รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์

Model and measure of Solving Problem Cyber Crime

ผู้ช่วยศาสตราจารย์พิเศษ พลตำรวจโท ดร.ณรงค์ กุลนิเทศ
หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย

บทคัดย่อ

การวิจัยเรื่อง รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์ มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย ศึกษากฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ เพื่อสร้างรูปแบบและมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ การวิจัยครั้งนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Methodology) โดยการประชุมกลุ่มย่อย (Focus Group) และผ่านเครื่องมือการแลกเปลี่ยนเรียนรู้ (Storytelling)

ผลการวิจัยพบว่า

1. สภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย สามารถแบ่งเป็นประเด็นสำคัญ คือ

   1) ปัญหาด้านข้อกฎหมาย - ฐานความผิด - เขตอำนาจ - ใครต้องเป็นผู้รับผิด - ลักษณะพยาน
   2) ปัญหาด้านเทคนิค - เทคนิคพัฒนาต่อเนื่อง - การศึกษา - เทคนิคในการเก็บหลักฐาน
   3) แนวทางการปฏิบัติ - การประสานแนวทางปฏิบัติ ระหว่าง - ตำรวจ - อัยการ - ศาล
   4) วัฒนธรรม - วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ

2. กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ที่สำคัญ เช่น พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์เป็นต้น และกำหนดกฎของระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ 4 ข้อ ได้แก่ 1) ความสมบูรณ์ของหลักฐาน 2) ระบุที่มาของหลักฐานได้ 3) บุคคลที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ และ 4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย

3. รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์ ที่สำคัญคือ การนำส่งวัตถุพยานในการตรวจพิสูจน์ทางอาชญากรรมไซเบอร์ เช่น อย่าเปิดเครื่องอุปกรณ์ถ้าหากว่าเครื่องปิดอยู่ เป็นต้น ด้านมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ เช่น ควรเร่งการออกกฎหมายให้ครอบคลุมการกระทำความผิด มากขึ้น เป็นต้น

คำสำคัญ : รูปแบบ / มาตรการในการแก้ปัญหา / อาชญากรรมไซเบอร์

Abstract

The research topics areModeling and measurement of Solving Problem Cyber Crime. The objectives are to Study the problems of cybercrime, Law and Forensic Cyber Crime in Thailand to Create Model and measure of Solving Problem Cyber Crime. The methodology of this research is qualitative research by Focus Group through the Storytelling.

The research results were as follow:

1. Study of the problems of cybercrime in Thailand can divided into:

   1) Issues of law - offense - jurisdiction - responsible person - the witness.

   2) Technical issues - The continuous development - education - evidence collection techniques.

   3) Guidelines - Coordination practices between - police - prosecutor - court.

   4) Culture –difference cultures in each country.

2. The laws relating to cybercrime as Computer-related Crime Act B.E. 2550. Electronic Transactions Act B.E. 2544. And Electronic Signatures Law etc. 4Rules of Forensic Cyber Crime are Preservation, Identification, Providing Expert and Rules of Evidence

3. Model and Measure of Solving of Cyber Crime is Delivering Cyber Crime evidence to identification; Do not turn on if the device is switched off. Measure of Solving of Cyber Crime, should accelerate the legislation to cover the offense etc.

Keywords: Model / Measure of Solving / Cyber Crime

บทนำ

ปัญหาอาชญากรรมไซเบอร์ที่เกิดขึ้นทั่วประเทศไทยในปัจจุบันทั้งการกระทำผิดเกี่ยวกับเว็บไซด์ที่ผิดกฎหมายในลักษณะความผิดในคดีทั่วไป โดยเฉพาะเว็บไซด์ที่กระทำความผิดเกี่ยวกับการจาบจ้วงสถาบันพระมหากษัตริย์ ซึ่งเป็นการกระทำผิดตาม ป.อาญามาตรา 112 และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีปริมาณที่กระทำผิดเป็นจำนวนมาก

ปัญหาทางด้านอาชญากรรมไซเบอร์มีปัญหาอยู่หลายประการ โครงสร้างทางกฎหมายทำให้เกิดปัญหาด้านการสืบสวนสอบสวนทางด้านอาชญากรรมไซเบอร์ กฎหมายและความรู้ของพนักงานสอบสวนตลอดจนการรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล ยังก้าวไปไม่ทันต่อการกระทำผิดทางด้านอาชญากรรมไซเบอร์ เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน (Globalization) ความรู้ทางด้านอาชญากรรมไซเบอร์ของเจ้าหน้าที่รัฐยังมีน้อย การศึกษาการค้นหา การเก็บรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล เป็นอีกเรื่องหนึ่งที่เจ้าหน้าที่รัฐยังไม่มีความรู้เพียงพอ การหาแนวทางและวิธีการตรวจพิสูจน์ให้มีวิธีการที่ทันสมัยมากยิ่งขึ้น เป็นเรื่องที่ต้องดำเนินการ

จากความเป็นมาดังกล่าวข้างต้น หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชานิติวิทยาศาสตร์

ร่วมกับคณาจารย์ที่มีความรู้และประสบการณ์การทำวิจัยและผู้มีความรู้ความเชี่ยวชาญทางด้านอาชญากรรมไซเบอร์จากหน่วยงานต่างๆ เช่น กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานพิสูจน์หลักฐานตำรวจ กรมสอบสวนคดีพิเศษ สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ สำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงเทคโนโลยีสารสนเทศ และอาจารย์ผู้มีประสบการณ์ทางด้านการวิจัยจากมหาวิทยาลัยต่าง ๆ จึงมีความสนใจที่จะทำการศึกษามาตรการในการแก้ปัญหาอาชญากรรมไซเบอร์ โดยการจัดการความรู้จากเอกสารงานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมไซเบอร์ ในแต่ละหน่วยงาน ผ่านการจัดกิจกรรมแลกเปลี่ยนเรียนรู้ เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยนำเข้า กระบวนการ ผลลัพธ์ รวมทั้งรูปแบบที่ดี (Best Practice) ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะของมาตรการในการแก้ปัญหาอาชญากรรมไซเบอร์ เพื่อนำมาพัฒนางานทางด้านดังกล่าว เพื่อให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้งคุ้มครองสิทธิและเสรีภาพ ด้วยความรวดเร็ว เที่ยงตรง และเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นมาตรการในการแก้ปัญหาอาชญากรรมไซเบอร์ให้เป็นที่ยอมรับ ศรัทธาและความเชื่อมั่นจากประชาชน และสังคมต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาสภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย
2. ศึกษากฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์
3. เพื่อสร้างรูปแบบและมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์

