เครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

Network and Knowledge management in Cyber Crime

พลตำรวจโท ดร.ณรงค์ กุลนิเทศ[1]

พันตำรวจเอก สมศักดิ์ หน่องพงษ์[2]

ผู้ช่วยศาสตราจารย์ พันตำรวจโท วรธัช วิชชุวาณิชย์[3]

นางสาวณิช วงศ์ส่องจ้า[4]

[1]หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

[2]กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ

[3]คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจสังกัด

[4]หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชานิติวิทยาศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา

บทคัดย่อ

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

1. 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

2. การจัดทำเครือข่ายทางด้านอาชญากรรมคอมพิวเตอร์ คือ การร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง วิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการ

ป้องกันปัญหาทางด้านอาชญากรรมคอมพิวเตอร์ รวมทั้งแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็บไซต์ (Black List) ร่วมกันจัดเวทีประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแลกเปลี่ยนข้อคิดเห็น และกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

3. การสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ จะนำปัญหาข้อขัดข้องในการปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์ ได้แก่ 1) ปัญหาที่เกิดก่อนการตรวจพิสูจน์ เช่น ความรู้ความสามารถเรื่องคอมพิวเตอร์ของพนักงานสอบสวนในการสอบสวนคดี 2) ปัญหาที่เกิดระหว่างการตรวจพิสูจน์ เช่น ข้อจำกัดของระบบคอมพิวเตอร์ หรือ Software และ 3) ปัญหาที่เกิดหลังการตรวจพิสูจน์ เช่น ผลการตรวจไม่เป็นประโยชน์ต่อรูปคดี มาใช้เป็นการสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

คำสำคัญ

เครือข่าย, การจัดการความรู้, อาชญากรรมคอมพิวเตอร์

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. 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.

2. 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.

3. Knowledge and create the handbook of prevention and suppression of cyber crime take 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.

Keywords

Network, Knowledge, Cyber Crime

บทนำ

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

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 (กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2555) จะเห็นได้ว่า การกระทำผิดตาม ป.อาญา มาตรา 112 ในปี 2555 มีการกระทำผิดสูงกว่าปี 2554 ถึง 82.46 เท่า หรือ สูงขึ้นถึงร้อยละ 8,146.31 ซึ่งจะเห็นว่าเป็นสถิติที่สูงขึ้นอย่างมากผิดปกติ จึงเป็นเหตุผลหนึ่งที่ควรนำเรื่องนี้มาศึกษา

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

มาตรา 17 ผู้ใดกระทำความผิดตาม พ.ร.บ. นี้นอกราชอาณาจักร 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 เพื่อรวบรวมข้อมูลเกี่ยวกับปัจจัยนำเข้า กระบวนการผลลัพธ์ รวมทั้งรูปแบบที่ดี (Best Practice) ตลอดจนปัญหา อุปสรรคและข้อเสนอแนะทางด้านเครือข่าย และการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์ เพื่อนำมาพัฒนางานทางด้านดังกล่าว ทำให้ประชาชนได้รับความคุ้มครองทางกฎหมาย รวมทั้งคุ้มครองสิทธิและเสรีภาพ ด้วยความรวดเร็ว เที่ยงตรงและเสมอภาค ประการสำคัญเพื่อนำผลการวิจัยที่ได้ไปเป็นแนวทางในการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ให้เป็นที่ยอมรับ ศรัทธาและความเชื่อมั่นจากประชาชนและสังคมต่อไป

วัตถุประสงค์ของการวิจัย

1) เพื่อพัฒนาหารูปแบบที่เหมาะสมในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

2) เพื่อสร้างเครือข่ายในการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์

3) เพื่อสร้างองค์ความรู้ และคู่มือทางด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์หลังจากมีการศึกษาวิธีการป้องกันและปราบปรามจากต่างประเทศ และนำมาประยุกต์ใช้

ขอบเขตการวิจัย

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

การทบทวนวรรณกรรม

แนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (ญาณพล ยั่งยืน, 2555)

วิวัฒนาการของอาชญากรรมคอมพิวเตอร์ (Computer Crime)

