสม่ำเสมอ

3) เผยแพร่ความรู้ทางหนังสือจากคู่มือด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ ซึ่งสามารถนำความรู้ไปใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

4) เผยแพร่ทาง CD แก่ผู้มีหน้าที่ในการปฏิบัติงานด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์เพื่อเป็นคู่มือในการปฏิบัติงานอย่างเป็นมาตรฐานเดียวกันอย่างเป็นรูปธรรม และมีประสิทธิภาพ

การจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

คณะผู้วิจัยใช้วงจร แนวคิดการจัดการความรู้เป็นเครื่องมือในการเก็บรวบรวมข้อมูล ดังนี้



ภาพ 3-3 วงจรแนวคิดการจัดการความรู้ด้านอาชญากรรมคอมพิวเตอร์

แนวคิดการจัดการความรู้

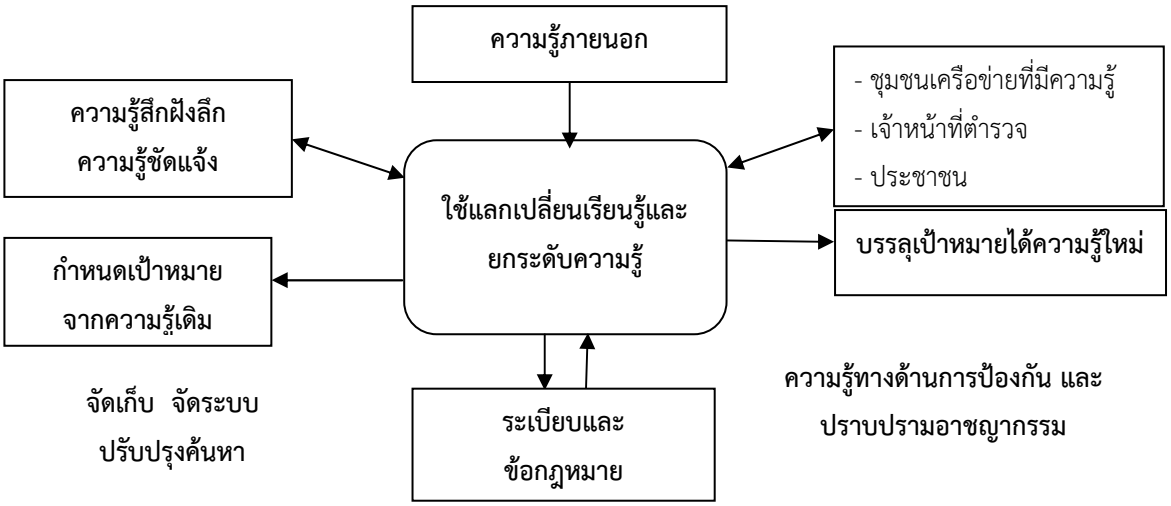
การจัดการความรู้ หมายถึง การรวบรวมความรู้ที่มีอยู่ในองค์กร ซึ่งกระจัดกระจายอยู่ในตัวบุคคลหรือเอกสาร มาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพ อันจะส่งผลให้องค์กรมีความสามารถในการปฏิบัติงานอย่างสูงสุด ความรู้มี 2 ประเภท คือ

1) ความรู้ที่ฝังอยู่ในคน (Tacit Knowledge) เป็นความรู้ที่ได้จากประสบการณ์ พรสวรรค์หรือสัญชาติญาณของแต่ละบุคคล ในการทำความเข้าใจในสิ่งต่างๆ เป็นความรู้ที่ไม่สามารถถ่ายทอดออกมาเป็นคำพูดหรือลายลักษณ์อักษรได้โดยง่าย เช่น ทักษะในการทำงาน งานฝีมือ หรือความคิดในเชิงวิเคราะห์ บางครั้งเรียกว่า เป็นความรู้แบบนามธรรม

ในการวิจัยครั้งนี้ หมายถึง ความสามารถและประสบการณ์ของเจ้าหน้าที่นิติวิทยาศาสตร์ เจ้าหน้าที่ตำรวจ ทหารและเจ้าหน้าที่ที่เกี่ยวข้องในการปฏิบัติงานในจังหวัดชายแดนภาคใต้ โดยวัดความสามารถจากการดำเนินการในการตรวจสถานที่เกิดเหตุ พิสูจน์หลักฐาน พิสูจน์เอกลักษณ์บุคคล จนสามารถทำให้ศาลพิพากษาลงโทษผู้กระทำความผิดได้

2) ความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่สามารถรวบรวมถ่ายทอดได้โดยผ่านวิธีต่างๆ เช่นการบันทึกเป็นลายลักษณ์อักษร ทฤษฎี คู่มือต่างๆ และบางครั้งเรียกว่าเป็นความรู้แบบรูปธรรม

ในการวิจัยครั้งนี้ หมายถึง ข้อกฎหมาย ระเบียบวิธีปฏิบัติ ซึ่งส่งผลต่อการปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ การแลกเปลี่ยนเรียนรู้ และยกระดับความรู้ของการจัดการความรู้ด้านอาชญากรรมคอมพิวเตอร์ จุดเริ่มต้นของการศึกษาต้องกำหนดเป้าหมายจากความรู้เดิม โดยรวบรวมข้อมูลจากความรู้ฝังลึก ความรู้ชัดแจ้ง โดยการประชุมกลุ่มและการศึกษาเชิงลึกจากหน่วยงานที่เกี่ยวข้อง จนกระทั่งบรรลุเป้าหมายและได้ความรู้ใหม่



ภาพ 3-4 องค์ประกอบของเครือข่ายการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

3.5 ขั้นตอนการดำเนินการจัดการความรู้ ทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

คณะผู้วิจัยได้ดำเนินการจัดการความรู้โดยการรวบรวมองค์ความรู้ด้านทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และเจ้าหน้าที่หน่วยงานอื่นที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ที่กระจัดกระจายอยู่ในตัวบุคคลหรือเอกสาร มาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ รวมทั้งปฏิบัติงานได้อย่างมีประสิทธิภาพ โดยความรู้มี 2 ประเภท
คือ ความรู้ที่ฝังอยู่ในคน (Tacit Knowledge) เป็นความรู้ที่ได้จากประสบการณ์ พรสวรรค์หรือสัญชาตญาณของแต่ละบุคคลในการทำความเข้าใจในสิ่งต่างๆ เป็นความรู้ที่ไม่สามารถถ่ายทอดออกมาเป็นคำพูดหรือลายลักษณ์อักษรได้โดยง่าย เช่น ทักษะในการทำงาน งานฝีมือ หรือการคิดเชิงวิเคราะห์ บางครั้งจึงเรียกว่าเป็นความรู้แบบนามธรรม และความรู้ที่ชัดแจ้ง (Explicit Knowledge) เป็นความรู้ที่สามารถรวบรวม ถ่ายทอดได้โดยผ่านวิธีการต่างๆ เช่น การบันทึกเป็นลายลักษณ์อักษร ทฤษฎี คู่มือต่าง ๆ และบางครั้งเรียกว่าเป็นความรู้แบบรูปธรรม

การดำเนินการเพื่อจัดการความรู้ครั้งนี้ จึงเป็นการจัดกิจกรรมการแลกเปลี่ยนเรียนรู้ (Story telling) เพื่อถอดบทเรียนทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์จากบุคคลต้นแบบผู้ทรงคุณวุฒิและผู้เชี่ยวชาญจากหน่วยงานที่เกี่ยวข้อง จำนวน 4 ครั้ง ผู้เข้าร่วมประชุมเข้าร่วมกิจกรรมแลกเปลี่ยนเรียนรู้ครั้งนี้ได้แก่

3.5.1 คณะผู้ดำเนินกิจกรรมและกลุ่มเป้าหมายในการวิจัย

ในการดำเนินการเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ คณะผู้วิจัยได้กำหนดคณะผู้ดำเนินกิจกรรม หรือผู้รับผิดชอบโครงการ คณะที่ปรึกษาโครงการ และกลุ่มเป้าหมาย (Knowledge Practitioner, KP) หรือผู้ที่มีความรู้ (Explicit Knowledge) และเป็นผู้ที่จะต้องเข้าร่วมแลกเปลี่ยนเรียนรู้ในครั้งนี้ ได้แก่

คณะผู้ดำเนินงาน

คณะนักวิจัยโครงการฯ ประกอบด้วย

1. พล.ต.ท.ดร.ณรงค์	กุลนิเทศ	หัวหน้าโครงการฯ
2. พ.ต.อ.สมศักดิ์	หน่องพงษ์	นักวิจัยโครงการฯ
3. ผศ.พ.ต.ท.วรธัช	วิชชุวาณิชย์	นักวิจัยโครงการฯ
4. นางสาวณิช	วงศ์ส่องจ้า	นักวิจัยโครงการฯ

3.5.2 กลุ่มเป้าหมายที่เข้าร่วมกิจกรรมการแลกเปลี่ยนเรียนรู้ (Story telling) ประกอบด้วย เจ้าหน้าที่ฝ่ายสืบสวน อัยการ ศาล กรมสอบสวนคดีพิเศษ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่มีความรู้และประสบการณ์เรื่องการสืบสวนสอบสวนและมีความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ สื่อมวลชน เจ้าหน้าที่องค์กรเอกชนที่มีประสบการณ์เกี่ยวกับงานทางด้านอาชญากรรมคอมพิวเตอร์ ชุมชนเครือข่ายที่มีความรู้ประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์

3.5.3 ขั้นตอนในการปฏิบัติงาน คณะผู้วิจัยกำหนดขั้นตอนต่างๆ ไว้ในแผนการปฏิบัติงานพร้อมกับรายละเอียดในการปฏิบัติทุกขั้นตอนในการดำเนินการเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ ผลที่ได้รับจากการปฏิบัติงาน มีขั้นตอนดังนี้

ขั้นตอนที่ 1 รวบรวมกรณีและรายชื่อเจ้าหน้าที่สืบสวนสอบสวนที่มีประสบการณ์เกี่ยวกับงานทางด้านอาชญากรรมคอมพิวเตอร์

คณะผู้วิจัยทำหนังสือจากหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา ขอความร่วมมือไปยังเจ้าหน้าที่ฝ่ายสืบสวน อัยการ ศาล กรมสอบสวนคดีพิเศษ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอข้อมูลด้านสถิติงาน กรณีศึกษาที่น่าสนใจ และให้จัดส่งรายชื่อเจ้าหน้าที่ฝ่ายสืบสวนและสอบสวนที่มีประสบการณ์ทางด้านอาชญากรรมคอมพิวเตอร์ และมีผลงานในการปฏิบัติงานที่ประสบความสำเร็จให้กับมหาวิทยาลัยราชภัฏสวนสุนันทา เพื่อดำเนินการตามขั้นตอนการจัดประชุมเพื่อแลกเปลี่ยนเรียนรู้ต่อไป และดำเนินการจัดเก็บความรู้ที่ได้จากการเล่าเรื่อง (Story telling) ด้วยการนำความรู้ที่ได้มากลั่นกรอง เรียบเรียง และพร้อมที่จะเผยแพร่ต่อไป

ต่อมาคณะผู้วิจัยได้รับข้อมูลด้านสถิติงาน บัญชีรายชื่อของเจ้าหน้าที่ฝ่ายสืบสวนสอบสวนและอาชญากรรมคอมพิวเตอร์ที่มีประสบการณ์ของหน่วยงานต่างๆ ดังกล่าวข้างต้น พร้อมกับกรณีศึกษาเกี่ยวกับด้านอาชญากรรมคอมพิวเตอร์ เพื่อใช้เป็นข้อมูลในการทำงานวิจัยในเรื่องนี้ต่อไป

ขั้นตอนที่ 2 การประชุมครั้งที่ 1 เพื่อร่วมกันวิเคราะห์ข้อกฎหมายและระเบียบที่เกี่ยวข้องทางด้านอาชญากรรมคอมพิวเตอร์

คณะผู้วิจัยได้ทำหนังสือเชิญผู้ทรงคุณวุฒิซึ่งมีประสบการณ์ทางด้านการสืบสวนสอบสวน และด้านกฎหมาย ของสำนักงานตำรวจแห่งชาติ อัยการ ศาล และหน่วยงานต่าง ๆ ในกระทรวงยุติธรรม และผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ ของสำนักงานพิสูจน์หลักฐานตำรวจ และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เข้าร่วมประชุมในวันจันทร์ ที่ 17 ธันวาคม 2555 เวลา 09.00 – 12.00 น. ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี

มหาวิทยาลัยราชภัฏสวนสุนันทา เพื่อรวบรวมระเบียบ ข้อบังคับ และระเบียบที่เกี่ยวข้องกับการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ โดยร่วมกันวิเคราะห์ข้อกฎหมาย และระเบียบที่เกี่ยวข้องกับการสืบสวนสอบสวน และการรวบรวมพยานหลักฐาน ความน่าเชื่อถือของวัตถุพยาน ปัญหาและวิธีการในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ เพื่อพัฒนาปรับปรุงกฎหมายหรือระเบียบดังกล่าวให้มีความเหมาะสมต่อการปฏิบัติงานของเจ้าหน้าที่ในสภาวการณ์ปัจจุบัน ผู้เข้าร่วมประชุม ประกอบด้วยหัวหน้าโครงการและคณะนักวิจัย กลุ่มเป้าหมายที่เข้าร่วมแลกเปลี่ยนเรียนรู้ ประกอบด้วยผู้แทนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร พนักงานสอบสวน กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กองพิสูจน์หลักฐานกลาง สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานอัยการสูงสุด และอาจารย์โรงเรียนนายร้อยตำรวจ

ตาราง 3-11 บันทึกผลสรุปการเล่าเรื่อง (Storytelling) รายบุคคล ครั้งที่ 1

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำกอง **ฝ่ายพัฒนากฎหมาย** **สำนักงานวิชาการ** **สำนักงานอัยการสูงสุด**	กล่าวถึงภาพรวมของกฎหมาย ระเบียบ คำสั่ง และประกาศต่างๆ ที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ลักษณะของการกระทำความผิด - การกระทำความผิดต่อตัวคอมพิวเตอร์เอง - การกระทำความผิดลักษณะที่ใช้คอมพิวเตอร์เป็นเครื่องมือ หรือเป็นอุปกรณ์ในการกระทำผิด - การกระทำความผิดโดยใช้คอมพิวเตอร์เป็นแหล่งเก็บข้อมูล พนักงานสอบสวนส่วนใหญ่ยังขาดความเข้าใจในเรื่องอาชญากรรมคอมพิวเตอร์ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** พนักงานอัยการ ให้คำแนะนำแก่พนักงานสอบสวนในประเด็นข้อกฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ในการสรุปสำนวนการสอบสวน **<u>วิธีการสู่ความสำเร็จ/ เทคนิค/ กลยุทธ์</u>** 1. จะต้องมีความแม่นยำในข้อกฎหมายที่เกี่ยวข้องต่างๆ 2. เคยรับราชการตำรวจมาก่อน ทำให้เข้าใจขั้นตอนการปฏิบัติงานของเจ้าหน้าที่ตำรวจ **<u>บุคลิกลักษณะผู้เล่า</u>** 1. มีความเป็นผู้นำ มีปฏิญาณไหวพริบ มีความมุ่งมั่น 2. มีความรู้ ความสามารถและประสบการณ์สูง และมีความพร้อมในการเล่า และเสนอแนวคิดที่เป็นประโยชน์อย่างมากต่อ การใช้หลักกฎหมายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
พนักงานสอบสวน ระดับชำนาญการพิเศษ กรมสอบสวนคดีพิเศษ	กล่าวว่า ในส่วนของการกระทำผิดนั้น ตามกฎหมายนั้นเป็นเรื่องที่กว้างมาก ซึ่งเป็นเรื่องที่มีมานานแล้ว เพียงแต่ว่าในปัจจุบันมีช่องทางในการกระทำความผิดที่ง่ายยิ่งขึ้นและเป็นเครือข่ายมากขึ้น ในส่วนการเก็บพยานหลักฐานนั้นขาดความน่าเชื่อถือ เพราะขาดวิธีการเก็บ และการรักษาไม่ได้มาตรฐาน และในเรื่องของการเรียนรู้ของเจ้าหน้าที่จะต้องมีทักษะและความชำนาญพอสมควรถึงจะปฏิบัติหน้าที่ได้ ในมุมมองของด้านกฎหมายนั้นส่วนใหญ่กฎหมายที่ออกมาจะรองรับข้อมูลรูปแบบของการกระทำความผิดในรูปแบบใหม่ๆ อยู่แล้ว เช่น การเข้าถึงข้อมูลในคอมพิวเตอร์ การเปลี่ยนแปลงของเทคโนโลยีมีอยู่ตลอดเวลาจึงจำเป็นต้องศึกษาจากต่างประเทศมาปรับใช้ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** การตรวจพิสูจน์ทางคอมพิวเตอร์ ต้องรักษาความถูกต้องและความน่าเชื่อถือของพยานวัตถุ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค/ กลยุทธ์</u>** 1. จะต้องมีฝึกอบรมเพิ่มเติมอยู่ตลอดเวลา 2. ต้องมีการฝึกอบรมและฝึกทักษะในขั้นตอนการปฏิบัติงานต่าง ๆ อยู่ตลอดอย่างต่อเนื่อง **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ ความสามารถและประสบการณ์สูง เสนอแนวคิดที่เป็นประโยชน์อย่างมากต่อการใช้หลักกฎหมายในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
กลุ่มงานคณาจารย์ คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ	จากประสบการณ์จากทำงานวิจัยทางด้านการค้ามนุษย์นั้น การใช้กฎหมาย และพ.ร.บ. อาจจะคล้ายๆกัน อาจจะรวมไปถึงอาชญากรรมข้ามชาติ ซึ่งการกระทำความผิดนั้นเหมือนกันและบางกรณีก็เกี่ยวโยงกันในหลายๆ ฐานความผิด คำนิยามของเจ้าหน้าที่จะมีอยู่ 2 อย่าง คือ พนักงานตาม ป.วิ อาญา และพนักงานเจ้าหน้าที่ตาม พ.ร.บ. ซึ่งจะมีอำนาจหน้าที่ในการตรวจค้น และต้องมีการสืบสวนเฉพาะ ในด้านการทำคู่มือควรจะมีการวิพากษ์คู่มือว่าจะนำไปใช้ได้จริงหรือไม่ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** เคยมีประสบการณ์ในการอบรมหลักสูตรทางด้านอาชญากรรมคอมพิวเตอร์ ส่วนใหญ่จะเน้นไปด้านการเก็บพยานหลักฐาน การหา software ต่างๆ การหาความเชื่อถือของพยานหลักฐานเมื่อขึ้นไปสู่ชั้นศาล **<u>วิธีการสู่ความสำเร็จ/ เทคนิค/ กลยุทธ์</u>** 1. การฝึกอบรมอยู่ตลอดเวลา 2. ต้องรู้จักประยุกต์ใช้หลักกฎหมายอื่นๆ เข้าด้วยกัน **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ ความสามารถและความรับผิดชอบสูง
ฝ่ายอำนวยการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ	กล่าวถึงการปฏิบัติงานของกองบังคับปราบปรามอาชญากรรมทางเทคโนโลยี ซึ่งมีเจ้าหน้าที่เชี่ยวชาญโดยเฉพาะ และกลุ่มงานสนับสนุนโดยผ่านการอบรมมาอย่างดี โดยจะมีการร่วมมือในการปฏิบัติงานกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ทางกองบังคับปราบปรามอาชญากรรมทางเทคโนโลยี จะเริ่มโครงการให้ความรู้กับตำรวจในสถานีตำรวจทั่วประเทศ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การให้ความรู้แก่ผู้ปฏิบัติงานอยู่ตลอดเวลา และต้องตามเทคโนโลยีที่มีการพัฒนาอยู่ตลอดเวลาให้ทัน **<u>บุคลิกลักษณะผู้เล่า</u>** สุขุม ใจเย็น มีความรู้ ความสามารถและความรับผิดชอบสูง

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
ผู้อำนวยการกลุ่มงานสืบสวนทางเทคโนโลยีสารสนเทศ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี	กล่าวสรุปเป็นข้อ ๆ สำหรับการให้ความเห็นดังนี้ 1.ในการทำเครือข่ายเป็นเรื่องที่ดีมาก 2.การทำคู่มือ ควรทำเป็น Case by Case 3.การปฏิบัติเชิงนโยบาย ในการจัดทำข้อมูลการจราจร การจัดเก็บข้อมูลความลับของประเทศ ของทางราชการ และส่วนบุคคล โดยต้องทำการบูรณาการกันทุกๆ หน่วยงาน 4.ต้องให้ข้อกฎหมายทุกฉบับมีความเชื่อมโยงกัน **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** การติดตามสถานการณ์ดำเนินการในปัจจุบัน ต้องตามให้ทันด้านเทคโนโลยี และเก็บรวบรวมข้อมูลให้ถูกวิธีและได้มาตรฐาน **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** ในงานด้านเทคนิคต้องสะท้อนไปถึงเครื่องมือ และมาตรฐาน รวมไปถึงคนที่ปฏิบัติงาน ด้านการบริหารการจัดการ และสิ่งที่สำคัญ คือ ต้องมีการบูรณาการร่วมกัน **<u>บุคลิกลักษณะผู้เล่า</u>** สุขุม ใจเย็น มีความรู้ ความสามารถและความรับผิดชอบสูง
นักวิทยาศาสตร์ (สบ4) กลุ่มงานยาเสพติด สำนักงานพิสูจน์หลักฐานตำรวจ	กล่าวถึง ในด้านกฎหมายมีการออกกฎหมายมาค่อนข้างดีที่สามารถครอบคลุมได้ทั่วถึง ด้าน พ.ร.บ.คอมพิวเตอร์นั้น จะกำหนดให้มีหลักฐานที่เป็นดิจิตอล และอาจจะต้องปรับปรุงถ้อยคำต่างๆ ให้ชัดเจน และรวมไปถึงการพิสูจน์พยานหลักฐานนั้น **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** การประสานงานขอข้อมูลไปยังต่างประเทศต้องเป็นแบบทั้งส่วนตัวและเป็นแบบทางการ ซึ่งจะช่วยให้การทำงานประสบความสำเร็จอย่างรวดเร็ว **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การฝึกอบรมให้ความรู้และประสบการณ์การทำงาน รวมไปถึงการเก็บและรักษาอุปกรณ์ และ software ต่างๆ ให้เป็นไปตามมาตรฐานสากล **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ ความสามารถและความรับผิดชอบสูง

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ	ผู้เล่าเล่าประเด็นด้านความรู้ของเจ้าหน้าที่ตำรวจบางท่าน ที่มีการประสบการณ์ทำงานนานๆ อาจจะยังไม่มีความรู้มากนัก และอำนาจของเจ้าหน้าที่นั้น ยังไม่มีอำนาจเพียงพอ ตาม ป.วิอาญาในการขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ต (ISP) ได้ ซึ่งอาจจะมีปัญหาและความล่าช้าของการขอข้อมูลนั้นยังพบอยู่บ่อยครั้ง และหนังสือที่ทางผู้ให้บริการอินเทอร์เน็ตตอบมานั้น ผู้ที่ลงนามในหนังสือ คือ นิติกรของทางบริษัทที่ให้บริการทางอินเทอร์เน็ตแต่ละราย ซึ่งมักจะเป็นปัญหาในการขึ้นให้การเป็นพยานในชั้นศาลเนื่องจากไม่สามารถตอบคำถามของทนายฝ่ายจำเลยหรือศาลได้ ส่วนของคู่มือควรจะต้องทำเป็น Case by Case ไปน่าจะดีกว่า และควรเพิ่มการอบรม โดยเชิญอาจารย์ทางด้าน Network Security มาให้ความรู้ก็จะเป็นการดีมากยิ่งขึ้น **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** สามารถอธิบายให้กับพนักงานสอบสวน ในประเด็นการขอข้อมูลจากผู้ให้บริการทางอินเทอร์เน็ต (ISP) **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การใช้หลักฐานทางนิติวิทยาศาสตร์ประสานขอความร่วมมือระหว่างหน่วยงาน **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ในเรื่องการสืบสวนสอบสวน มีความสามารถและความรับผิดชอบสูง
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ	ผู้เล่า ได้สะท้อนถึงผู้ที่ได้รับผลกระทบ ในด้านระเบียบและข้อกฎหมายต้องมีความทันสมัย และต้องมีการนำไปใช้อย่างเป็นรูปธรรมจริงๆ ซึ่งต้องสามารถนำไปใช้ได้จริงๆ ทุกๆ ข้อ และในการหาเครือข่าย ถ้าหากเน้นไปถึงด้านประชาชน เราควรน่าจะต้องรวมไปถึง Webmaster ของเว็บไซต์ต่างๆ นั้นด้วย และในหลายกรณีเรามีการให้ทางภาคเอกชน หรือ บุคคลทั่วไปที่มีความรู้เฉพาะด้านมาให้การช่วยเหลือในการปฏิบัติงานของเจ้าหน้าที่เราเหมือนกรณีอาสาสมัครของมูลนิธิต่าง ๆ ดังนั้นเราควรจะต้องมีการคัดกรองบุคคลและข้อมูลของผู้ที่เข้ามาช่วยงานเราด้วย โดยต้องคำนึงถึงระดับผู้ที่ต้องใช้กฎหมายและระดับของผู้ปฏิบัติด้วย

