การศึกษากระบวนการระบบพิสูจน์หลักฐานอาชญากรรมไซเบอร์

Study of process scientific crime detection system cyber crime

ณิช วงศ์ส่องจ้า*

บทคัดย่อ

การวิจัยเรื่อง การศึกษากระบวนการระบบพิสูจน์หลักฐานอาชญากรรมไซเบอร์ มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์ปัจจัยที่ส่งผลต่อประสิทธิภาพการพิสูจน์หลักฐาน และเพื่อพัฒนาองค์ความรู้เพื่ออธิบายประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย การวิจัยครั้งนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Methodology) และระเบียบวิธีวิจัยเชิงปริมาณ (Quantitative Methodology)

ผลการวิจัยพบว่า

1. ปัจจัยที่ส่งผลต่อประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทยสามารถแบ่งเป็นประเด็นสำคัญ คือ

1) ปัจจัยด้านข้อกฎหมาย-ฐานความผิด-เขตอำนาจ-ใครต้องเป็นผู้รับผิด-ลักษณะพยาน

2) ปัจจัยด้านเทคนิค -เทคนิคพัฒนาต่อเนื่อง-การศึกษา-เทคนิคในการเก็บหลักฐาน

3) ปัจจัยด้านแนวทางการปฏิบัติ-การประสานแนวทางปฏิบัติระหว่าง-ตำรวจ-อัยการ-ศาล

4) ปัจจัยด้านวัฒนธรรม–วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ

2. องค์ความรู้เพื่ออธิบายประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย คือ กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ที่สำคัญ เช่น พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติที่ว่าด้วยการทำธุรกรรมทางเล็กทรอนิกส์ พ.ศ.2544 และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น และกำหนดกฎของระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ 4 ข้อ ได้แก่ 1) ความสมบูรณ์ของหลักฐาน 2) ระบุที่มาของหลักฐานได้ 3) บุคคลที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ และ 4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย

คำสำคัญ : ระบบพิสูจน์หลักฐาน, อาชญากรรมไซเบอร์

.....

*บัณฑิตศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิตและวิทยาศาสตรมหาบัณฑิต สาขานิติวิทยาศาสตร์
มหาวิทยาลัยราชภัฏสวนสุนันทา

Abstract

The Research topic of Study of process scientific crime detection system cyber crime. There is an objective to analyze the factors affecting the efficiency and to development of knowledge to explain the efficiency of cyber crime in Thailand. This Research by the methodology of qualitative and quantitative research.

The research results were as follow :

1. Factors affecting the efficiency of cyber crime in Thailand can divided are:

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

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

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

4) Culture- aculture that is different in each country.

2. Development of knowledge to explain the efficiency of cyber crime in Thailand. The laws relating to cyber crime as Computer-related Crime Act B.E. 2550. Electronic Transactions Act B.E. 2544. And Electronic Signatures Law etc. And Rules of Forensic Cyber Crime 4 items are Preservation, Identification, Providing Expert and Rules of Evidence.

Keywords : Scientific Crime Detection System, Cyber Crime

1. หลักการและเหตุผล

จากการเจริญเติบโตอย่างรวดเร็วของเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีแนวโน้มจะขยายตัวต่อไปอีกเรื่อย ๆ ได้นำมาซึ่งความสะดวกสบายความรวดเร็วฉับไว ส่งผลให้ชีวิตประจำวันของผู้คนในยุคเทคโนโลยีสารสนเทศง่ายขึ้น แต่อย่างไรก็ตามนอกจากประโยชน์มหาศาลที่ผู้ใช้ได้รับจากเทคโนโลยีอันทันสมัยนี้ สิ่งที่แฝงมาด้วยคือภัยร้ายที่อาจคุกคามชีวิตและทำให้สูญเสียทรัพย์สินเงินทองได้อย่างง่ายดายอีกด้วย