จากอดีตเรื่อยมาจนถึงยุคของอาชญากรรมเครือข่าย (Cyber Crime) หรืออาชญากรรมอินเทอร์เน็ต (Internet Crime) ในปัจจุบัน ที่กำลังกลายเป็นปัญหาสำคัญ และแก้ไม่ตกของประเทศทั้งหลาย ในอันที่จะหาวิธีในการป้องกัน และปราบปรามการกระทำความผิดเหล่านี้ ทั้งนี้เพื่อให้ทราบที่มา และเห็นถึงความเปลี่ยนแปลงเป้าหมายการกระทำความผิดจากสิ่งที่กฎหมายประสงค์จะคุ้มครอง (Rechtsgut) ไปสู่อีกสิ่งหนึ่ง ซึ่งเกิดขึ้นในช่วงระยะเวลาเพียงไม่กี่สิบปีเท่านั้น จนหลาย ๆ ประเทศ รวมทั้งประเทศไทยเองจำเป็นต้องเร่งบัญญัติกฎหมายใหม่ขึ้นมารองรับ รวมทั้งเพื่อเป็นประโยชน์ต่อการวิเคราะห์หาแนวโน้มขอบเขต ความเสียหายอื่น ๆ ที่อาจขยายตัวต่อไปตามวิวัฒนาการทางเทคโนโลยีในอนาคตด้วย

ลักษณะของอาชญากรรมคอมพิวเตอร์ / อินเทอร์เน็ต (จตุชัย แพงจันทร์, 2547)

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

1) คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (Computers as incidental to crime) การกระทำความผิดในลักษณะนี้ “บทบาท” ของคอมพิวเตอร์ จะไม่มีความสำคัญมากนัก กล่าวคือ คอมพิวเตอร์ไม่ใช่สาระสำคัญในกระทำความผิด แม้ผู้กระทำความผิดไม่มีคอมพิวเตอร์ ความผิดที่ได้กระทำเหล่านั้นก็สามารถสำเร็จลงได้เหมือนกัน ดังนั้น คอมพิวเตอร์จึงเป็นเพียงอุปกรณ์เสริม หรือช่วยอำนวยความสะดวกให้กับการกระทำความผิดในรูปแบบเดิม ๆ เท่านั้น เช่น ใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับการค้ายาเสพติด, ใช้คอมพิวเตอร์ในการติดต่อสื่อสาร ในองค์กรอาชญากรรม หรือ ใช้คอมพิวเตอร์ในการเก็บสะสมภาพลามกเด็ก เป็นต้น

2) คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (Computers as a tool in the commission of a crime) คอมพิวเตอร์เข้ามามีบทบาทหรือเป็นส่วนสำคัญที่จะทำให้การกระทำความผิดสำเร็จลงได้ ความผิดในกลุ่มนี้ส่วนใหญ่มักเป็นเรื่องของอาชญากรรมอินเทอร์เน็ต ยกตัวอย่าง เช่น การเผยแพร่ภาพลามกอนาจารหรือข้อความที่มีเนื้อหาเป็นภัยต่อสังคม หรือความมั่นคงผ่านทางเครือข่าย, การพนันบนเครือข่าย, การหมิ่นประมาทผู้อื่นด้วยการโฆษณาโดยอาศัยเครือข่ายอินเทอร์เน็ต, การละเมิดทรัพย์สินทางปัญญาด้วยการดาวน์โหลด หรือทำซ้ำผลงานอันมีลิขสิทธิ์ต่าง ๆ, การลักลอบหรือขโมยใช้บริการสารสนเทศ, การฟอกเงินทางอิเล็กทรอนิกส์ หรือการโอนเงินที่ได้มาจากการกระทำความผิดผ่านทางอินเทอร์เน็ตเพื่อให้เกิดความยากลำบากต่อการตามหาต้นตอของเงินเหล่านั้น, การฉ้อโกงผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น

