การส่งเสริมการศึกษาในวิชาอาชญากรรมไซเบอร์

The Promotion of Education in Cybercrime

ปรเมศวร์ กุมารบุญ
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

Poramez Kumarnboon
Faculty of Political Science, Chulalongkorn University

บทคัดย่อ

บทความวิชาการนี้เป็นบทความปริทัศน์ เพื่อรวบรวม จัดหมวดหมู่ แยกแยะองค์ประกอบของวิชาอาชญากรรมไซเบอร์ และเสนอความเห็นเพื่อยกระดับให้มีความเป็นวิชาการ มีทิศทาง และเห็นความจำเป็นอย่างชัดเจนในการบูรณาการวิชาการศึกษาอาชญากรรมไซเบอร์สำหรับโรงเรียนนายร้อยตำรวจ เพื่อให้เป็นสถาบันการศึกษาหลักของชาติในการผลิตบุคคลากรด้านกระบวนการยุติธรรมยุคดิจิทัล และเตรียมความพร้อมรับมือภัยคุกคามจากโลกอนาคตที่กำลังคืบคลานเข้ามาอย่างรุนแรง

คำสำคัญ: อาชญากรรมไซเบอร์, ยุติธรรมยุคดิจิทัล, พยานหลักฐานดิจิทัล

Abstract

This review article compiles the classification of cybercrime and offers academic opinions for upgrading cybercrime to be academic. The purpose is to see the direction and necessity of integrating cybercrime education into the Royal Police Cadet Academy to be the main educational institution of the nation to produce criminal justice personnel in the digital era and prepare them for combatting the threats of the future world.

Keywords: Cybercrime, Digital Justice, Digital Evidence

บทนำ

นับจากโลกมีคอมพิวเตอร์ถือกำเนิดขึ้นไม่นานก็มี อาชญากรรมคอมพิวเตอร์ (Computer crime) เกิดขึ้น จากการทำลายเครื่องคอมพิวเตอร์ทางกายภาพและทำลายข้อมูลคอมพิวเตอร์ สังคมเริ่มตระหนักว่าสิ่งเหล่านี้มีมูลค่ามากกว่าความเสียหายในรูปทรัพย์สิน และส่งผลเสียหายใหญ่หลวงต่อคนจำนวนมาก จึงค่อยๆ พัฒนาเป็นกฎหมายอาญาต่อมา

M.E.Kabay (2008) ได้อ้างถึงอาชญากรรมคอมพิวเตอร์เกิดขึ้นครั้งแรก ในปี ค.ศ. 1969 จากการที่นักศึกษาแคนาดารวมตัวประท้วงศาสตราจารย์ผู้หนึ่งในมหาวิทยาลัยที่กระทำการเหยียดเชื้อชาติ และเมื่อตำรวจมาถึงก็เกิดจลาจลวุ่นวายขึ้น จนเกิดไฟลุกไหม้ห้องคอมพิวเตอร์ของมหาวิทยาลัยถูกทำลาย มูลค่าเสียหายราว 2 ล้านดอลลาร์ และนักศึกษาถูกจับ 97 คน

M.E.Kabay (2008) ยังได้อธิบายถึงประวัติศาสตร์อาชญากรรมคอมพิวเตอร์ในยุคแรก คือการทำลายคอมพิวเตอร์ทางกายภาพ ทุบ ทำลาย ถูกยิง ถูกระเบิด ซึ่งเกิดจากอุบัติเหตุบ้าง เกิดจากการก่อวินาศกรรม (Computer sabotages) และการจารกรรมอุตสาหกรรม (Industrial espionage) ในช่วงปี ค.ศ. 1960s-1970s ต่อมาเกิดการขโมยข้อมูล เปลี่ยนแปลงข้อมูล บุคคล ธุรกิจ และธนาคาร เช่น ปลอมบัตรเครดิต ปลอมบัญชีธนาคาร เป็นยุคแรกของ Identity Theft และเกิดอาชีพ Dumpster Diver (คนคุ้ยขยะ) ทำหน้าที่ขุดคุ้ยขยะหาข้อมูล ใบเสร็จ สำเนาบัตรเครดิต ข้อมูลลูกค้า ข้อมูลธุรกิจ ไปขายต่อให้อาชญากรนำข้อมูลมาปลอมแปลงเพื่อใช้งานเป็นอาชีพที่สร้างรายได้มากในอเมริกา โดยมีอาชญากรวัยรุ่นชื่อดังอย่าง Jerry Neal Schneider เป็นผู้นำ สร้างความเสียหายต่อธุรกิจหลายแห่ง กระทั่งเริ่มมีการเข้าถึงข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุคปี 1980s (ยังไม่มีอินเทอร์เน็ต)