ปัจจุบันมีหน่วยงานของต่างประเทศหลายหน่วยงานที่ทำการสำรวจข้อมูลสถิติเกี่ยวกับความเสียหายที่เกิดขึ้นจากอาชญากรรมไซเบอร์ เช่น CSI, IPRI ส่วนหน่วยงานของไทยที่ทำหน้าที่เก็บรวบรวมสถิติทางด้านอาชญากรรมไซเบอร์ ได้แก่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย หรือ ไทยเซิร์ท หน่วยงานเทคโนโลยีเพื่อความมั่นคงของประเทศ สังกัดศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือ เนคเทค ภายใต้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจากรายงานการสำรวจความเสียหายที่เกิดขึ้นของ CSI ประเทศสหรัฐอเมริกา พบว่าความเสียหายที่เกิดขึ้นจากการขโมยข้อมูลทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมาคือ การฉ้อโกงทางคอมพิวเตอร์และการปล่อยไวรัสตามลำดับ ในขณะที่ AusCert ประเทศ ออสเตรเลีย ได้ทำการสำรวจความเสียหายที่เกิดจากการก่ออาชญากรรมไซเบอร์ พบว่า ความเสียหายที่เกิดขึ้นจากการขโมยข้อมูล

ทางคอมพิวเตอร์มีมูลค่าสูงที่สุด รองลงมาคือการปล่อยไวรัสและการเข้าถึงอินเทอร์เน็ตหรือเมล์โดยไม่ได้รับ อนุญาตจากคนในองค์กรตามลำดับ (ศูนย์พัฒนาทักษะและการเรียนรู้ ICT แม่ฮ่องสอน, 2557)

จากผลสำรวจปี พ.ศ. 2553 อาชญากรรมออนไลน์ของนอร์ตันระบุว่า มากกว่า 2 ใน 3 ของผู้ใช้อินเทอร์เน็ต ซึ่งเป็นวัยผู้ใหญ่ประมาณร้อยละ 69 ตกเป็นเหยื่อของอาชญากรรมออนไลน์ถึง 14 คนต่อวินาที ส่งผลให้มีเหยื่ออาชญากรรมออนไลน์มากกว่า 1 ล้านคน ทุกวัน ทั้งนี้ ผลสำรวจเกี่ยวกับการป้องกันภัยคุกคามบนอินเทอร์เน็ต ฉบับที่ 16 รายงานว่า จำนวนของอุปกรณ์สื่อสารไร้สายที่มีความเสี่ยงต่อภัยคุกคามออนไลน์เพิ่มขึ้นกว่าร้อยละ 42 ในปี พ.ศ. 2553 เมื่อเปรียบเทียบกับปี พ.ศ. 2552 นับเป็นสัญญาณเตือนว่าอาชญากรออนไลน์กำลังพุ่งความสนใจและเป้าหมายมายัง อุปกรณ์สื่อสารไร้สาย โดยรายงานจำนวนระบบปฏิบัติการของอุปกรณ์สื่อสารไร้สายใหม่ ๆ ที่ได้รับภัยคุกคามเพิ่มขึ้นจาก 115 ชนิด ในปี พ.ศ. 2552 เป็น 163 ชนิด ในปี พ.ศ. 2553 (Happyman Natchy, 2557)

ผลสำรวจเกี่ยวกับการป้องกันภัยคุกคามบนอินเทอร์เน็ตฉบับที่ 16 ของนอร์ตัน พบว่ามีซอฟต์แวร์แปลกปลอมที่มีเอกลักษณ์และมีความหลากหลายกว่า 286 ล้านชนิด จากปี พ.ศ. 2552 ที่มีเพียง 240 ล้านชนิด คิดเป็นอัตราเพิ่มขึ้นร้อยละ 19 อย่างไรก็ตาม จากจำนวนผู้ตอบแบบสอบถามพบว่า มีผู้ใช้อินเทอร์เน็ตผ่านโทรศัพท์เคลื่อนที่เพียงร้อยละ 16 ที่ติดตั้งระบบรักษาความปลอดภัยบนโทรศัพท์เคลื่อนที่ที่อัพเดทล่าสุด (นุชนาฎ ฟ้าแสงสรรค์, 2554)