ขอบเขตของการวิจัย

1) ขอบเขตด้านเนื้อหา

การวิจัยครั้งนี้เป็นการจัดการความรู้โดยการเก็บรวบรวมข้อมูลที่กระจัดกระจายอยู่ในรูปแบบของเอกสาร สถิติคำพิพากษาคดี สำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งวิธีการรวบรวมพยานหลักฐานและพิสูจน์หลักฐานอาชญากรรมไซเบอร์ และองค์ความรู้ที่อยู่ในตัวบุคคลผู้ปฏิบัติงานมาทำการจัดการความรู้ใหม่อย่างเป็นระบบ

2) ขอบเขตด้านระเบียบวิธีวิจัย

ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Methodology) โดยการประชุมกลุ่มย่อย (Focus Group) และผ่านเครื่องมือการแลกเปลี่ยนเรียนรู้ (Storytelling) โดยการจัดเวทีให้กลุ่มเป้าหมายได้แลกเปลี่ยนเรียนรู้ ประสบการณ์ ความคิดเห็น โดยเข้าร่วมกิจกรรม AAR (After Action Review) หลังจากนั้นผู้วิจัยจะนำข้อค้นพบมาทำการถอดบทเรียน โดยนำแนวคิดทฤษฎีที่เกี่ยวข้อง คือ แนวคิด การวิเคราะห์ SWOT และแนวคิดการวิเคราะห์ระบบ (System Analysis) นอกจากนี้ยังทำการสัมภาษณ์เจาะลึก กลุ่มเป้าหมายที่เป็นตัวแบบที่ดีที่สามารถให้ข้อมูลของแต่ละหน่วยงานที่เกี่ยวข้อง

3) ขอบเขตด้านกลุ่มประชากรเป้าหมาย

ประชากรเป้าหมายแบ่งออกเป็น 6 กลุ่ม โดยคัดเลือกจากประชากรซึ่งมีประสบการณ์เกี่ยวกับ

การทำสำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งวิธีการรวบรวมพยานหลักฐานและพิสูจน์หลักฐานอาชญากรรมไซเบอร์ การสุ่มตัวอย่างเป็นแบบเจาะจง (Purposive Sampling) โดยเลือกจากผู้ที่มีความรู้และประสบการณ์ที่เกี่ยวข้องกับอาชญากรรมไซเบอร์เป็นลักษณะแบบลูกโซ่ (Snowball Sampling) การวิจัยประเภทนี้จะเป็นกลุ่มตัวอย่างที่เป็นผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญพิเศษเฉพาะด้าน ซึ่งผู้ชำนาญของแวดวงของกลุ่มดังกล่าวทราบดี และให้การยอมรับ จึงสามารถแนะนำให้เป็นกลุ่มตัวอย่างได้ (พิสิต ฤทธิ์จรูญ หน้า 104) และประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ สอดคล้องกับประเภทของอาชญากรรมไซเบอร์ ซึ่งมี 6 ประเภท รวมประชากรเป้าหมาย ดังนี้

1) ข้าราชการตำรวจ ประกอบด้วย

1.1) เจ้าหน้าที่ตำรวจฝ่ายสืบสวน และสอบสวนจากหน่วยงานในพื้นที่

1.2) เจ้าหน้าที่ตำรวจพิสูจน์หลักฐานเกี่ยวกับอาชญากรรมไซเบอร์

1.3) เจ้าหน้าที่ตำรวจ กองบังคับปราบปรามเทคโนโลยีสารสนเทศ

1.4) เจ้าหน้าที่ตำรวจจากสำนักงานเทคโนโลยีสารสนเทศ และการสื่อสาร

2) เจ้าหน้าที่จากกระทรวงเทคโนโลยีสารสนเทศ

3) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากมหาวิทยาลัย

4) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมไซเบอร์ทั้งที่มีการพิพากษาลงโทษผู้กระทำผิด และยกฟ้องเนื่องจากพยานหลักฐานไม่พอในชั้นศาล

5) อัยการที่เคยดำเนินคดีเกี่ยวกับอาชญากรรมไซเบอร์ ทั้งที่มีการพิพากษาลงโทษผู้กระทำผิด และยกฟ้องเนื่องจากพยานหลักฐานไม่พอในชั้นศาล

6) ประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ โดยพิจารณาจากสำนวนการสอบสวนของพนักงานสอบสวนที่เป็นรูปแบบที่ดี (Best Practice) และรูปแบบที่ไม่ดี (Bad Practice) (สอดคล้องกับประเภทของอาชญากรรมไซเบอร์)

ผู้วิจัยคัดเลือกกลุ่มเป้าหมายจากกรุงเทพมหานครและปริมณฑล โดยคัดเลือกหน่วยงานที่อยู่ในกรุงเทพมหานคร โดยกองบัญชาการตำรวจนครบาล เป็นตัวแทน และปริมณฑล โดยตำรวจภูธรภาค 1 ตำรวจภูธรภาค 2 และตำรวจภูธรภาค 7 เป็นตัวแทน ซึ่งหน่วยงานดังกล่าวมีสถิติที่สูงมากเกี่ยวกับการกระทำผิดเกี่ยวกับคดีอาชญากรรมไซเบอร์ ซึ่งรวมอยู่ในเรื่องการลักทรัพย์ การยักยอกทรัพย์ ความผิดเกี่ยวกับทรัพย์ คดีหมิ่นประมาท คดีการเผยแพร่วัตถุที่เป็นลามกอนาจาร ข้อมูลสถิติในการกระทำความผิดดังกล่าวในปี 2553 (สถิติของ สตช.ล่าสุด รวบรวมได้ในปี 2553)

4) ขอบเขตด้านพื้นที่ในการศึกษา

การศึกษาในครั้งนี้ดำเนินการในเขตพื้นที่กรุงเทพมหานครและปริมณฑล โดยกองบัญชาการตำรวจนครบาล เป็นตัวแทนของการศึกษา และปริมณฑล โดยตำรวจภูธรภาค 1 ตำรวจภูธรภาค 2 และตำรวจภูธรภาค 7 เป็นตัวแทนของการศึกษา ซึ่งหน่วยงานดังกล่าวมีสถิติที่สูงมากเกี่ยวกับการกระทำผิดเกี่ยวกับคดีอาชญากรรมไซเบอร์

การทบทวนวรรณกรรม

1. ฐานความผิดเกี่ยวกับคอมพิวเตอร์ (พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550)

ความผิดตาม พ.ร.บ.คอมพิวเตอร์ 2550 แบ่งออกเป็น 4 หมวดใหญ่ ดังนี้

1) ส่วนที่ 1 ความผิดฐานเข้าถึงโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ (Unauthorized Access) ซึ่งระบุไว้ในมาตรา 5, 6, 7 และ 8

2) ส่วนที่ 2 ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (Computer Distortion) มาตรา 9, 10 และ 12