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ (ต่อ)	**<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** สามารถอธิบายให้กับเจ้าหน้าที่ทุกฝ่ายที่เกี่ยวข้องให้เห็นถึงความสำคัญของสถานที่เกิดเหตุ และการปนเปื้อนของวัตถุพยาน **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การใช้หลักฐานทางนิติวิทยาศาสตร์มาช่วยเหลือในการพิสูจน์การกระทำความผิดของคนร้าย **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ในเรื่องการสืบสวนสอบสวน มีความสามารถและความรับผิดชอบสูง
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ	ได้กล่าวประเด็นในข้อกฎหมาย จะมีประเด็นที่สำคัญ คือ ฐานความผิดและเขตอำนาจในการดำเนินการตามกฎหมาย เช่น เขตอำนาจการสอบสอน เป็นต้น ควรวางแผนให้เป็นระบบ การใช้เทคโนโลยีสมัยใหม่นี้ มีวิธีการกระทำความผิดที่แยบยล และพัฒนาวิธีการอย่างรวดเร็ว ในประเด็นการตรวจสถานที่เกิดเหตุในด้านการก่ออาชญากรรมคอมพิวเตอร์นั้น จะต้องทำตามขั้นตอน เช่น การตรวจสอบสถานะของการทำงานของโปรแกรมในคอมพิวเตอร์นั้น ก่อนการเข้าถึงข้อมูลที่บรรจุเป็นหลักฐานทางดิจิตอลนั้น ต้องมีแนวทางการปฏิบัติอย่างเป็นระบบและเป็นขั้นตอน ตั้งแต่การเปิดปิดระบบ การเข้าถึงข้อมูล วิธีการดึงข้อมูล เป็นต้น ส่วนการจัดทำคู่มือนั้น ต้องให้ความรู้ในระดับเบื้องต้น และแนวทางการปฏิบัติงานของทุกๆหน่วยงานที่เกี่ยวข้อง เพื่อสามารถนำไปใช้ประโยชน์ร่วมกันได้ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ความสำคัญของพยานหลักฐานต่างๆ ที่ได้จากสถานที่เกิดเหตุ ถือเป็นหัวใจสำคัญในการสืบสวนสอบสวน เพื่อหาตัวคนกระทำความผิด **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การประสานงานขอความร่วมมือจากหน่วยงานต่างๆ และการใช้หลักฐานทางนิติวิทยาศาสตร์มาช่วยเหลือการทำงานของเจ้าหน้าที่ตำรวจ **<u>บุคลิกลักษณะผู้เล่า</u>** มีไหวพริบ ประสบการณ์ มีความสามารถและความรับผิดชอบสูง

ตาราง 3-11 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ	ได้กล่าวถึงปัญหาการบังคับการใช้กฎหมาย ทางเจ้าหน้าที่ตำรวจไม่มีความมั่นใจว่า อยู่ในอำนาจของพนักงานสอบสวนหรือไม่ หรือเป็นอำนาจของพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ และมักจะเป็นปัญหาโต้แย้งกันอยู่ในเรื่องการขอข้อมูลทางคดี หรือการประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้องไม่ว่าจะเป็นผู้ให้บริการทางอินเทอร์เน็ต หรือเจ้าหน้าที่ในส่วนของภาคราชการด้วยกันเอง และปัญหาอีกประเด็น คือ แนวทางการปฏิบัติ ควรจะต้องมีหน่วยงานที่เป็นศูนย์กลางในการขอข้อมูลเพื่อนำไปใช้ประโยชน์และเรื่องการขยายผล เพราะทุกวันนี้ทางเจ้าหน้าที่ผู้ปฏิบัติต้องขอข้อมูลเป็นยังผู้ให้บริการทางอินเทอร์เน็ตทุกราย ทำให้เสียเวลาในการรอการตรวจสอบข้อมูลที่เกี่ยวข้องของแต่ละค่าย ถ้ามีหน่วยงานกลางในการดำเนินการในเรื่องนี้ก็จะช่วยให้การทำงานสะดวก และรวดเร็วขึ้น และมีประเด็นอื่นที่สำคัญเช่นกัน เช่น การเข้าสถานที่เกิดเหตุต้องปฏิบัติอย่างไร ต้องมีการบันทึกการทำงานในทุกๆ ขั้นตอนเพื่อป้องกันการผิดพลาดที่อาจจะเกิดขึ้นได้ ไม่ว่าการทำให้วัตถุพยานถูกปนเปื้อนโดยไม่ได้ตั้งใจ ซึ่งจะเป็นข้อต่อสู้ทางคดีของทางฝ่ายผู้ต้องหาได้และที่สำคัญอีกประเด็นก็คือ ระดับความรู้ของเจ้าหน้าที่เรายังไม่เพียงพอในการปฏิบัติงาน จึงต้องการให้มีการจัดฝึกอบรมให้ความรู้กับทุกๆ หน่วยงานที่เกี่ยวข้อง **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** สามารถอธิบายให้กับเจ้าหน้าที่ทุกฝ่ายที่เกี่ยวข้องให้เห็นถึงความสำคัญของอาชญากรรมคอมพิวเตอร์ และการรักษาความน่าเชื่อถือของพยานหลักฐานทางคอมพิวเตอร์ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การใช้หลักฐานทางนิติวิทยาศาสตร์มาช่วยเหลือในการพิสูจน์การกระทำความผิดของคนร้าย และการประสานงานขอความร่วมมือจากหน่วยงานต่างๆ ในการทำงาน **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ในเรื่องการสืบสวนสอบสวน มีความมุ่งมั่นและความรับผิดชอบสูง

สรุปกิจกรรม AAR (Action After Review) สรุปกิจกรรม AAR (Action After Review) ในการประชุมครั้งที่ 1 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)”

คณะผู้วิจัยได้สรุปเป้าหมายของการประชุมครั้งนี้ คือ ได้มีการแลกเปลี่ยนความรู้ที่เกี่ยวกับการสืบสวนสอบสวน และด้านกฎหมาย โดยรวบรวมข้อมูล ปัญหาในการปฏิบัติและประสบการณ์ในการทำงานด้านอาชญากรรมคอมพิวเตอร์ ส่วนที่บรรลุเป้าหมายเกินคาด คือ การรวบรวมข้อมูล ปัญหาในการปฏิบัติหน้าที่ตามกฎหมาย การแลกเปลี่ยนเรียนรู้ของแต่ละฝ่ายได้อย่างเต็มที่ และประสบการณ์จากผู้เล่าท่านอื่นๆ และเห็นมุมมองต่างๆ มากขึ้น และเป้าหมายส่วนส่วนที่ไม่บรรลุ เช่น ปัญหาในการบังคับใช้กฎหมายของเจ้าหน้าที่ที่ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ และสิ่งที่ได้เรียนรู้ ที่เป็นประโยชน์ที่สุด คือความรู้ในเรื่องกฎหมายต่าง ๆ ที่เกี่ยวข้อง เช่น อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตาม พ.ร.บ.คอมพิวเตอร์ พ.ศ.2550 และอำนาจหน้าที่ของพนักงานสอบสวน โดยสิ่งที่ได้รับจะนำกลับไปหาข้อมูลเพิ่มเติม เพื่อที่จะแก้ไขปัญหาที่รับทราบมาจากการแลกเปลี่ยนเรียนรู้

ภาพ 3-5 การประชุมครั้งที่ 1 เพื่อร่วมกันวิเคราะห์ข้อกฎหมายและระเบียบที่เกี่ยวข้องทางด้านอาชญากรรมคอมพิวเตอร์ วันจันทร์ที่ 17 ธันวาคม พ.ศ. 2555 เวลา 9.00–12.00 น.
ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

ขั้นตอนที่ 3 การประชุมครั้งที่ 2 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)”

กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)” ได้จัดประชุมวันจันทร์ที่ 28 มกราคม 2556 เวลา 9.00 – 12.00 น. ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา เรื่องขั้นตอนและวิธีการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ผู้เข้าร่วมกิจกรรมแลกเปลี่ยนเรียนรู้ได้แก่ หัวหน้าโครงการและคณะนักวิจัย พนักงานสอบสวน กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กองพิสูจน์หลักฐานกลาง สำนักงานพิสูจน์หลักฐานตำรวจ กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี กลุ่มงานผู้เชี่ยวชาญ กองทะเบียนประวัติอาชญากร สำนักงานอัยการสูงสุด ผู้พิพากษา และอาจารย์โรงเรียนนายร้อยตำรวจ โดยวัตถุประสงค์ของการจัดกิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ การเล่าเรื่อง (Storytelling) เพื่อให้ผู้เข้าร่วมกิจกรรมได้แลกเปลี่ยนความรู้ขั้นตอน และวิธีการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ และเพื่อให้ผู้เข้าร่วมกิจกรรมได้ฝึกทักษะการเล่าเรื่องและถ่ายทอดสู่ผู้อื่น รูปแบบการดำเนินกิจกรรมแลกเปลี่ยนเรียนรู้ (Storytelling) ครั้งนี้ ให้ผู้เข้าร่วมแลกเปลี่ยนเรียนรู้เล่าเรื่องจากประสบการณ์เกี่ยวกับกรณีศึกษาเกี่ยวกับความรู้ขั้นตอนและวิธีการปฏิบัติงานของเจ้าหน้าที่ผู้รับผิดชอบในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ พฤติการณ์การกระทำผิดของคนร้าย ปัญหาอุปสรรคในการปฏิบัติงาน และและปัจจัยที่นำไปสู่ความสำเร็จในการปฏิบัติงาน

ก่อนจะเริ่มเล่าเรื่องนั้น ประธานในที่ประชุมทำหน้าที่เป็นคุณอำนวยได้อธิบายถึงความเป็นมาและวัตถุประสงค์ของการวิจัย และแนวคิดการจัดการความรู้

ตาราง 3-12 บันทึกผลสรุปการเล่าเรื่อง (Storytelling) รายบุคคล ครั้งที่ 2

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำ **สำนักงานอัยการสูงสุด**	เจ้าหน้าที่และพนักงานของรัฐที่เกี่ยวข้องในการดำเนินคดี ยังขาดความรู้ ความเข้าใจ เกี่ยวกับหลักการต่างๆ ในระบบคอมพิวเตอร์ ข้อมูลเทคโนโลยีสารสนเทศ ความเข้าใจใน การพิจารณาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ตลอดจนการปรับใช้กฎหมายพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการดำเนินคดี การจัดการความรู้ จำเป็นต้องได้รับความร่วมมือทั้งฝ่ายเทคโนโลยี และเจ้าหน้าที่ฝ่ายกฎหมาย ประกอบกัน จึงจะสามารถรวมรวมองค์ความรู้สำคัญที่จะใช้ในการดำเนินคดีประเภทนี้ได้ ส่วนด้านเครือข่ายและการจัดการด้านอาชญากรรมคอมพิวเตอร์ เนื่องจากมีความจำเป็นที่ต้องใช้ข้อมูล จากเครือข่ายหลายภาคส่วน จึงควรระบุแบ่งกลุ่มให้ง่ายต่อการประสานงาน และความเข้าใจของเจ้าหน้าที่

ตาราง 3-12 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำ **สำนักงานอัยการสูงสุด (ต่อ)**	**<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ได้กล่าวถึงหน่วยงานของตนเอง (สำนักงานอัยการสูงสุด) ที่ได้จัดทำคู่มือให้แก่พนักงานอัยการ สำหรับการสอบสวน และดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** โดยคู่มือดังกล่าวที่หน่วยงานของตนเองจัดทำขึ้นมานั้น จะอธิบายแนวทางการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ในเบื้องต้น รูปแบบคดีและพยานหลักฐาน มีลักษณะเฉพาะ และกฎหมาย พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ และความเชี่ยวชาญในงานที่ตนเองรับผิดชอบอยู่ และมีปฏิภาณไหวพริบในการแสดงความคิดเห็น
นักวิทยาศาสตร์ (สบ 2) **กลุ่มงานตรวจพิสูจน์** **อาชญากรรมทางคอมพิวเตอร์** **กองพิสูจน์หลักฐานกลาง**	ได้กล่าวถึงประเด็นการขึ้นให้การในฐานะพยานผู้เชี่ยวชาญ ต่อศาลในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์นั้น มีปัญหาในการจัดลำดับการขึ้นให้การต่อศาล และความเข้าในเข้าใจในคดีอย่างถ่องแท้ของทางอัยการ ซึ่งทำให้การให้ปากคำต่อศาลไม่มีความน่าเชื่อถือ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ผู้เล่าสามารถเล่าถึงประสบการณ์ในการเป็นพยานผู้เชี่ยวชาญต่อศาล เมื่อทางฝ่ายจำเลยมีทนายเข้าร่วมมากถึง 40 คน ส่วนผู้เล่านั้นเป็นเพียงผู้เดียวที่เป็นพยานฝ่ายโจทก์ที่ขึ้นให้การต่อศาล **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** ผู้เล่าใช้ความรู้ ความสามารถที่ได้จากการปฏิบัติงานมาปรับใช้ในการให้ปากคำต่อศาล **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่ามีความรู้ ความสามารถและประสบการณ์สูง และเสนอแนะแนวคิดให้กับผู้เข้าร่วมประชุมได้เป็นอย่างดี

ตาราง 3-12 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
รองผู้กำกับการกลุ่มงานผู้เชี่ยวชาญกองประวัติอาชญากร	ได้กล่าวถึงปัญหา และอุปสรรคในปัจจุบันเกี่ยวกับการเก็บข้อมูลจากแผนประทุษกรรมที่เกิดขึ้นนั้น ยังไม่สามารถนำมาใช้ประโยชน์ได้เพียงพอ แต่สามารถนำมาเป็นข้อมูลสนับสนุนในการค้นหาอาชญากรรมคอมพิวเตอร์ เช่น สมุดภาพ ประวัติผู้ค้นหา **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** สามารถอธิบายให้เห็นถึงความสำคัญของอาชญากรรมคอมพิวเตอร์ และการรักษาความน่าเชื่อถือของพยานหลักฐานทางคอมพิวเตอร์ รวมไปถึงประสบการณ์ในการปฏิบัติงานที่ผ่านมา **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การใช้หลักฐานทางนิติวิทยาศาสตร์มาช่วยเหลือในการพิสูจน์การกระทำความผิดของคนร้าย และการประสานงานขอความร่วมมือจากหน่วยงานต่างๆ ในการทำงาน **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ ความสามารถในเรื่องการสืบสวนสอบสวน
ผู้อำนวยการกลุ่มงานสืบสวนทางเทคโนโลยีสารสนเทศ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี	ได้กล่าวถึงปัญหา และอุปสรรคในมุมมองของพนักงานสอบสวนที่มักจะยึดการปฏิบัติงานแบบเดิมๆ เพราะขาดความรู้ ไม่เข้าใจถึงระบบคอมพิวเตอร์ เมื่อนำพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์จึงไม่ทราบวิธีการเก็บหลักฐาน จึงทำให้บางครั้งสามารถนำไปใช้ประโยชน์ไม่ได้ จึงอยากให้มีการจัดอบรมให้พนักงานสอบสวนเพื่อการเพิ่มเติมความรู้เพื่อการปฏิบัติงานไปในทิศทางเดียวกัน **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ผู้เล่ากล่าวถึงประสบการณ์ในการจัดการอบรมให้กับพนักงานสอบสวน ในเรื่ององค์ความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** ผู้เล่าสามารถเล่าประสบการณ์ ถ่ายทอดความรู้ และสามารถแนะแนวทางการปฏิบัติงานเพิ่มเติมให้แก่ผู้ที่เกี่ยวข้อง **<u>บุคลิกลักษณะผู้เล่า</u>** มีความสามารถในการถ่ายทอดความรู้ และประสบการณ์อย่างดี

ตาราง 3-12 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง	กล่าวถึงปัญหา และอุปสรรคในการเก็บพยานหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ในสถานที่เกิดเหตุ รวมถึงการเก็บรักษาพยานหลักฐานที่ถูกต้อง **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ทางสำนักงานพิสูจน์หลักฐานจะรับหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์โดยตรงเท่านั้น **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การเก็บรักษาพยานหลักฐานที่ถูกต้อง ด้านการเข้าสถานที่เกิดเหตุต้องวางกรอบและขอบเขตอำนาจ หากเมื่อตรวจพบพยานหลักฐานที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ควรจะให้ผู้เชี่ยวชาญเข้าที่เกิดเหตุเท่านั้น เพื่อเป็นการป้องกันความเสียหายต่อพยานหลักฐาน **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่ามีความรู้ และประสบการณ์ในการทำงานสูง และสามารถถ่ายทอดให้ผู้อื่นได้เป็นอย่างดี
ผู้พิพากษาศาลแขวงจังหวัดนครปฐม	กล่าวถึงการรับฟังพยานหลักฐานในชั้นศาล บางครั้งตัวผู้พิพากษาเองยังไม่มีความรู้เพียงพอ และระบบพยานหลักฐานในการดำเนินคดียังไม่เป็นระบบ จึงทำให้ยากต่อการปฏิบัติงาน และควรจะจัดการอบรมเพิ่มความรู้ให้เป็นไปในทิศทางเดียวกัน โดยอาจจะเชิญวิทยากรจากหน่วยงานต่างประเทศเพื่อเป็นการสร้างมาตรฐาน และการปฏิบัติงานที่ทันสมัย และมีมาตรการในการป้องกันการเสียหายที่จะถูกฟ้อง **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** การตรวจพิสูจน์ทางคอมพิวเตอร์ ต้องรักษาความถูกต้องและความน่าเชื่อถือของพยานวัตถุ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** การพิจารณาคดีในชั้นศาลของผู้เล่าจะดำเนินการตามหลักของ Chain of Custody **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ และความเชี่ยวชาญในงานที่ตนเองรับผิดชอบอยู่ และมีปฏิภาณไหวพริบในการแสดงความคิดเห็น

สรุปกิจกรรม AAR (Action After Review) สรุปกิจกรรม AAR (Action After Review) ในการประชุมครั้งที่ 2 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)”

เป้าหมายของการร่วมประชุมในครั้งนี้ เพื่อแลกเปลี่ยนความรู้ที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ และรวบรวมข้อมูล ปัญหาในการปฏิบัติงานของเจ้าหน้าที่ โดยเป้าหมายที่บรรลุเกินคาด เพราะประสบการณ์จากผู้เข้าร่วมประชุมท่านอื่นๆ ทำให้เห็นมุมมองต่างๆ มากขึ้น ส่วนเป้าหมายที่ไม่บรรลุ คือ การปฏิบัติงานร่วมกันของหน่วยงานต่างๆ เช่น พนักงานสอบสวนกับผู้ให้บริการทางด้านเทคโนโลยี และการแก้ไขปัญหาที่ยังไม่ชัดเจน และสิ่งที่ได้เรียนรู้ที่เป็นประโยชน์ที่สุด คือ การนำความคิดเห็นมุมมองต่างๆ ไปปรับวิสัยทัศน์ในการปฏิบัติงาน และความร่วมมือกันระหว่างพนักงานสอบสวนกับนักนิติวิทยาศาสตร์ เพื่อนำไปสู่ความสำเร็จอย่างแท้จริง โดยจะนำกลับพิจารณาจัดหลักสูตรอบรมเพิ่มเติมเกี่ยวกับอาชญากรรมคอมพิวเตอร์

ภาพ 3-6 การประชุมครั้งที่ 2 การแลกเปลี่ยนเรียนรู้ค้นหาปัญหาและอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้องด้านอาชญากรรมคอมพิวเตอร์
วันจันทร์ ที่ 28 มกราคม พ.ศ. 2556 เวลา 9.00–12.00 น.
ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

ขั้นตอนที่ 4 การประชุมครั้งที่ 3 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)”

กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)” ได้จัดประชุมวันจันทร์ที่ 1 กรกฎาคม 2556 เวลา 9.30 – 12.00 น. ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา เพื่อสัมมนาให้เกิดการแลกเปลี่ยนความรู้ ในการดำเนินงานทางด้านอาชญากรรมคอมพิวเตอร์ในภาพรวมทั้งหมด แล้วนำมาถอดบทเรียนเพื่อสร้างคู่มือการจัดการความรู้และสร้างเครือข่ายองค์กรในการป้องกันและปราบปรามอาชญกรรมคอมพิวเตอร์ ผู้เข้าร่วมกิจกรรมแลกเปลี่ยนเรียนรู้ได้แก่ หัวหน้าโครงการและคณะนักวิจัย พนักงานสอบสวน กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม กองพิสูจน์หลักฐานกลาง สำนักงานพิสูจน์หลักฐานตำรวจ กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี กลุ่มงานผู้เชี่ยวชาญ กองทะเบียนประวัติอาชญากร สำนักงานอัยการสูงสุด ผู้พิพากษา และอาจารย์โรงเรียนนายร้อยตำรวจ โดยวัตถุประสงค์ของการจัดกิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ การเล่าเรื่อง (Storytelling) เพื่อให้ผู้เข้าร่วมกิจกรรมได้แลกเปลี่ยนความรู้ขั้นตอน และวิธีการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์เชิงบูรณาการของทุกหน่วยงานที่เกี่ยวข้องกับอาชญากรรมด้านคอมพิวเตอร์

ตาราง 3-13 บันทึกผลสรุปการเล่าเรื่อง (Storytelling) รายบุคคล ครั้งที่ 3

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำ **สำนักงานอัยการสูงสุด**	กล่าวถึงปัญหาที่จำเป็นเร่งด่วนคือเรื่อง การกระจายองค์ความรู้ไปสู่เจ้าหน้าที่ผู้ปฏิบัติงานทุกภาคส่วน สำนักงานอัยการ ยังขาดองค์ความรู้ทางด้านนี้อยู่ การจะสานคดีต่อก็จะเกิดปัญหาและอุปสรรคมาก ซึ่งอัยการในต่างจังหวัดไม่รู้เกี่ยวกับคำศัพท์พื้นฐานทางด้านคอมพิวเตอร์ และยังไม่มีความเชี่ยวชาญโดยตรง โดยยกตัวอย่างของประเทศสหรัฐอเมริกา ที่มีหลายๆ หน่วยงาน ช่วยในการทำคดีทางด้านอาชญากรรมคอมพิวเตอร์ โดยมาจากทั้งระดับท้องถิ่น ระดับมลรัฐ ระดับรัฐบาลกลาง รวมไปถึงทางด้านเอกชน โดยมีรูปแบบหนึ่งที่น่าสนใจ คือ ในห้องงานทางด้านนิติวิทยาศาสตร์ของเขา พบว่ามีด้านหนึ่งเขาจะส่งเสริมให้เจ้าหน้าที่ทุกระดับสามารถใช้งานเครื่องคอมพิวเตอร์ในการคัดลอก ถ่ายโอน หรือตรวจสอบข้อมูลเบื้องต้นด้วยตนเองได้ หากส่วนได้ที่ไม่สามารถทำเองได้ เช่น กู้ข้อมูลที่ถูกลบไปแล้ว หรือข้อมูลที่ต้องเข้ารหัส ถึงจะส่งต่อให้ระดับผู้เชี่ยวชาญ ในภาพของกฎหมายจึงขอเสนอแบ่งออกเป็น 3 กลุ่ม คือ 1.กลุ่ม Collector คือ ผู้เก็บรวบรวมพยานหลักฐาน 2. กลุ่ม Examiner คือ ผู้ทำการตรวจพิสูจน์ และ 3. กลุ่ม Expert

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำ **สำนักงานอัยการสูงสุด (ต่อ)**	แต่ในประเทศไทยยังทำแบบที่หากผู้ใดทำอะไรได้ก็รับหน้าที่ทำอย่างนั้นไปทั้ง 3 กระบวนการ แม้อัยการ หรือพนักงานสอบสวนเองก็ไม่สามารถแนะนำพยาน และผู้เสียหายในการรวบรวมพยานหลักฐานได้ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** มีอยู่คดีหนึ่งที่เราสามารถทำได้คือ คดีฆ่าผู้ว่าราชการ ปรีณะ ที่มีการแยกบทบาทการทำหน้าที่อย่างชัดเจน ส่วนหนึ่งที่มีหน้าที่เก็บหลักฐานก็เก็บหลักฐานไป พอหลักฐานถูกเก็บมาก็นำมาตรวจและผลการตรวจสอบได้อะไรบ้าง และผู้เชี่ยวชาญไม่ได้แตะต้องพยานหลักฐานใดๆทั้งสิ้น แต่ดูจากผลการตรวจพิสูจน์ และประมวลผลว่า เหตุการณ์นั้นเกิดขึ้นอย่างไร เกิดอะไรบ้าง โดยอาศัยพยานหลักฐานที่ได้ จะเห็นได้ว่ากฎหมายไทยจะใช้คำว่าผู้เชี่ยวชาญอย่างเดียว และใช้ผู้เชี่ยวชาญครบทุกมิติทั้ง 3 ส่วน ซึ่งตรงนี้ถ้านำมาเปรียบเทียบกับคดีทางด้านอาชญากรรมคอมพิวเตอร์ ซึ่งมีคดีจำนวนมากที่อาศัยพยานหลักฐานทางคอมพิวเตอร์มาเกี่ยวข้องกับกระบวนการทางคอมพิวเตอร์ โดยเฉพาะสื่อทางอินเตอร์เน็ท กระบวนการบางอย่างที่เห็นว่าจะเป็นประโยชน์มาก โดยที่เราจะเห็นว่าทำอย่างไรโดยที่เราไม่ต้องแบกองค์ความรู้อยู่ที่ผู้เชี่ยวชาญที่จบมาโดยตรง เพื่อให้พนักงานสอบสวนได้รวบรวมบางอย่างได้ด้วยตนเอง โดยที่ยังไม่ต้องใช้เครื่องมือ และความรู้ที่ลึกซึ้งมากนัก **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** 1. ควรให้ความรู้พื้นฐานในการตรวจพิสูจน์หลักฐานทางด้านอาชญากรรมคอมพิวเตอร์แก่พนักงานอัยการ และพนักงานสอบสวนผู้ที่เกี่ยวข้องกับพยานหลักฐานโดยตรง 2. การแก้ไขปัญหาควรเริ่มจากการกระจายองค์ความรู้ไปสู่ผู้ที่เกี่ยวข้อง หรือแม้กระทั่งประชาชนที่เป็นผู้เสียหาย โดยอาจให้ข้อมูลเบื้องต้นเพื่อเป็นการประชาสัมพันธ์ก็ได้ **<u>บุคลิกลักษณะผู้เล่า</u>** มีความรู้ ความสามารถสูง และเสนอปัญหา อุปสรรคที่พบ และมีประโยชน์ต่อการการจัดการความรู้ด้านอาชญากรรมคอมพิวเตอร์ได้ดี