จากนั้นในยุค ค.ศ.1990s การทำลายข้อมูลคอมพิวเตอร์จาก ไวรัส ได้ก่อตัวขึ้นพร้อมกับอินเทอร์เน็ตถือกำเนิดขึ้น จากอาชญากรรมคอมพิวเตอร์ กลายเป็น อาชญากรรมไซเบอร์ (Cybercrime) เมื่อการทำลายอุปกรณ์คอมพิวเตอร์ และข้อมูลคอมพิวเตอร์ ได้เปลี่ยนช่องทางการทำความเสียหายผ่านอินเทอร์เน็ต และปัจจุบันอาชญากรรมไซเบอร์เติบโตกว้างไกลมากดังจะได้กล่าวต่อไป

Cyber crime หรือ “อาชญากรรมไซเบอร์” ผู้เขียนยังไม่พบที่ใดให้นิยามไว้เป็นทางการชัดเจน จึงขอเรียกว่า “อาชญากรรมไซเบอร์” แม้ในบางครั้งได้ปรากฏเห็นเรียก Cyber crime ว่า “อาชญากรรมคอมพิวเตอร์” ซึ่งผู้เขียนเห็นว่า Cybercrime แตกต่างกับ Computer Crime ตรงการเชื่อมต่ออินเทอร์เน็ต ดังที่กล่าวถึงประวัติศาสตร์ข้างต้น

นอกจากนั้นการใช้คำว่า "คอมพิวเตอร์" เป็นความหมายที่แคบกว่าคำว่า ไซเบอร์ (Cyber) เพราะนอกจากคอมพิวเตอร์ (ข้อมูล ชุดคำสั่ง อุปกรณ์อิเล็กทรอนิกส์ และหน่วยประมวลผล ตามมาตรา 7

พรบ. คอมพิวเตอร์) แล้วอาชญากรรมไซเบอร์ยังหมายรวมถึงการเจาะเข้าถึงโครงข่ายโทรคมนาคม (Telecommunications Network) อุปกรณ์โทรคมนาคม (Telecommunications Equipment) ไปจนถึงเนื้อหา (Contents) และการนำเทคโนโลยีการสื่อสารผ่านอินเทอร์เน็ตไปประกอบอาชญากรรม (Larry และ Lars E. Daniel, 2559)

อาชญากรรมไซเบอร์เติบโตกว้างขวางไปมากมายหลายมิติในปัจจุบัน กล่าวคือ เป็นอาชญากรรมที่จะเกิดขึ้นไม่ได้ “หากไม่มีการใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่ออินเทอร์เน็ต” และปัจจุบันตำรวจทั่วโลกกำลังเผชิญหน้ากับความท้าทายจากภัยคุกคามในรูปแบบใหม่แห่งศตวรรษที่ 21