3) คอมพิวเตอร์ในฐานะที่เป็นเป้าหมาย หรือวัตถุแห่งการกระทำความผิด (Computers as the target of the crime) อาชญากรรมในลักษณะนี้ถือเป็นความผิดประเภทที่มีปัญหาทางด้านกฎหมายมากที่สุดในปัจจุบันเนื่องจากมีรูปแบบการกระทำความผิดแบบใหม่ทั้งหมดไม่ว่าจะเป็น วิธีการ หรือวัตถุที่ถูกกระทำต่อ จนไม่อาจตีความกฎหมายเดิมที่มีอยู่ให้ครอบคลุมได้ และจำเป็นต้องบัญญัติกฎหมายใหม่เพื่อกำหนดฐานความผิดใหม่ขึ้นมา เนื่องจากผู้กระทำความผิดมีเป้าหมายอยู่ที่ระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์เป็นสำคัญทั้งนี้อาจเป็นการเข้าถึง ทำลาย เปลี่ยนแปลง หรือกระทำด้วยประการใด ๆ เพื่อให้ระบบ และข้อมูลดังกล่าวได้รับความเสียหาย เปลี่ยนแปลงไปจากเดิม โดยตนเองอาจได้รับประโยชน์จากการกระทำดังกล่าวด้วยหรือไม่ก็ตาม

การสืบหาตัวผู้กระทำความผิดทางคอมพิวเตอร์ / อินเทอร์เน็ต

อาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ตกำลังสร้างความเสียหายอย่างมาก ปัจจุบันประเทศต่าง ๆ จึงจำต้องช่วยกันหาทางรับมือกับอาชญากรรมเหล่านี้กันอย่างเร่งด่วน เพียงแต่ในที่สุดแล้ว หลายประเทศก็

ยังประสบปัญหาต่าง ๆ ในการป้องกันและปราบปรามการกระทำความผิดชนิดนี้อยู่ดี โดยอาจแยกสภาพปัญหาออกได้เป็น 3 ส่วน ดังต่อไปนี้

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

2) สภาพปัญหาในส่วนของมาตรการตามกฎหมายวิธีสบัญญัติ (กฎหมายที่ว่าด้วยวิธีการในทางปฏิบัติ หรือใช้บังคับกฎหมายสารบัญญัติ) 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

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 และผลงานวิจัยที่เกี่ยวข้องมาใช้เป็นกรอบในการวิเคราะห์ข้อมูลที่ได้รับ

จากแบบสอบถามและการสัมภาษณ์บุคลากรผู้เชี่ยวชาญที่เกี่ยวข้อง ผลการศึกษาพบว่า ปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยมีแนวโน้มเพิ่มขึ้นเนื่องจากการขยายตัวของประชากรอินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างรวดเร็ว ในขณะที่ผู้ใช้อินเทอร์เน็ตในสังคมไทย ยังขาดความรู้ความเข้าใจ และการปลูกฝังด้านจริยธรรมและวัฒนธรรมการใช้งานเทคโนโลยีเชิงสร้างสรรค์ ทำให้เกิดปัญหาการนำเทคโนโลยีไปใช้ในทางมิชอบตามมาส่วนบุคลากรที่มีความรู้ความสามารถด้านการรักษาความปลอดภัยคอมพิวเตอร์และเครือข่ายของประเทศไทยมีจำนวนจำกัด รวมทั้งภาครัฐไม่มีนโยบายและองค์กรเกี่ยวกับการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์โดยตรง ประกอบกับปัญหาทางด้านกฎหมาย ซึ่งปัจจุบันยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ออกมาบังคับใช้ ทำให้เกิดปัญหาในการดำเนินคดีกับผู้กระทำผิด

Guofu Ma และคณะ (2554) ได้ทำการศึกษาวิจัยเรื่อง รูปแบบพื้นฐานวงแหวนหลักฐานและห่วงโซ่หลักฐานของงานทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์ พบว่า การพัฒนาเทคโนโลยีที่เกี่ยวข้องกับการพิจารณาคดีทางด้านนิติวิทยาศาสตร์คอมพิวเตอร์อยู่บ่อยครั้ง ซึ่งส่วนใหญ่เป็นงานด้านทางวิทยาศาสตร์ และงานด้านคอมพิวเตอร์ และยังไม่สามารถทำให้มีความเชื่อมโยงกับการพิจารณาคดีตามกฎหมายได้มากนัก ซึ่งส่วนใหญ่จะศึกษาเฉพาะด้านเทคนิคของหลักฐานทางคอมพิวเตอร์เท่านั้น ในการศึกษานี้จึงศึกษาคุณลักษณะทั่วไปของพยานหลักฐาน วัตถุประสงค์ ความเกี่ยวข้อง และความถูกต้องของกฎหมาย เพื่อเป็นบรรทัดฐานในการสร้างแบบจำลองของนิติวิทยาศาสตร์คอมพิวเตอร์บนพื้นฐานของวงแหวนและห่วงโซ่ของหลักฐาน