3) ส่วนที่ 3 ความผิดฐานเผยแพร่ข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย (Dissemination of Illegal Content) มาตรา 14, 15 และ 16

4) ส่วนที่ 4 หมวดเบ็ดเตล็ด (Miscellaneous) ซึ่งระบุความผิดที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไว้หลายประเภท เช่น ความผิดเกี่ยวกับการส่งอีเมล์ขยะ (Junk mail หรือ spamming) (มาตรา 11) การจำหน่ายหรือเผยแพร่ชุดคำสั่ง เพื่อใช้เป็นเครื่องมือในการกระทำความผิด (มาตรา 13) ฯลฯ

2. ประเภทอาชญากรรมไซเบอร์ อาจแบ่งได้ ดังนี้

1) ข้อมูลทางการทหารและข้อมูลทางราชการลับ

2) จารกรรมทรัพย์สินทางปัญญาและข้อมูลด้านธุรกิจ

3) จารกรรมเงินและทำให้เกิดการติดขัดทางด้านพาณิชย์

4) การโต้ตอบเพื่อล้างแค้น

5) การก่อการร้าย เช่น ทำลายข้อมูล ก่อกวนการทำงานของระบบ หรือหน่วยงานที่สำคัญและเสนอข้อมูลที่ผิด

6) การเข้าสู่ระบบเพียงเพื่อแสดงให้เห็นว่ามีความสามารถทำได้

3. แนวโน้มอาชญากรรมไซเบอร์ ขึ้นกับปัจจัยต่อไปนี้

จะเพิ่มขึ้นพร้อมกับการขยายตัวและการเข้าถึงที่ง่ายขึ้นของระบบเครือข่ายการสื่อสาร

1) การใช้คอมพิวเตอร์ในการปลอมแปลง และเลียนแบบสินค้า ปลอมเอกสาร ตัดต่อภาพถ่าย จะมีมากขึ้นและกว้างขวางขึ้น

2) การละเมิดทรัพย์สินทางปัญญาจะเพิ่มขึ้น ทั้งนี้รวมถึงการจารกรรมความลับทางอุตสาหกรรม การค้า และสงครามข้อมูลข่าวสาร

3) มีการเข้าสู่ระบบฐานข้อมูลแบบไม่ถูกต้องเพื่อกระทำสิ่งที่ไม่ได้รับอนุญาต

4) กลุ่มอาชญากรและผู้ก่อการร้ายจะใช้เทคโนโลยีคอมพิวเตอร์ในกิจการของกลุ่มเพิ่มมากขึ้น

4. กระบวนการการจัดการความรู้

การวิจัยครั้งนี้ เป็นการจัดการความรู้โดยการเก็บรวบรวมข้อมูลที่กระจัดกระจายอยู่ในรูปของเอกสาร สถิติต่าง ๆ คำพิพากษาคดี สำนวนการสอบสวน กระบวนการสืบสวน การรวบรวมพยานหลักฐานและพิสูจน์หลักฐานดิจิตอล รูปแบบที่ดี (Best Practice) รูปแบบที่ไม่ดี (Bad Practice) โดยผ่านกระบวนการแลกเปลี่ยนเรียนรู้ (Storytelling) โดยจัดเวทีให้กลุ่มเป้าหมายได้แลกเปลี่ยนความรู้ ประสบการณ์ ความคิดเห็นและเข้าร่วมกิจกรรม AAR (After Action Review) การสัมภาษณ์แบบเจาะลึก (Indepth Interview) รวมทั้งการสนทนากลุ่มย่อย (Focus Group Discussion) หลังจากนั้นผู้วิจัยนำข้อค้นพบที่ได้รับมาถอดบทเรียน

โดยนำแนวคิด ทฤษฎีที่เกี่ยวข้อง คือ แนวคิดการวิเคราะห์ SWOT แนวคิดการวิเคราะห์ระบบ (System Analysis) มีรายละเอียดโดยสรุป ดังนี้

1) กิจกรรมการเล่าเรื่อง (Storytelling)
2) การทบทวนหลังกิจกรรม (AAR - After Action Review)
3) การสัมภาษณ์แบบเจาะลึก (In-depth Interview)
4) การสนทนากลุ่มย่อย (Focus Group Discussion)
5) การวิเคราะห์ SWOT (SWOT Analysis)
6) การวิเคราะห์ระบบ (System Analysis)

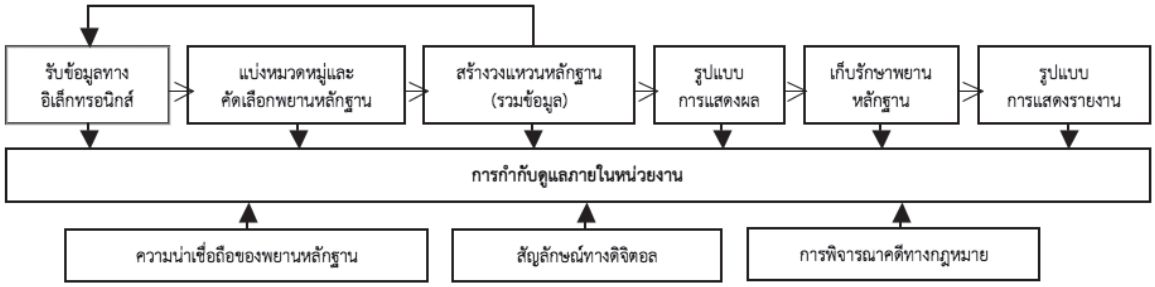
งานวิจัยที่เกี่ยวข้อง

สินเลิศ สุขุม (2543) ได้ทำการศึกษาวิจัยเรื่อง ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ผลการวิจัยพบว่า ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ ได้แก่ ปัจจัยในด้านระยะเวลาในการทำงานเกี่ยวข้องกับคอมพิวเตอร์ และความสามารถเกี่ยวกับการใช้คอมพิวเตอร์

นัยนรัตน์ งานแสง (2547) ได้ทำการศึกษาวิจัยเรื่อง อาชญากรรมคอมพิวเตอร์ : ศึกษาเฉพาะกรณีปัจจัยที่มีผลต่อการเกิดปัญหาอาชญากรรมอินเทอร์เน็ต ผลการศึกษาพบว่า ปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มขึ้นเนื่องจากการขยายตัวของประชากรอินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้อินเทอร์เน็ตในสังคมไทย ยังขาดความรู้ความเข้าใจ และการปลูกฝังด้านจริยธรรมและวัฒนธรรมการใช้งานเทคโนโลยีเชิงสร้างสรรค์ ทำให้เกิดปัญหาการนำเทคโนโลยีไปใช้ในทางมิชอบตามมาส่วนบุคลากรที่มีความรู้ความสามารถด้านการรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายของประเทศไทยมีจำนวนจำกัด รวมทั้งภาครัฐไม่มีนโยบายและองค์กรเกี่ยวกับการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์โดยตรง ประกอบกับปัญหาทางด้านกฎหมาย