แนวทางหลักของกฎหมายในการกำกับดูแลอาชญากรรมไซเบอร์ของไทยนั้น เริ่มแรกได้รับอิทธิพลมาจาก Convention on Cyber crime โดยสภาแห่งยุโรป (The Council of Europe) และกฎหมายหลายฉบับของสหรัฐอเมริกา เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Fraud and Abuse Act 1986) ซึ่งเป็นกฎหมายกำหนดฐานความผิด เช่น การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเกินขอบเขตที่ได้รับอนุญาต กฎหมาย แคนสแปม (CAN - SPAM Act ย่อมาจาก Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003) เป็นการกำหนดมาตรฐานการห้ามการส่งอีเมลขยะ กฎหมายการขโมยข้อมูลระบุตัวตน และการปลอมตน (Identity Theft and Assumption Deterrence Act) ส่วนในฝั่งอังกฤษ เช่น กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) และกฎหมายการคุ้มครองข้อมูล (Data Protection Act) เป็นต้น ซึ่งรากฐานเหล่านี้ก็ได้เกิดเป็น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) ได้ประกาศบังคับใช้เป็นการทั่วไปแล้ว

พ.ร.บ.คอมพิวเตอร์ฯ มิได้เพียงแค่ห้ามกระทำความผิดทางอาญาต่อคอมพิวเตอร์ และหากแต่รวมถึงการนำคอมพิวเตอร์ไปก่ออาชญากรรมด้วย โดยเฉพาะเป็นภัยต่อความมั่นคงของชาติและระบบเศรษฐกิจปัจจุบัน (ตุลาคม 2561) ร่าง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... ได้ผ่านการทบทวนจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และมีการเปิดการรับฟังความคิดเห็นมาแล้วหลายครั้ง โดยมีต้นแบบมาจากกฎหมาย Cybersecurity Act 2018 ของประเทศสิงคโปร์

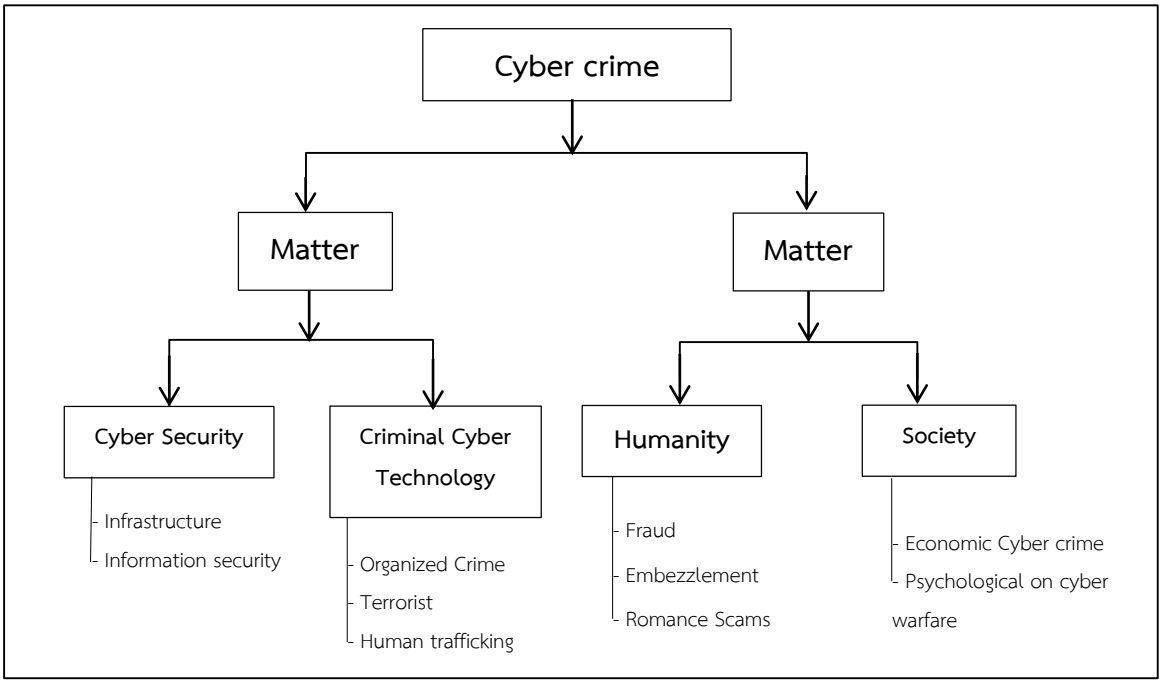
ความท้าทายของอาชญากรรมไซเบอร์ในศตวรรษที่ 21 มิใช่เพียงแค่การเจาะระบบ ขโมยข้อมูล แก้ไขข้อมูล ทำลายข้อมูล ที่เรียกว่าความมั่นคงปลอดภัยข้อมูล (Cyber Security) อีกต่อไป แต่กลับเกิดการนำเทคโนโลยีดิจิทัลด้านการสื่อสารมาประกอบอาชญากรรมในเกือบทุกประเภท มีวิวัฒนาการเป็นเทคโนโลยีอาชญากร (Criminal Technology) และยังเกิดอาชญากรรมประเภทใหม่ๆ อันเป็นผลกระทบ