Matthew Tart (2555) ได้ทำการศึกษาวิจัยเรื่อง หลักการและวิธีการสำรวจสำหรับการวิเคราะห์ตำแหน่งเสาโทรศัพท์ย้อนหลัง พบว่า โทรศัพท์มือถือมีข้อมูลที่สำคัญและสามารถนำไปใช้ในการสืบคดีหรือเป็นพยานหลักฐานที่ใช้ในชั้นศาล ซึ่งยังมีข้อมูลอื่นๆที่มีความเกี่ยวข้อกับโทรศัพท์มือถือที่ทำให้ได้ข้อมูลในการสืบสวนมากขึ้นไปอีก เช่น ข้อมูลการโทรเข้าออกซึ่งมีการเชื่อมโยงกับซิมการ์ดและระบบของผู้ให้บริการเครือข่ายโทรศัพท์มือถือซึ่งใช้ในการคิดค่าบริการโทรศัพท์มือถือด้วย นอกจากนี้การวิเคราะห์ตำแหน่งเสาสัญญาณโทรศัพท์ย้อนหลัง ร่วมกับข้อมูลอื่นๆจากการสำรวจหรือข้อมูลทางภูมิศาสตร์ สามารถระบุตำแหน่งของโทรศัพท์มือถือในช่วงเวลาที่มีการใช้งานโทรศัพท์มือถือได้ รายงานนี้นำเสนอภาพรวมของ หลักการของเครื่องโทรศัพท์มือถือ และสัญญาณโทรศัพท์มือถือกระทำต่อกัน รวมไปถึงวิธีการเก็บข้อมูลในรูปแบบต่างและการแปลผล และข้อดีข้อเสียของแต่ละวิธีการ ในรายงานนี้กล่าวถึงเฉพาะการวิเคราะห์จากสัญญาณโทรศัพท์ 2จี เท่านั้น และมีปัจจัยแต่ละพื้นที่มีความแตกต่างในด้านภูมิศาสตร์ และ ผู้ให้บริการเครือข่ายโทรศัพท์มือถือ แต่ในส่วนของหลักการสามารถใช้ได้กับเครือข่ายโทรศัพท์มือถือทั้ง 2จี (GSM) และ 3จี (UTMS) และไม่ได้กล่าวถึงการวิเคราะห์ตำแหน่งเสาสัญญาณโทรศัพท์ตามเวลาจริง

วิธีดำเนินการวิจัย

1. ระเบียบวิธีวิจัย

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. ขั้นตอนการวิจัย

การประชุมเพื่อทำการแลกเปลี่ยนเรียนรู้ ประชุมร่วมกันระหว่างทีมถอดบทเรียน โดยเชิญผู้เชี่ยวชาญในด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และเจ้าหน้าที่ตำรวจ หน่วยงานที่เกี่ยวข้องเครือข่ายที่มีประสบการณ์และความเชี่ยวชาญ 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)

3. การเก็บรวบรวมข้อมูล

ในการการวิจัยครั้งนี้ ผู้วิจัย คือเครื่องมือสำคัญในการเก็บรวบรวมข้อมูล โดยใช้วิธีการถ่ายทอดได้โดยผ่านทางวิธีการจัดกิจกรรมการจัดการความรู้ ซึ่งในแต่ละครั้งจะทำการบันทึกเทปการจัดกิจกรรมการจัดการความรู้ ซึ่งได้รับอนุญาตจากผู้ให้ข้อมูลแล้ว หลังจากการจัดกิจกรรมการจัดการความรู้ ข้อมูลจากเทปบันทึกจะถูกนำมาถอดข้อความ และบันทึกลงในคอมพิวเตอร์ ผู้วิจัยตรวจสอบความถูกต้องชัดเจนครบถ้วนของข้อมูลจากการฟังเทปซ้ำอีกครั้ง และถ่ายภาพนั้นไว้เป็นหลักฐานประกอบ