ปัญหาทางด้านอาชญากรรมไซเบอร์มีปัญหาอยู่หลายประการ เช่น โครงสร้างทางกฎหมายทำให้เกิดปัญหาด้านการสืบสวนสอบสวนทางด้านอาชญากรรมไซเบอร์ กฎหมายและความรู้ของพนักงานสอบสวน ตลอดจนการรวบรวมพยานหลักฐาน และพิสูจน์หลักฐานดิจิตอล ยังก้าวไปไม่ทันต่อการกระทำผิดทางด้านอาชญากรรมไซเบอร์ เพราะปัจจุบันวิวัฒนาการของการกระทำผิดดังกล่าวก้าวไปไกลมาก เนื่องจากความเจริญก้าวหน้าทางเทคโนโลยีและสารสนเทศ ซึ่งเป็นลักษณะของโลกไร้พรมแดน (Globalization) ความรู้ทางด้านอาชญากรรมไซเบอร์ของเจ้าหน้าที่รัฐยังมีน้อย การศึกษา การค้นหา การเก็บรวบรวมพยานหลักฐาน และระบบพิสูจน์หลักฐาน เป็นอีกเรื่องหนึ่งที่เจ้าหน้าที่รัฐยังไม่มีความรู้เพียงพอ การหาแนวทางและวิธีการตรวจพิสูจน์ให้มีวิธีการที่ทันสมัยมากยิ่งขึ้น เป็นเรื่องที่ต้องดำเนินการ

จากความเป็นมาดังกล่าวข้างต้น ผู้วิจัยมีความสนใจที่จะทำการศึกษากระบวนการระบบพิสูจน์หลักฐานอาชญากรรมไซเบอร์ โดยศึกษาจากเอกสาร งานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ รวมทั้งจากประสบการณ์ของผู้ปฏิบัติงานทางด้านอาชญากรรมไซเบอร์ ในแต่ละหน่วยงาน เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยนำเข้า กระบวนการ ผลลัพธ์ รวมทั้งรูปแบบที่ดี (Best Practice) ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะของระบบพิสูจน์หลักฐานอาชญากรรมไซเบอร์เพื่อนำมาพัฒนางาน รวมทั้งใช้แบบสอบถามกับผู้ที่ปฏิบัติงานที่เกี่ยวข้องกับงานทางด้านดังกล่าว เพื่อนำผลการวิจัยที่ได้ไปเป็นองค์ความรู้ในการแก้ปัญหาอาชญากรรมไซเบอร์

2. วัตถุประสงค์

2.1 เพื่อศึกษาวิเคราะห์ปัจจัยที่ส่งผลต่อประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย

2.2 เพื่อพัฒนาองค์ความรู้เพื่ออธิบายประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย

3. ระเบียบวิธีวิจัย

ในการวิจัยครั้งนี้ ผู้วิจัยใช้แนวทางการวิจัยแบบผสมผสาน ระหว่างการวิจัยเชิงคุณภาพ (Qualitative Research) และการวิจัยเชิงปริมาณ (Quantitative Research) โดยทำการศึกษาควบคู่กันไป ดังนี้

3.1 การวิจัยในแนวทางเชิงคุณภาพ (Qualitative Research)

ผู้วิจัยได้ทำการเก็บข้อมูลเชิงลึกกับกลุ่มตัวอย่าง ผลที่ได้จากการวิเคราะห์ข้อมูลเพื่อสนับสนุนการวิจัยเชิงปริมาณ ผู้วิจัยได้กำหนดวิธีการวิจัยที่จะนำมาใช้ในการวิจัยครั้งนี้ เพื่อให้ได้มา ซึ่งข้อมูลตามวัตถุประสงค์ของการวิจัยที่ถูกต้องและเชื่อถือได้ ประกอบด้วยการค้นคว้าจากเอกสารและบทความทางวิชาการที่เกี่ยวข้องจากหลายแห่ง โดยผู้วิจัยคัดเลือกจากประชากรผู้ที่มีความรู้ และประสบการณ์เกี่ยวกับการทำสำนวนการสอบสวน รายงานการสืบสวน กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมทั้งวิธีการรวบรวมพยานหลักฐานและพิสูจน์หลักฐานอาชญากรรมไซเบอร์ และประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ สอดคล้องกับประเภทของอาชญากรรมไซเบอร์ ซึ่งมี 6 ประเภท รวมประชากรเป้าหมาย ดังนี้