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
อัยการประจำกอง ฝ่ายพัฒนากฎหมาย สำนักงานวิชาการ สำนักงานอัยการสูงสุด	กล่าวถึงภาพรวมของการกระทำความผิดด้านอาชญากรรมคอมพิวเตอร์ หลายๆด้าน เช่น การกระทำความผิด แบบ Hacker การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด วิธีการเก็บพยานหลักฐานของผู้เสียหาย โดยไม่รู้ถึงวิธี การเก็บ และวิธีการนำหลักฐานมารวบรวมเพื่อแจ้งความ และการยึดคอมพิวเตอร์นั้นต้องมีหมายค้นหรือไม่ **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** เวลาเข้าตรวจค้นสถานที่เกิดเหตุนั้น ควรจะทำการถ่ายภาพสถานที่เกิดเหตุ และการเก็บรวบรวมพยานหลักฐานมักจะมีปัญหาทั้งเรื่องการเก็บพยานหลักฐานชิ้นนั้น เก็บมาจากส่วนไหน ควรเก็บทุกชิ้นที่ประกอบกันอยู่หรือไม่ หรือในการบรรจุของกลางไม่ปฏิบัติตามระเบียบเทคโนโลยี เมื่อนำส่งตรวจพิสูจน์อาจจะไม่สามารถตรวจได้ หากเป็นไปได้ควรจะทำการเก็บ DNA ก่อนการบรรจุจึงจะส่งตรวจ **<u>บุคลิกลักษณะผู้เล่า</u>** มีความเป็นผู้นำ ความรู้ ความสามารถ และมีประสบการณ์ในการทำงานสูง
กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ	กล่าวถึงประเด็นการใช้ในข้อมูลในส่วนกลางของเครือข่ายโทรศัพท์มือถือ และข้อมูลที่เป็นประโยชน์ในการพิสูจน์หลักฐาน **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** สมัยก่อนจะมีหมายจับค้างเก่าอยู่เยอะ เพราะการเชื่อมโยงกันระหว่างหน่วยงานมีอยู่น้อย ต่อมาทางฝ่ายตำรวจจึงมีการเชื่อมโยงกับหน่วยงานที่มากขึ้น สามารถทำให้จับหมายค้างเก่าได้มากถึง 50 % **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** ถ้าเราสามารถนำข้อมูลที่มีอยู่มาเป็นฐานข้อมูลร่วมกันในแต่ละหน่วยงาน เช่น กระทรวง ICT อาจขอข้อมูลจากต่างประเทศด้วย ซึ่งอาจจะทำให้การทำงานได้รวดเร็ว และเป็นประโยชน์มากขึ้น **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่าสามารถแสดงความคิดเห็นที่เป็นประโยชน์ และมีความรู้ในการปฏิบัติงาน

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
นักวิทยาศาสตร์ (สบ 2) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง	ประเด็นการตรวจพิสูจน์หลักฐาน ในด้านการบริหารเบื้องต้นนั้น มีประเด็นใหญ่ๆหลายๆประเด็น คือ 1.เรื่องงบประมาณ เมื่อมีความเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็ว งบประมาณที่ กองพิสูจน์หลักฐานจัดสรรให้ไม่เพียงพอกับเครื่องมือที่ต้องการจัดซื้อ เช่น การเปลี่ยนแปลงของระบบปฏิบัติการ และอุปกรณ์ต่างๆ แต่ปัจจุบันไม่เป็นไปอย่างนั้น เพราะอุปกรณ์เทคโนโลยีที่ล้ำสมัย มักจะรวมมาในตัวเดียวกัน ตั้งแต่สมาร์ทโฟน แท็บเล็ต หรือโน้ตบุ๊ค และอุปกรณ์ที่จะใช้ตรวจพิสูจน์ก็ได้หมดใบอนุญาตไปบางส่วน ซึ่งใบอนุญาตมีราคาแพง 2.ปัญหาการรวบรวมพยานหลักฐานของพนักงานสอบสวน โดยที่พนักงานสอบสวนประมาณ 80-90% ยังไม่เข้าใจถึงหลักการการรวบรวมพยานหลักฐาน เช่น เรื่องลิขสิทธิ์เพลง โดยมีการรวบรวมพยานหลักฐานของทางร้านคาราโอเกะ โดยยึดคอมพิวเตอร์มาเป็นพยานหลักฐาน และต้องการหารูปแบบลิขสิทธิ์ แต่ปัญหาเกิดอยู่ที่ต้องการหาว่าเพลงนี้มีลิขสิทธิ์หรือไม่ โดยที่ผู้ตรวจไม่รู้จักเพลงนี้ เราจะแก้ปัญหาด้วยการให้ผู้เสียหายนำตัวอย่างเพลงที่เป็นของแท้มาเปรียบเทียบ ซึ่งทุกคดีที่มีรูปแบบนี้ก็จะไม่มารับผลตรวจพิสูจน์ ประเด็นที่ทำให้คิดได้ว่า พนักงานสอบสวนที่รับแจ้งมานั้น ไม่ได้ตรวจสอบเลยว่า คนที่มาแจ้งนั้นเขาเป็นเจ้าของลิขสิทธิ์เพลงจริงหรือไม่ และเมื่อตรวจสอบไม่ได้ก็จะส่งคืน **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** ทางกองพิสูจน์หลักฐานกลาง ได้มีการเปลี่ยนแปลงการจัดซื้อโดยมองหาความร่วมมือกับหน่วยงานอื่นๆ โดยหาเครือข่ายร่วมเพื่อสนับสนุน และแลกเปลี่ยนเครื่องมือกัน **<u>บุคลิกลักษณะผู้เล่า</u>** มีความสุขุม รอบคอบ และเล่าข้อเท็จจริงที่พบในการปฏิบัติหน้าที่ และเล่าข้อมูลเกี่ยวกับคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ได้อย่างน่าฟัง และเป็นประโยชน์อย่างยิ่ง

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
รองผู้กำกับการกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี	กล่าวถึงการทำงานด้าน Forensic ของต่างประเทศได้อธิบายให้อัยการฟังว่า ของเขามีความจำเป็นมากที่จะให้ความสำคัญแยกระหว่าง examiner กับ expert ค่อนข้างมาก คือ ถ้าเป็นexaminer จะอธิบายได้แค่ข้อเท็จจริงว่านำอะไรมาตรวจ ด้วยวิธีการใด และผลเป็นอย่างไรสิ่งที่ห้ามก็คือไม่ให้แสดงความคิดเห็นว่าอนุมานไปถึงอะไรได้บ้าง แต่คนที่ทำหน้าที่ expert อาจจะไม่ได้ทำหน้าที่ตรวจพิสูจน์โดยตรง แต่เป็นคนที่เอาข้อมูลต่างๆ มาแล้วให้ความเห็นว่าสิ่งที่บ่งชี้คืออะไรได้บ้าง และมีข้อจำกัดอย่างไร แต่ในประเทศไทยเราใช้ผู้เชี่ยวชาญทุกด้าน **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** วิธีการแก้ปัญหา เราจะใช้หลักการเกี่ยวกับDigital Evidence ว่าพยานหลักฐานดิจิตอลนั้นเป็นอย่างไร **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** วางหลักการปฏิบัติพื้นฐานกว้างๆที่สามารถปฏิบัติได้ในการปฏิบัติงานทางด้านอาชญากรรมคอมพิวเตอร์ จนรู้กระบวนการขั้นตอน เช่น จะเก็บอะไร จะรักษาอย่างไร จะพยายามรวบรวมคำถามที่สำคัญ เป็นต้น **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่าสามารถถ่ายทอดหลักการจากประสบการณ์ในการทำงานได้เป็นอย่างดี และมีไหวพริบในการโต้ตอบคำถาม
ผู้พิพากษาศาลแขวงจังหวัดนครปฐม	กล่าวถึงเรื่องการนำเสนอพยานหลักฐาน และการรับฟังพยานหลักฐานซึ่งปัจจุบันก็มีพยานบุคคล พยานวัตถุ พยานเอกสาร เราสามารถตรวจสอบได้ในด้านพยานหลักฐานอาชญากรรมคอมพิวเตอร์ มันอาจจะเกิดจาก พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2550 ที่เริ่มใช้ คดีที่ขึ้นอาจจะยังน้อยอยู่ **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ยกตัวอย่างเช่น คดีของอากง เรื่องคอมพิวเตอร์ได้ไปขอประสานงานไปยังเครือข่ายโทรศัพท์ข้อมูลของเขาถ้าจัดเก็บ ไม่ถูกต้อง เกิดความเสียหายและประเด็นนี้ไม่มีความน่าเชื่อถือ และเรื่องการนำเสนอพยานหลักฐานในชั้นศาล คำพิพากษา

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
ผู้พิพากษาศาลแขวงจังหวัดนครปฐม (ต่อ)	**<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** 1. ควรให้ความรู้พื้นฐานในการตรวจพิสูจน์หลักฐานทางด้านอาชญากรรมคอมพิวเตอร์แก่ผู้พิพากษาด้วย 2. การกระจายองค์ความรู้ไปสู่ผู้ที่เกี่ยวข้อง **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่ามีความสุขุม และความมุ่งมั่นในการเล่า และถ่ายทอดประสบการณ์ที่ผ่านมาได้อย่างมีประสิทธิภาพ
พนักงานสอบสวนระดับชำนาญการพิเศษกรมสอบสวนคดีพิเศษ	กล่าวถึงเรื่องของการดำเนินคดี ในหัวข้อการจัดการองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์ จะตรงกับบทบาทของเจ้าหน้าที่ตำรวจ ก็คือ 2 บทบาท 1.เกี่ยวกับเรื่องของการรักษาความสงบเรียบร้อย 2.เรื่องของการดำเนินคดี ในส่วนที่สำคัญเรื่องของการดำเนินคดีในด้านของกฎหมายลักษณะพยานการนำเสนอเข้าสู่ขบวนการสอบสวนสู่ชั้นศาล **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** การเรียนรู้ซึ่งกันและกัน เป็นเรื่องดีก็ทำสม่ำเสมอ ถ้ามีการอบรมก็จะพยายามกระจายองค์ความรู้ในการดำเนินการเบื้องต้น และให้ความรู้ด้วยการแลกเปลี่ยน จากประสบการณ์ที่ผ่าน ๆ มาก็มีบางส่วนต้องการประสบการณ์ทำงานโดยเฉพาะเป็นเชิงเทคนิค **<u>วิธีการสู่ความสำเร็จ/ เทคนิค / กลยุทธ์</u>** เรื่องการตรวจพิสูจน์ ผู้ตรวจพิสูจน์ไม่ค่อยเข้าใจเนื้อหาคดี จึงมีวิธีการทำแบบฟอร์ม สรุปพฤติกรรมตัวย่อ โดยสังเขป คือไม่ต้องการรายละเอียด โดยไม่ต้องเปิดเผยให้รู้ทั้งสำนวน และอธิบายให้เข้าใจว่าต้องการอะไร เวลากระทำความผิดก็จะรู้เป็นพยานหลักฐานประเภทใด เกี่ยวข้องกันอย่างไร เพื่อให้ทำการสืบค้นได้ง่ายขึ้น **<u>บุคลิกลักษณะผู้เล่า</u>** ผู้เล่าสามารถแนะแนวคิดที่เป็นประโยชน์ และมีความรู้

ตาราง 3-13 (ต่อ)

ชื่อผู้เล่า	ประเด็นเรื่องเล่า (โดยสรุป)
นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง	กล่าวถึงเรื่องเครื่องมือ และอุปกรณ์ที่ใช้ในการตรวจพิสูจน์หลักฐานทางด้านคอมพิวเตอร์ว่า มีการร่วมมือกันระหว่างหน่วยงานที่เกี่ยวข้อง ทั้งภาครัฐ และเอกชนเป็นอย่างดี เพื่อความสะดวกและรวดเร็วในการตรวจพิสูจน์หลักฐาน **<u>สิ่งที่ผู้เล่าภาคภูมิใจ</u>** ขณะนี้การพิสูจน์หลักฐานทางด้านคอมพิวเตอร์ของทางสำนักงานพิสูจน์หลักฐานได้เพิ่มศักยภาพในการตรวจหลักฐาน โดยกระจายไปยังศูนย์ต่างๆในประเทศไทย เช่น นครราชสีมา สงขลา เชียงใหม่ เป็นต้น ในด้านเทคโนโลยีเรามีความก้าวหน้าพอสมควร และผู้เชี่ยวชาญก็มีความรู้ **<u>บุคลิกลักษณะผู้เล่า</u>** มีความเป็นผู้นำ ความรู้ ความสามารถ และประสบการณ์สูง สามารถแสดงความคิดเห็นที่เป็นประโยชน์ได้อย่างดี

สรุปกิจกรรม AAR (Action After Review) ในการประชุมครั้งที่ 3 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Story Telling)”

เป้าหมายของการร่วมประชุมในครั้งนี้ เพื่อแลกเปลี่ยนความรู้ที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ และรวบรวมข้อมูล ปัญหาในการปฏิบัติงานของเจ้าหน้าที่ เพื่อสร้างคู่มือในการจัดการความรู้ที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ โดยเป้าหมายที่บรรลุเกินคาด จากประสบการณ์จากผู้เข้าร่วมประชุมท่านอื่นๆ ทำให้เห็นมุมมองต่างๆ มากขึ้น และสามารถนำไปปฏิบัติงานในส่วนที่ตนเองรับผิดชอบได้ไม่มากก็น้อย ส่วนเป้าหมายที่ไม่บรรลุ คือ การปฏิบัติงานร่วมกันของหน่วยงานต่างๆ ที่เกี่ยวข้องกัน และการแก้ไขปัญหาที่ยังไม่ชัดเจน และสิ่งที่ได้เรียนรู้ที่เป็นประโยชน์ที่สุด คือ การนำความคิดเห็นมุมมองต่างๆ ไปปรับวิสัยทัศน์ในการปฏิบัติงาน และความร่วมมือกันระหว่างหน่วยงาน เพื่อนำไปสู่ความสำเร็จอย่างแท้จริง โดยจะนำกลับพิจารณาจัดหลักสูตรอบรมเพิ่มเติมเกี่ยวกับอาชญากรรมคอมพิวเตอร์

ภาพ 3-7 การประชุมครั้งที่ 3 การแลกเปลี่ยนเรียนรู้ค้นหาปัญหาและอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้องด้านอาชญากรรมคอมพิวเตอร์
วันจันทร์ ที่ 1 กรกฎาคม พ.ศ. 2556 เวลา 9.30–12.00 น.
ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

บทที่ 4
ผลที่ได้จากการดำเนินการเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

4.1 สภาพการณ์ทางด้านอาชญากรรมคอมพิวเตอร์

4.1.1 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) พระราชกฤษฎีกาว่าด้วยการควบคุมดูและธุรกิจบริการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ.2551

10) พระราชกฤษฎีกากำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์มาบังคับใช้ 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) หลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติหลักเกณฑ์เกี่ยวกับคุณสมบัติของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

18) ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ออก พ.ศ. 2555

4.1.2 ปัจจุบันหน่วยงานที่รับผิดชอบดำเนินการคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ได้แก่ สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งสำนักงานตำรวจจะเป็นด่านแรกในการดำเนินการ สืบสวน สอบสวน ป้องกัน และปราบปราม อาชญากรรมทางคอมพิวเตอร์

4.1.3 ปัจจุบันการดำเนินชีวิตประจำวันของเรา จะพึ่งพาเทคโนโลยีเป็นหลักโดยเฉพาะการใช้งานอินเทอร์เน็ต จนกลายเป็นสังคมออนไลน์ที่มีการกระจายข้อมูลข่าวสารผ่านระบบอินเทอร์เน็ตอยู่ตลอดเวลา ซึ่งมีทั้งข้อมูลที่เป็นนจริงและข้อมูลที่เป็นเท็จ ดังนั้น เครือข่ายชุมชนออนไลน์ จึงเป็นช่องทางหนึ่งที่สำคัญในการช่วยเหลือการทำงานของทางราชการ ในการสืบสวน สอบสวน ป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพราะจะมีข้อมูลข่าวสารที่เป็นประโยชน์ต่อผู้ใช้งาน (Users) ในการป้องกันการตกเป็นเหยื่อของอาชญากรทางเทคโนโลยี ดังนั้นในการแก้ไขปัญหาดังกล่าว เราต้องมีการร่วมกันระหว่างหน่วยงานภาครัฐ และหน่วยงานภาคเอกชน โดยควรมีการรวมกลุ่มกันของผู้ประกอบการเว็บไซต์ต่างๆ เพื่อรวมตัวกันเป็นชุมชนออนไลน์ในการเผยแพร่ข้อมูลข่าวสารที่เป็นประโยชน์ต่อสังคมออนไลน์ เพื่อ

1) ร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง และวิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการป้องกันปัญหาดังกล่าว

2) ร่วมแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็ปไซต์ (Black List)

3) จัดเวทีให้มีการร่วมงานประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแรกเปลี่ยนข้อคิดเห็น และกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

4.2 รูปแบบของคดีที่ต้องให้ความสำคัญและนำส่งวัตถุพยานของกลางตรวจพิสูจน์ทางคอมพิวเตอร์

4.2.1 คดีลักทรัพย์

- วัตถุพยานของกลางที่สงสัยว่าเป็นของที่ถูกโจรกรรมไปนำส่งตรวจสืบค้นข้อมูลจากวัตถุพยานของกลางที่มีการเก็บข้อมูลแบบดิจิตอล เพื่อหาและเปรียบเทียบกับข้อมูลของผู้เสียหายว่าเกี่ยวพันกันหรือไม่อย่างไร เช่น นำเครื่องคอมพิวเตอร์ที่ส่งสัยว่าเป็นเครื่องที่ถูกโจรกรรมไปตรวจหาข้อมูลเพื่อเปรียบเทียบกับข้อมูลการใช้งานที่ผู้เสียหายมีอยู่

4.2.2 คดีเกี่ยวกับชีวิต

- ของกลางที่มีการเก็บข้อมูลแบบดิจิตอลซึ่งอยู่ในที่เกิดเหตุ นำส่งตรวจสืบค้นข้อมูล เพื่อหาและเปรียบเทียบความสัมพันธ์กับข้อมูลของผู้เสียหายหรือคนร้าย เช่น ในที่เกิดเหตุที่พบศพถูกฆ่าแล้วเผามีบัตรประจำตัวประชาชนถูกเผาเหลือแต่ส่วนที่เป็นแถบแม่เหล็กตกอยู่สามารถนำส่งตรวจเพื่อสืบค้นข้อมูลที่มีอยู่ในแถบแม่เหล็กได้

4.3.3 คดีระเบิด

- ที่มีการใช้โทรศัพท์เป็นตัวจุดชนวนระเบิด หลังจากมีการระเบิดแล้วพบซิมการ์ดโทรศัพท์ตกในที่เกิดเหตุ สามารถนำส่งตรวจหาข้อมูลที่มีอยู่ในซิมการ์ดได้

4.2.4 คดีละเมิด

- กรณีมีการนำข้อมูลของผู้เสียออกเผยแพร่ เช่น การนำภาพผู้เสียหายไปตัดต่อดัดแปลงให้เสียหาย การทำซ้ำของข้อมูลผู้อื่นอันเป็นข้อมูลเฉพาะตัวที่ต้องขออนุญาตก่อน เช่นการ Copy สิทธิบัตรทางอิเล็กทรอนิกส์ของผู้อื่น

4.2.5 คดีผู้ก่อการร้าย

- กรณีมีการใช้เครื่องคอมพิวเตอร์เชื่อมต่ออินเตอร์เน็ตเพื่อส่งข้อมูลที่ใช้ในการก่อการร้าย

4.2.6 คดีเกี่ยวกับการปลอมแปลง

- เช่น มีการแก้ไข และเปลี่ยนแปลงข้อมูลของผู้เสียหาย

4.2.7 คดีค้ายา

- เช่นมีการขนยาบ้าขณะหลบหนีตำรวจแล้วทิ้งรถไปสามารถตรวจหาข้อมูลที่สามารถเชื่อมโยงไปถึงตัวคนร้ายได้ เช่น มีของกลางที่เป็นโทรศัพท์, กล้องถ่ายภาพ, บัตรที่มีการบันทึกข้อมูลระบบดิจิตอลสามารถส่งตรวจหาข้อมูลได้

4.3 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

4.4 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 พึงระวังเช่นเดียวกับกรณีคดีอื่นๆ ทั่วไป ว่าการเปลี่ยนแปลงที่ไม่คาดคิดต่อวัตถุพยานต่างๆ อาจก่อให้เกิดอันตรายแก่ตัวเจ้าหน้าที่ที่กำลังปฏิบัติหน้าที่อยู่ได้

การใช้ขั้นตอนการดำเนินการที่ถูกต้องเหมาะสม จะช่วยให้มั่นใจว่าเกิดความปลอดภัยแก่เจ้าหน้าที่รวมถึงบุคคลอื่นๆ ที่อยู่ในสถานที่เกิดเหตุนั้นด้วย

2) กฎสำคัญ (Golden Rules)

มีหลักการในการปฏิบัติทั่วๆ ไปเมื่อเข้าไปถึงที่เกิดเหตุที่อาจมีเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เกี่ยวข้องด้วยอยู่หลายหลักการด้วยกัน เช่น

2.1 ความปลอดภัยของเจ้าพนักงาน

รักษาสถานที่เกิดเหตุและจัดการให้เกิดความปลอดภัย หากเชื่ออย่างมีเหตุผลว่ามีเครื่องคอมพิวเตอร์เกี่ยวข้องในคดีที่คุณทำการสืบสวนสอบสวนอยู่ ให้ดำเนินการเก็บรักษาพยานหลักฐานโดยทันที

2.2 คำนึงว่ามีอำนาจตามกฎหมายให้เข้ายึดเครื่องคอมพิวเตอร์เรียบร้อยหรือยัง (การสำรวจในขั้นเบื้องต้น, หมาย ค้น เป็นต้น)

ห้ามทำการเปิดไฟล์ใดๆ 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 และพฤติการณ์ของความผิด ความรู้ความสามารถของผู้ต้องสงสัยเกี่ยวกับคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์หรือเครื่องคอมพิวเตอร์ใดที่เกี่ยวข้องกับคดี

3.2 ให้หัวหน้าชุดปราบปรามจัดชุดรักษาความปลอดภัย เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าหรือออกสถานที่เกิดเหตุ และป้องกันมิให้เกิดการปนเปื้อนต่อพยานหลักฐานใดๆ โดยแบ่งชุดรักษาความปลอดภัยออกเป็น 2 ส่วน คือ

3.2.1 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ

3.2.2 ชุดรักษาความปลอดภัยภายในสถานที่เกิดเหตุ

3.3 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุ ปิดกันสถานที่เกิดเหตุด้วยเทปปิดกัน พื้นที่เกิดเหตุ (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 ชุดรักษาความปลอดภัยรอบสถานที่เกิดเหตุนำตัวผู้ต้องสงสัยบุคคลที่ไม่เกี่ยวข้อง 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 กรณีตรวจพบภัยคุกคามหรืออันตรายร้ายแรงตามดุลยพินิจของชุดรักษา ความปลอดภัยรอบสถานที่เกิดเหตุให้อพยพเจ้าหน้าที่และบุคลากรที่เกี่ยวข้องออกจากพื้นที่นั้นๆ 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

4.5 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/หรือกล้องวิดีโอและ/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) และถุงมือป้องกันไฟฟ้าสถิต (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 ตามภาพ 4-1
- วาดภาพแผนผังและติดป้ายสายไฟต่างๆ เพื่อดูว่าสายใด