นารี กิตติสมบูรณ์สุข (2548) ได้ทำการศึกษาวิจัยเรื่อง การแสวงหาพยานหลักฐานที่เป็นข้อมูลส่วนบุคคลจากข้อมูลอิเล็กทรอนิกส์ในอาชญากรรมคอมพิวเตอร์ พบว่า อาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่ร้ายแรงเป็นภัยต่อสังคมรูปแบบหนึ่งที่ก่อให้เกิดความเสียหายแก่ระบบเศรษฐกิจเป็นอย่างมาก แทบทุกประเทศต่างก็เล็งเห็นถึงอันตรายจากอาชญากรรมประเภทนี้ และผลกระทบที่เกิดกับกฎหมายอาญาของประเทศต่าง ๆ ทั่วโลก เนื่องจากกฎหมายอาญาที่ใช้อยู่ไม่เพียงพอที่จะดำเนินคดีกับอาชญากรได้ จึงพยายามหามาตรการทางกฎหมายใหม่ เพื่อค้นหาวิธีการป้องกันและปราบปราม

Guofu Ma และคณะ (2554) ได้ทำการศึกษาวิจัยเรื่อง รูปแบบพื้นฐานวงแหวนหลักฐานและห่วงโซ่หลักฐานของงานทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์ พบว่า คุณลักษณะทั่วไปของพยานหลักฐาน วัตถุประสงค์ ความเกี่ยวข้อง และความถูกต้องของกฎหมาย เพื่อเป็นบรรทัดฐานในการสร้างแบบจำลองของนิติวิทยาศาสตร์คอมพิวเตอร์บนพื้นฐานของวงแหวนและห่วงโซ่ของหลักฐาน ดังแสดงในภาพที่ 1



ภาพ 1 รูปแบบพื้นฐานวงแหวนหลักฐานและห่วงโซ่หลักฐานของงานนิติวิทยาศาสตร์คอมพิวเตอร์

วิธีดำเนินการวิจัย

1. ระเบียบวิธีวิจัย

การวิจัยครั้งนี้เป็นการจัดการความรู้โดยการเก็บรวบรวมข้อมูลที่กระจัดกระจายอยู่ในรูปแบบของเอกสาร สถิติคำพิพากษาคดี สำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งวิธีการรวบรวมพยานหลักฐานและพิสูจน์หลักฐานอาชญากรรมไซเบอร์ และองค์ความรู้ที่อยู่ในตัวบุคคลผู้ปฏิบัติงานมาทำการจัดการความรู้ใหม่อย่างเป็นระบบ โดยการประชุมกลุ่มย่อย (Focus Group) และผ่านเครื่องมือการแลกเปลี่ยนเรียนรู้ (Storytelling) โดยการจัดเวทีให้กลุ่มเป้าหมายได้แลกเปลี่ยนเรียนรู้ ประสบการณ์ ความคิดเห็น โดยเข้าร่วมกิจกรรม AAR (After Action Review) หลังจากนั้นผู้วิจัยจะนำข้อค้นพบมาทำการถอดบทเรียน โดยนำแนวคิดทฤษฎีที่เกี่ยวข้อง คือ แนวคิด การวิเคราะห์ SWOT และแนวคิดการวิเคราะห์ระบบ นอกจากนี้ยังทำการสัมภาษณ์เจาะลึก กลุ่มเป้าหมายที่เป็นตัวแบบที่ดีที่สามารถให้ข้อมูลของแต่ละหน่วยงานที่เกี่ยวข้อง โดยคัดเลือกจากประชากร ซึ่งมี 6 ประเภท ดังนี้

1) ข้าราชการตำรวจ ประกอบด้วย

1.1) เจ้าหน้าที่ตำรวจฝ่ายสืบสวน และสอบสวนจากหน่วยงานในพื้นที่

1.2) เจ้าหน้าที่ตำรวจพิสูจน์หลักฐานเกี่ยวกับอาชญากรรมไซเบอร์

1.3) เจ้าหน้าที่ตำรวจ กองบังคับปราบปรามเทคโนโลยีสารสนเทศ

1.4) เจ้าหน้าที่ตำรวจจากสำนักงานเทคโนโลยีสารสนเทศ และการสื่อสาร

2) เจ้าหน้าที่จากกระทรวงเทคโนโลยีสารสนเทศ

3) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากมหาวิทยาลัย

4) ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมไซเบอร์ทั้งที่มีการพิพากษาลงโทษผู้กระทำผิด และยกฟ้องเนื่องจากพยานหลักฐานไม่พอในชั้นศาล

5) อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมไซเบอร์ทั้งที่มีการพิพากษาลงโทษผู้กระทำผิด และยกฟ้องเนื่องจากพยานหลักฐานไม่พอในชั้นศาล

6) ประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ โดยพิจารณาจากสำนวนการสอบสวนของพนักงานสอบสวนที่เป็นรูปแบบที่ดี (Best Practice) และรูปแบบที่ไม่ดี (Bad Practice) (สอดคล้องกับประเภทของอาชญากรรมไซเบอร์)

2. เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการดำเนินการวิจัยครั้งนี้ คือ การแลกเปลี่ยนเรียนรู้ (Storytelling) โดยมีการประชุมคณะวิจัยและทีมงานเพื่อมอบหมายหน้าที่การงานและกำหนดการดำเนินการวิจัยตลอดโครงการ

และนำเสนอผลการวิจัยโดยเป็นผู้ทรงคุณวุฒิ เข้าร่วมพิจารณา และให้ข้อเสนอแนะการดำเนินงานวิจัย ดังนี้

(1) จัดเวทีแลกเปลี่ยนเรียนรู้ที่กรุงเทพมหานครและปริมณฑล ครั้งที่ 1 โดยเชิญกลุ่มเป้าหมายที่มีความรู้ ประสบการณ์ และความเชี่ยวชาญทางด้านกฎหมาย การทำสำนวนการสอบสวน รายงานการสืบสวน การรวบรวมพยานหลักฐานและพิสูจน์หลักฐานดิจิตอล ภัยบนอินเตอร์เน็ต และรูปแบบการกระทำผิดทางด้านอาชญากรรมไซเบอร์ จากหน่วยงานที่เกี่ยวข้องในเขตกรุงเทพมหานคร เป็นตัวแทน

(2) จัดเวทีแลกเปลี่ยนเรียนรู้ครั้งที่ 2 ที่กรุงเทพมหานคร โดยเชิญผู้ทรงคุณวุฒิทางด้านอาชญากรรมไซเบอร์และด้านการวิจัยเข้าร่วมพิจารณาและให้ข้อเสนอแนะการดำเนินงานวิจัย

3. การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ คณะผู้วิจัยจะดำเนินการบันทึกเทป บันทึกวิดีโอ จดบันทึก สังเกต และถ่ายภาพการแลกเปลี่ยนเรียนรู้ (Storytelling) ทุกครั้ง จากนั้นจึงนำข้อค้นพบมาทำการถอดบทเรียน เรียบเรียงและวิเคราะห์ข้อมูลตามวัตถุประสงค์ และผลที่จะได้รับ และนำมาตรวจทานอีกครั้ง เพื่อรวบรวมองค์ความรู้ที่ได้ในแต่ละครั้ง เมื่อได้ข้อมูลที่ถอดบทเรียนในแต่ละครั้ง คณะผู้วิจัยจะทำการประชุมนักวิจัยเพื่อนำเสนอผลการจัดกิจกรรม และจัดการความรู้ในแต่ละครั้ง และเชิญผู้ทรงคุณวุฒิเข้าร่วมวิพากษ์แสดงความคิดเห็น และให้ข้อเสนอแนะ ที่มีประโยชน์ต่อการวิจัย

4. การวิเคราะห์ข้อมูล

คณะผู้วิจัยจะทำการประมวลผลและวิเคราะห์ข้อมูล โดยใช้เทคนิคการวิเคราะห์ข้อมูลแบบเนื้อหา (Content Analysis) เพื่อกำหนดหัวข้อ กลุ่มหัวข้อแนวคิดที่สำคัญ (Topic /Category) และแบบแผนแนวคิดสำคัญอันเป็นแก่นสารของการวิจัย (Pattern/Themes) เพื่อถอดบทเรียน ข้อค้นพบจากเวทีการแลกเปลี่ยนเรียนรู้ และนำมาวิเคราะห์ให้อยู่ในรูปแบบการพรรณนา ตาราง แผนภูมิ และรูปภาพ เพื่อให้เกิดระบบ และองค์ความรู้ได้มากยิ่งขึ้น

ผลการวิจัย

1. สภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย สามารถสรุปได้ดังนี้

1) ปัญหาด้านข้อกฎหมาย - ฐานความผิด - เขตอำนาจ - ใครต้องเป็นผู้รับผิด - ลักษณะพยาน

2) ปัญหาด้านเทคนิค - เทคนิคพัฒนาต่อเนื่อง - การศึกษา - เทคนิคในการเก็บหลักฐาน

3) แนวทางการปฏิบัติ - การประสานแนวทางปฏิบัติ ระหว่าง - ตำรวจ - อัยการ - ศาล

4) วัฒนธรรม - วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ

แนวทางแก้ไขปัญหา

1) กำหนดกฎหมายอาชญากรรมทางคอมพิวเตอร์ ที่มีบทบัญญัติเกี่ยวกับการบุกรุกทางเครือข่ายทั้งจากภายในและภายนอกประเทศ

2) จัดตั้ง กองบังคับการสืบสวนอาชญากรรมทางคอมพิวเตอร์ ในสังกัดสำนักงานตำรวจแห่งชาติ และ ศูนย์รักษาความปลอดภัยข้อมูลในเครือข่าย (Thai CERT) ในสังกัดของ NECTEC เพื่อเป็นแหล่งศึกษา วิจัย ติดตามเทคนิค รวบรวม กรรมวิธีการ HACK และแนวทางป้องกัน ตลอดจนการสืบสวนติดตามผู้กระทำผิด รวมทั้งการจัดเก็บประวัติ Hacker ต่าง ๆ ไว้และการประสานงานกับหน่วยงานที่เกี่ยวข้องทั้งในและนอกประเทศ

3) รวบรวม รายชื่อและที่ติดต่อของ บุคลากร ผู้เชี่ยวชาญ ทางด้านนี้ ทั้งในและต่างประเทศ เพื่อประโยชน์ในการประสานงาน ขอคำแนะนำ ช่วยเหลือ ในกรณีเกิดเหตุวิกฤติ

4) กำหนดแผนสำรอง กรณีระบบเครือข่ายหลักของประเทศ ไม่สามารถใช้งานได้

5) เผยแพร่ประชาสัมพันธ์ ให้ความรู้แก่ บุคคลทั่วไปให้ตระหนักถึงภัยที่อาจเกิดขึ้น รวมทั้งการเผยแพร่ความรู้เพื่อให้ทราบถึงแนวทางการป้องกัน

2. กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์

2.1 กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ ดังนี้

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

2) พ.ร.บ.ที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เพื่อรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้เสมอด้วยกระดาษ อันเป็นการรองรับนิติสัมพันธ์ต่าง ๆ 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

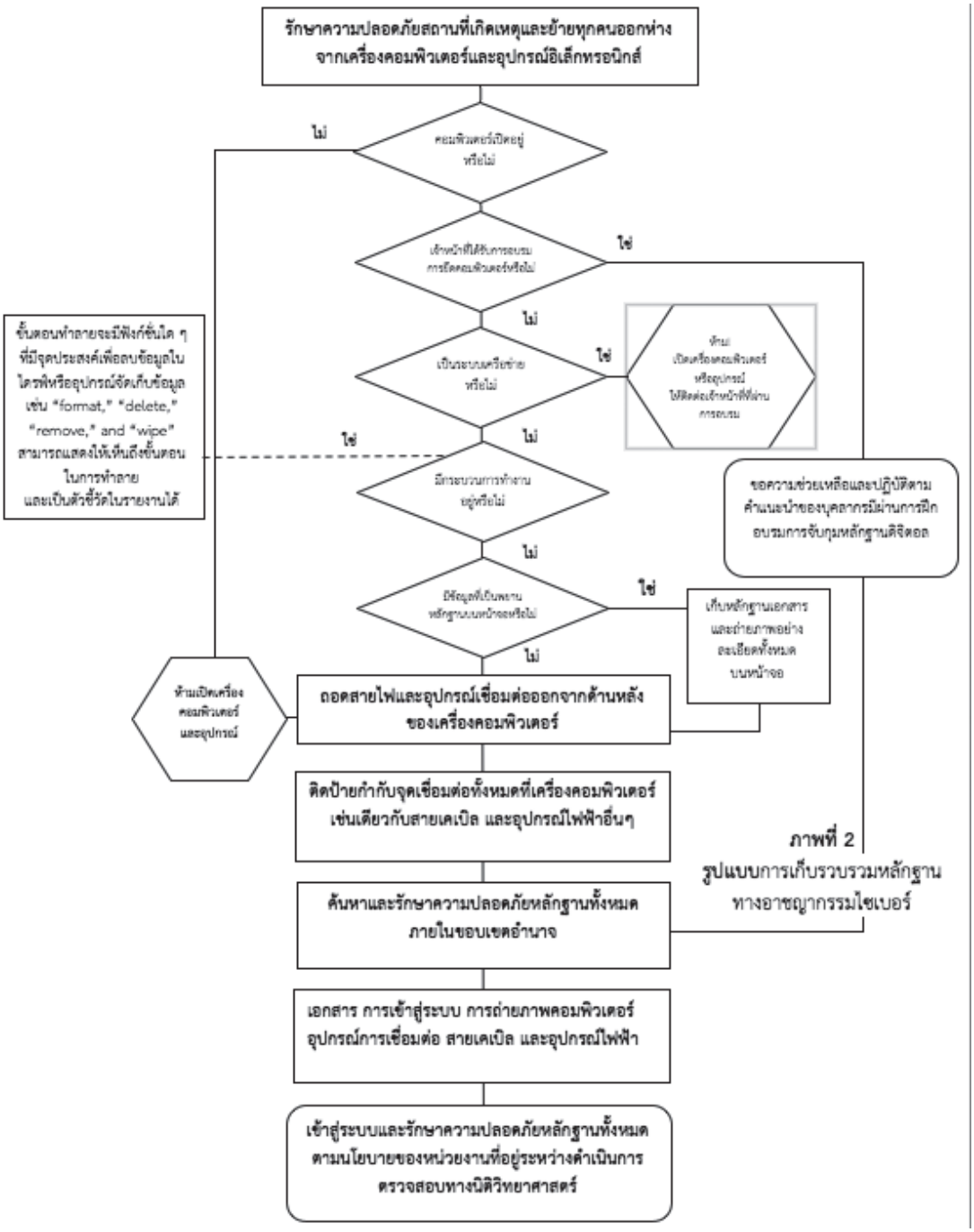
2.2 ระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์