จากการมีเทคโนโลยีสมัยใหม่เกิดขึ้น ซึ่งนอกจากทำให้อาชญากรนำไปประกอบอาชญากรรมสำเร็จผลได้ง่าย ยังทำให้การสืบสวนจับกุมเป็นไปได้ยาก ดังปรากฏการณ์อาชญากรรมร่วมสมัยที่เกิดขึ้นหลายรูปแบบในปัจจุบัน

บทความนี้จึงรวบรวม จัดหมวดหมู่ แยกแยะองค์ประกอบของวิชาอาชญากรรมไซเบอร์ และเสนอความเห็นเพื่อยกระดับให้มีความเป็นวิชาการ มีทิศทาง และเห็นความจำเป็นอย่างชัดเจนในการบูรณาการวิชาการศึกษาอาชญากรรมไซเบอร์ เพื่อให้นิสิต นักศึกษา และสถาบันการศึกษาได้นำไปใช้ประโยชน์ในการศึกษาแขนงต่างๆ และรัฐจะได้เตรียมความพร้อมรับมือภัยคุกคามจากโลกอนาคตที่กำลังคืบคลานเข้ามาอย่างรุนแรง

1. การริเริ่มสร้างองค์ความรู้ด้านอาชญากรรมไซเบอร์ให้เป็นวิชาการ

อาชญากรรมไซเบอร์ยังไม่มีการจัดหมวดหมู่เพื่อการศึกษาอย่างเป็นวิชาการที่ชัดเจน ต่างฝ่ายต่างศึกษากันไปในหลายมิติ แต่ในบทความนี้ผู้เขียนขอริเริ่มต้นจัดหมวดหมู่การศึกษาอาชญากรรมไซเบอร์ ตามปรัชญาการวิจัยในมิติทาง ภววิทยา (Ontology) ที่แตกต่างกัน (รัตนะ บัวสนธ์,2560) เพื่อที่จะเข้าไปถึงความรู้หรือความจริงด้วยวิธีที่แตกต่างกัน โดยแบ่งเป็น ภววิสัย (Objective) และอัตวิสัย (Subjective) เพื่อจะเลือกใช้วิธีวิทยาอันมีเครื่องมือในการวิจัยที่มี ญาณวิทยา (Epistemology) แตกต่างกัน เพื่อประโยชน์ในการวิจัยของผู้อื่นต่อไป



ภาพที่ 1 การจัดหมวดหมู่การศึกษาวิชาอาชญากรรมไซเบอร์

จากภาพที่ 1 เบื้องต้นผู้เขียนได้พยายามเสนอวิธีการ แยกแยะ จัดหมวดหมู่อาชญากรรมไซเบอร์แบ่งไว้เป็น 2 หลักใหญ่ คือ การก่ออาชญากรรมไซเบอร์ที่จับต้องได้ (Objective) เป็นการกระทำทางวัตถุ (Matter) หรือเป็นภววิสัย ใช้วิธีการวิจัยทางวิทยาศาสตร์ และการก่ออาชญากรรมไซเบอร์ที่จับต้องไม่ได้ (Subjective) เป็นการกระทำต่อจิตใจ (Mind) หรืออัตวิสัย ใช้วิธีวิจัยทางสังคมศาสตร์หรือมนุษยศาสตร์ การก่ออาชญากรรมไซเบอร์ที่กระทำต่อวัตถุ (Matter) หรืออาชญากรรมทางเทคโนโลยีการสื่อสาร เช่น เรื่อง Cyber security และ Criminal communication technology อธิบายได้ดังนี้