3.1.1 ข้าราชการตำรวจ

3.1.2 เจ้าหน้าที่จากกระทรวงเทคโนโลยีสารสนเทศ

3.1.3 นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากมหาวิทยาลัย

3.1.4 ผู้พิพากษาที่มีประสบการณ์ในการพิจารณาคดีเกี่ยวกับอาชญากรรมไซเบอร์

3.1.5 อัยการที่เคยดำเนินการส่งฟ้องเกี่ยวกับอาชญากรรมไซเบอร์

3.1.6 ประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์

3.2 การวิจัยเชิงปริมาณ (Quantitative Research)

ผู้วิจัยได้ทำการวิจัยเชิงปริมาณโดยมีวัตถุประสงค์ เพื่อทดสอบ และยืนยันแบบจำลองสมการโครงสร้าง และความสัมพันธ์ของตัวแปร โดยการสร้างแบบสอบถาม ซึ่งประกอบด้วยตัวแปรต่าง ๆ ตามกรอบแนวคิดการวิจัยที่ได้จากการทบทวนวรรณกรรม โดยมีการทดสอบคุณภาพของเครื่องมือ ทดสอบความเชื่อมั่นของเครื่องมือ ก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่าง แล้วนำผลที่ได้มาวิเคราะห์ข้อมูลทางสถิติ โดยผู้วิจัยคัดเลือกกลุ่มตัวอย่างทำการศึกษาและเก็บรวบรวมข้อมูลแบบสอบถามจากประชากรซึ่งเป็นพนักงานสอบสวนในเขตพื้นที่กองบังคับการตำรวจนครบาล 1-9 เพราะเป็นพื้นที่ที่มีการกระจายตัวของประชากรอย่างหนาแน่น และมีแนวโน้มทางการเจริญของพื้นที่ในด้านเทคโนโลยีสมัยใหม่ค่อนข้างรวดเร็ว พนักงานสอบสวนของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบัญชาการตำรวจสอบสวนกลาง และเจ้าหน้าที่ของกระทรวงเทคโนโลยีและการสื่อสาร ซึ่งคดีที่เกี่ยวข้องกับอาชาญากรรมไซเบอร์อาจรวมอยู่ในเรื่องการลักทรัพย์ การยักยอกทรัพย์ ความผิดเกี่ยวกับทรัพย์คดีหมิ่นประมาท คดีการเผยแพร่วัตถุที่เป็นลามกอนาจาร

4. ผลการวิจัย

จากการวิจัยศึกษาในแนวทางเชิงคุณภาพ (Qualitative Research) โดยการเก็บข้อมูลเชิงลึกกับกลุ่มตัวอย่างเพื่อให้ได้มาซึ่งข้อมูลตามวัตถุประสงค์ของการวิจัยนั้น พบว่า

4.1 ปัจจัยที่ส่งผลต่อประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย สามารถสรุปได้ดังนี้

4.1.1 ปัญหาด้านข้อกฎหมาย-ฐานความผิด-เขตอำนาจ-ใครต้องเป็นผู้รับผิด-ลักษณะพยาน

4.1.2 ปัญหาด้านเทคนิค -เทคนิคพัฒนาต่อเนื่อง-การศึกษา-เทคนิคในการเก็บหลักฐาน

4.1.3 แนวทางการปฏิบัติ -การประสานแนวทางปฏิบัติ ระหว่าง -ตำรวจ-อัยการ-ศาล

4.1.4 วัฒนธรรม– วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ

โดยมีแนวทางแก้ไขปัญหา ดังนี้

1) กำหนดกฎหมายอาชญากรรมทางคอมพิวเตอร์ ที่มีบทบัญญัติเกี่ยวกับการบุกรุกทางเครือข่ายทั้งจากภายในและภายนอกประเทศ