เนื่องจากกฎหมายของแต่ละประเทศในเรื่องของการนำเสนอหลักฐานนั้นมีความแตกต่างกัน จึงได้มีการกำหนดกฎของการนำหลักฐานดิจิตอลไปใช้ในชั้นศาล ซึ่งเป็นกฎที่มีการคิดค้นและพัฒนาในต่างประเทศจนได้รับการยอมรับมากที่สุด ซึ่งมีด้วยกันทั้งหมด 4 ข้อ ดังนี้

1) ความสมบูรณ์ของหลักฐาน (Preservation)
2) ระบุที่มาของหลักฐานได้ (Identification)
3) บุคคลผู้ที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ (Providing Expert)
4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย (Rules Of Evidence)

3. รูปแบบและมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์

3.1 รูปแบบการเก็บรวบรวมหลักฐานทางอาชญากรรมไซเบอร์



ภาพที่ 2
รูปแบบการเก็บรวบรวมหลักฐานทางอาชญากรรมไซเบอร์

3.2 มาตรการในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมไซเบอร์

3.2.1 มาตรการในเชิงบริหาร

1) เร่งออกกฎหมายอาชญากรรมทางคอมพิวเตอร์ รวมทั้งระเบียบปฏิบัติที่เกี่ยวข้อง

2) กำหนดกลุ่ม ผู้พิพากษา หรือจัดตั้งศาล IT ขึ้นมาเพื่อให้พิจารณาคดีความด้าน IT เป็นการเฉพาะ เช่นเดียวกับ ศาลทรัพย์สินทางปัญญา

3) กำหนดกลุ่ม พนักงานอัยการ หรือจัดตั้งอัยการกองพิเศษ ขึ้นมาเพื่อให้พิจารณาคดีความด้าน IT เป็นการเฉพาะ

4) จัดตั้ง กองบังคับการสืบสวนอาชญากรรมไซเบอร์ ในสังกัดสำนักงานตำรวจแห่งชาติ เพื่อให้เป็นหน่วยงานที่คอย ตรวจตรา เฝ้าระวัง ค้นหา การกระทำผิดบนอินเทอร์เน็ตตลอดเวลา 24 ชั่วโมง รวมทั้ง การสืบสวนเฉพาะทางด้านเทคนิค เพื่อได้ทราบถึงแหล่ง ที่มาหรือผู้กระทำผิดแล้วส่งข้อมูลให้หน่วยที่เกี่ยวข้อง สืบสวนสอบสวนต่อไป อีกทั้งควรทำหน้าที่ตรวจพิสูจน์เครื่องคอมพิวเตอร์ของกลาง ค้นหาหลักฐาน เป็นการช่วยเหลือหน่วยปฏิบัติ และมีหน้าที่รับแจ้งเหตุเบื้องต้นจากผู้เสียหาย เพื่อประสานงานกับผู้ที่เกี่ยวข้อง เพื่อจำกัดความเสียหายให้น้อยลงโดยเร็ว และเพื่อเก็บรวบรวมหลักฐานในทันทีก่อนที่จะถูกเปลี่ยนแปลง หรือสูญหายไป

5) จัดตั้ง ศูนย์รักษาความปลอดภัยข้อมูลในเครือข่าย (Thai CERT) ในสังกัดของ NECTEC เพื่อเป็นศูนย์กลางในการประสานงานกับหน่วยงานและผู้เกี่ยวข้อง ทั้งในและต่างประเทศ และเป็นศูนย์รวมความรู้ แนวทางปฏิบัติ เพื่อการป้องกันภัยของข้อมูลในเครือข่าย

6) กสท. กำชับให้ ผู้บริการอินเทอร์เน็ต (ISP) ปฏิบัติตามสัญญาอย่างเคร่งครัด รวมทั้งต้องกำชับให้ ISP กวดขันและกำชับให้ ผู้ให้บริการต่อช่วงของตน ปฏิบัติตามสัญญาอย่างเคร่งครัด

7) กำหนดให้มีช่องทางติดต่อสื่อสารพิเศษ ระหว่าง NECTEC (Thai CERT), ตำรวจ, กสท. ISP และ สถาบันการศึกษาที่ต่อเชื่อมอินเทอร์เน็ตโดยไม่ผ่าน ISP ในประเทศ การสื่อสารดังกล่าวเป็นคล้าย Hot Line ในระดับของผู้ปฏิบัติทางเทคนิค โดยให้แต่ละฝ่ายแจ้ง ชื่อ-นามสกุล, ตำแหน่ง, โทรศัพท์ที่ทำงาน, โทรศัพท์ที่บ้าน, โทรศัพท์มือถือ, เพจเจอร์ และอี-เมล์ เพื่อใช้ในการติดต่อประสานงานได้โดยตรง