1.1 Cyber security (ความมั่นคงทางไซเบอร์หรือความมั่นคงระบบคอมพิวเตอร์)

Cyber security เป็นเรื่องอาชญากรรมไซเบอร์พื้นฐานที่ทราบกันดีทั่วไปว่า เป็นการก่ออาชญากรรมที่เกี่ยวข้องกับ เจาะระบบ ถอดรหัส ทำลายข้อมูล แก้ไขข้อมูล ทำลายระบบ ขโมยข้อมูล เป็นต้น โดยแบ่งแยกโปรแกรมคอมพิวเตอร์ที่ทำลาย Cyber security เป็น 2 ประเภท คือ

1.1.1 โปรแกรมที่เหยื่อไปติดเชื้อมาเอง

โปรแกรมทำลายคอมพิวเตอร์ที่แอบแฝงมากับไฟล์หรืออีเมล์หรือจากเว็บไซต์ ที่เรียกว่า Malware (มัลแวร์) ซึ่งเป็นอันตรายต่อคอมพิวเตอร์ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล Malware แบ่งออกได้หลากหลายประเภท เช่น

- Virus คือ โปรแกรมทำลายข้อมูลและระบบคอมพิวเตอร์
- Worm คือ โปรแกรมที่เคลื่อนที่ไปในเครือข่ายได้เอง
- Trojan Horse คือ โปรแกรมที่แอบทำงานแบบลับๆ ด้วยการเปิดให้มีการบุกรุกเข้าสู่ระบบ
- Zombie คือ โปรแกรมที่ทำหน้าที่ให้เครื่องคอมพิวเตอร์นั้นเป็นเครื่องมือโจมตีเครื่องอื่นต่อไป
- Botnet คือ โปรแกรมขนาดเล็กที่ฝังตัวโดยที่เจ้าของไม่รู้ตัว อาชญากรจะสั่งคอมพิวเตอร์ที่มี BOT ฝังอยู่ โจมตีเครื่องแม่ข่ายเพื่อสร้างความเสียหายให้แก่ระบบและองค์กรได้
- Ransomware เป็น Malware ที่ทำการบล็อกไฟล์เหยื่อไม่ให้ใช้งานได้ เช่น ไฟล์ เอกสาร ภาพ วิดีโอ แล้วอาชญากรก็จะส่งข้อความมา “เรียกค่าไถ่” เพื่อให้ส่งรหัสปลดล็อกไฟล์คืนมา
- ฯลฯ

1.1.2 โปรแกรมที่อาชญากรใช้มุ่งเจาะจงเลือกเหยื่อ

แม้ในยุคแรกอาชญากรยังไม่ได้มีเทคนิคพิเศษมาก เพียงใช้วิธีการคาดเดารหัสผ่าน (Brute Force Attack) คือ การพยายามเข้าสู่ระบบด้วยการเดารหัสผ่านของเหยื่อเป้าหมาย ซึ่งเหยื่อก็มักใช้ชื่อจริง ชื่อเล่น วันเดือนปีเกิด หมายเลขโทรศัพท์ ที่เกรงว่าตนเองลืมง่ายมาใช้งาน ทำให้ง่ายต่อการเข้าถึงข้อมูล แต่ต่อมาเริ่มมีการเขียนโปรแกรมทำลายระบบคอมพิวเตอร์ที่อาชญากรมุ่งเจาะจงเลือกเหยื่อหรือองค์กรเพื่อเจาะระบบรักษาความปลอดภัยเข้ามาทำลายหรือขโมยข้อมูลที่เรียกว่า Hacker และ Cracker เช่น