2) จัดตั้งกองบังคับการสืบสวนอาชญากรรมทางคอมพิวเตอร์ ในสังกัดสำนักงานตำรวจแห่งชาติ และ ศูนย์รักษาความปลอดภัยข้อมูลในเครือข่าย (Thai CERT) ในสังกัดของ NECTEC เพื่อเป็นแหล่งศึกษา วิจัย ติดตามเทคนิค รวบรวม กรรมวิธีการ HACK และแนวทางป้องกัน ตลอดจนการสืบสวนติดตามผู้กระทำผิด รวมทั้งการจัดเก็บประวัติ Hacker ต่าง ๆ ไว้ และการประสานงานกับหน่วยงานที่เกี่ยวข้อง ทั้งในและนอกประเทศ

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

4) กำหนดแผนสำรอง กรณีระบบเครือข่ายหลักของประเทศ ไม่สามารถใช้งานได้

5) เผยแพร่ประชาสัมพันธ์ ให้ความรู้แก่ บุคคลทั่วไปให้ตระหนักถึงภัยที่อาจเกิดขึ้น รวมทั้งการเผยแพร่ความรู้เพื่อให้ทราบถึงแนวทางการป้องกัน

4.2 องค์ความรู้เพื่ออธิบายประสิทธิภาพการพิสูจน์หลักฐานของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย

4.2.1 กฎหมายที่เกี่ยวข้องกับ พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550

4.2.2 ระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์

เนื่องจากกฎหมายของแต่ละประเทศในเรื่องของการนำเสนอหลักฐานนั้น มีความแตกต่างกัน จึงได้มีการกำหนดกฎของการนำหลักฐานดิจิตอลไปใช้ในชั้นศาล ซึ่งเป็นกฎที่มีการคิดค้นและพัฒนาในต่างประเทศจนได้รับการยอมรับมากที่สุด ซึ่งมีด้วยกันทั้งหมด 4 ข้อ ดังนี้

1) ความสมบูรณ์ของหลักฐาน (Preservation)

2) ระบุที่มาของหลักฐานได้ (Identification)

3) บุคคลผู้ที่ดูแลหรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ (Providing Expert)

4) หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย (Rules of Evidence)

5. ข้อเสนอแนะ

5.1 ข้อเสนอแนะในการนำผลการศึกษาไปใช้

5.1.1 อาชญากรรมไซเบอร์มีรูปแบบต่าง ๆ และเปลี่ยนแปลงไปตามสถานการณ์ และคิดค้นรูปแบบไปเรื่อย ๆ ในรูปแบบ จึงต้องมีการพัฒนาตามไปเรื่อย ๆ วิธีการ และรูปแบบเดิม ๆ พยานหลักฐานอาจจะใช้ไม่ได้ในบางครั้ง ทำให้เกิดปัญหาทางคดีได้ ควรจะเริ่มต้นที่ตัวผู้ใช้บังคับกฎหมายก่อนเป็นอันดับแรก และเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้ได้รับความรู้ที่ตรงต่อเป้าหมาย ซึ่งอาจจะทำให้ยังไม่มีความรู้เกี่ยวกับเรื่องคอมพิวเตอร์มากนัก จึงทำงานโดยมีประสิทธิภาพไม่เต็มที่