8) กำหนดให้ ISP ทุกแห่ง ตั้งเวลาเครื่อง ให้ตรงตามมาตรฐาน

9) สร้างแนวร่วมในหมู่ของผู้ใช้อินเทอร์เน็ต ให้ช่วยกันสอดส่องดูแล และแจ้งเบาะแส หากพบเห็นการกระทำผิดบนอินเทอร์เน็ต ไปยังหน่วยงานที่เกี่ยวข้อง รวมทั้งอาจใช้แนวร่วมนี้เป็นพลังในการต่อต้านสิ่งที่ไม่เหมาะสมบนอินเทอร์เน็ต

3.2.2 มาตรการในทางปฏิบัติ

กรณีเว็บไซต์ผิดกฎหมาย จาบจ้วง เป็นภัยต่อความมั่นคงของชาติ และที่ไม่เหมาะสม

1) ในส่วนของเว็บไซต์ผิดกฎหมายเว็บไซต์จาบจ้วงเว็บไซต์เป็นภัยต่อความมั่นคงของชาติ และเว็บไซต์ที่ไม่เหมาะสมนั้น ควรกำหนดให้ ฝ่ายตำรวจ เป็นศูนย์กลางแจ้งเวียนไปยัง ISP และผู้ดูแลระบบของสถาบันการศึกษา (ที่ไม่ผ่าน ISP ในประเทศ) ทำการปิดกั้นเว็บไซต์ดังกล่าวไม่ให้สามารถเรียกได้จากในประเทศ รวมทั้งแจ้งไปยัง NECTEC (Thai CERT) และ กสท. เพื่อทราบ การแจ้งเวียนดังกล่าวควรใช้ อี-เมล์ ที่ได้ตกลงกันไว้เป็นหลัก โดยจะส่งถึงระดับผู้ บริหารของ ISP และระดับผู้ปฏิบัติ (Admin.)

ของ ISP นั้นด้วย เว้นแต่เป็นกรณีเร่งด่วน อาจใช้โทรศัพท์แจ้งไปก่อน แล้วจึงส่ง อี-เมล์ ตามไปภายหลัง

2) การใช้ อี-เมล์ ในการติดต่อนั้น ควรเป็น อี-เมล์ ที่มีการเข้ารหัสรักษาความปลอดภัยไว้ด้วย หากผู้รับเกิดความสงสัย ให้โทรศัพท์สอบถามกลับไป ตามหมายเลขโทรศัพท์ที่กำหนดไว้ เพื่อเป็นการยืนยันความถูกต้อง

3) เมื่อผู้ปฏิบัติ (Admin.) ของ ISP แต่ละรายรวมทั้งผู้ดูแลระบบของสถาบันการศึกษาฯ ได้รับแจ้งทาง อี-เมล์ ดังกล่าวแล้ว และอาจตรวจสอบแล้วว่า เว็บไซต์ดังกล่าวเข้าข่ายอยู่ในประเภทข้างต้นจริง ก็ให้ดำเนินการปิดกั้นเว็บไซต์นั้นในทันที โดยไม่จำเป็นต้องรอขออนุมัติ จากผู้บริหารของ ISP นั้นก่อน อนึ่งเมื่อได้ดำเนินการปิดกั้นแล้ว ให้ส่ง อี-เมล์ แจ้งให้ฝ่ายตำรวจทราบด้วย

4) ภายใน 3 วันทำการ นับจากได้มีการแจ้งให้ปิดกั้นเว็บไซต์นั้นแล้ว แต่ ISP นั้นยังไม่ดำเนินการให้ฝ่ายตำรวจทำเป็นหนังสือราชการ และส่ง อี-เมล์ แจ้งไปยังผู้บริหาร ISP นั้นทราบอีกครั้ง และสำเนาแจ้งให้ กสท. และ NECTEC ทราบ หากภายใน 15 วัน (นับแต่การแจ้งให้ทราบครั้งแรก) ISP นั้นยังไม่ดำเนินการ โดยไม่มีเหตุผลชี้แจง ให้ กสท.ดำเนินการตามที่สัญญาได้กำหนดไว้ และให้ NECTEC ดำเนินการปลดสายสัญญาณของ ISP นั้นออกจาก PIE หรือระบบอื่นๆ

5) หากเว็บไซต์ดังกล่าว ใช้ Server ในประเทศที่อยู่ในความรับผิดชอบของ ISP ใด หรือของผู้ให้บริการเช่าช่วงต่อจาก ISP ใด ให้ ISP นั้นยุติการให้บริการในทันที แล้วให้ส่งข้อมูลของผู้เช่าพื้นที่ใน Server นั้นให้ฝ่ายตำรวจทราบ มิฉะนั้นอาจถือได้ว่าเป็นผู้ร่วมกระทำความผิดด้วย

6) ในกรณีของ เว็บไซต์จาบจ้วง เว็บไซต์เป็นภัยต่อความมั่นคงของชาติ และเว็บไซต์ที่ไม่เหมาะสมลบหลู่ศาสนา อาจขอความร่วมมือไปยังกลุ่มแนวร่วมผู้ใช้อินเทอร์เน็ต ผู้รักชาติให้ช่วยกันต่อต้านและประนามเว็บไซต์ดังกล่าวได้อีกทางหนึ่ง

ข้อเสนอแนะ

1. ข้อเสนอแนะในการนำผลการศึกษาไปใช้

1) อาชญากรรมไซเบอร์มีรูปแบบต่าง ๆ และเปลี่ยนแปลงไปตามสถานการณ์ และคิดค้นรูปแบบไปเรื่อย ๆ ในรูปแบบ และการแก้ไขปัญหานั้น จึงต้องมีการพัฒนาตามไปเรื่อย ๆ วิธีการ และรูปแบบเดิม ๆ อาจจะใช้ไม่ได้ในบางครั้ง และเป็นพยานหลักฐานที่อ่อน ทำให้เกิดปัญหาทางคดีได้ ควรจะเริ่มต้นที่ตัวผู้ใช้บังคับกฎหมายก่อนเป็นอันดับแรก และเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้ได้รับความรู้ที่ตรงต่อเป้าหมาย เพราะบางหน่วยงานอาจจะมีการโยกย้าย สับเปลี่ยนตำแหน่ง อาจจะทำให้ยังไม่มีความรู้เกี่ยวกับเรื่องคอมพิวเตอร์มากนัก จึงทำงานไม่สะดวก และมีประสิทธิภาพไม่เต็มที่ ดังนั้นการแต่งตั้งโยกย้ายผู้ปฏิบัติงานที่มีความชำนาญหน่วยงานที่เกี่ยวข้องต้องคำนึงถึงเรื่องนี้ด้วย