ผลการวิจัย

1. ลักษณะหรือรูปแบบอาชญากรรมคอมพิวเตอร์

1) การเข้าถึงระบบข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) ตัวอย่างเช่น การเจาะระบบ/รหัส (Hacking) หรือการบุกรุกทางคอมพิวเตอร์ (Computer Trespass) เพื่อทำลายระบบ

คอมพิวเตอร์ 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

2. การสร้างเครือข่ายชุมชนออนไลน์

1) ร่วมแบ่งปันข้อมูลเกี่ยวกับรูปแบบกลโกง และวิธีการป้องกันตนเองจากเหล่าอาชญากรทางเทคโนโลยี และข้อมูลอื่นที่เป็นประโยชน์ต่อการป้องกันปัญหาดังกล่าว

2) ร่วมแบ่งปันข้อมูลเกี่ยวกับรายชื่อผู้ที่มีพฤติกรรมกระทำความผิดบนเว็บไซต์ของแต่ละเว็บไซต์ (Black List)

3) จัดเวทีให้มีการร่วมงานประชุมสัมมนาด้านเครือข่ายชุมชนออนไลน์เพื่อแรกเปลี่ยนข้อคิดเห็น และกลวิธีที่นำมาใช้เพื่อช่วยลดปัญหาการก่ออาชญากรรมทางเทคโนโลยี อยู่ตลอดเวลาอย่างต่อเนื่อง

3. องค์ความรู้ และการสร้างคู่มือการจัดการความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์

ระบบงานด้านอาชญากรรมคอมพิวเตอร์ เป็นนวัตกรรมใหม่เพื่อการพิสูจน์หลักฐานทางคอมพิวเตอร์ในการกระทำผิด โดยองค์ความรู้ทางเทคโนโลยีคอมพิวเตอร์ รวมกับการใช้ในแนวทางการสืบสวนสอบสวน และการสร้างความน่าเชื่อถือของพยานหลักฐานที่ได้ ซึ่งถือได้ว่าจะทำให้มีน้ำหนักมากที่สุด

1) ให้ความรู้แก่พนักงานสอบสวน และผู้เกี่ยวข้องของสถานีตำรวจทุกแห่ง ทั้งในพื้นที่กองบัญชาการตำรวจนครบาล กองบัญชาการตำรวจภูธรภาคต่าง ๆ และหน่วยงานสนับสนุน ในการรับแจ้งความดำเนินคดีด้านอาชญากรรมคอมพิวเตอร์ เขตกอำนาจการสอบสวน เพราะการกระทำความผิดของ

คนร้ายนั้นสามารถกระทำความผิดได้ทั่วประเทศ 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

เนื่องจากการเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นการทำให้เกิดความเสียหายต่อสิทธิความเป็นส่วนตัว และความลับของข้อมูล และเมื่อสามารถเข้าถึงคอมพิวเตอร์ได้แล้ว ผู้กระทำการดังกล่าวก็สามารถจะก่อให้เกิดความเสียหายอย่างใดๆ ได้อีกอาศัยเหตุผลดังกล่าว จึงสมควรกำหนดให้การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจเป็นความผิดอาญาทันทีที่มีการเข้าถึงคอมพิวเตอร์

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

การป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ ควรจะต้องอาศัยทั้งมาตรการทางกฎหมายและมาตรการอย่างอื่นควบคู่กันไปเสมอ ในส่วนของมาตรการทางกฎหมาย นอกจากจะต้องมีการแก้ไข