- Spoofing คือ เทคนิคการเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ระยะไกลโดยการปลอมแปลงที่ IP Address ของเหยื่อที่เข้าถึงได้ง่าย และลักลอบเข้าไปในคอมพิวเตอร์นั้น
- Sniffer คือ โปรแกรมดักจับข้อมูลที่ส่งผ่านเครือข่ายคอมพิวเตอร์ ทำให้ทราบรหัสผ่าน (Password) ของบุคคลอื่นที่ส่งผ่านเครือข่ายคอมพิวเตอร์
- Modification คือ การเปลี่ยนแปลงข้อมูล อาชญากรอาจอยู่ใน ISP ซึ่งสามารถตรวจจับแพ็กเก็ตข้อมูลที่รับส่งในเครือข่ายนั้นได้ โดยอ่านข้อมูลจากผู้ส่งแล้วแก้ไขข้อมูลก่อนส่งไปยังผู้รับ ทำให้ได้ข้อมูลที่ผิดพลาด
- Denial of service คือ การปฏิเสธการให้บริการ โดย Server ถูกโจมตีจากหลายวิธีหรือถูกเรียกเข้าชมเว็บไซต์จำนวนมาก ทำให้เว็บไซต์ไม่สามารถทำงานปกติได้
- ฯลฯ

1.2 Criminal communication technology หรือ Criminal cyber technology (นวัตกรรมเทคโนโลยีการสื่อสารเพื่อการประกอบอาชญากรรม)

Petter Gotschalk (2010) เป็นการนำนวัตกรรมเทคโนโลยีการสื่อสารเพื่อนำไปประกอบอาชญากรรมประเภทต่างๆ ซึ่งมิใช่เทคโนโลยีที่ผลิตขึ้นมาเป็นการเฉพาะ หากแต่เป็นนวัตกรรมที่หาได้ทั่วไป เช่น

- Identity Theft คือ การที่อาชญากรใช้อินเทอร์เน็ตหรือสมาร์ตโฟนเอาข้อมูลส่วนตัวของเหยื่อไปสวมรอยใช้ เช่น เอาชื่อไปเปิดบัญชีธนาคาร ทำบัตรเครดิต ทำธุรกรรมการเงิน ยืมเงินเพื่อน
- การใช้ Dark web เครือข่าย Tor network และเงินเสมือน (Crypto currency) ในการประกอบอาชญากรรม เพื่อการค้ายาเสพติด การจ้างสังหาร เส้นทางการเงินก่อการร้าย ฯลฯ

- การใช้นวัตกรรมเทคโนโลยีการสื่อสารกับ โดรน เพื่อสอดแนม จารกรรม และก่อวินาศกรรม
- Phishing เป็นการโจรกรรมข้อมูลทางอินเตอร์เน็ตในรูปแบบของการสร้าง web site เลียนแบบเพื่อให้เหยื่อ login หรือกรอกข้อมูลเพื่อล่อลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น เอาเลขที่บัตรเครดิต และ user name/password
- ฯลฯ

การก่ออาชญากรรมไซเบอร์ที่กระทำต่อ จิตใจ (Mind) หรือเรื่องที่จับต้องไม่ได้ แบ่งเป็น 2 ประเภท คือ การก่ออาชญากรรมไซเบอร์ที่กระทำต่อจิตใจ ในระดับบุคคล และในระดับสังคม อธิบายได้ดังนี้

1) การก่ออาชญากรรมไซเบอร์ที่กระทำต่อจิตใจในระดับบุคคล

การก่ออาชญากรรมไซเบอร์ที่ใช้เทคโนโลยีการสื่อสารมาช่วยให้อาชญากรก่ออาชญากรรมได้ง่ายขึ้น โดยการปฏิบัติการจิตวิทยาหรือกล่าวได้ว่ากระทำต่อจิตใจในระดับบุคคล เช่น