ภาพ 4-1 สายไฟด้านหลังเครื่อง

เชื่อมต่ออยู่กับอุปกรณ์ใด

- 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

ภาพ 4-2 เครื่องคอมพิวเตอร์เครือข่าย

4. เครื่องคอมพิวเตอร์พกพาที่ไม่ได้เปิดใช้งาน (Laptop Turn-off)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลำดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและ สายเชื่อมต่ออื่นๆ
- ชุดตรวจค้นและรวบรวมพยานหลักฐานบันทึกรายละเอียดของเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องลงในบันทึกการยึดหลักฐาน (Evidence Collection Form) ให้ครบถ้วน
- ชุดเทคนิคและการถ่ายภาพ ดาเนินการถ่ายภาพพยานหลักฐานอย่างชัดเจนโดยต้องครอบคลุมถึงหมายเลขเครื่อง (Serial Number) ยี่ห้อของอุปกรณ์ และ รุ่นของอุปกรณ์ (Model) (ถ้ามี) ถ่ายภาพสายไฟและสายเชื่อมต่อตลอดจนอุปกรณ์ต่อพ่วงต่างๆ (DVD-Drive และ External Drive) ให้ครบถ้วนชัดเจน เพื่อแสดงถึงสภาพของพยานหลักฐานเมื่อเข้าเก็บหลักฐาน

- ถอดแบตเตอรี่ออกจากตัวเครื่อง
- ถอดสายไฟและสายเชื่อมต่อ ตลอดจนอุปกรณ์ต่อพ่วงออกจากเครื่องคอมพิวเตอร์
- ปิดเทปป้องกันการปนเปื้อนพยานหลักฐาน (Evidence Tape) บริเวณจุดเชื่อมต่ออุปกรณ์ เช่น ช่องเชื่อมต่อสายไฟ ช่องเชื่อมต่อ USB ช่องเชื่อมต่อ Mouse และ Keyboard เป็นต้น
- ชุดเทคนิคและการถ่ายภาพ ดำเนินการถ่ายภาพพยานหลักฐานที่ถูกปิดเทปปนเปื้อนพยานหลักฐานเรียบร้อยแล้ว เพื่อแสดงถึงสภาพของพยานหลักฐานที่เจ้าหน้าที่ได้ทำการจัดเก็บ
- ชุดตรวจค้นและรวบรวมพยานหลักฐานบรรจุอุปกรณ์คอมพิวเตอร์ลงในบรรจุภัณฑ์เฉพาะด้าน อ้างอิงจากหัวข้อกลยุทธ์การบริหารจัดการบรรจุภัณฑ์พยานหลักฐานในสถานที่เกิดเหตุ
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานหลังจากบรรจุภัณฑ์เรียบร้อยแล้ว
- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบความสมบูรณ์และเตรียมความพร้อมสำหรับการขนส่ง
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยาน หลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน
- หัวหน้าชุดปราบปราม ตรวจสอบพร้อมลงลายมือชื่อรับรองการเก็บรวบรวมหลักฐานให้ชัดเจน
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน
- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

5. กรณีตรวจค้นเครื่องคอมพิวเตอร์พกพาที่เปิดใช้งาน (Laptop Turn-on)

- ตรวจสอบให้มั่นใจว่าผู้ปฏิบัติงานรวบรวมพยานหลักฐานสวมอุปกรณ์ป้องกันไฟฟ้าสถิตและผู้ปฏิบัติงานเป็นผู้ที่ผ่านการอบรมการเก็บรวบรวมพยานหลักฐานอย่างถูกต้องมาแล้ว
- ชุดเทคนิคและการถ่ายภาพ ถ่ายภาพพยานหลักฐานและบริเวณที่ตรวจพบให้ชัดเจนและจัดทำป้ายแสดงหมวดและลาดับพยานหลักฐาน (Evidence Tag) และแถบสัญลักษณ์ (Label) สำหรับสายไฟและสายเชื่อมต่ออื่นๆ
- ในกรณีที่เครื่องคอมพิวเตอร์พกพาไม่ได้ทาการเปิดหน้าจอ ให้ชุดตรวจค้นและรวบรวมพยาน หลักฐานเปิดหน้าจอแสดงผล 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) ถ่ายภาพสายไฟและสายเชื่อมต่อตลอดจนอุปกรณ์ต่อพ่วงต่างๆ (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 ส่งพยานหลักฐานให้ชุดขนส่งและคุ้มครองพยานหลักฐาน ลงลายมือชื่อในฐานะผู้ส่งต่อพยานหลักฐาน (Released by) และส่งมอบเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐาน ให้ชุดขนส่งและคุ้มครองพยานหลักฐานลงลายมือชื่อผู้รับพยานหลักฐาน (Received by) ให้ชัดเจน

- ชุดตรวจค้นและรวบรวมพยานหลักฐานตรวจสอบอุปกรณ์จัดเก็บอุปกรณ์ที่ใช้ในการปฏิบัติงานเพื่อเตรียมความพร้อมก่อนเสร็จสิ้นปฏิบัติการ

6. สื่อบันทึกข้อมูล (Storage Media)

สิ่งที่ควรรู้เบื้องต้น : สื่อบันทึกข้อมูลถูกใช้เพื่อเก็บข้อมูลจากอุปกรณ์อิเล็กทรอนิกส์ อุปกรณ์อิเล็กทรอนิกส์บางชนิดมีพื้นที่ความจุที่ตายตัวในตัวของมันเองแต่ในบางครั้งก็จำเป็นต้องมีการถ่ายโอนข้อมูลขึ้นมา อุปกรณ์จำนวนมาก ในปัจจุบันสามารถที่จะเก็บข้อมูลลงภายในพื้นที่ความจุของตัวเอง และยังสามารถเก็บข้อมูลลงในสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Removable media) อีกด้วย สื่อบันทึกข้อมูลที่เคลื่อนย้ายได้นั้นใช้ได้ทั้งเพื่อทำการถ่ายโอนข้อมูลและเพื่อเก็บข้อมูลไว้ในตัวเอง

ภาพ 4-3 รูปแบบสื่อบันทึกข้อมูล

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 (บันทึกเวลาตามขั้นตอน ถ่ายรูปตามลำดับเวลา ถ่ายวิดีโอ บรรยาย)
- เก็บวัตถุพยานทุกชนิด ให้ห่างจากแม่เหล็ก เครื่องรับส่งวิทยุ 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 บันทึกข้อมูลลงในเอกสารห่วงโซ่ผู้ครอบครองพยานหลักฐานพร้อมลงลายมือชื่อผู้เก็บรวบรวมพยานหลักฐานให้ชัดเจน
- 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 ไม่ควรเก็บในที่มีความร้อนสูง หรือในที่ที่มีความชื้นหรือความเย็น 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 บางส่วนของอุปกรณ์มีลักษณะเป็นสิ่งที่ไวต่อการสัมผัสซึ่ง อาจทำลายพยานหลักฐานที่มีได้

- 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

4.6 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)

4.7 ขั้นตอนการปฏิบัติเพื่อบรรจุพยานหลักฐานลงบรรจุภัณฑ์ในสถานที่เกิดเหตุ (Crime Scene Evidence Package Protocol)

4.7.1 ชุดตรวจค้นและรวบรวมพยานหลักฐาน บรรจุหลักฐานในลงบรรจุภัณฑ์เฉพาะด้านทันทีหลังจากปฏิบัติตาม ขั้นตอนการปฏิบัติเพื่อตรวจค้นและรวบรวมหลักฐานในที่เกิดเหตุ เรียบร้อยแล้ว

4.7.2 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 และลงลายมือชื่อผู้เก็บรวบรวมให้ชัดเจน
- 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

4.8 การบริหารจัดการขนส่งพยานหลักฐาน (Evidence Transportation Management)

หนึ่งในปัจจัยสำคัญของการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐานนั้นก็คือ การขนส่งพยานหลักฐานจากสถานที่เกิดเหตุไปยังห้องปฏิบัติการ ซึ่งมีปัจจัยที่ต้องให้ความสาคัญซึ่งอาจส่งผลต่อพยานหลักฐานได้ดังนั้นการขนส่งพยานหลักฐานจึงต้องปฏิบัติตามขั้นตอนอย่างเคร่งครัด การขนส่งเคลื่อนย้ายพยานหลักฐาน ต้องใช้ยานพาหนะที่เหมาะสม และระมัดระวังไม่ก่อให้เกิดความเสียหายต่อพยานหลักฐาน จัดทำรายการพยานหลักฐานให้ครบถ้วน

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าชุดปราบปราม
- ชุดตรวจค้นและรวบรวมพยานหลักฐาน
- ชุดขนส่งและคุ้มครองพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- รถขนส่งพยานหลักฐาน

4.8.1 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

4.8.2 ปัจจัยสำคัญที่ต้องให้ความสำคัญระหว่างการขนส่งพยานหลักฐาน

1) การขนส่งพยานหลักฐานต้องใช้รถขนส่งพยานหลักฐานที่ได้รับการออกแบบมาโดยเฉพาะ

2) หลีกเลี่ยงการใช้งานคลื่นวิทยุหรืออุปกรณ์ใดๆ ที่อาจก่อให้เกิดคลื่นวิทยุและคลื่นสนามแม่เหล็ก

3) หลักเลี่ยงเส้นทางที่มีเสาไฟฟ้าแรงสูง หรือมีคลื่นสนามแม่เหล็กแรงสูง

4.9 การบริหารจัดการและจัดเก็บพยานหลักฐาน (Evidence Retention Management)

หนึ่งในปัจจัยสำคัญของการรักษาและสงวนไว้ซึ่งความถูกต้องแท้จริงของพยานหลักฐานที่ได้รับจากสถานที่เกิดเหตุนั้น คือการจัดเก็บและรักษาสภาพของพยานหลักฐานในห้องเก็บพยานหลักฐาน ซึ่งมีปัจจัยที่ต้องให้ความสำคัญซึ่งและต้องปฏิบัติตามขั้นตอนอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐาน
- ชุดดูแลห้องเก็บพยานหลักฐาน

- ชุดขนส่งและคุ้มครองพยานหลักฐาน

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- ตู้เก็บพยานหลักฐาน

4.9.1 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

4.9.2 กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าหน่วยดูแลห้องเก็บพยานหลักฐานในฐานะผู้รับผิดชอบห้องเก็บพยานหลักฐานจำเป็นต้องจัดตารางกำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

1) ความถูกต้องครบถ้วนของพยานหลักฐานที่จัดเก็บ เทียบกับรายการตามเอกสาร

2) ความถูกต้องสมบูรณ์ทางกายภาพของพยานหลักฐานในปัจจุบัน เทียบกับข้อมูลสภาพของหลักฐานเมื่อได้รับมา

4.10 การเตรียมความพร้อมทางอุปกรณ์และเครื่องมือด้านการตรวจวิเคราะห์หลักฐาน (Computer Forensic Tools and Equipment Preparation)

4.10.1 การจัดเตรียมเครื่องมือสำหรับการตรวจวิเคราะห์หลักฐาน

การตรวจวิเคราะห์พยานหลักฐานถือเป็นกระบวนการสำคัญในการสืบสวนสอบสวนอาชญากรรมที่เกี่ยวกับเทคโนโลยี เนื่องจากพยานหลักฐานทางอิเล็กทรอนิกส์มีเอกลักษณ์และแตกต่างจากพยานหลักฐานชนิดอื่น จึงต้องมีกระบวนการที่เหมาะสมและและต้องใช้เครื่องมืออุปกรณ์เฉพาะทางที่มีคุณภาพ ดังนั้นการจัดเตรียมอุปกรณ์เครื่องมือก่อนดำเนินการตรวจวิเคราะห์หลักฐาน จึงถือเป็นสิ่งจำเป็นที่ต้องปฏิบัติอย่างเคร่งครัด

ผู้ปฏิบัติงานที่เกี่ยวข้อง

- หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน
- เจ้าหน้าที่ประจำห้องปฏิบัติการ

เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง

- เครื่องมือและโปรแกรมสำหรับการทำสำเนาหลักฐาน

- เครื่องมือและโปรแกรมสำหรับการตรวจวิเคราะห์หลักฐาน
- สื่อจัดเก็บสำเนาข้อมูล
- เอกสารการปฏิบัติงาน

4.10.2 ขั้นตอนการปฏิบัติเพื่อจัดเตรียมเครื่องมือสำหรับการตรวจวิเคราะห์หลักฐานและการทดสอบ (Computer Forensic Tools Preparation and Testing Protocol)

1) เจ้าหน้าที่ประจำห้องปฏิบัติการ ตรวจสอบความถูกต้องและครบถ้วนของเครื่องมือที่ต้องใช้งานในแต่ละคดี

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

3) เจ้าหน้าที่ประจำห้องปฏิบัติการตรวจสอบและจัดเตรียมอุปกรณ์สำหรับการจัดทำสำเนาหลักฐาน

4) หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน ควบคุมดูแลกระบวกการปฏิบัติงานและตรวจสอบความถูกต้องพร้อมลงลายมือชื่อรับรอง

4.10.3 กำหนดการทบทวนและตรวจสอบความถูกต้องของพยานหลักฐานที่จัดเก็บ

หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐานในฐานะผู้รับผิดชอบห้องห้องปฏิบัติการวิเคราะห์หลักฐานจำเป็นต้องจัดตารางกาหนดการทบทวนและตรวจสอบความถูกต้องของเครื่องมือและซอฟต์แวร์ เป็นประจำทุกสัปดาห์ โดยให้ความสำคัญกับปัจจัยดังนี้

1) เครื่องมือและซอฟต์แวร์สามารถใช้งานได้เป็นปกติ
2) เครื่องมือและซอฟต์แวร์มีลิขสิทธิ์ที่ถูกต้อง

4.11 การทำลายข้อมูลในสื่อเก็บข้อมูล (Media Sanitization and Cleaned Evidence Preparation)

4.11.1 การทำลายข้อมูลด้วยวิธีการเขียนทับในสื่อเก็บข้อมูล

การทำลายข้อมูลด้วยวิธีการเขียนทับ (Wiping) ถือเป็นกระบวนการสำคัญในการรับรองความถูกต้องของสื่อเก็บข้อมูล เพื่อให้แน่ใจว่าจะไม่มีข้อมูลเดิมจากหลักฐานในคดีอื่นๆ หลงเหลืออยู่ในสื่อจัดเก็บข้อมูลดังกล่าว ซึ่งจะทำให้กระบวนการในการตรวจพิสูจน์หลักฐานมีความถูกต้อง โปร่งใสและน่าเชื่อถือ จึงต้องมีการจัดทำขั้นตอนการทำลายข้อมูลด้วยวิธีการเขียนทับในสื่อเก็บข้อมูลขึ้น

ผู้ปฏิบัติที่เกี่ยวข้อง

- หัวหน้าผู้ดูแลห้องปฏิบัติการวิเคราะห์หลักฐาน
- เจ้าหน้าที่ประจำห้องปฏิบัติการ
- เครื่องมือและอุปกรณ์ที่เกี่ยวข้อง
- เครื่องมือและซอฟต์แวร์สำหรับการทำลายข้อมูลด้วยวิธีการเขียนทับ
- สื่อจัดเก็บสำเนาข้อมูล

- เอกสารการปฏิบัติงาน

4.11.2 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)

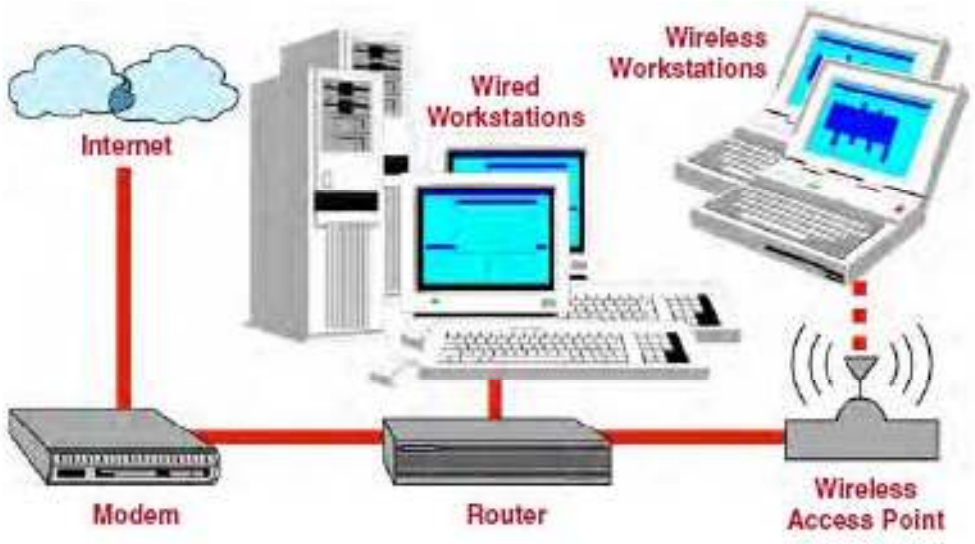
- อาจมีความจำเป็นต้องป้องกันความถูกต้องเที่ยงตรงของการสืบสวนสอบสวน โดยต้องปกป้องผู้ให้ข้อมูล รักษาความลับทางการค้าหรือทรัพย์สินทางปัญญา

Special Master

- การพิจาณาตามกฎหมายพิเศษเกี่ยวกับแพทย์ นักกฎหมาย คู่สามีภรรยา นักหนังสือพิมพ์และนักศาสนา เป็นต้น

4.12 องค์ประกอบพื้นฐานของระบบเน็ตเวิร์คในบ้าน (Home Network Basic Elements)

ตามที่เห็นในภาพ เน็ตเวิร์คภายในบ้านมักประกอบด้วยโมเด็ม เราท์เตอร์และเครื่องคอมพิวเตอร์ตั้งโต๊ะหรือแล็ปท็อป



ภาพ 4-4 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

4.13 รายการอาชญากรรมทางเทคโนโลยีและพยานหลักฐานทางดิจิตอล หรืออุปกรณ์อิเล็กทรอนิกส์อื่นๆ

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 และบันทึกต่างๆ
   - 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 และบันทึกต่างๆ
- โปรแกรมเกมส์คอมพิวเตอร์ (Computer Games)
- ซอฟท์แวร์การเปิดภาพและตกแต่งภาพ (Digital Photo Software)
- ภาพพิมพ์รูปถ่ายต่างๆ (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
   - ไฟล์การตั้งค่าต่างๆ (Configuration files)
   - อีเมล์ จดหมาย และบันทึกต่างๆ
   - โปรแกรมต่างๆ (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 และบันทึกต่างๆ
   - ประวัติทางการเงิน (Financial Records)
   - ข้อมูลจราจรทางคอมพิวเตอร์
   - พินัยกรรมและเอกสารทางกฎหมาย
   - ประวัติทางการรักษา (Medical records)
   - ประวัติการใช้งานโทรศัพท์และการชาระเงิน (Telephone and Billing Records)
   - บันทึกและไดอารีส่วนตัว (Personal Writings and Diaries)
   - แผนที่
   - ภาพถ่ายของเหยื่อหรือผู้ต้องสงสัย
   - ภาพถ่ายที่ระลึกถึงการฆาตกรรมต่างๆ
6) พยานหลักฐานสำคัญที่เกี่ยวข้องกับการกระทำความผิดภายในประเทศ
   - สมุดที่อยู่
   - ไดอารี
   - อีเมล์ จดหมาย และบันทึกต่างๆ
   - 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)
- รูปภาพเช็คหรือใบสั่งจ่ายเงินต่างๆ
- โปรแกรมทำธุรกรรมออนไลน์ (Online Banking Software)
- ลายเซ็นปลอม (Reproductions of Signatures)
- สมุดที่อยู่
- ปฏิทิน
- รูปภาพธนบัตรต่างๆ
- ข้อมูลลูกค้า
- ฐานข้อมูล
- อีเมล์ จดหมาย และบันทึกต่างๆ
- 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 และบันทึกต่างๆ
- ข้อมูลทางการเงิน
- รูปภาพต่างๆ
- ข้อมูลจราจรทางคอมพิวเตอร์
- เอกสารทางกฎหมายต่างๆ

- รายการโทรศัพท์
- การค้นหาข้อมูลต่างๆ 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 และบันทึกต่างๆ
- 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 และบันทึกต่างๆ
- 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
- หมายเลขโทรศัพท์ของบุคคลต่างๆ
- อีเมล์ จดหมาย และบันทึกต่างๆ
- 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 ต่างๆ สำหรับฮาร์ดแวร์และซอฟท์แวร์
- Backdrops
- Credit card reader/writer
- ซอฟท์แวร์ของกล้องดิจิตอล
- ซอฟท์แวร์ของเครื่อง Scanner
- เทมเพลตของข้อมูลบุคคลต่างๆ
- ใบสูติบัตร
- บัตรเงินสด (Check cashing card)
- ภาพถ่ายดิจิตอล
- ใบขับขี่
- ลายเซ็นต์อิเล็กทรอนิกส์
- ข้อมูลสำหรับทำใบขับขี่ปลอม
- เอกสารการประกันภัยปลอม
- บัตรประกันสังคม
- กิจกรรมทางอินเทอร์เน็ตที่เกี่ยวข้องกับการขโมยข้อมูลบุคคล
- การโพสต์อีเมล์ หรือชื่อ newsgroup
- ไฟล์เอกสารที่ถูกลบทิ้ง
- ใบสั่งของออนไลน์
- ข้อมูลการซื้อขายออนไลน์
- ข้อมูลจราจรทางคอมพิวเตอร์
- เครื่องมือต่างๆ 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)

4.14 แนวทางคำถามสำหรับคดีทางด้านอาชญากรรมคอมพิวเตอร์

ในการใช้คำถามเหล่านี้ควรจะต้องมีข้อมูลเบื้องต้นก่อนเพื่อช่วยในการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ โดยข้อมูลเบื้องต้นที่ควรทราบมีดังต่อไปนี้

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

4.14.1 คำถามทั่วไปสำหรับผู้ทำการสืบสวนสอบสวน ซึ่งอาจจะใช้ถามในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ดังต่อไปนี้

- ได้เครื่องคอมพิวเตอร์นี้มาเมื่อไหร่ เป็นเครื่องใหม่หรือเป็นเครื่องใช้แล้ว
- ใครเป็นผู้ใช้งานที่เข้าถึงฮาร์ดแวร์และซอฟท์แวร์

- สื่ออิเล็กทรอนิกส์ต่างๆ ของเครื่องคอมพิวเตอร์นั้น เช่น แผ่นฟล็อปปี้ ธัมพ์ไดร์ฟ ฯลฯ ถูกเก็บอยู่ที่ใด
- ลายพิมพ์นิ้วมือของใครที่อาจพบบนอุปกรณ์อิเล็กทรอนิกส์
- หากมีคนอื่นที่เข้าถึงเครื่องคอมพิวเตอร์นั้น ฮาร์ดแวร์หรือซอฟท์แวร์ใดที่สามารถเข้าถึงทุกสิ่งทุกอย่างที่อยู่บนเครื่องคอมพิวเตอร์ หรือเข้าถึงเพียงแค่ไฟล์ โฟล์เดอร์ หรือโปรแกรมที่ต้องการได้
- มีใครกี่คนที่ใช้เครื่องคอมพิวเตอร์เครื่องนี้ เป็นใครบ้าง
- ผู้ใช้งานคอมพิวเตอร์แต่ละคนมีประสบการณ์ในการใช้งานคอมพิวเตอร์ในระดับใด
- ผู้ใช้งานแต่ละคนนั้นใช้งานเครื่องคอมพิวเตอร์ในช่วงเวลาใดของวันบ้าง
- Username บนเครื่องคอมพิวเตอร์นั้นมีอะไรบ้าง
- โปรแกรมอะไรบ้างที่ผู้ใช้งานแต่ละคนใช้
- เครื่องคอมพิวเตอร์นั้นต้องการ username และ password ในการเข้าใช้งานหรือไม่ ถ้าใช่username และ password นั้นมีอะไรบ้าง
- มีซอฟท์แวร์อะไรในเครื่องบ้างไหมที่ต้องใช้พาสเวิร์ด
- เครื่องคอมพิวเตอร์นั้นมีการเชื่อมต่อกับอินเทอร์เน็ตอย่างไร (ใช้ DSL, ผ่านสายโทรศัพท์ ระบบ lanหรืออื่นๆ)
- เหยื่อหรือผู้ต้องสงสัยมีอีเมล์หรือไม่ ใช้อีเมล์ของอะไร (yahoo, AOL, gmail, hotmail หรืออื่นๆ)
- หากมีอีเมล์เข้ามาเกี่ยวข้องในคดี ให้ถามเหยื่อหรือผู้ต้องสงสัยถึงชื่ออีเมล์ต่างๆ ของเขา
- โปรแกรมอีเมล์ใดที่ผู้ต้องสงสัยหรือเหยื่อใช้
- เหยื่อหรือผู้ต้องสงสัยสามารถเข้าถึงเครื่องคอมพิวเตอร์ของตนเองได้จากระยะไกลหรือไม่ (สามารถเข้าถึงเครื่องตัวเองเมื่ออยู่ไกลจากบ้านหรือออฟฟิศได้หรือไม่)
- มีผู้ใช้เครื่องคนใดใช้พื้นที่เก็บบันทึกข้อมูลออนไลน์หรือใช้พื้นที่เก็บบันทึกข้อมูลแบบ remotestorage หรือไม่
- มีโปรแกรมใดหรือไม่ที่ถูกใช้เพื่อล้างข้อมูลในคอมพิวเตอร์นั้น
- ในเครื่องคอมพิวเตอร์นั้นมีโปรแกรมสำหรับการเข้ารหัสหรือเครื่องมือในการทำ wiping ฮาร์ดไดร์ฟหรือไม่
- เครื่องคอมพิวเตอร์นั้นเปิดทำงานอยู่ตลอดเวลาใช่หรือไม่

4.14.2 คำถามสำหรับคดีอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ ใช้ถามเจาะจงกรณีความผิดและเจาะจงกับบุคคล ดังต่อไปนี้

กรณีการขโมยข้อมูลส่วนบุคคลและคดีทางด้านการเงิน :

คำถามที่ใช้ถามเหยื่อ :

- คุณรู้ถึงความผิดปกติใดๆ ที่เกิดกับ account ของคุณหรือไม่

- Account ใดที่นำข้อมูลไปใช้ให้เกิดความเสียหาย
- คุณได้ให้ข้อมูลส่วนตัวกับใครหรือหน่วยงานใดหรือไม่
- คุณให้ข้อมูลนั้นไปเพื่ออะไร
- เมื่อเร็วๆ นี้คุณได้กรอกข้อมูลสมัครใช้บัตรเครดิตหรือเอกสารเงินกู้ใดๆ หรือไม่
- คุณเก็บข้อมูลส่วนตัวของคุณไว้ในเครื่องคอมพิวเตอร์หรือไม่
- มีข้อมูลใบเสร็จหรือ statement ทางการเงินถูกส่งไปให้ทางเมล์อย่างผิดปกติหรือไม่
- คุณได้ตรวจสอบรายการการใช้บัตรเครดิตบ้างหรือไม่

4.14.3 คำถามที่ใช้ถามกับบุคคลเป้าหมายหรือผู้ต้องสงสัย:

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

4.14.4 อาชญากรรมทางคอมพิวเตอร์ที่เกี่ยวข้องกับเด็ก:

คำถามที่ใช้ถามเหยื่อ :

- เหยื่อได้ออนไลน์ให้ห้องแชทใดๆ หรือไม่
- เหยื่อใช้อินเทอร์เน็ต อีเมล์หรือแชทจากเครื่องคอมพิวเตอร์เครื่องอื่นๆ หรือไม่ ถ้าใช่ใช้ที่ใด
- เหยื่อได้ให้ข้อมูลจริงกับคนอื่นที่ออนไลน์อยู่หรือไม่ เช่น ชื่อจริง อายุ ที่อยู่ เป็นต้น
- อีเมล์ของเหยื่อคืออะไร หรือใช้ชื่ออะไรในการออนไลน์เล่นแชต และเล่นแชตในห้องใด
- มีรายชื่อใครบ้างที่อยู่ในลิสต์การเล่นแชทของเหยื่อ
- เหยื่อได้ทำการเก็บบันทึก chat logs ไว้หรือไม่
- เหยื่อใช้อีเมล์หรือแชตของที่ใด ด้วยโปรแกรมอะไร
- มีพฤติการณ์ที่เน้นออกไปในทางเพศในรูปภาพหรือการติดต่อพูดคุยกันหรือไม่
- เหยื่อเคยได้รับภาพหรือของขวัญจากผู้ต้องสงสัยหรือไม่

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

- เครื่องคอมพิวเตอร์ทั้งหมดของผู้ต้องสงสัยอยู่ที่ใด
- ผู้ต้องสงสัยทำการเก็บข้อมูลไว้ที่อื่นหรือไม่ เช่น เก็บใน external hard drive หรือที่เก็บข้อมูลออนไลน์ เป็นต้น
- ผู้ต้องสงสัยใช้ชื่อใดในการออนไลน์ และเข้าคุยในห้องแชตใด ด้วยชื่ออะไร
- ผู้ต้องสงสัยได้ทำการติดต่อกับใครทางอิเล็กทรอนิกส์หรือไม่
- ผู้ต้องสงสัยทำการติดต่อกับผู้อื่นนั้นด้วยวิธีได้ (ทางอีเมล์ แชต เป็นต้น)

- ผู้ต้องสงสัยดูภาพลามกอนาจารเด็กโดยใช้เครื่องคอมพิวเตอร์หรือไม่ ถ้าใช่ผู้ต้องสงสัยได้รูปภาพเหล่านั้นมาได้อย่างไร
- ผู้ต้องสงสัยได้ทำการส่งรูปภาพเหล่านั้นไปยังบุคคลอื่นๆ หรือไม่
- ผู้ต้องสงสัยตระหนักหรือไม่ว่าเขากำลังดูภาพเด็กๆ โดยไม่ยอมรับว่าเป็นภาพที่เครื่องคอมพิวเตอร์สร้างขึ้น
- ผู้ต้องสงสัยมีการสมัครใช้บริการ hi5, MSN, ICQ หรือไม่

4.14.5 การบุกรุกหรือการเจาะเข้าระบบ (คำถามเกี่ยวของกับระบบเครือข่าย):

คำถามระบบเครือข่ายภายในบ้าน :

- คุณสามารถทำการหาว่าสายเน็ตเวิร์คต่างๆ 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 โดยทันที่เพื่อการสืบสวนสอบสวนในขั้นต่อไปได้หรือไม่
- ได้มีการติดต่อบุคคลจากหน่วยงานบังคับใช้กฎหมายอื่นๆ หรือยัง

4.14.6 การกระทำความผิดที่เกี่ยวข้องกับอีเมล์

คำถามที่ใช้ถามเหยื่อ :

- ขอข้อมูลอีเมล์ของเหยื่อและผู้ให้บริการอีเมล์นั้น
- ขอ username และ e-mail account ทั้งหมดของเหยื่อ

- ขอสำเนาอีเมล์ที่เหยื่อได้รับ อย่าเปิดเครื่องคอมพิวเตอร์เพื่อทำการสำเนาอีเมล์นั้น

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

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

4.14.7 การกระทำความผิดที่เกี่ยวข้องกับ Instant Messaging และ IRC

คำถามที่ใช้ถามเหยื่อ :

- ถามเหยื่อว่าได้เก็บ log การใช้งานในระหว่างแชทหรือไม่
- ขอชื่อที่เหยื่อใช้ในการออนไลน์รวมทั้งอีเมล์แอดเดรส
- ขอสำเนาทั้งหมดที่เหยื่อได้ทำการปรินท์ออกมา
- ซอฟท์แวร์ใด หรือผู้ให้บริการแชทใดที่เหยื่อใช้

คำถามที่ใช้ถามบุคคลเป้าหมายหรือผู้ต้องสงสัย :

- ขอชื่อที่ผู้ต้องสงสัยใช้ในการออนไลน์รวมทั้งอีเมล์แอดเดรส
- ขอพาสเวิร์ดทั้งหมดและซอฟท์แวร์ที่เกี่ยวข้อง รวมทั้ง username ที่ใช้โดยผู้ต้องสงสัย

4.14.8 แนวทางการดำเนินการกับกรณีการขโมยข้อมูลส่วนบุคคลออนไลน์

การป้องกัน

- อย่าให้ข้อมูลต่อไปนี้กับใครที่ไม่รู้จัก

วัน/สถานที่เกิด, ที่อยู่, หมายเลขบัตรประกันสังคม, หมายเลขโทรศัพท์, หมายเลขบัตรเครดิต

- ดูรายการการใช้บัตรเครดิตอย่างน้อยปีละครั้ง
- ดูให้แน่ใจว่าการโอนเงินทางอินเทอร์เนตนั้นปลอดภัยหรือไม่ โดยสังเกตที่ลูกกุญแจล็อกที่ทางด้านล่างขวาของเว็บเบราเซอร์ก่อนทำการกรอกข้อมูลส่วนตัวใดๆ
- หากไม่จำเป็นจริงๆ อย่าเก็บข้อมูลทางการเงินไว้ในเครื่องคอมพิวเตอร์
- ก่อนทำการทิ้งเครื่องคอมพิวเตอร์ ให้ทำลายข้อมูลทั้งหมดที่อยู่ในฮาร์ดไดร์ฟทิ้งไป โดยใช้เครื่องมือที่ใช้ทำการ wipe เนื่องจากการ format ไม่ช่วยทำลายข้อมูลได้มากนัก
- ใช้พาสเวิร์ดที่แข็งแรงและไม่ตั้งค่าให้โปรแกรมใดๆ จำพาสเวิร์ดไว้
- ใช้ซอฟท์แวร์ป้องกันไวรัสและไฟร์วอล เพื่อป้องกันการถูกขโมยข้อมูลจากเครื่องคอมพิวเตอร์ และช่วยป้องกันการเข้ามาของโปรแกรมประสงค์ร้ายต่างๆ (malware) การดำเนินการ
- ติดต่อธนาคารหรือผู้ออกบัตรเครดิตเพื่อรายงานการฉ้อโกงที่เกิดขึ้น
- ใช้การเตือนการฉ้อโกง (fraud aleart)

4.15 รายการอุปกรณ์และเครื่องมือสำหรับการปฏิบัติงาน

เนื่องจากอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีนั้นมีการเปลี่ยนแปลงรูปแบบและวิธีการใหม่ๆ อยู่ตลอดเวลาดังนั้นหน่วยงานที่เกี่ยวข้องจึงจาเป็นต้องมีการพัฒนาและจัดเตรียมเครื่องมือที่ทันสมัย เพื่อให้สามารถดำเนินการสืบสวนสอบสวนอาชญากรรมได้อย่างรวดเร็วและมีประสิทธิภาพ และด้วยเหตุนี้จึงต้องมีการกำหนดรายการอุปกรณ์และเครื่องมือมาตรฐานประจาหน่วยงาน โดยมีรายละเอียด ดังนี้

4.15.1 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

4.15.2 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)

4.15.3 ซอฟต์แวร์สำหรับงานตรวจวิเคราะห์หลักฐาน (Computer Forensic Software)

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

4.16 ห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์

ห้องปฏิบัติการตรวจวิเคราะห์หลักฐานอิเล็กทรอนิกส์ ถือเป็นหัวใจสำคัญของการตรวจวิเคราะห์หลักฐานทางอิเล็กทรอนิกส์ เนื่องจากการดำเนินกิจกรรมต่างๆ ต้องอยู่ภายใต้สภาพแวดล้อมที่เหมาะสมและปลอดภัยทั้งต่อพยานหลักฐานและเจ้าหน้าที่ผู้ปฏิบัติงาน ดังนั้นห้องปฏิบัติการฯ ควรจะมีลักษณะทางกายภาพในด้านต่างๆ ดังนี้

4.16.1 ข้อกำหนดด้านสภาพแวดล้อมของห้องปฏิบัติการ

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

4.16.2 ข้อกำหนดด้านความปลอดภัยทางด้านกายภาพของห้องปฏิบัติการ

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

4.16.3 มาตรฐานบุคลากรและความรับผิดชอบ (Forensic Officer and Responsibility)

ด้วยเหตุที่ว่าอาชญากรรมที่เกี่ยวกับเทคโนโลยีนั้น ถือเป็นอาชญากรรมที่มีความซับซ้อนและแตกต่างไปจากอาชญากรรมในรูปแบบอื่น เนื่องจากอาชญากรรมดังกล่าวนั้นเกี่ยวข้องและสัมพันธ์กับระบบเครือข่ายและเทคโนโลยีคอมพิวเตอร์อยู่เสมอ จึงทำให้การสืบสวนและสอบสวนอาชญากรรมในลักษณะนี้จำเป็นต้องอาศัยเจ้าหน้าที่ผู้เชี่ยวชาญ ที่มีความรู้และความเข้าใจในเทคโนโลยีคอมพิวเตอร์และเครือข่าย เพื่อให้สามารถดำเนินการสืบสวนและสอบสวนได้อย่างมีประสิทธิภาพสมบูรณ์ ดังนั้นจึงต้องมีการกำหนดตำแหน่งและคุณสมบัติการพิจารณาเจ้าหน้าที่ขึ้น เพื่อใช้เป็นมาตรฐานในการคัดเลือกบุคลากรของหน่วยงานต่อไป

4.16.4 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
สรุปผลการศึกษาและข้อเสนอแนะ

5.1 สรุปผลการศึกษา

5.1.1 สภาพปัญหาอาชญากรรมคอมพิวเตอร์ในสังคมไทยปัจจุบัน

ปัจจุบันเทคโนโลยีคอมพิวเตอร์ เปรียบเสมือนวิถีชีวิตของมนุษย์นับวันจะยิ่งทวีความสำคัญเพิ่มมากขึ้นเรื่อยๆ และยังมีอิทธิพลมากพอที่จะเปลี่ยนแปลงวิถีชีวิตมนุษย์ไปในทิศทางต่างๆ ได้ ทำให้สถานการณ์เกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มมากขึ้น เนื่องจากการขยายตัวของผู้ใช้งานคอมพิวเตอร์ในประเทศไทยเพิ่มสูงขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้งานคอมพิวเตอร์ในสังคมไทย ยังขาดความรู้ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีสารสนเทศอย่างแท้จริง อีกทั้งสังคมไทยยังขาดการเอาใจใส่ในประเด็นการปลูกฝังจริยธรรม คุณธรรม จรรยาบรรณเกี่ยวกับการใช้งานอินเตอร์เน็ตหรือสังคมออนไลน์ในทางที่เหมาะสม ทำให้ผู้ใช้ (Users) บางส่วนขาดจริยธรรมนำเทคโนโลยีไปใช้ในทางที่มิชอบ ประกอบกับผู้ใช้อินเตอร์เน็ตไม่ตระหนักถึงความสำคัญด้านความปลอดภัยคอมพิวเตอร์และเครือข่าย ละเลยการป้องกันตนเองและไม่รู้สึกถึงความรับผิดชอบของตนเองต่อการใช้เครือข่ายร่วมกัน ในขณะที่อินเตอร์เน็ตขยายตัวไปอย่างรวดเร็ว อาชญากรรมคอมพิวเตอร์ก็มีแนวโน้มเพิ่มขึ้น แต่จำนวนบุคลากรด้านความปลอดภัยคอมพิวเตอร์และเครือข่ายกลับมีจำนวนจำกัด ซึ่งไม่เพียงพอต่อการดูแลระบบทั้งภาครัฐและภาคเอกชน ทำให้ระบบเครือข่ายในประเทศไทยขาดการควบคุมดูแลด้านความมั่นคงปลอดภัยของผู้ใช้งาน

ปัญหาทางด้านกฎหมาย ความแตกต่างกันของอาชญากรรมคอมพิวเตอร์และอาชญากรรมพื้นฐานทำให้เกิดปัญหา ไม่ว่าจะเป็นประเด็นของการตีความ การกำหนดฐานความผิด การประเมินความเสียหายจากการกระทำความผิด เขตอำนาจศาล ผู้รับผิดชอบ ความแตกต่างทางกฎหมาย และการสืบสวนตลอดจนการรวบรวมพยานหลักฐาน เพื่อพิสูจน์ความผิดของอาชญากรรมคอมพิวเตอร์เป็นประเด็นหรือช่องโหว่ที่กระทบต่อการปฏิบัติในการดำเนินคดีทุกขั้นตอน ไม่ว่าจะเป็นการสืบสวน สอบสวน การเก็บและรวบรวมพยานหลักฐาน การตรวจพิสูจน์พยานหลักฐานต่างๆ การพิจารณาและการพิพากษาคดี ซึ่งเมื่อกฎหมายอาชญากรรมทางคอมพิวเตอร์มีผลบังคับใช้ ก็จะส่งผลในทางปฏิบัติตามมา เนื่องจากปัญหาด้านความรู้ความเข้าใจ เกี่ยวกับเทคโนโลยีและอาชญากรรมคอมพิวเตอร์ของบุคลากรในสายกระบวนการยุติธรรม ไม่ว่าจะเป็น ตำรวจ อัยการ ศาล ล้วนแล้วแต่เป็นจุดอ่อนในกระบวนการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์เป็นอย่างยิ่ง ดังนั้น สิ่งที่ควรจะคำนึงมากที่สุดในเวลานี้ คือ ทำอย่างไรเราถึงจะได้ประยุกต์ใช้หรือประมาณการณ์ที่จะนำไปใช้ได้อย่างถูกต้องและถูกวิธี เพื่อไม่ให้คอมพิวเตอร์และอินเตอร์เน็ตกลายเป็นภัยหรืออันตรายต่อมนุษย์และสังคม

กระบวนการจัดการปัญหาคดีทางด้านอาชญากรรมคอมพิวเตอร์ในประเทศไทยยังไม่มีรูปธรรมที่ชัดเจนมากนัก ประการสำคัญ คือ ความรู้ ความเข้าใจในเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต

การประยุกต์ใช้กฎหมายต่างๆ และการรักษาความน่าเชื่อถือของพยานหลักฐานที่ได้ ในการใช้ลงโทษคนร้าย หน่วยงานที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ มีการทำงานในลักษณะต่างหน่วยต่างทำ และเนื่องจากพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายซึ่งบังคับใช้ได้ไม่นานไม่เอื้อต่อการปฏิบัติงานจริงในบางประเด็น เช่น การดำเนินงานหลายๆ อย่าง ได้ให้อำนาจเฉพาะพนักงานเจ้าหน้าที่ในการดำเนินงานเท่านั้น ทำให้เจ้าหน้าที่ตำรวจโดยเฉพาะพนักงานสอบสวนหลายพื้นที่เกิดปัญหาในการขอข้อมูลจากผู้ให้บริการทางอินเทอร์เน็ต ว่าเป็นอำนาจของผู้ใดกันแน่ จะต้องมีการฝึกอบรมความรู้ทางเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต และการประยุกต์ใช้กฎหมายต่างๆ แก่เจ้าหน้าที่ที่เกี่ยวข้องตลอดเวลา เพื่อให้ทันต่อการพัฒนาทางเทคโนโลยีที่มีการพัฒนาที่รวดเร็วอย่างมาก รวมถึงรูปแบบและวิธีการกระทำความผิดของคนร้ายที่จะพัฒนาเปลี่ยนแปลงไปตามการพัฒนาทางเทคโนโลยีที่เกิดขึ้น

จากการที่ปัจจุบันสภาพสังคมของเรากลายเป็นสังคมออนไลน์ที่ทุกคนสามารถติดตามข้อมูลข่าวสารผ่านระบบอินเทอร์เน็ตได้แบบรวดเร็วทันที (Online Real Time) ดังนั้น การที่เราจะมีผู้ให้บริการเว็บไซต์ต่างๆ มารวมตัวกันในการแลกเปลี่ยนข้อมูลข่าวสารที่ตัวผู้ให้บริการเว็บไซต์แต่ละเว็บไซต์ได้ทำการเก็บรวบรวมปัญหาต่างๆ ที่เกิดขึ้นกับเว็บไซต์ของตนเอง โดยรวมตัวกันเป็นเครือข่ายชุมชนออนไลน์ จึงเป็นช่องทางหนึ่งที่สำคัญในการช่วยเหลือการทำงานของทางราชการ ในการสืบสวน สอบสวน ป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพราะจะมีข้อมูลข่าวสารที่เป็นประโยชน์ต่อผู้ใช้งาน (Users) ในการป้องกันการตกเป็นเหยื่อของอาชญากรทางเทคโนโลยี ดังนั้นในการแก้ไขปัญหาดังกล่าว เราต้องมีการร่วมกันระหว่างหน่วยงานภาครัฐ และหน่วยงานภาคเอกชน โดยควรมีการรวมกลุ่มกันของผู้ประกอบการเว็บไซต์ต่างๆ เพื่อรวมตัวกันเป็นชุมชนออนไลน์ในการเผยแพร่ข้อมูลข่าวสารที่เป็นประโยชน์ต่อสังคมออนไลน์

5.1.2 ประโยชน์ของเครือข่ายชุมชนออนไลน์

1) ร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง และวิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการป้องกันปัญหาดังกล่าว

2) ร่วมแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็ปไซต์ (Black List)

3) จัดเวทีให้มีการร่วมงานประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแรกเปลี่ยนข้อคิดเห็นและกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

5.1.3 กฎ 4 ประการในการรักษาความน่าเชื่อของพยานหลักฐานทางคอมพิวเตอร์

1) ต้องไม่กระทำให้เกิดการเปลี่ยนแปลงใด ๆ ในพยานหลักฐาน

2) กรณีที่มีความจำเป็นไม่สามารถหลีกเลี่ยงการเปลี่ยนแปลงของพยานหลักฐานได้ ต้องสามารถอธิบายได้ และพยายามให้เกิดการเปลี่ยนแปลงน้อยที่สุดเท่าที่จะเป็นไปได้

3) บันทึกรายละเอียดต่าง ๆ ทุกขั้นตอนที่กระทำกับพยานหลักฐานทางอิเล็กทรอนิกส์ และหากใช้เครื่องมืออื่นที่ได้รับมาตรฐานเช่นเดียวกันจะต้องได้รับผลลัพธ์แบบเดียวกัน

4) ผู้ที่เป็นเจ้าของคดี ต้องทำให้แน่ใจว่าได้ปฏิบัติถูกต้องตามกฎหมายและกฎในการรักษาความน่าเชื่อถือของพยานหลักฐาน

5.1.4 การวิจัยเพื่อจัดทำคู่มือเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

กระบวนการของการจัดทำคู่มือเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เพื่อสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ตำรวจและหน่วยงานต่างๆ ที่เกี่ยวข้อง เครื่องมือที่ใช้ในการวิจัยนี้ คือ การประชุมเพื่อแลกเปลี่ยนความรู้ (Storytelling) เพื่อรวบรวมความรู้ที่ฝังลึกอยู่ในตัวบุคคล เช่น ประสบการณ์ พรสวรรค์ หรือสัญชาตญาณ และความรู้ชัดแจ้ง เช่น จากทฤษฎี ข้อกฎหมาย ระเบียบและวิธีการปฏิบัติงาน ขั้นตอนการพิสูจน์หลักฐาน รวมทั้งรวบรวมปัญหา อุปสรรค และข้อเสนอแนะ แนวทางการปรับปรุงและพัฒนาระบบงานด้านการจัดการเกี่ยวกับคดีทางด้านอาชญากรรมคอมพิวเตอร์ ให้มีประสิทธิภาพมากยิ่งขึ้น โดยเชิญกลุ่มเป้าหมายเข้าร่วมประชุมแลกเปลี่ยนความรู้และแสดงความคิดเห็น ประกอบไปด้วย ผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญด้านอาชญากรรมคอมพิวเตอร์ของสำนักงานตำรวจแห่งชาติ, กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม, กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ที่ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์, เจ้าหน้าที่ฝ่ายสืบสวน, พนักงานสอบสวน, พนักงานอัยการ, ผู้พิพากษา, ผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยบนระบบเครือข่ายและด้านอาชญากรรมคอมพิวเตอร์จากหน่วยงานเอกชน และสื่อมวลชนต่างๆ ที่เกี่ยวข้องกับงานด้านอาชญากรรมคอมพิวเตอร์ มาประชุมเพื่อแลกเปลี่ยนความรู้ ประสบการณ์ และแสดงความคิดเห็นร่วมกับคณะผู้วิจัยโดยได้สรุปในเชิงเสนอแนะดังนี้

5.2 ข้อเสนอแนะแนวทางในการแก้ไขปัญหาและอุปสรรค

5.2.1 พนักงานสอบสวน ยังขาดความรู้ความเข้าใจในเรื่องของระบบคอมพิวเตอร์ และระบบอินเทอร์เน็ต เมื่อผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที เพราะไม่รู้กระบวนการในการทำงานที่เกิดขึ้น ซึ่งเป็นปัญหาใหญ่ที่จะต้องมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยีระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต และกฎหมายที่เกี่ยวข้องแก่พนักงานสอบสวนทั่วประเทศ โดยเฉพาะประเด็นการตั้งคำถามของพนักงานสอบสวน เป็นเพราะขาดความรู้ทำให้ตั้งคำถามอย่างไม่มีทิศทาง และรวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติหน้าที่ด้วย

5.2.2 พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐาน ในหลายกรณีไม่มีความน่าเชื่อถือเนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of custody) ซึ่งเป็นการพิสูจน์ความเชื่อมโยงของพยานหลักฐานกับการกระทำความผิด กระบวนการส่งต่อวัตถุพยานจะต้องมีการบันทึกรายละเอียดของวัตถุพยานซึ่งเริ่มตั้งแต่การตรวจพบ และเก็บวัตถุพยานในสถานที่เกิดเหตุรวมถึงผู้จัดส่ง-ผู้รับ ผู้ตรวจพิสูจน์ตลอดทั้งกระบวนการสืบสวนสอบสวน ดังนั้น จึงต้องมีการบันทึกเป็นหลักฐานตามลำดับเวลา เพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้นๆ หากขาดการต่อเนื่องของการครอบครองวัตถุพยาน เมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือในชั้นศาล

5.2.3 สำนักงานศาล และสำนักงานอัยการสูงสุด ควรมีการจัดตั้งหน่วยงานเฉพาะขึ้นมาดูแลรับผิดชอบคดีทางด้านอาชญากรรมคอมพิวเตอร์เป็นการเฉพาะ เพราะสำนักงานตำรวจแห่งชาติ และกรมสอบสวนคดีพิเศษ ได้มีการจัดตั้งหน่วยงานเฉพาะเพื่อดูแลรับผิดชอบคดีทางด้านอาชญากรรมคอมพิวเตอร์แล้ว เนื่องจากเป็นคดีที่ต้องทำความเข้าใจในเรื่องของเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต ที่มีความซับซ้อนและเข้าใจยากในบางกรณีเพราะเป็นเรื่องเทคนิคเฉพาะ อีกทั้งมีคดีทางด้านอาชญากรรมคอมพิวเตอร์เกิดขึ้นจำนวนมาก และมีแนวโน้มว่าเพิ่มมากขึ้นทุกปี

5.2.4 บทบาทของสื่อมวลชนในบางกรณีมีผลกระทบต่อการปฏิบัติงาน และการนำเสนอรายละเอียดในทางคดีที่นำไปเผยแพร่ต่อสาธารณชน บางครั้งสื่อมวลชนมีการนำเสนอข้อมูลส่วนที่สำคัญในการนำวิธีการหรือผลลัพธ์ในการทำงานของเจ้าหน้าที่ไปเปิดเผย คนร้ายจึงไม่ทิ้งร่องรอยในการกระทำความผิดไว้หรือมีการใช้เทคโนโลยีที่ซับซ้อนมากขึ้นในการอำพรางหรือหลบซ่อนตัวเอง ทำให้เจ้าหน้าที่ปฏิบัติงานยากลำบากขึ้น ซึ่งเป็นจุดอ่อนต่อการปฏิบัติงานของเจ้าหน้าที่

5.2.5 เห็นควรสรรหาบุคลากรเพื่อมาปฏิบัติหน้าที่ทางด้านคดีอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น เพื่อรองรับปัญหาทางด้านคดีอาชญากรรมคอมพิวเตอร์ที่เพิ่มมากขึ้น

5.2.6 จัดซื้อวัสดุอุปกรณ์ในการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับคดีทางด้านอาชญากรรมทางคอมพิวเตอร์ที่มีความทันสมัย ใช้เวลาในการตรวจพิสูจน์น้อย เคลื่อนย้ายได้ง่าย และให้ผลการตรวจพิสูจน์ที่ถูกต้อง แน่นอน เพื่อลดระยะเวลาและปริมาณงาน เช่น ซอฟต์แวร์การกู้ข้อมูลที่ถูกลบไปแล้ว เป็นต้น

เอกสารอ้างอิง

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2555). **สถิติคดีอาญาของการกระทำผิดเกี่ยวกับการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนดลยีประจำปี พ.ศ. 2552-2555**. กองบัญชาการตำรวจสนอบสวนกลาง.