ปรับปรุงกฎหมายอาญาสารบัญญัติ เพื่อกำหนดฐานความผิดให้ครอบคลุมถึงการกระทำความผิดรูปแบบใหม่ที่อยู่นอกขอบเขตของกฎหมายที่ใช้บังคับอยู่เดิมแล้ว ยังต้องปรับปรุงกฎหมายอาญาวิธีสบัญญัติ เพื่อให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างมีประสิทธิภาพและเป็นธรรมด้วย และที่สำคัญ คือ ลักษณะของการกระทำความผิดต่อคอมคอมพิวเตอร์ที่มักจะเป็นกระทำความผิดข้ามประเทศ ดังนั้นจึงต้องให้มีการร่วมมือกับประเทศต่างๆ เพื่อให้การดำเนินกับผู้กระทำความผิดเป็นไปอย่างมีประสิทธิภาพ และรวดเร็ว

ภาครัฐควรกำหนดนโยบายระดับชาติให้ชันเจน ทั้งในเรื่องนโยบายด้านการรักษาความมั่นคงคอมพิวเตอร์และเครือข่าย และการปราบปรามอาชญากรรมทางคอมพิวเตอร์ รวมทั้งผลักดันกฎหมายและมาตรการต่างๆ ที่จะช่วยงานป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ให้สัมฤทธิ์ผลในทางปฏิบัติอย่างเร่งด่วน เช่น การจัดตั้งองค์กรที่รับผิดชอบในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ในระดับชาติ เพื่อกำหนดนโยบายระดับสูงลงสู่ระดับปฏิบัติ

มาตรการอื่นๆ ที่ควรจะนำมากำหนดในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ ได้แก่

7.1 ด้านการพัฒนาบุคลากร

1) ควรมีการกำหนดผู้รับผิดชอบในการจัดทำหลักสูตรการฝึกอบรมต่างๆ เพื่อเตรียมความพร้อมของของบุคลากรในกระบวนการยุติธรรมทุกระดับ

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

3) ภาครัฐและเอกชน ควรส่งเสริมให้มีการเรียนการสอนด้านเทคโนโลยีการรักษาความปลอดภัยของระบบคอมพิวเตอร์

7.2 การบริหารและการจัดการองค์กร

1) ควรมีการจัดทำฐานข้อมูลเพื่อรวบรวมเว็บไซต์ที่มีพฤติกรรมการให้บริการแก่ผู้ใช้งานอินเตอร์เน็ตในทางที่ไม่เหมาะสม เพื่อประโยชน์ในการศึกษา และเป็นข้อมูลสนับสนุนให้แก่หน่วยงานที่เกี่ยวข้อง

7.3 ด้านเทคโนโลยี

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

7.4 ด้านมาตรการทางสังคม

1) ควรมีการกำหนดแผนการรณรงค์ประชาสัมพันธ์ ให้มีการพัฒนาและสร้างเสริมจริยธรรม เพื่อสร้างแนวปฏิบัติดีหรือวัฒนธรรมการใช้เทคโนโลยีที่ถูกต้องให้แก่คนในสังคมรวมทั้งสร้าง

วัฒนธรรมของความมั่นคง (Culture of Security) ในการใช้โครงสร้างพื้นฐานสารสนเทศหรือข่ายคอมพิวเตอร์ และการใช้งานอินเทอร์เน็ต โดยเริ่มจากสถาบันการศึกษา ครอบครัว และชุมชน

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

สรุปผล และอภิปรายผลการศึกษา

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

กระบวนการจัดการปัญหาคดีทางด้านอาชญากรรมคอมพิวเตอร์ในประเทศไทยยังไม่มีรูปธรรมที่ชัดเจนมากนัก ประการสำคัญ คือ ความรู้ ความเข้าใจในเทคโนโลยี ระบบคอมพิวเตอร์ ระบบอินเทอร์เน็ต การประยุกต์ใช้กฎหมายต่างๆ และการรักษาความน่าเชื่อถือของพยานหลักฐานที่ได้ ในการใช้ลงโทษคนร้าย หน่วยงานที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ มีการทำงานในลักษณะต่างหน่วยต่างทำ และเนื่องจาก พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ 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