2) พนักงานสอบสวน รวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติหน้าที่ ยังขาดความรู้ความเข้าใจในเรื่องของระบบคอมพิวเตอร์ และระบบอินเทอร์เน็ต เมื่อผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที เพราะไม่ทราบถึงกระบวนการในการทำงานที่เกิดขึ้น จึงควรมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยี อาชญากรรมไซเบอร์ และกฎหมายที่เกี่ยวข้องแก่พนักงานสอบสวนทั่วประเทศ โดยเฉพาะประเด็นการตั้งคำถามของพนักงานสอบสวน เป็นเพราะขาดความรู้ทำให้ตั้งคำถามอย่างไม่มีทิศทาง

3) พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐาน ในหลายกรณีไม่มีความน่าเชื่อถือ เนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of custody) ซึ่งเป็นการพิสูจน์ความเชื่อมโยงของพยานหลักฐานกับการกระทำความผิด ดังนั้น หน่วยงานที่เกี่ยวข้องจะต้องมีระเบียบข้อบังคับที่ชัดเจนในการบันทึกหลักฐานตามลำดับเวลา เพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้น ๆ หากขาดการต่อเนื่องของการครอบครองวัตถุพยานเมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือในชั้นศาล

4) หน่วยงานที่เกี่ยวข้องควรจัดตั้งงบประมาณในการจัดซื้อวัสดุอุปกรณ์ในการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับคดีทางด้านอาชญากรรมทางไซเบอร์ที่มีความทันสมัย ใช้เวลาในการตรวจพิสูจน์น้อย เคลื่อนย้ายได้ง่าย และให้ผลการตรวจพิสูจน์ที่ถูกต้อง แน่นอน เพื่อลดระยะเวลาและปริมาณงาน

5) การก่ออาชญากรรมของผู้กระทำความผิดส่วนใหญ่อุปกรณ์ที่ใช้อันดับต้น ๆ คือ โทรศัพท์มือถือ ซึ่งคนร้ายจะใช้ติดต่อสื่อสาร ดังนั้นรัฐบาลควรมีนโยบายให้มีการลงทะเบียนหมายเลขโทรศัพท์มือถือทุกหมายเลขทันทีที่เปิดใช้บริการให้เหมือนกับการปฏิบัติในพื้นที่สามจังหวัดชายแดนภาคใต้

6) หน่วยงานที่เกี่ยวข้องควรสร้างความสัมพันธ์กับต่างประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีที่รวดเร็วกว่าประเทศไทย และทำการเปิดเครือข่ายกับต่างประเทศให้มากที่สุดทั้งทางยุโรป และอเมริกา เพื่อร่วมกันแก้ไขปัญหาอาชญากรรมไซเบอร์

7) หน่วยงานที่เกี่ยวข้องควรสร้างความตระหนัก (Awareness) คือ การสังเกตการณ์กระทำความผิดที่เกิดขึ้น หรืออาจเกิดขึ้น ในสังคม หรือลักษณะความผิดที่เคยเกิดขึ้นในประเทศอื่น มาเป็นบทเรียนให้ศึกษา ทำความเข้าใจ และเผยแพร่ความรู้ในการป้องกันแก้ไขปัญหาให้แก่ประชาชน และเจ้าหน้าที่ในกระบวนการยุติธรรม

8) หน่วยงานที่เกี่ยวข้องควรมีการตรวจสอบ (Audit) คือ การใช้มาตรการต่าง ๆ ที่มีอยู่แล้วไปสอดส่องดูแลผู้ให้บริการประเภทต่าง ๆ และผู้ใช้บริการ ก่อนเกิดการกระทำความผิด เพื่อป้องกันอาชญากร

9) หน่วยงานที่เกี่ยวข้องควรมีการวิเคราะห์ (Analysis) คือ การศึกษารูปแบบการกระทำความผิดที่เกิดขึ้น อย่างเป็นระบบ ร่วมกัน ทั้งผู้เสียหาย ผู้ให้บริการ และเจ้าหน้าที่ในกระบวนการยุติธรรม เพื่อหาทางแก้ไขปัญหา และดำเนินคดีอย่างมีประสิทธิภาพ

10) หน่วยงานที่เกี่ยวข้องควรสร้างเครือข่ายพันธมิตร (Alliance) คือ การประสานงานให้ความช่วยเหลือ ร่วมมือกันทั้งภาครัฐ และเอกชน ทั้งต่างองค์กร และภายในแต่ละองค์กร ซึ่งจะช่วยให้การรวบรวมพยานหลักฐาน ข้อเท็จจริงต่าง ๆ ที่ยุ่งยากซับซ้อน และกระจายอยู่ในองค์กรต่าง ๆ สามารถทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยการประสานงานความร่วมมืออย่างเป็นระบบ เช่น การผลักดันอย่างโดดเด่นและเป็นรูปธรรมชัดเจน โดยในประเทศสหรัฐอเมริกา ได้ใช้ชื่อความร่วมมือในลักษณะนี้ว่า Task Force

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป

1) ควรศึกษารูปแบบและมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ในส่วนภูมิภาคอื่น ๆ เพราะมิติของอาชญากรรมไซเบอร์ในแต่ละภูมิภาคอาจจะไม่เหมือนกัน จะทำให้ได้รูปแบบและวิธีการอื่นที่นำมาใช้ในการพัฒนา และแก้ไขปัญหาอาชญากรรมไซเบอร์มีมากยิ่งขึ้น โดยเฉพาะการศึกษาอาชญากรรมไซเบอร์ในต่างประเทศ จะทำให้การพัฒนาในเรื่องรูปแบบและมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ มีความทันสมัยอยู่ตลอดเวลา

2) เจ้าหน้าที่ของรัฐที่ปฏิบัติงานทางด้านการแก้ไขปัญหาอาชญากรรมไซเบอร์ และการตรวจพิสูจน์หลักฐานทางด้านอาชญากรรมไซเบอร์ จะต้องมีการพัฒนาการปฏิบัติงานให้มีความเท่าเทียม และมีความก้าวหน้ามากกว่าอาชญากร โดยเฉพาะความสนใจในการศึกษางานวิจัยของต่างประเทศ ที่มีความก้าวหน้าในรูปแบบของการแก้ไขปัญหาอาชญากรรมไซเบอร์ การศึกษาหาความรู้ และผลการศึกษาวิจัยที่เกี่ยวข้องจะเป็นประโยชน์ต้องการปฏิบัติงานได้อย่างจริงจัง และเป็นรูปธรรมมากยิ่งขึ้น เพราะการศึกษาวิจัยเป็นเรื่องที่มีความสำคัญมาก รวมทั้งให้ความสนใจต่อวิวัฒนาการของเทคโนโลยีมีความเจริญ และสลับซับซ้อนมากยิ่งขึ้น

เอกสารอ้างอิง

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

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

สินเลิศ สุขุม. (2543). **ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ.** ปริญญาสังคมวิทยามหาบัณฑิต จุฬาลงกรณ์มหาวิทยาลัย

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.