- คดี Romance scams การใช้ Social media หลอกให้รักทางออนไลน์แล้วเสียทรัพย์
- แชร์ลูกโซ่ การฉ้อโกง การหลอกขาย ICO, Token, Binary Option และ IQ Option เป็นต้น
- Cyber Bullying การกลั่นแกล้ง ข่มเหงรังแกทางออนไลน์
- Vishing (เกิดจากประสมคำว่า voice และ phishing) อาชญากรใช้การลวงขอข้อมูลส่วนตัวและข้อมูลด้านการเงินผ่านทางโทรศัพท์อินเทอร์เน็ตหรือ VoIP (แก๊ง คอลเซ็นเตอร์)
- ฯลฯ

2) การก่ออาชญากรรมไซเบอร์ที่กระทำต่อจิตใจในระดับสังคม

เป็นการก่ออาชญากรรมไซเบอร์ที่ใช้เทคโนโลยีการสื่อสารมาประกอบอาชญากรรม โดยกระทำต่อจิตใจในระดับสังคมหรือกล่าวได้ว่าเป็นการปฏิบัติการจิตวิทยามวลชนบนสื่ออินเทอร์เน็ต เช่น

- Hoax คือ ข่าวหลอกลวง เพื่อสร้างเรตติ้งให้เว็บไซต์ขายโฆษณาหรือสร้างความสับสนในสังคม
- Information Operation การใช้เนื้อหา (Content) แย่งชิงความเชื่อมวลชนหรือครอบความจริงให้คนในสังคมเข้าใจไปในทิศทางที่ต้องการ

- Psychological on cyber warfare คือ การทำสงครามปฏิบัติการจิตวิทยาบนสื่ออินเทอร์เน็ตเพื่อปลุกระดมทางการเมือง หรือสร้างอาชญากรรมแห่งความเกลียดชัง (Hate Crime) เพื่อสร้างความแตกแยกจนทำลายล้างกันเองในที่สุด เป็นการทำลายความมั่นคงของชาติ และถืออาชญากรรมไซเบอร์ที่รุนแรงที่สุด
- ฯลฯ

จากการหมวดหมู่แนวทางการศึกษาอาชญากรรมไซเบอร์ดังรูปที่ 1 จะเห็นได้ว่า แท้จริงนอกจากเรื่อง Cyber Security แล้ว นอกนั้นเป็นงานตำรวจทั้งหมด นับตั้งแต่ Criminal communication technology การใช้เทคโนโลยีการสื่อสารเพื่อประกอบอาชญากรรม ซึ่งตำรวจต้องเรียนรู้และค้นหาแนวทางการสืบสวนจับกุม รวบรวมพยานหลักฐาน ตลอดจนแนวทางป้องกัน

FATF (2015) ได้อธิบายถึงแนวทางการป้องกันและปราบปรามอาชญากรรมการฉ้อโกงสินทรัพย์ดิจิทัล (Fraud and Scam) รวมถึงคดีการฉ้อโกง ต้มตุ๋น ทางออนไลน์เป็นคดีอาญาที่ต้องมาแจ้งความที่ตำรวจก่อนทั้งสิ้น เจ้าหน้าที่ตำรวจต้องสอบสวน รวบรวมพยานหลักฐาน เพื่อดำเนินคดี

ส่วน Psychological on cyber warfare เป็นการปฏิบัติการจิตวิทยาบนสื่ออินเทอร์เน็ตสร้างความไม่สงบในสังคมและทำลายความมั่นคง ซึ่งงานความมั่นคงภายในราชอาณาจักรก็คือภารกิจตำรวจ

2. สร้างความเป็นศาสตร์ให้วิชาอาชญากรรมไซเบอร์

รัตนะ บัวสนธ์ (2560) ได้ให้ความหมายของความเป็นศาสตร์หรือวิทยาศาสตร์ ซึ่งในภาษาอังกฤษตรงกับคำว่า “Science” หมายถึง ความรู้หรือสาขาวิชาที่เกิดจากการค้นหาความรู้หรือความจริงมาจัดไว้อย่างเป็นระบบ