5.1.2 พนักงานสอบสวน รวมถึงเจ้าหน้าที่สืบสวนที่ปฏิบัติหน้าที่ ยังขาดความรู้ความเข้าใจในเรื่องของระบบคอมพิวเตอร์ และระบบอินเทอร์เน็ต เมื่อผู้เสียหายมาร้องทุกข์ทำให้ไม่สามารถดำเนินการตามกฎหมายได้ในทันที จึงควรมีการฝึกอบรมเพิ่มเติมความรู้ทางเทคโนโลยีอาชญากรรมไซเบอร์ และกฎหมายที่เกี่ยวข้องแก่พนักงานสอบสวนทั่วประเทศ โดยเฉพาะประเด็นการตั้งคำถามของพนักงานสอบสวน เป็นเพราะขาดความรู้ทำให้ตั้งคำถามอย่างไม่มีทิศทาง

5.1.3 พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐาน ในหลายกรณีไม่มีความน่าเชื่อถือ เนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of custody) ซึ่งเป็นการพิสูจน์ความเชื่อมโยงของพยานหลักฐานกับการกระทำความผิด ดังนั้น หน่วยงานที่เกี่ยวข้องจะต้องมีระเบียบข้อบังคับที่ชัดเจนในการบันทึกหลักฐานตามลำดับเวลา เพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้น ๆ หากขาดการต่อเนื่องของการครอบครองวัตถุพยาน เมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือในชั้นศาล

5.1.4 หน่วยงานที่เกี่ยวข้องควรจัดตั้งงบประมาณในการจัดซื้อวัสดุอุปกรณ์ในการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับคดีทางด้านอาชญากรรมทางไซเบอร์ที่มีความทันสมัย และใช้เวลาในการตรวจพิสูจน์น้อย เคลื่อนย้ายได้ง่าย และให้ผลการตรวจพิสูจน์ที่ถูกต้อง แน่นอน เพื่อลดระยะเวลาและปริมาณงาน

5.1.5 การก่ออาชญากรรมของผู้กระทำความผิดส่วนใหญ่อุปกรณ์ที่ใช้อันดับต้น ๆ คือ โทรศัพท์มือถือ ซึ่งคนร้ายจะใช้ติดต่อสื่อสาร ดังนั้น รัฐบาลควรมีนโยบายให้มีการลงทะเบียนหมายเลขโทรศัพท์มือถือทุกหมายเลขทันทีที่เปิดใช้บริการให้เหมือนกับการปฏิบัติในพื้นที่สามจังหวัดชายแดนภาคใต้

5.1.6 หน่วยงานที่เกี่ยวข้องควรสร้างความสัมพันธ์กับต่างประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีที่รวดเร็วกว่าประเทศไทย และทำการเปิดเครือข่ายกับต่างประเทศให้มากที่สุดทั้งทางยุโรป และอเมริกา เพื่อร่วมกันแก้ไขปัญหาอาชญากรรมไซเบอร์

5.1.7 หน่วยงานที่เกี่ยวข้องควรสร้างความตระหนัก คือ การสังเกตการณ์กระทำความผิดที่เกิดขึ้น หรืออาจเกิดขึ้น ในสังคม หรือลักษณะความผิดที่เคยเกิดขึ้นในประเทศอื่น มาเป็นบทเรียนให้ศึกษา ทำความเข้าใจ และเผยแพร่ความรู้ในการป้องกันแก้ไขปัญหาให้แก่ประชาชน และเจ้าหน้าที่ในกระบวนการยุติธรรม

5.1.8 หน่วยงานที่เกี่ยวข้องควรมีการตรวจสอบ คือ การใช้มาตรการต่าง ๆ สอดส่องดูแลผู้ให้บริการประเภทต่าง ๆ และผู้ใช้บริการ ก่อนเกิดการกระทำความผิด เพื่อป้องกันอาชญากร

5.1.9 หน่วยงานที่เกี่ยวข้องควรมีการวิเคราะห์ คือ การศึกษารูปแบบการกระทำความผิดที่เกิดขึ้นอย่างเป็นระบบร่วมกัน ทั้งผู้เสียหาย ผู้ให้บริการ และเจ้าหน้าที่ในกระบวนการยุติธรรม เพื่อหาทางแก้ไขปัญหา และดำเนินคดีอย่างมีประสิทธิภาพ