จตุชัย แพงจันทร์ และคณะ. (2547). **เจาะระบบ Network ฉบับสมบูรณ์**. (ครั้งที่ 2). นนทบุรี: บริษัท ไอดีซี อินโฟดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด.

เชาวลิต อัตถศาสตร์. (2554). **Cyber Law กฎหมายกับอินเทอร์เน็ต.** กรุงเทพมหานคร: โปรวิชั่น.

ญาณพล ยั่งยืน. **อาชญากรรมทางคอมพิวเตอร์ (Computer - Related Crime)**. สืบค้นเมื่อ สิงหาคม 5, 2555 จากhttp://elearning.aru.ac.th/4000108/hum07/topic3/linkfile/print5.htm

ธเนศ ขำเกิด. (2532). **การจัดบรรยากาศและสิ่งแวดล้อมที่ดีในโรงเรียน.** มิตรครู.

นารี กิตติสมบูรณ์สุข. (2548). **การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์**. ปริญญานิติศาสตรมหาบัณฑิต. มหาวิทยาลัยธุรกิจบัณฑิตย์.

นัยนรัตน์ งานแสง. (2547). **อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมบนอินเทอร์เน็ต**. ปริญญาศิลปศาสตรมหาบัณฑิต. มหาวิทยาลัยธรรมศาสตร์.

ประพนธ์ ผาสุกยืด. (2549). **การจัดการความรู้.** สถาบันส่งเสริมการจัดการความรู้เพื่อสังคม (สคส.). บริษัท ใยไหม ครีเอทีฟกรุ๊ป จำกัด.

ประพนธ์ ผาสุกยืด. (2550). **การจัดการความรู้จากหลักคิดสู่การปฏิบัติจริง.** กรุงเทพฯ: สำนักพิมพ์ใยไหม.

ไพบูลย์ ปะวะเสนะ. **การบริหารจัดการความรู้ Knowledge Management (KM)**. 2547. สืบค้นเมื่อ มีนาคม 29, 2550 จากhttp://www.cgd.go.th/Library/knowledge/article/KM.pdf

ยืน ภู่วรวรรณ. (2546)**.การจัดการความรู้ทั่วไปสำหรับองค์กร (Knowledge Management: KM).**ในการสัมมนาวิชาการ “การจัดการความรู้: ยุทธศาสตร์และเครื่องมือ” (Knowledge Management: Strategies &Tools).

วรภัทร์ ภู่เจริญ. (2548). **องค์กรแห่งการเรียนรู้ และการบริหารความรู้ = Learning organization & knowledge management** (ครั้งที่ 3). กรุงเทพฯ: อริยชน.

วิจารณ์ พานิช. (2547). **องค์กรการเรียนรู้และการจัดการความรู้**. กรุงเทพฯ

วีรวุธ มาฆะศิรานนท์. (2542). **การทำตลาด 23 วิธี** (ครั้งที่ 2). กรุงเทพฯ: เอ็กซเปอร์เน็ท.

ศรันย์ ชูเกียรติ. (2541). **“เทคโนโลยีสารสนเทศในการจัดการองค์ความรู้” ในองค์กรกลยุทธ์เพื่อความสำเร็จภายใต้สภาวการณ์ปัจจุบัน**. ว.จุฬาลงกรณ์ธุรกิจปริทัศน์.

สินเลิศ สุขุม. (2543). **ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ**. ปริญญา สังคมวิทยามหาบัณฑิต. จุฬาลงกรณ์มหาวิทยาลัย

สำนักกำกับการใช้เทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.(2551). **เอกสารการประชุมกำหนดแนวทางปฏิบัติทางนิติวิทยาศาสตร์ด้านคอมพิวเตอร์เพื่อการปฏิบัติงานตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550**.

Carcia. (1991). **38 UCLA Law Review**. S.1043 ff

Greenleaf, Graham. (1995). **Information Technology and Law.** 69 The Australian Law Journal.

Guofu Ma, Zixian Wang, Likun Zou, Qian Zhang a*. (2011). **Computer Forensics Model Based on Evidence Ring and Evidence Chain**. The Central Institute for Correctional Police.

Kantrowiz, B. and A. Rogers. (1994). **The Birth of the Internet**. Newsweek. Newsweek. **V.29.6.1992**, S.44 f.

Matthew Tart, Iain Brodie, Nicholas Gleed, James Matthews, **Historic cell site analysis – Overview of principles and survey methodologies**, Digital Investigation, Volume 8, Issues 3–4, February 2012

Sieber, **“Information Technology Crime”,** 1994, S 200.

Sieber, **“The International Handbook on Computer Crime”**, S 23.

Sieber, Bilanzgen eines ‘Musterverfahrens’. **Zu dem rechtskraftigen Abschlub des Verfahrens BGHZ** 94, S. 276 (Inkassoprogramm), in : CR 1986, 699 ff.

ผู้มีคุณูปการ

การศึกษาวิจัยโครงการเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ ได้รับการสนับสนุนจาก สำนักงานกองทุนสนับสนุนการวิจัย (สกว.) และได้รับความอนุเคราะห์จากบุคคลหลายฝ่าย ดังนี้

1.	นายอำพล	บุญประภากร	ผู้พิพากษาศาลแขวง จังหวัดนครปฐม
2.	รศ.พ.ต.อ.กู้เกียรติ	เจริญบุญ	อัยการประจำกอง ฝ่ายพัฒนากฎหมาย สำนักงานวิชาการ สำนักงานอัยการสูงสุด
3.	รศ.พ.ต.อ.ดร.กิตต์ธนทัต	เลอวงศ์รัตน์	กลุ่มงานคณาจารย์ คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ
4.	พ.ต.อ.ดร.วิวัฒน์	สิทธิสรเดช	นักวิทยาศาสตร์ (สบ4) กลุ่มงานยาเสพติด สำนักงานพิสูจน์หลักฐานตำรวจ
5.	พ.ต.อ. ศิริพงษ์	ติมุลา	รองผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
6.	พ.ต.อ.อัษฎางค์	ม่วงศรี	ผู้กำกับการกลุ่มงานบริหารจัดการระบบเครื่องคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศกลาง (ศกท.)
7.	พ.ต.อ.อนุชิต	บุญญะปฏิภาค	นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง
8.	พ.ต.ท. ดร.สฤษดิ์	สืบพงศ์ศิริ	กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
9.	ผศ.พ.ต.ท.สุรัตน์	สาเรือง	กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
10.	พ.ต.ท.ดรัณ	จาดเจริญ	รองผู้กำกับการกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี
11.	พ.ต.ท.พัฒนะ	ศุกรสุต	พนักงานสอบสวน ระดับชำนาญการพิเศษ กรมสอบสวนคดีพิเศษ
12.	พ.ต.ท.พจน์	ฟอร์ตี้	รองผู้กำกับการกลุ่มงานผู้เชี่ยวชาญ กองประวัติอาชญากร

13.	พ.ต.ต.นิติ	อินทุลักษณ์	นักวิทยาศาสตร์ (สบ 2) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง
14.	พ.ต.ต.หญิง กนกพร	แสนแก้ว	กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
15.	นายปกรณ์	ธรรมโรจน์	อัยการประจำสำนักงานอัยการสูงสุด
16.	นายเอกลักษณ์	หลุ่มชมแข	มูลนิธิกระจกเงา
17.	นางพัชรินทร์	ยศสมนึก	บรรณาธิการข่าวอาชญากรรม TNN24
18.	นายมานะชัย	บุญเอก	ผู้อำนวยการกลุ่มงานสืบสวนทางเทคโนโลยี สารสนเทศ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยี
19.	นายณัฐพงษ์	ลิ้มแดงสกุล	ผู้อำนวยการฝ่ายนิติดิจิตอล กองปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ภาคผนวก ก

ตาราง 1 แผนปฏิบัติการของโครงการ (เดือนกันยายน 2555 – มีนาคม 2556)

กิจกรรม	ระยะเวลา	สถานที่	ผลที่ได้รับ
1.ทำหนังสือจากมหาวิทยาลัยราชภัฏสวนสุนันทาถึงผู้บังคับบัญชาตำรวจ และหน่วยที่เกี่ยวข้อง เพื่อขอข้อมูลด้านสถิติงาน และคัดเลือกกรณีศึกษาที่น่าสนใจ พร้อมทั้งขอให้หน่วยเสนอรายชื่อเจ้าหน้าที่ที่มีความรู้ความสามารถในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์	ก.ย.-ต.ค. 2555	สำนักงานโครงการฯ	1.รายชื่อ เบอร์โทรศัพท์ และที่อยู่ของกลุ่มเป้าหมาย ที่มีคุณสมบัติตรงกับเป้าหมายการวิจัย 2.ข้อมูลด้านสถิติ และพื้นที่เพื่อศึกษาได้กรณีศึกษาเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์
1.จัดการประชุมครั้งที่ 1 ที่กรุงเทพมหานคร เพื่อแลกเปลี่ยนเรียนรู้ขั้นตอนวิธีการในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ 2.วิเคราะห์ข้อกฎหมายและระเบียบที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ 3.เพื่อแลกเปลี่ยนเรียนรู้เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์	17 ธ.ค.2555	มหาวิทยาลัยราชภัฏสวนสุนันทา	1. ได้ข้อกฎหมายและระเบียบที่ผ่านการแก้ไขปรับปรุงให้มีความเหมาะสมต่อการใช้งานในสถานการณ์ปัจจุบัน 2. ได้ทราบนโยบายในการบริหารจัดการและปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ 3. ได้แนวทางแก้ไขปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจและหน่วยงานที่เกี่ยวข้องด้านอาชญากรรมคอมพิวเตอร์
1.จัดการประชุมครั้งที่ 2 ที่กรุงเทพมหานคร เพื่อแลกเปลี่ยนเรียนรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ 2.ค้นหาวิธีการปฏิบัติงาน นโยบายในการบริหารจัดการ รวมทั้งปัญหาอุปสรรคในการปฏิบัติงานของเจ้าหน้าที่ตำรวจ และหน่วยงานที่เกี่ยวข้อง ในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ 3.สร้างฐานความรู้ในการรวบรวมพยานหลักฐานที่เกี่ยวข้องกับงานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์	28 ม.ค.2556	มหาวิทยาลัยราชภัฏสวนสุนันทา	

ตาราง 2 รายชื่อผู้เข้าร่วมประชุม

การจัดประชุม ครั้งที่ 1 เพื่อแลกเปลี่ยนเรียนรู้การวิเคราะห์ข้อกฎหมายระเบียบที่เกี่ยวข้องและขั้นตอนในการปฏิบัติงานทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ วันจันทร์ที่ 17 ธันวาคม พ.ศ.2555 ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

ชื่อ-สกุล	ตำแหน่ง
1. รศ.พ.ต.อ.กู้เกียรติ เจริญบุญ	อัยการประจำกอง ฝ่ายพัฒนากฎหมาย สำนักงานวิชาการ สำนักงานอัยการสูงสุด
2. พ.ต.ท.พัฒนะ ศุกรสุต	พนักงานสอบสวน ระดับชำนาญการพิเศษ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม
3. นายมานะชัย บุญเอก	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
4. พ.ต.อ.ดร.วิวัฒน์ สิทธิสรเดช	กองพิสูจน์หลักฐานกลาง
5. รศ.พ.ต.อ.ดร.กิตต์ธนทัต เลอวงศ์รัตน์	รศ.(สบ 5) กลุ่มงานคณาจารย์ คณะตำรวจศาสตร์ รร.นรต.
6. ผศ.พ.ต.ท.สุรัตน์ สาเรือง	ผศ.(สบ 3) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ รร.นรต.
7. พ.ต.ท.ดร.สฤษดิ์ สืบพงษ์ศิริ	อจ.(สบ 3) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ รร.นรต.
8. พ.ต.ต.หญิง กนกพร แสนแก้ว	อจ.(สบ 2) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ รร.นรต.
9. พล.ต.ท.ดร.ณรงค์ กุลนิเทศ	ผู้อำนวยการแผนงาน
10. พ.ต.อ.สมศักดิ์ หน่องพงษ์	นักวิจัย
11. ผศ.พ.ต.ท.วรธัช วิชชุวาณิชย์	นักวิจัย
12. นางสาวณิช วงศ์ส่องจ้า	นักวิจัย

ตาราง 3 รายชื่อผู้เข้าร่วมการประชุม

การจัดประชุม ครั้งที่ 2 เพื่อแลกเปลี่ยนเรียนรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ขั้นตอนและวิธีการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ วันจันทร์ที่ 28 มกราคม พ.ศ. 2556 ณ ห้องประชุม 26108 อาคาร 26 ชั้น 1 คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา

ชื่อ-สกุล	ตำแหน่ง
1. นายอำพล บุญประภากร	ผู้พิพากษาศาลแขวง จังหวัดนครปฐม
2. นายปกรณ์ ธรรมโรจน์	อัยการประจำสำนักงานอัยการสูงสุด สำนักงานอัยการพิเศษฝ่ายคดีเศรษฐกิจและทรัพยากร 2 สำนักงานอัยการสูงสุด
3. พ.ต.อ.อนุชิต บุญญะปฏิภาค	นวท.(สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง

4. พ.ต.ท.ดรัณ จาดเจริญ	รอง ผกก.กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี
5. พ.ต.ท.พจน์ ฟอร์ตี้	รอง ผกก. กลุ่มงานผู้เชี่ยวชาญ กองทะเบียนประวัติอาชญากร
6. พ.ต.ต.นิติ อินทุลักษณ์	นวท.(สบ 2) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง
7. พล.ต.ท.ดร.ณรงค์ กุลนิเทศ	หัวหน้าโครงการวิจัย
8. พ.ต.อ.สมศักดิ์ หน่องพงษ์	นักวิจัย
9. ผศ.พ.ต.ท.วรธัช วิชชุวาณิชย์	นักวิจัย
10. นางสาวณิช วงศ์ส่องจ้า	นักวิจัย

ภาคผนวก ข

การประชุมครั้งที่ 1 เพื่อร่วมกันวิเคราะห์ข้อกฎหมายและระเบียบที่เกี่ยวข้องทางด้านอาชญากรรมคอมพิวเตอร์

ผู้เข้าร่วมประชุม

1. พล.ต.ท.ดร.ณรงค์	กุลนิเทศ	ผู้อำนวยการแผนงาน
2. พ.ต.อ.สมศักดิ์	หน่องพงษ์	นักวิจัย
3. ผศ.พ.ต.ท.วรธัช	วิชชุวาณิชย์	นักวิจัย
4. นางสาวณิช	วงศ์ส่องจ้า	นักวิจัย
5. รศ.พ.ต.อ.กู้เกียรติ	เจริญบุญ	อัยการประจำกอง ฝ่ายพัฒนากฎหมาย สำนักงานวิชาการ สำนักงานอัยการสูงสุด
6. พ.ต.ท.พัฒนะ	ศุกรสุต	พนักงานสอบสวน ระดับชำนาญการพิเศษ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม
7. นายมานะชัย	บุญเอก	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
8. พ.ต.อ.ดร.วิวัฒน์	สิทธิสรเดช	กองพิสูจน์หลักฐานกลาง
9. รศ.พ.ต.อ.ดร.กิตต์ธนทัต	เลอวงศ์รัตน์	รองศาสตราจารย์ (สบ 5) กลุ่มงานคณาจารย์ คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ
10. ผศ.พ.ต.ท.สุรัตน์	สาเรือง	ผู้ช่วยศาสตราจารย์ (สบ 3) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
11. พ.ต.ท.ดร.สฤษดิ์	สืบพงษ์ศิริ	อาจารย์ (สบ 3) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
12. พ.ต.ต.หญิง กนกพร	แสนแก้ว	อาจารย์ (สบ 2) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

ผู้เข้าร่วมประชุมได้แสดงความคิดเห็นในประเด็นที่เกี่ยวข้องดังนี้

รศ.พ.ต.อ.กู้เกียรติ เจริญบุญ :

“กล่าวถึงกฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ สามารถสรุปภาพรวมของกฎหมาย ดังนี้

1.พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ.2550

2.พ.ร.บ.ที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

3.ประกาศกระทรวงเทคโนโลยีและสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

4.ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนการสอบสวนและการดำเนินคดีกับผู้กระทำความผิดว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

5.ประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์ เรื่องการรับรองสิ่งพิมพ์ออก พ.ศ.2555

6.ประมวลกฎหมายอาญา หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ของลักษณะ 7 ความผิดเกี่ยวกับการปลอมและการแปลง มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6 และ มาตรา 269/7

7.พ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ.2547 ซึ่งให้อำนาจพนักงานเจ้าหน้าที่

8.กฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ ฉบับที่ 2 พ.ศ. 2555

9.กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ. 2551

ลักษณะของการกระทำความผิด

1.การกระทำความผิดต่อตัวคอมพิวเตอร์เอง

2.การกระทำความผิดลักษณะที่ใช้คอมพิวเตอร์เป็นเครื่องมือ หรือเป็นอุปกรณ์ในการกระทำผิด

3.การกระทำความผิดโดยใช้คอมพิวเตอร์เป็นแหล่งเก็บข้อมูล

กฎหมายที่กล่าวมาข้างต้นนั้นมีลักษณะส่วนดีและส่วนเสีย คือ ในการที่มีกฎหมายที่เกี่ยวข้องต่างๆนั้น ปัญหาส่วนใหญ่อยู่ที่ผู้บังคับใช้ โดยเฉพาะตำรวจเจ้าหน้าที่ที่เกี่ยวข้องเองนั้น ยังไม่มีความรู้มากนัก เช่น กฎหมายด้านกระบวนการจราจรคอมพิวเตอร์นั้น ยังไม่รู้ว่าจะต้องเริ่มจากตรงไหน ขั้นตอนเป็นอย่างไร การค้นตาม พ.ร.บ. นั้น จะต้องมีหมายค้น ซึ่งยังไม่มีความชำนาญ ส่วนเวลาเข้าค้นนั้น ไม่มีวิธีการในการค้น การเข้าถึงข้อมูลผิดวิธี และผิดพลาดในการสืบค้น ซึ่งอาจจะต้องมีวิธีการถ่ายทอดและอบรมให้ความรู้ที่ถูกต้องให้กับตำรวจตามสถานีตำรวจทุกๆแห่ง เพื่อการสืบค้นที่ถูกต้อง ปัญหาที่กล่าวมานั้นจะส่งผลไปถึงเวลานำสืบในชั้นศาล โดยมีจุดบอดคือ เมื่อเข้าไปค้น ไม่ได้ทำการถ่ายภาพไว้ แล้วเคลื่อนย้ายของกลางออกมา โดยไม่ได้สังเกตอุปกรณ์ที่จะค้นย้าย และเวลาในการสืบค้นนั้น เมื่อได้ค้นแล้วไม่ได้บันทึกว่าใครเป็นผู้เกี่ยวข้องกับของกลาง

หรือสถานที่ค้นหรือไม่ และเทคนิคในการนำสืบนั้นยากมาก โดยต้องย้อนมาถึงพนักงานที่ทำการจับและค้นนั้นยังไม่มีความรู้มากพอ”

พ.ต.ท.พัฒนะ ศุกรสุต :

“ในส่วนของการกระทำผิดนั้น ตามกฎหมายนั้นเป็นเรื่องที่กว้างมาก ซึ่งเป็นเรื่องที่มีมานานแล้ว เช่น เรื่องการหลอกขายของ การล่อลวงทำธุรกรรมทางการเงิน เพียงแต่ว่าในปัจจุบันมีช่องทางในการกระทำความผิดที่ง่ายยิ่งขึ้นและเป็นเครือข่ายมากขึ้น เช่น การส่งข้อความทางโทรศัพท์ การโพสต์ข้อความทางอินเตอร์เน็ต ประเด็นที่สำคัญอีกอย่าง คือ เจ้าหน้าที่นั้นขาดความรู้ แต่จริงๆแล้วตามกฎหมายนั้น ประกาศชัดเจนว่าเจ้าหน้าที่ที่ทำหน้าที่ด้านนี้ต้องผ่านการเรียนวิชา หรืออบรมหลักสูตรด้านนี้มา ถึงจะปฏิบัติหน้าที่นี้ได้ ซึ่งจริงๆแล้วเจ้าหน้าที่ไม่มีการเพียงพอต่อคดีที่เกิดขึ้น แต่ถ้าถามว่าหากไม่มีเจ้าหน้าที่ที่กล่าวมานั้น แต่ใช้พนักงานสอบสวนตาม ป.วิอาญา นั้นได้หรือไม่ มันจะทำให้เกิดปัญหาหรือไม่ ในส่วนการเก็บพยานหลักฐานนั้นขาดความน่าเชื่อถือ เพราะขาดวิธีการเก็บ และการรักษาไม่ได้มาตรฐาน และในเรื่องของการเรียนรู้ของเจ้าหน้าที่จะต้องมีทักษะและความชำนาญพอสมควรถึงจะปฏิบัติหน้าที่ได้ ในมุมมองของด้านกฎหมายนั้นส่วนใหญ่กฎหมายที่ออกมาจะรองรับข้อมูลรูปแบบของการกระทำความผิดในรูปแบบใหม่ๆ อยู่แล้ว เช่น การเข้าถึงข้อมูลในคอมพิวเตอร์ การเปลี่ยนแปลงของเทคโนโลยีมีอยู่ตลอดเวลาจึงจำเป็นต้องศึกษาจากต่างประเทศมาปรับใช้”

รศ.พ.ต.อ.ดร.กิตต์ธนทัต เลอวงศ์รัตน์ :

“จากประสบการณ์จากทำงานวิจัยทางด้านการค้ามนุษย์นั้น การใช้กฎหมาย และพ.ร.บ. อาจจะคล้ายๆกัน อาจจะรวมไปถึงอาชญากรรมข้ามชาติ ซึ่งการกระทำความผิดนั้นเหมือนกันและบางกรณีก็เกี่ยวโยงกันในหลาย ๆ ฐานความผิด เช่น การมีเครือข่ายเชื่อมโยงข้ามชาติ การก่อการร้ายโดยทางด้านกฎหมายมีระบุอยู่ 3-4 มาตรา คำนิยามของเจ้าหน้าที่จะมีอยู่ 2 อย่าง คือ พนักงานตาม ป.วิอาญา และพนักงานเจ้าหน้าที่ตาม พ.ร.บ. ซึ่งจะมีอำนาจหน้าที่ในการตรวจค้น และต้องมีการสืบสวนเฉพาะ เคยมีประสบการณ์ในการอบรมหลักสูตรทางด้านอาชญากรรมคอมพิวเตอร์ ส่วนใหญ่จะเน้นไปด้านการเก็บพยานหลักฐาน การหา software ต่างๆ การหาความเชื่อถือของพยานหลักฐานเมื่อขึ้นไปสู่ชั้นศาล ในด้านการทำคู่มือควรจะมีการวิพากษ์คู่มือว่าจะนำไปใช้ได้จริงหรือไม่”