กฎ 4 ประการในการรักษาความน่าเชื่อถือของพยานหลักฐานทางคอมพิวเตอร์

1) ต้องไม่กระทำให้เกิดการเปลี่ยนแปลงใด ๆ ในพยานหลักฐาน

2) กรณีที่มีความจำเป็นไม่สามารถหลีกเลี่ยงการเปลี่ยนแปลงของพยานหลักฐานได้ ต้องสามารถอธิบายได้ และพยายามให้เกิดการเปลี่ยนแปลงน้อยที่สุดเท่าที่จะเป็นไปได้

3) บันทึกรายละเอียดต่าง ๆ ทุกขั้นตอนที่กระทำกับพยานหลักฐานทางอิเล็กทรอนิกส์ และหากใช้เครื่องมืออื่นที่ได้รับมาตรฐานเช่นเดียวกันจะต้องได้รับผลลัพธ์แบบเดียวกัน

4) ผู้ที่เป็นเจ้าของคดี ต้องทำให้แน่ใจว่าได้ปฏิบัติถูกต้องตามกฎหมายและกฎในการรักษาความน่าเชื่อถือของพยานหลักฐาน

การวิจัยเพื่อจัดทำคู่มือเครือข่ายและการจัดการความรู้ทางด้านอาชญากรรมคอมพิวเตอร์

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

ข้อเสนอแนะ

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

2) พยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐาน ในหลายกรณีไม่มีความน่าเชื่อถือเนื่องจากขาดการครอบครองวัตถุพยานตามหลักสากล (Chain of custody) ซึ่งเป็นการพิสูจน์ความเชื่อมโยงของพยานหลักฐานกับการกระทำความผิด กระบวนการส่งต่อวัตถุพยานจะต้องมีการบันทึกรายละเอียดของวัตถุพยานซึ่งเริ่มตั้งแต่การตรวจพบ และเก็บวัตถุพยานในสถานที่เกิดเหตุรวมถึงผู้จัดส่ง – ผู้รับ ผู้ตรวจพิสูจน์ ตลอดทั้งกระบวนการสืบสวนสอบสวน ดังนั้นจึงต้องมีการบันทึกเป็นหลักฐานตามลำดับเวลา เพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้นๆ หากขาดการต่อเนื่องของการครอบครองวัตถุพยาน เมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือในชั้นศาล

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

4) บทบาทของสื่อมวลชนในบางกรณีมีผลกระทบต่อการปฏิบัติงาน และการนำเสนอรายละเอียดในทางคดีที่นำไปเผยแพร่ต่อสาธารณชน บางครั้งสื่อมวลชนมีการนำเสนอข้อมูลส่วนที่สำคัญในการนำวิธีการ หรือผลลัพธ์ในการทำงานของเจ้าหน้าที่ไปเปิดเผย คนร้ายจึงไม่ทิ้งร่องรอยในการกระทำความผิดไว้ หรือมีการใช้เทคโนโลยีที่ซับซ้อนมากขึ้นในการอำพรางหรือหลบซ่อนตัวเอง ทำให้เจ้าหน้าที่ปฏิบัติงานยากลำบากขึ้น ซึ่งเป็นจุดอ่อนต่อการปฏิบัติงานของเจ้าหน้าที่

5) เห็นควรสรรหาบุคลากรเพื่อมาปฏิบัติหน้าที่ทางด้านคดีอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นเพื่อรองรับปัญหาทางด้านคดีอาชญากรรมคอมพิวเตอร์ที่เพิ่มมากขึ้น

6) จัดซื้อวัสดุอุปกรณ์ในการตรวจพิสูจน์หลักฐานที่เกี่ยวข้องกับคดีทางด้านอาชญากรรมทางคอมพิวเตอร์ที่มีความทันสมัย ใช้เวลาในการตรวจพิสูจน์น้อย เคลื่อนย้ายได้ง่าย และให้ผลการตรวจพิสูจน์ที่ถูกต้องแน่นอน เพื่อลดระยะเวลาและปริมาณงาน เช่น ซอฟต์แวร์การกู้ข้อมูลที่ถูกลบไปแล้ว เป็นต้น

เอกสารอ้างอิง

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

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

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

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

สินเลิศ สุขุม. (2543). **ปัจจัยที่มีผลต่อประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมคอมพิวเตอร์ ของเจ้าหน้าที่ตำรวจกองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ**. 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.

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.