5.1.10 หน่วยงานที่เกี่ยวข้องควรสร้างเครือข่ายพันธมิตร คือ การประสานงาน ให้ความช่วยเหลือ ร่วมมือกันทั้งภาครัฐ และเอกชน ทั้งต่างองค์กร และภายในแต่ละองค์กร ซึ่งจะช่วยให้การรวบรวมพยานหลักฐาน ข้อเท็จจริงต่าง ๆ ที่ยุ่งยากซับซ้อน และกระจายอยู่ในองค์กรต่าง ๆ สามารถทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น โดยการประสานงานความร่วมมืออย่างเป็นระบบ เช่น การผลักดันอย่าง โดดเด่น และเป็นรูปธรรมชัดเจน

5.2 ข้อเสนอแนะในการวิจัยครั้งต่อไป

5.2.1 ควรศึกษาระบบพิสูจน์หลักฐานอาชญากรรมไซเบอร์ในส่วนภูมิภาคอื่น ๆ เพราะมิติของอาชญากรรมไซเบอร์ในแต่ละภูมิภาคอาจจะไม่เหมือนกัน จะทำให้ได้รูปแบบและวิธีการอื่นที่นำมาใช้ในการพัฒนา และแก้ไขปัญหาอาชญากรรมไซเบอร์มีมากยิ่งขึ้น และมีความทันสมัยอยู่ตลอดเวลา

5.2.2 เจ้าหน้าที่ของรัฐที่ปฏิบัติงานทางด้านการแก้ไขปัญหาอาชญากรรมไซเบอร์ และการตรวจพิสูจน์หลักฐานทางด้านอาชญากรรมไซเบอร์ จะต้องมีการพัฒนาการปฏิบัติงานให้มีความเท่าเทียม และมีความก้าวหน้ามากกว่าอาชญากร โดยเฉพาะความสนใจในการศึกษางานวิจัยของต่างประเทศที่มีความก้าวหน้า การศึกษาหาความรู้ และผลการศึกษาวิจัยที่เกี่ยวข้องจะเป็นประโยชน์ต้องการปฏิบัติงานได้อย่างจริงจัง และเป็นรูปธรรมมากยิ่งขึ้น เพราะการศึกษาวิจัยเป็นเรื่องที่มีความสำคัญมาก รวมทั้งให้ความสนใจต่อวิวัฒนาการของเทคโนโลยีมีความเจริญ และสลับซับซ้อนมากยิ่งขึ้น

6. รายการอ้างอิง

ณรงค์ กุลนิเทศ. (2557). **รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์.** วารสารบัณฑิตศึกษา มหาวิทยาลัยราชภัฏสวนสุนันทา.

นุชนาฎ ฟ้าแสงสรรค์. (2554). **โจรไซเบอร์! กวาดเงิน 114 พันล้าน US/ปี**. ค้นเมื่อวันที่ 1 กุมภาพันธ์ 2558, จาก http://news.voicetv.co.th/technology/19589.html

ศูนย์พัฒนาทักษะและการเรียนรู้ ICT แม่ฮ่องสอน. (2557). **สถิติเกี่ยวกับอาชญากรรมคอมพิวเตอร์**. ค้นเมื่อวันที่ 4 พฤศจิกายน 2557, จาก www.mhsict.org

Happyman Natchy. (2557). **ผลศึกษาจากนอร์ตัน คำนวณผลเสียหายจากอาชญากรรมออนไลน์ทั่วโลก มีมูลค่า 114 พันล้านเหรียญสหรัฐฯ ต่อปี และนับเป็นการเปิดเผยผลสำรวจของอาชญากรรมออนไลน์ที่มีขนาดใหญ่ที่สุด มีผู้ตกเป็นเหยื่อกว่าล้านคนต่อวัน**. ค้นเมื่อวันที่ 1 กุมภาพันธ์ 2558, จาก http://happytechblog.blogspot.com/2011/10/114.html