พ.ต.อ.สมศักดิ์ หน่องพงษ์ :

“ด้านเจ้าหน้าที่ของ ปอท. จะมีเจ้าหน้าที่ที่เชี่ยวชาญเฉพาะกลุ่มงานสนับสนุน โดยผ่านการอบรมมาอย่างดี โดยจะมีการร่วมมือในการปฏิบัติงานกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร(ICT) ปัญหาที่มักเกิดขึ้นนั้น เช่น เมื่อมีคดีเกิดขึ้นเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เมื่อผู้ร้องเรียนมาแจ้งความที่สถานีตำรวจนั้น ทางตำรวจจะปัดความรับผิดชอบมาให้ทาง ปอท. ทันที โดยตอนนี้ทาง ปอท. กับ ICT จะเริ่ม

โครงการให้ความรู้กับตำรวจในสถานีตำรวจทั่วประเทศ เมื่อมีคดีที่เกี่ยวกับอาชญากรรมทางด้านคอมพิวเตอร์นั้น พนักงานสอบสวนจะต้องดำเนินการอย่างไรบ้าง”

นายมานะชัย บุญเอก :

“ขอกล่าวเป็นข้อ ๆ สำหรับการให้ความเห็นดังนี้ครับ

1.ในการทำเครือข่ายเป็นเรื่องที่ดีมาก

2.การทำคู่มือ ควรทำเป็น Case by Case

3.การปฏิบัติเชิงนโยบาย ในการจัดทำข้อมูลการจราจร การจัดเก็บข้อมูลความลับของประเทศ ของทางราชการ และส่วนบุคคล โดยต้องทำการบูรณาการกันทุกๆ หน่วยงาน

4.ต้องให้ข้อกฎหมายทุกฉบับมีความเชื่อมโยงกัน

5.สถานการณ์ดำเนินการในปัจจุบัน ต้องตามให้ทันด้านเทคโนโลยี และเก็บรวบรวมข้อมูลให้ถูกวิธีและได้มาตรฐาน

6.ในงานด้านเทคนิคต้องสะท้อนไปถึงเครื่องมือ และมาตรฐาน รวมไปถึงคนที่ปฏิบัติงาน ด้านการบริหารการจัดการ และสิ่งที่สำคัญ คือ KM ที่ต้องมีการบูรณาการร่วมกัน

แนวทางแก้ไขขอให้งานวิจัยนี้เป็นการแก้ไขปัญหา และการบูรณาการทุกหน่วยงานที่เกี่ยวข้องร่วมกัน”

พ.ต.อ.ดร.วิวัฒน์ สิทธิสรเดช :

“ในด้านกฎหมายมีการออกกฎหมายมาค่อนข้างดี ที่สามารถครอบคลุมได้ทั่วถึง ด้าน พ.ร.บ. คอมพิวเตอร์นั้น จะกำหนดให้มีหลักฐานที่เป็นดิจิตอล และควรจะต้องปรับปรุงถ้อยคำต่างๆ ให้ชัดเจน และการประสานงานขอข้อมูลไปยังต่างประเทศนั้นยังจะต้องเป็นแบบส่วนตัว และยังไม่เป็นทางการ รวมไปถึงปัญหาในการพิสูจน์พยานหลักฐานนั้น ยังมีเจ้าหน้าที่ไม่เพียงพอ และการฝึกอบรมให้ความรู้และประสบการณ์การทำงานนั้นยังไม่เพียงพอ รวมไปถึงการเก็บและรักษาอุปกรณ์ และ software ต่างๆ ยังไม่ได้มาตรฐานเท่าที่ควร”

ผศ.พ.ต.ท.สุรัตน์ สาเรือง :

“ด้านความรู้ของเจ้าหน้าที่ บางท่านที่มีการประสบการณ์ทำงานนานๆ อาจจะยังไม่มีความรู้มากนัก และอำนาจของเจ้าหน้าที่นั้น ยังไม่มีอำนาจเพียงพอ ตาม ป.วิอาญาในการขอข้อมูลจากผู้ให้บริการอินเทอร์เน็ต (ISP) ได้ ซึ่งอาจจะมีปัญหาและความล่าช้าของการขอข้อมูลนั้นยังพบอยู่บ่อยครั้ง และหนังสือที่ทางผู้ให้บริการอินเทอร์เน็ตตอบมานั้น ผู้ที่ลงนามในหนังสือ คือ นิติกรของทางบริษัทที่ให้บริการทางอินเทอร์เน็ตแต่ละราย ซึ่งมักจะเป็นปัญหาในการขึ้นให้การเป็นพยานในชั้นศาลเนื่องจากไม่สามารถตอบคำถามของทนายฝ่ายจำเลย หรือศาลได้ ส่วนของคู่มือควรจะต้องทำเป็น Case by Case ไปน่าจะดีกว่า และควรเพิ่มการอบรม โดยเชิญอาจารย์ทางด้าน Network Security มาให้ความรู้ก็จะเป็นการดีมากยิ่งขึ้น”

พ.ต.ท.ดร.สฤษดิ์ สืบพงศ์ศิริ :

"ขอสะท้อนถึงผู้ที่ได้รับผลกระทบ ในด้านระเบียบและข้อกฎหมายต้องมีความทันสมัย และต้องมีการนำไปใช้อย่างเป็นรูปธรรมจริงๆ ซึ่งต้องสามารถนำไปใช้ได้จริงๆ ทุกๆ ข้อ และในการหาเครือข่าย ถ้าหากเน้นไปถึงด้านประชาชน เราควรน่าจะต้องรวมไปถึง Webmaster ของเว็ปไซต์ต่างๆ นั้นด้วย และในหลายกรณีเรามีการให้ทางภาคเอกชน หรือ บุคคลทั่วไปที่มีความรู้เฉพาะด้านมาให้การช่วยเหลือในการปฏิบัติงานของเจ้าหน้าที่เราเหมือนกรณีอาสาสมัครของมูลนิธิต่าง ๆ ดังนั้นเราควรจะต้องมีการคัดกรองบุคคลและข้อมูลของผู้ที่เข้ามาช่วยงานเราด้วยหรือไม่ ซึ่งต้องมีการทำ KM กัน โดยต้องคำนึงถึงระดับผู้ที่ต้องใช้กฎหมายและระดับของผู้ปฏิบัติด้วย"

พ.ต.ต.หญิง กนกพร แสนแก้ว :

"สำหรับในข้อกฎหมายนั้น จะมีประเด็นที่สำคัญ คือ ฐานความผิดและเขตอำนาจในการดำเนินการตามกฎหมาย เช่น เขตอำนาจการสอบสอน เป็นต้น โดยการวางแผนให้เป็นระบบ และติดตามผลการดำเนินการด้วย การรับผิดชอบในคดีนั้น การรักษาพยานหลักฐานยังไม่สามารถทำได้อย่างเป็นระบบ และไม่มีวิธีการที่ถูกต้อง การใช้เทคโนโลยีสมัยใหม่นี้ มีวิธีการกระทำความผิดที่แยบยล และพัฒนาวิธีการอย่างรวดเร็ว ในประเด็นการตรวจสถานที่เกิดเหตุในด้านการก่ออาชญากรรมคอมพิวเตอร์นั้น จะต้องทำตามขั้นตอน เช่น การตรวจสอบสถานะของการทำงานของโปรแกรมในคอมพิวเตอร์นั้น ก่อนการเข้าถึงข้อมูลที่บรรจุเป็นหลักฐานทางดิจิตอลนั้น ต้องมีแนวทางการปฏิบัติอย่างเป็นระบบและเป็นขั้นตอน ตั้งแต่การเปิดปิดระบบ การเข้าถึงข้อมูล วิธีการดึงข้อมูล เป็นต้น ส่วนการจัดทำคู่มือนั้น ต้องให้ความรู้ในระดับเบื้องต้น และแนวทางการปฏิบัติงานของทุกๆหน่วยงานที่เกี่ยวข้อง เพื่อสามารถนำไปใช้ประโยชน์ร่วมกันได้"

ผศ.พ.ต.ท.วรธัช วิชชุวาณิชย์ :

"ในการบังคับการใช้กฎหมายนั้น เรากลับไม่มีความมั่นใจในการใช้ ว่าการดำเนินการในเรื่องต่างๆ นั้น ว่าอยู่ในอำนาจของพนักงานสอบสวนหรือไม่ หรือเป็นอำนาจของพนักงานเจ้าหน้าที่ตาม พรบ. คอมพิวเตอร์ และมักจะเป็นปัญหาโต้แย้งกันอยู่ในเรื่องการขอข้อมูลทางคดี หรือการประสานงานกับเจ้าหน้าที่ที่เกี่ยวข้องไม่ว่าจะเป็นผู้ให้บริการทางอินเทอร์เน็ต หรือเจ้าหน้าที่ในส่วนของภาคราชการด้วยกันเอง และปัญหาอีกประเด็น คือ แนวทางการปฏิบัติ ควรจะต้องมีหน่วยงานที่เป็นศูนย์กลางในการขอข้อมูลเพื่อนำไปใช้ประโยชน์และเรื่องการขยายผล เพราะทุกวันนี้ทางเจ้าหน้าที่ผู้ปฏิบัติต้องขอข้อมูลเป็นยังผู้ให้บริการทางอินเทอร์เน็ตทุกราย ทำให้เสียเวลาในการรอการตรวจสอบข้อมูลที่เกี่ยวข้องของแต่ละค่าย ถ้ามีหน่วยงานกลางในการดำเนินการในเรื่องนี้ก็จะช่วยให้การทำงานสะดวก และรวดเร็วขึ้น และมีประเด็นอื่นที่สำคัญเช่นกัน เช่น การเข้าสถานที่เกิดเหตุต้องปฏิบัติอย่างไร ต้องมีการบันทึกการทำงานในทุกๆ ขั้นตอนเพื่อป้องกันการผิดพลาดที่อาจจะเกิดขึ้นได้ ไม่ว่าการทำให้วัตถุพยานถูกปนเปื้อนโดยไม่ได้ตั้งใจ ซึ่งจะเป็นข้อต่อสู้ทางคดีของทางฝ่ายผู้ต้องหาได้และที่สำคัญอีกประเด็นก็คือ ระดับความรู้ของเจ้าหน้าที่เรายังไม่เพียงพอในการปฏิบัติงาน จึง

ต้องการให้มีการจัดฝึกอบรมให้ความรู้กับทุกๆ หน่วยงานที่เกี่ยวข้อง โดยให้องค์ความรู้พื้นฐานที่ใกล้เคียงกัน ด้านการสร้างเครือข่ายนั้นต้องมีการดึงเอาภาคเอกชนมามีส่วนร่วมเพื่อการพัฒนาที่ดียิ่งขึ้น”

การประชุมครั้งที่ 2 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Storytelling)”

ผู้เข้าร่วมประชุม

1. พล.ต.ท. ดร. ณรงค์	กุลนิเทศ	ผู้อำนวยการแผนงาน
2. พ.ต.อ.สมศักดิ์	หน่องพงษ์	นักวิจัย
3. ผศ.พ.ต.ท.วรธัช	วิชชุวาณิชย์	นักวิจัย
4. นางสาวณิช	วงศ์ส่องจ้า	นักวิจัย
5. นายอำพล	บุญประภากร	ผู้พิพากษาศาลแขวง จังหวัดนครปฐม
6. นายปกรณ์	ธรรมโรจน์	อัยการประจำสำนักงานอัยการสูงสุด สำนักงานอัยการพิเศษฝ่ายคดีเศรษฐกิจและทรัพยากร 2 สำนักงานอัยการสูงสุด
7. พ.ต.อ.อนุชิต	บุญญะปฏิภาค	นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง
8. พ.ต.ท.ดรัณ	จาดเจริญ	รองผู้กำกับการ กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี
9. พ.ต.ท.พจน์	ฟอร์ตี้	รองผู้กำกับการ กลุ่มงานผู้เชี่ยวชาญ กองทะเบียนประวัติอาชญากร
10.พ.ต.ต.นิติ	อินทุลักษณ์	นักวิทยาศาสตร์ (สบ 2) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง

ผู้เข้าร่วมประชุมได้แสดงความคิดเห็นในประเด็นที่เกี่ยวข้องดังนี้

นายปกรณ์ ธรรมโรจน์ :

“สำนักงานอัยการสูงสด ได้จัดทำคู่มือ พนักงานอัยการ สำหรับการสอบสวน และดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ โดยคู่มือดังกล่าว จะอธิบายแนวทางการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ ในเบื้องต้น โดยคดีความผิดเกี่ยวกับคอมพิวเตอร์ มีองค์ความรู้เป็นจำนวนมาก รูปแบบคดีและพยานหลักฐาน มี

ลักษณะเฉพาะ และกฎหมาย พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งใช้ดำเนินคดีประเภทนี้ โดยตรงยังค่อนข้างใหม่ เจ้าหน้าที่และพนักงานของรัฐที่เกี่ยวข้องในการดำเนินคดี ยังขาดความรู้ ความเข้าใจ เกี่ยวกับหลักการต่างๆ ในระบบคอมพิวเตอร์ ข้อมูลเทคโนโลยีสารสนเทศ ความเข้าใจในการพิจารณาพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ ตลอดจนการปรับใช้กฎหมายพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในการดำเนินคดี การจัดการความรู้ จำเป็นต้องได้รับความร่วมมือทั้ง ฝ่ายเทคโนโลยี และเจ้าหน้าที่ฝ่ายกฎหมาย ประกอบกัน จึงจะสามารถรวมรวมองค์ความรู้สำคัญที่จะใช้ในการดำเนินคดีประเภทนี้ได้ แต่ปัจจุบัน ความร่วมมือระหว่างองค์กร และหน่วยงานต่างๆ ยังไม่เป็นรูปธรรม

ด้านเครือข่ายและการจัดการด้านอาชญากรรมคอมพิวเตอร์ เนื่องจากมีความจำเป็นที่ต้องใช้ข้อมูลจากเครือข่ายหลายภาคส่วน จึงควรระบุแบ่งกลุ่มให้ง่ายต่อการประสานงาน และความเข้าใจของเจ้าหน้าที่

1. ภาครัฐ

1.1 หน่วยงานดำเนินคดี สำนักงานตำรวจแห่งชาติ , สำนักงานสอบสวนคดีพิเศษ , สำนักงานอัยการสูงสุด

1.2 หน่วยงานสนับสนุน กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

2. องค์กรอิสระ

2.1 เนคเทค (รวบรวม และวิจัย องค์ความรู้ด้านคอมพิวเตอร์) ,

2.2 สำนักราชบัณฑิตยสถาน (รวบรวมคำศัพท์ด้านคอมพิวเตอร์ เผยแพร่ต่อประชาชน)

3. ภาคเอกชน

3.1 บริษัทฯ ผู้ให้บริการเชื่อมต่อเครือข่ายอินเตอร์เน็ต (ISP)

3.2 บริษัทฯ ผู้ให้บริการโทรศัพท์เคลื่อนที่ ซึ่งปัจจุบันใช้เชื่อมต่ออินเตอร์เน็ตได้

3.3 บริษัทฯ ผู้ให้บริการโทรศัพท์พื้นฐาน

นอกจากนี้ ยังมีเครือข่ายของธนาคารพาณิชย์ ที่สามารถ ช่วยเหลือในการดำเนินคดีได้ เนื่องจากธนาคารดูแลระบบการเงิน ซึ่งอาชญากรรมหลายประเภท มีความเชื่อมโยงกับผลประโยชน์ทางการเงิน

ส่วนประเด็นแนวทางพัฒนาการมีเครือข่าย และการจัดการความรู้ จะเห็นได้ว่า ปัจจุบันมีเอกสารและสื่อบันทึกข้อมูลในการดำเนินคดี ของประเทศต่างๆ เผยแพร่ ในสื่อสารธารณะ เป็นจำนวนมาก สามารถนำมา เปรียบเทียบ วิเคราะห์ และปรับใช้ เพื่อเป็นแนวทางสำหรับการพัฒนาได้ อย่างไรก็ตาม เนื่องจากกฎหมาย และสภาพสังคม มีความแตกต่างกัน ในแต่ละประเทศ การนำความรู้ในการดำเนินคดีของประเทศต่างๆ มาปรับใช้กับประเทศไทย จำเป็นต้องเข้าใจความแตกต่าง และเลือกสิ่งที่สามารถใช้ได้จริง และไม่ทำให้เกิดอุปสรรคขัดข้องในการดำเนินคดี”

พ.ต.ต.นิติ อินทุลักษณ์ :

"ประเด็นการขึ้นให้การในฐานะพยานผู้เชี่ยวชาญ โดยประสบปัญหาว่าถูกขึ้นให้การเป็นปากแรก โดยทางฝ่ายจำเลยได้มีการเตรียมทีมทนายมาถึง 30 – 40 คน แต่ฝ่ายเรามีแค่ 1 คน คือตัวผมในฐานะพยานผู้เชี่ยวชาญ และเราก็จะถูกทำให้ไม่มีความน่าเชื่อถือ โดยที่ทางอัยการ ก็ไม่สามารถดำเนินอะไรได้ ซึ่งก็เป็นปัญหาในการจัดลำดับการขึ้นให้การ หรือ การเข้าใจในคดีอย่างถ่องแท้ของทางอัยการ ซึ่งจะรวมไปถึงศาลด้วย"

พ.ต.ท.พจน์ ฟอร์ตี้ :

"ปัจจุบันการเก็บข้อมูลจากแผนประทุษกรรม ยังไม่สามารถนำมาใช้ประโยชน์ได้ แต่สามารถนำมาเป็นข้อมูลสนับสนุนในการค้นหาอาชญากรรมคอมพิวเตอร์ เช่น สมุดภาพ ประวัติผู้ค้นหา แต่ปัญหาที่พบคือยังได้รับข้อมูลน้อยมาก"

พ.ต.ท.ดรัณ จาดเจริญ :

"มุมมองของพนักงานสอบสวนมักจะยึดการปฏิบัติงานแบบเดิมๆ เพราะขาดความรู้ ไม่เข้าใจถึงระบบคอมพิวเตอร์ เมื่อนำพยานหลักฐานที่เกี่ยวข้องกับคอมพิวเตอร์จึงไม่ทราบวิธีการเก็บหลักฐาน จึงทำให้บางครั้งสามารถนำไปใช้ประโยชน์ไม่ได้ จึงอยากให้มีการจัดอบรมให้พนักงานสอบสวนเพื่อการเพิ่มเติมความรู้เพื่อการปฏิบัติงานไปในทิศทางเดียวกัน"

พ.ต.อ.อนุชิต บุญญะปฏิภาค :

"การเก็บพยานหลักฐานในคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ ทางสำนักงานพิสูจน์หลักฐานจะรับหลักฐานโดยตรงเท่านั้น และการเก็บรักษาพยานหลักฐานที่ถูกต้อง ด้านการเข้าสาถนที่เกิดเหตุควรวางกรอบและขอบเขตอำนาจ หากเมื่อตรวจพบพยานหลักฐานที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ควรจะให้ผู้เชี่ยวชาญเข้าที่เกิดเหตุเท่านั้น เพื่อเป็นการป้องกันความเสียหายต่อพยานหลักฐาน"

นายอำพล บุญประภากร :

"การรับฟังพยานหลักฐานในชั้นศาล บางครั้งตัวผู้พิพากษาเองยังไม่มีความรู้เพียงพอ และระบบพยานหลักฐานในการดำเนินคดียังไม่เป็นระบบ จึงทำให้ยากต่อการปฏิบัติงาน หาแต่จะดำเนินการตามหลักของ Chain of Custody และควรจะจัดการอบรมเพิ่มความรู้ให้เป็นไปในทิศทางเดียวกัน โดยอาจจะเชิญวิทยากรจากหน่วยงานต่างประเทศเพื่อเป็นการสร้างมาตรฐาน และการปฏิบัติงานที่ทันสมัย และมีมาตรการในการป้องกันการเสียหายที่จะถูกฟ้อง"

การประชุมครั้งที่ 3 กิจกรรมแบ่งปันแลกเปลี่ยนเรียนรู้ “การเล่าเรื่อง (Storytelling)”

ผู้เข้าร่วมประชุม

1. พล.ต.ท. ดร. ณรงค์	กุลนิเทศ	ผู้อำนวยการแผนงาน
2. พ.ต.อ.สมศักดิ์	หน่องพงษ์	นักวิจัย
3. ผศ.พ.ต.ท.วรธัช	วิชชุวาณิชย์	นักวิจัย
4. นางสาวณิช	วงศ์ส่องจ้า	นักวิจัย
5. นายอำพล	บุญประภากร	ผู้พิพากษาศาลแขวง จังหวัดนครปฐม
6. นายปกรณ์	ธรรมโรจน์	อัยการประจำสำนักงานอัยการสูงสุด สำนักงานอัยการพิเศษฝ่ายคดีเศรษฐกิจและทรัพยากร 2 สำนักงานอัยการสูงสุด
7. รศ.พ.ต.อ.กู้เกียรติ	เจริญบุญ	อัยการประจำกอง ฝ่ายพัฒนากฎหมาย สำนักงานวิชาการ สำนักงานอัยการสูงสุด
8. พ.ต.อ.อนุชิต	บุญญะปฏิภาค	นักวิทยาศาสตร์ (สบ 4) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง
9. พ.ต.ท.ดรัณ	จาดเจริญ	รองผู้กำกับการ กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี
10. ผศ.พ.ต.ท.สุรัตน์	สาเรือง	ผู้ช่วยศาสตราจารย์ (สบ 3) กลุ่มงานคณาจารย์ คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ
11.พ.ต.ต.นิติ	อินทุลักษณ์	นักวิทยาศาสตร์ (สบ 2) กลุ่มงานตรวจพิสูจน์อาชญากรรมทางคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง

ผู้เข้าร่วมประชุมได้แสดงความคิดเห็นในประเด็นที่เกี่ยวข้องดังนี้

นายปกรณ์ ธรรมโรจน์

"จริงๆปัญหามีอยู่ทุกขั้นตอน แต่ปัญหาที่จำเป็นเร่งด่วนคือเรื่อง การกระจายองค์ความรู้ไปสู่เจ้าหน้าที่ผู้ปฏิบัติงานทุกภาคส่วน สำนักงานอัยการเองก็ยังขาดองค์ความรู้ทางด้านนี้อยู่ การจะสานคดีต่อก็จะเกิดปัญหาและอุปสรรคมาก โดยได้มีโอกาสไปบรรยายให้อัยการในต่างจังหวัด ก็ยังไม่รู้เกี่ยวกับคำศัพท์พื้นฐานทางด้านคอมพิวเตอร์เท่าไรนัก ปัจจุบันคดีที่เกี่ยวกับกับพยานหลักฐานทางคอมพิวเตอร์ สื่ออินเตอร์เน็ทค่อนข้างเยอะ และกระบวนการที่เราจำเป็นต้องใช้ในการสืบสวนสอบสวนที่ยังไม่ถึงกับมีความเชี่ยวชาญโดยตรง ถ้าเราสามารถแยกกระบวนการบางอย่างออกมาได้ เราจะได้ประโยชน์เป็นจำนวนมาก โดยยกตัวอย่างของประเทศสหรัฐอเมริกา แล้วได้เจอกลุ่มงานของเขา ที่มีหลายๆหน่วยงานมาช่วยกันในการทำคดีทางด้านอาชญากรรมคอมพิวเตอร์ มาจากทั้งระดับท้องถิ่น ระดับมลรัฐ ระดับรัฐบาลกลาง รวมไปถึงทางด้านเอกชน โดยมีรูปแบบหนึ่งที่น่าสนใจ คือ ในห้องงานทางด้านนิติวิทยาศาสตร์ของเขา พบว่า มีด้านหนึ่งเขาจะส่งเสริมให้เจ้าหน้าที่ทุกระดับสามารถใช้งานเครื่องคอมพิวเตอร์ในการคัดลอก ถ่ายโอน หรือตรวจสอบข้อมูลเบื้องต้นด้วยตนเองได้ โดยมีแนวคิดว่า ระดับผู้เชี่ยวชาญของเขามีจำนวนไม่เพียงพอ จึงพยายามจะตัดงานในส่วนที่เจ้าหน้าที่ทั่วไปที่มีความรู้พื้นฐาน และสามารถที่จะทำเองได้ โดยพยายามแนะนำวิธีการและเอาคู่มือที่อำนวยความสะดวกมาให้กับเจ้าหน้าที่ปฏิบัติงานด้วยตนเองได้ หากส่วนได้ที่ไม่สามารถทำเองได้ เช่น กู้ข้อมูลที่ถูกลบไปแล้ว หรือข้อมูลที่ต้องเข้ารหัส ถึงจะส่งต่อให้ระดับผู้เชี่ยวชาญ ในภาพของกฎหมายจึงขอเสนอแบ่งออกเป็น 3 กลุ่ม คือ 1.กลุ่ม Collector คือ ผู้เก็บรวบรวมพยานหลักฐาน 2. กลุ่ม Examiner คือ ผู้ทำการตรวจพิสูจน์ และ 3. กลุ่ม Expert แต่ในประเทศไทยยังทำแบบที่หากผู้ใดทำอะไรได้ก็รับหน้าที่ทำอย่างนั้นไปทั้ง 3 กระบวนการ แต่มีอยู่คดีหนึ่งที่เราสามารถได้คือ คดีฆ่าผู้ว่าราชการ ปรีณะ ที่มีการแยกบทบาทการทำหน้าที่อย่างชัดเจน ส่วนหนึ่งที่มีหน้าที่เก็บหลักฐานก็เก็บหลักฐานไป พอหลักฐานถูกเก็บมาก็นำมาตรวจและผลการตรวจสอบได้อะไรบ้าง และผู้เชี่ยวชาญไม่ได้แตะต้องพยานหลักฐานใดๆทั้งสิ้น แต่ดูจากผลการตรวจพิสูจน์ และประมวลผลว่า เหตุการณ์นั้นเกิดขึ้นอย่างไร เกิดอะไรบ้าง โดยอาศัยพยานหลักฐานที่ได้ จะเห็นได้ว่ากฎหมายไทยจะใช้คำว่าผู้เชี่ยวชาญอย่างเดียว และใช้ผู้เชี่ยวชาญครบทุกมิติทั้ง 3 ส่วน ซึ่งตรงนี้ถ้านำมาเปรียบเทียบกับคดีทางด้านอาชญากรรมคอมพิวเตอร์ ซึ่งมีคดีจำนวนมากที่อาศัยพยานหลักฐานทางคอมพิวเตอร์มาเกี่ยวข้องกับกระบวนการทางคอมพิวเตอร์ โดยเฉพาะสื่อทางอินเตอร์เน็ท กระบวนการบางอย่างที่เห็นว่าจะเป็นประโยชน์มาก โดยที่เราจะเห็นว่าทำอย่างไรโดยที่เราไม่ต้องแบกองค์ความรู้อยู่ที่ผู้เชี่ยวชาญที่จบมาโดยตรง เพื่อให้พนักงานสอบสวนได้รวบรวมบางอย่างได้ด้วยตนเอง โดยที่ยังไม่ต้องใช้เครื่องมือ และความรู้ที่ลึกซึ้งมากนัก ปัญหาที่พบส่วนมากก็คือ แม้อัยการ หรือพนักงานสอบสวนเองก็ไม่สามารถแนะนำพยาน และผู้เสียหายในการรวบรวมพยานหลักฐานได้ พยานหลักฐานในคดีฉ้อโกงทางอินเตอร์เน็ท ซื้อขายออนไลน์ โดยผู้เสียหายเป็นคนรวบรวมมาแบบไม่มีความรู้ ไม่ครบถ้วน โดยที่บอกได้ถึง

หลักฐานการกระทำความผิด แต่บอกข้อมูลที่บ่งชี้ถึงผู้กระทำความผิดไม่ได้ โดยที่ไม่รู้ถึงความน่าเชื่อถือของพยานหลักฐานพวกนี้ โดยที่เมื่อมาถึงอัยการก็ไม่มีการให้ตรวจสอบซ้ำ พอไปถึงศาลเพื่อสืบพยานข้อมูลต่างๆก็หายไป”

พันตำรวจโทดรัณ จาดเจริญ

“ได้มีทีมงาน Forensic ของต่างประเทศได้อธิบายให้อัยการฟังว่า ของเขามีความจำเป็นมากที่จะให้ความสำคัญแยกระหว่าง examiner กับ expert ค่อนข้างมาก คือ ถ้าเป็น examiner จะอธิบายได้แค่ข้อเท็จจริงว่า นำอะไรมาตรวจ ด้วยวิธีการใด และผลเป็นอย่างไร สิ่งที่ห้ามก็คือไม่ให้แสดงความคิดเห็นว่าอนุมานไปถึงอะไรได้บ้าง แต่คนที่ทำหน้าที่ expert อาจจะไม่ได้ทำหน้าที่ทำการตรวจพิสูจน์โดยตรง แต่เป็นคนที่เอาข้อมูลต่างๆ มาแล้วให้ความเห็นว่าสิ่งที่บ่งชี้คืออะไรได้บ้าง และมีข้อจำกัดอย่างไร แต่ในประเทศไทยเราใช้ผู้เชี่ยวชาญทุกด้าน”

พันตำรวจเอกอนุชิต บุญญปฏิภาค

“ในขณะนี้การพิสูจน์หลักฐานทางด้านคอมพิวเตอร์ของทางสำนักงานพิสูจน์หลักฐานได้เพิ่มศักยภาพในการตรวจหลักฐาน โดยกระจายไปยังศูนย์ต่างๆในประเทศไทย เช่น นครราชสีมา สงขลา เชียงใหม่ เป็นต้น ในด้านเทคโนโลยีเรามีความก้าวหน้าพอสมควร และผู้เชี่ยวชาญก็มีความรู้”

ร้อยตำรวจเอกนิติ อินทุลักษณ์

“ในประเด็นการตรวจพิสูจน์หลักฐาน ขณะนี้ได้มีการทำงานในด้านการบริหารเบื้องต้น ซึ่งประเด็นของการตรวจคดีทางด้านคอมพิวเตอร์ ก็มีประเด็นใหญ่ๆหลายๆประเด็น คือ 1.เรื่องงบประมาณ เมื่อมีความเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็ว งบประมาณที่กองพิสูจน์หลักฐานจัดสรรให้ไม่เพียงพอกับเครื่องมือที่ต้องการจัดซื้อ เช่น การเปลี่ยนแปลงของระบบปฏิบัติการ และอุปกรณ์ต่างๆ โดยทางเราได้มีการเปลี่ยนแปลงการจัดซื้อโดยมองหาความร่วมมือกับหน่วยงานอื่นๆ โดยหาเครือข่ายร่วมเพื่อสนับสนุน และแลกเปลี่ยนเครื่องมือกัน แต่ปัจจุบันไม่เป็นไปอย่างนั้น เพราะอุปกรณ์เทคโนโลยีที่ล้ำสมัย มักจะรวมมาในตัวเดียวกัน ตั้งแต่สมาร์ทโฟน แท็บเล็ต หรือโน้ตบุ๊ค และอุปกรณ์ที่จะใช้ตรวจพิสูจน์ก็ได้หมดใบอนุญาตไปบางส่วน ซึ่งใบอนุญาตมีราคาแพง 2.ปัญหาการรวบรวมพยานหลักฐานของพนักงานสอบสวน โดยที่พนักงานสอบสวนประมาณ 80-90% ยังไม่เข้าใจถึงหลักการการรวบรวมพยานหลักฐาน เช่น เรื่องลิขสิทธิ์เพลง โดยมีการรวบรวมพยานหลักฐานของทางร้านคาราโอเกะ โดยยึดคอมพิวเตอร์มาเป็นพยานหลักฐาน และต้องการหารูปแบบลิขสิทธิ์ แต่ปัญหาเกิดอยู่ที่ต้องการหาว่าเพลงนี้มีลิขสิทธิ์หรือไม่ โดยที่ผู้ตรวจไม่รู้จักเพลงนี้ เราจะแก้ปัญหาด้วยการให้ผู้เสียหายนำตัวอย่างเพลงที่เป็นของแท้มาเปรียบเทียบ ซึ่งทุกคดีที่มีรูปแบบนี้ก็จะไม่มารับผลตรวจพิสูจน์เลย ประเด็นที่ทำให้คิดได้ว่า พนักงานสอบสวนที่รับแจ้งมานั้น ไม่ได้ตรวจสอบเลยว่า คนที่มาแจ้งนั้นเขาเป็นเจ้าของลิขสิทธิ์เพลงจริงหรือไม่ และเมื่อตรวจสอบไม่ได้ก็จะส่งคืน”

ผู้ช่วยศาสตราจารย์ พันตำรวจโท วรธัช วิชชุวาณิชย์

"จะเห็นว่าปัญหาที่หลายๆท่านถามจากประสบการณ์หรืออะไรก็แล้วแต่ ย้อนกลับไปในการประชุมครั้งที่ 1, ครั้งที่ 2 ที่เคยได้คุยกันว่า แผนกอาชญากรรมคอมพิวเตอร์หรือท่านอัยการ คุณมีแล้วรึยังแผนกอาชญากรรมคอมพิวเตอร์กับแผนกคดีนักการเมือง เราก็เคยเป็นคำถามกันเอาไว้ เราจะเกิดปัญหาว่าพยานผู้เชี่ยวชาญเวลาขึ้นให้การในชั้นศาลของนิติที่เคยพูดในครั้งที่แล้ว ทนายความฝั่งจำเลยลุ่ม 20 ต่อ 1 มันก็เป็นเรื่องที่ ถ้าในชั้นศาลเรามี ทางอัยการมีความรู้ก็สามารถคลี่คลายคดีที่เกี่ยวข้องในอาชญากรรมคอมพิวเตอร์ความสำคัญคือในเรื่องความเข้าใจของตัววัตถุพยาน ในหลายคดีเราไม่ใช่ใช้องค์ความรู้ด้าน IT อย่างเดียวในการจับกุมคนร้าย แต่ก่อนจะใช้วิธีการสืบสวนสอบสวนคนร้ายก็ได้ในการแกะรอย ปัญหาสำคัญคดีนี้คือทำอย่างไรให้วัตถุพยานมีความน่าเชื่อถือ ทั้งในแง่ของการสืบสวนและการสั่งฟ้องอัยการ ถ้าฝ่ายหนึ่งเป็นปัญหาเริ่มต้นจากฝั่งตำรวจ ฝ่ายผู้ตรวจก็ตรวจไม่ออก ไม่รู้จะตรวจอะไร การสื่อสารอาจจะทำความเข้าใจกันลำบาก สรุปตรงนี้ว่า ในมุมมองของฝั่งตำรวจจะทำงานเป็นยังไง เรามีวิธีคลี่คลายอย่างไร แล้วในฝั่งของอัยการก็จะดูและบอกว่าพยานหลักฐาน แล้วก็อยากให้ทุกท่านที่มีมุมมองมาแชร์ประเด็นกันว่าจะทำยังไง"

รองศาสตราจารย์ พันตำรวจเอก กู้เกียรติ เจริญบุญ

"ภาพรวมของกระบวนการเหตุที่เกิดขึ้น เนื่องจากว่าคอมพิวเตอร์จะเข้ามามีส่วนเกี่ยวข้องเวลากระทำผิดเกี่ยวกับคอมพิวเตอร์ ประเด็นที่ 2 ใช้คอมพิวเตอร์เป็นเครื่องมือ ประเด็นที่ 3 คอมพิวเตอร์เป็นตัวเก็บ ความรู้ในด้านคอมพิวเตอร์ปัญหาอันดับแรก จะต้องแพร่ชาวบ้าน ผู้เสียหายถูกด่า ไม่รู้จะเก็บข้อมูลยังไง เก็บพยานหลักฐานเกี่ยวกับคอมพิวเตอร์ได้ยังไง ประเด็นตามมาก็รู้ว่าคือผู้เสียหาย ผู้เสียหายไม่รู้จะแจ้งความที่ไหน หน้าที่ของพนักงานสอบสวนก็คือ รวบรวมหลักฐานทุกชนิดผู้พิสูจน์ความผิดบริสุทธิ์ ปัญหาของพนักงานสอบสวนก็คือ 1. เปิดคอลเซ็นเตอร์ขอข้อมูลธนาคาร อำนาจในการขอข้อมูลในธนาคาร อำนาจในการขอข้อมูลธนาคาร มีไว้ตามตรา 3.2 ปัญหาอยู่ตรงที่ผู้ให้บริการทางคอมพิวเตอร์ บริษัทต่างๆ ปรากฏว่าไม่เหมือนคดีพิเศษ ไม่ยอมให้ ก็มีการถกเถียงขออำนาจในมาตรา 32 ของ (3) ทำไมคุณไม่ให้จนกระทั่งเรื่องไปถึงกฤษฎีกา เวลาตรวจคอมพิวเตอร์ต้องเอาแผนกตรวจที่เกิดเหตุเอาไปด้วย ก่อนที่จะยก เพื่อเอาไปตรวจดีเอ็นเอว่าใครใช้เครื่องนี้ ไม่อยากให้ผู้ตรวจพิสูจน์ให้ข่าวกับนักข่าว การที่คุณไปให้ข่าวคุณรู้ข้อมูลรายละเอียด เท่ากับคุณกำลังเปิดเผยข้อมูลสำนวนการสอบสวน เท่ากับเราเปิดเผยข้อมูล"

นายอำพล บุญประภากร

"ประเด็นแรก เรื่องการนำเสนอพยานหลักฐาน ซึ่งตรงนี้ก็แบ่งเป็นผู้ให้กับผู้รับ ซึ่งเท่าที่ประสบมาและมีปัญหา ในแง่ของที่เป็นผู้ให้คอมพิวเตอร์มาเป็นอย่างดี โดยเฉพาะลึกซึ้งลงไปอีก ประเด็นที่ 2 เรื่องการรับฟังพยานหลักฐาน ซึ่งปัจจุบันก็มีพยานบุคคล พยานวัตถุ พยานเอกสาร ซึ้งก็มีคำพิพากษาฎีกาออกมาเยอะแยะ เราสามารถไปตรวจสอบดูได้ ในด้านพยานหลักฐานอาชญากรรมคอมพิวเตอร์ มันอาจจะเกิดจากราชบัญญัติคอมพิวเตอร์ พ.ศ. 2550 พึงเริ่มใช้ คดีที่ขึ้น ศาลฎีกาอาจจะยังน้อยอยู่ ต้นทางชั้นพนักงานสอบสวนไม่ค่อยมี

คดีขึ้นมา ได้สืบแค่คดีช่อโกง อยากบอกให้พนักงานสอบสวนว่า ต่อให้เป็นคนไปรับจ้างเปิดบัญชี คำพิพากษาโดยให้เหตุผลว่าคนที่ไปรับจ้างเปิดบัญชี โดยที่ถอนเพียง 500 1000 บาท เป็นตัวต้นทางในการกระทำความผิด ถ้าไม่มีคนที่อยู่ท้ายขบวน ถ้าเราไม่ลงโทษ เราจะไม่สามารถไปลงโทษคนปลายทางได้เลย ในเมื่อคุณไปรับจ้างเปิดบัญชีที่ทุกคนต้องรู้อยู่แล้ว มันไม่เหมาะเป็นบัญชีเงินฝากของใครของมัน ในคำพิพากษาอย่างที่บอก พอได้มีในคำพิพากษาของฎีกาในบางครั้งก็ต้องมาดูศาลอุทรมีไหมศาลชั้นต้นมีไหม ซึ่งในบางคดีเขาก็ให้หลักการยกตัวอย่างเช่น คดีของอากง อันที่1 เรื่องคอมพิวเตอร์ไปขอประสานงานจากโทรศัพท์ ในคำพิพากษาเป็น file ที่มีความน่าเชื่อถือเพราะว่าเป็นบริษัทเป็นหมื่นล้าน ขอมูลของเขาถ้าจัดเก็บให้ถูกต้อง มันน่าจะเกิดความเสียหาย คือ ประเด็นนี้มันไม่น่าเชื่อถือ ในข้อมูลแหล่งที่เราไปเอามาน่าเชื่อถืออยู่แล้ว เพียงแต่จัดเก็บให้ถูกต้องตามวิชาการ อันที่ 2 เรื่องการนำเสนอพยานหลักฐานในชั้นศาล คำพิพากษา จะมีประเด็นเรื่อง 15 ตำแหน่ง ซึ่งจำเลยก็จะสู้ว่า ตำแหน่งที่ 15 มันคาดเคลื่อนไป เอาเครื่องคอมพิวเตอร์ไปแสดง 14 ตำแหน่ง โชว์ออกมาละตำแหน่งที่ 15 จะเห็นว่ามันไม่เป็นสาระ ณ จุดนี้เราเตรียมเอกสารไปสำคัญที่สุด ประเด็นที่ 3 เรื่องดีกว่าขาด คือ อะไรที่เป็นพยานหลักฐานได้ก็เตรียมไปให้หมด”

พันตำรวจโท พัฒนะ ศุกรสุต

“วิธีการแก้ปัญหา เราจะต้องทำสิ่งแรกก่อนว่าหลักการเรื่องยึดเกี่ยวกับ digital evidence พยานหลักฐานดิจิตอลนั้นเป็นอย่างไร หน่วยงานที่เอาอ้างบ่อยๆ เราก็ใช้อยู่แล้ว ต่อไปจะแตกเป็นรูปย่อยๆได้แล้ว เป็นกระบวนการในวิธีการปฏิบัติงานย่อยๆ ลงมา ถ้าเราว่างหลักตรงนี้เราจะทำต่อได้ สิ่งที่เราว่างหลักการไว้แล้ว ต่อไป หลักปฏิบัติพื้นฐานสำคัญ 6 ข้อสำคัญกว้างๆที่สามารถปฏิบัติได้ จนรู้กระบวนการขั้นตอน เช่น จะเก็บอะไร จะรักษานั้นอย่างไร การตั้งคำถามในคู่มือเกี่ยวกับเรื่อง แชท หรือเกี่ยวกับเรื่องฉ้อโกง หลอกลวง เขาก็จะพยายามรวบรวมคำถามที่สำคัญ ควรจะมีคู่มืออ่านง่ายๆ

“ปัจจัยที่ทำให้เคสนี้สำเร็จ จะได้เอาปัจจัยเป็นความรู้ เรากับมีมุมมองดำเนินการที่แตกต่างกัน มุมมองของเจ้าหน้าที่ เช่นเจ้าหน้าที่สืบสวนมุมมองอย่างไร จัดมาโชว์แถลงข่าว ในขณะที่มุมมองท่านอัยการมองเรื่องความบริสุทธิ์ของหลักฐาน พยานหลักฐานได้ชัดเจนไหม ขณะที่เราลงมามุมมองส่วนที่มันต่างกัน ใน 4 ด้าน การมองพยานหลักฐาน 1. ระบุว่าอะไรเป็นหลักฐานในเรื่องนี้ 2. จะรวบรวมหลักฐานอันนี้ยังไง 3. จะวิเคราะห์ยังไง 4. จะเล่าเรื่องนี้ยังไง ทั้งสืบสวนสอบสวนจะมองหลักฐาน 4 ด้านนี้เหมือนกัน”

ผู้ช่วยศาสตราจารย์ พันตำรวจโท วรธัช วิชชุวาณิชย์

“เท่าๆที่หลายท่านที่ให้คำแนะนำ พอเรามีความเจริญก้าวหน้าเทคโนโลยีทางด้านคอมพิวเตอร์ตอนนี้ทุกคนก็มุ่งเป้าความผิดทางคอมพิวเตอร์ เราก็ใช้เทคโนโลยีทางด้าน IT พยายามหาตัวคนร้ายใช้วิธีทางเทคโนโลยีโดยเฉพาะ IT แต่พอมาฟังประสบการณ์ แต่ละท่านก็มีความคิดเห็นบางที บางครั้งเราก็ย้อมกันกับมาไปในเรื่องง่ายๆ ในสมัยก่อน เราจัดแบบไหนเราก็จัดแบบนั้น เหมือนแก๊งคอเซ็นเตอร์ ราก็ตามข้อมูลบัญชีธนาคารเป็นเรื่องการสืบสวนธรรมดา แต่เราเอาเรื่องธรรมดาโยงกับเรื่อง IT ก็เป็นประเด็นสำคัญ อีกอันนึงที่

ท่านให้คำแนะนำว่าการทำงานในด้านนี้การตรวจพิสูจน์หรือการแกะรอยของต่างประเทศ มีภาคเอกชนร่วมด้วย ซึ่งก่อนประชุมกัน ก็ได้มีโอกาสคุยในเรื่องพวกนี้ว่า การศึกษาในเชิงนิติวิทยาศาสตร์ มีองค์ความรู้ในด้านนิติวิทยาศาสตร์ตอนนี้ผูกติดกับหน่วยงานของรัฐอย่างเดียว รับรองไม่มีเอกชนมาช่วย มันถึงเวลารึยัง ว่าจะต้องทำยังไงให้ภาคเอกชนเข้ามาช่วย ทุกวันนี้เราจะตรวจ DNA เกี่ยวกับเรื่องส่วนตัว แต่หน่วยที่สามารถตรวจได้ โรงพยาบาลตำรวจ สถาบันนิติวิทยาศาสตร์ โรงพยาบาลรามาอะไรก็แล้วแต่ ซึ่งพอเราร้องขอไป เขาไม่รับตรวจ ตรวจเฉพาะเป็นคดีความ”

พันตำรวจโท สุรัตน์ สาเรือง

“เรื่องของการตรวจจากเอกชน ตอนนี้ต้องยอมรับว่าทางรัฐก้าวหน้ากว่าในมุมที่หลักฐานการตรวจคอมพิวเตอร์ ตอนนี้ที่น่ากลัวคือเราโดยไม่มีคู่แข่ง เวลาที่เราขึ้นศาลในคดีคอมพิวเตอร์ ยกตัวอย่างเช่น คำสั่งที่พยานพูดได้มันทำอะไร มันมีรูปร่างแบบไหน ทำอะไรเกิดขึ้นในระบบ เราเรียกว่ามันเป็น SCL เป็นวัยยากรแบบหนึ่ง ยกตัวอย่างเช่น เลือกอะไรขึ้นมาจากที่ไหนใต้เงื่อนไขอะไร เห็นหน้าคอมพิวเตอร์ทั่วไป เพราะตัวที่เลือกขึ้นมาก็จะเป็น เบอร์โทร ในฐานนะเรียนด้านคอมพิวเตอร์ ตัวนี้ทำอะไร เป็นการเพิ่มข้อมูลเข้าไป ถ้าทำแบบนี้จะเกิดอะไรขึ้น ตอบไม่ได้ เพราะไม่เห็นโครงสร้าง ของ Database เขาเรียกว่า Database ใน Database ของ AIS ถ้าว่าง Database ถูกที่ถูกเวลาก็จะเพิ่ม ในฐานะที่เรียนคอมพิวเตอร์ตอบได้แค่นี้ ซึ่งไม่ใช้ในฐานนะตรวจ ในอนาคตสิ่งที่เจอหน้าคอมพิวเตอร์ก็จะเจอแบบนี้เป็นที่ปรึกษาฝ่ายจำเลย”

นายอำพล บุญประภากร

“ในเรื่องของการดำเนินคดี ในหัวข้อการจัดการองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์ จะตรงกับบทบาทของเจ้าหน้าที่ตำรวจ ก็คือ 2 บทบาท 1. เกี่ยวกับเรื่องของการรักษาความสงบเรียบร้อย 2. เรื่องของการดำเนินคดี ในส่วนที่สำคัญ เรื่องของการดำเนินคดี ตัวอยากจะนำเสนอว่าน่าจะพูดถึงเรื่องกฎหมายลักษณะพยาน จะเป็นหลักการหนึ่ง ที่จะมาตอบคำถามในหลายๆเรื่อง ความน่าเชื่อถืออะไรเป็นสิ่งที่รับฟังได้ คือไม่ได้ดึงมาตราแต่ละมาตราคุยกัน แต่เอาหลักการที่ดีในกฎหมาย ว่าใครเป็นคนไปหาหลักฐาน พอหาหลักฐานแล้วจะต้องหาอะไรที่รับฟังได้หรือไม่ได้ พอหลังจากนั้นก็คือ นำเสนอเข้าสู่ขบวนการสอบสวนสู่ศาล ประเด็นสุดท้ายของหลักทางกฎหมายทางพยาน ประเด็นนี้เราจะพูดถึงการชั่งน้ำหนักพยานความน่าเชื่อถือ ท่านจะพูดถึงการชั่งน้ำหนักไว้แต่ละชิ้น พยานบุคคลแต่ละปาก พยานเอกสารแต่ละชิ้น พยานวัตถุแต่ละชิ้น ท่านพูดว่ามีองค์ประกอบอะไรที่ควรคำนึงถึงบ้าง พอเห็นรายละเอียดก็จะพอมองออกว่า ดึงพยานหลักฐาน 1 ชิ้นออกมาควรคำนึงถึงหลักอะไรบ้าง ที่จะทำให้เสียความน่าเชื่อถือไป อะไรที่เป็นประเด็นข้อสงสัยความน่าเชื่อถือจะต้องเอาอะไรไปเสริมพอจะรับฟังได้ มีน้ำหนักให้รับฟังได้ พอหลังจากการชั่งน้ำหนักพยานแต่ละชิ้น แต่ละปากแล้วก็มีอีกหลักหนึ่งในการคนหาความจริงในภาพรวมว่า หลักฐานทั้งหมดที่นำมาประกอบการเป็นสำนวน พยานวัตถุแต่ละชิ้น พยานบุคคลแต่ละปาก พยานเอกสารแต่ละชิ้น พอมองในภาพรวมข้อบ่งชี้ไปในทางไหนเพียงพอที่จะนำเสนอพิสูจน์ประเด็นของการกระทำความผิดหรือไม่