ศาสตร์ที่เกิดจากการค้นหาความรู้หรือความจริงจากวัตถุ (Objective) ที่จับต้องได้ เช่น เคมี ฟิสิกส์ ชีววิทยา เรียกว่า วิทยาศาสตร์ธรรมชาติ ส่วนการค้นหาความรู้หรือความจริงจากสิ่งที่จับต้องตวงวัดไม่ได้ (Subjective) อันเกิดจากการสังเกตปรากฏการณ์ในสังคมนำมาวิเคราะห์อย่างเป็นระบบ หากมุ่งศึกษาปรากฏการณ์ที่เกี่ยวข้องระหว่างมนุษย์กับมนุษย์เรียกว่า สังคมศาสตร์ และ หากมุ่งศึกษาปรากฏการณ์ที่เป็นปัจเจกของมนุษย์เรียกว่า มนุษยศาสตร์

รัตนะ บัวสนธ์ (2560) ยังได้อธิบายถึง “เป้าหมายของศาสตร์” มี 4 ประการ คือ บรรยายปรากฏการณ์ อธิบายสาเหตุปรากฏการณ์ ทำนายปรากฏการณ์ และควบคุมปรากฏการณ์ที่จะเกิดขึ้น

วิทยาศาสตร์มีความเป็นศาสตร์สูงที่สุด ทำซ้ำกี่ครั้งผลก็เหมือนเดิมสามารถ บรรยาย อธิบาย ทำนาย และควบคุมได้ ซึ่งอาชญากรรมไซเบอร์ที่กระทำต่อวัตถุ เช่น เรื่อง Cyber security และ Criminal

communication technology เป็นเรื่องวิทยาศาสตร์หรือวิศวกรรมศาสตร์ จึงต้องใช้วิธีวิทยาการวิจัยแบบวัตถุวิสัยหรือภววิสัย (Objective) เป็นกระบวนวิธีวิจัยแบบวิทยาศาสตร์ในการสร้างความรู้

ส่วนสังคมศาสตร์หรือมนุษยศาสตร์ อาจจะมีความเป็นศาสตร์น้อยกว่าวิทยาศาสตร์ธรรมชาติ บางทฤษฎีอาจจะสามารถ บรรยาย อธิบาย ปรากฏการณ์ได้ แต่ยังไม่สามารถ ทำนาย และควบคุมปรากฏการณ์ได้ ซึ่งอาชญากรรมไซเบอร์ที่กระทำต่อจิตใจ เช่น เรื่อง Romance scam และ Cyber bullying จึงต้องใช้วิธีวิทยาการวิจัยแบบ อัตวิสัย (Subjective) หรือกระบวนวิธีวิจัยแบบสังคมศาสตร์ในการสร้างความรู้

นับแต่อดีตเทคโนโลยีการสื่อสาร และการประกอบอาชญากรรมมีความสัมพันธ์กันในระดับหนึ่ง แต่มีการทำงานวิจัยด้านนี้น้อยมาก อันอาจเกี่ยวเนื่องกับการมองข้ามศาสตร์ (Cross-Disciplinary) ระหว่างสาขาวิชาของผู้ที่ศึกษาวิจัยงานด้านอาชญาวิทยามักเป็นผู้ที่มีพื้นฐานมาจากสายสังคมศาสตร์มากกว่าด้านวิศวกรรมศาสตร์หรือวิทยาศาสตร์เทคโนโลยี ทำให้การมองสาเหตุการเกิดอาชญากรรมจากการมีเทคโนโลยีการสื่อสารใหม่เกิดขึ้นในสังคมมาทำเป็นงานวิจัยจึงมีน้อย และปัจจุบันวิชาอาชญากรรมไซเบอร์เป็น Multi-Disciplinary ทั้ง นิติศาสตร์ รัฐศาสตร์ วิทยาศาสตร์ วิศวกรรมศาสตร์ และสังคมศาสตร์ หากทว่าเป้าหมายที่ต้องการงานวิจัยจำเป็นต้องเข้าใจว่าศาสตร์แต่ละอย่างคืออะไร แล้วบริหารจัดการงานวิจัยด้วยวิธีวิทยาแบบใด

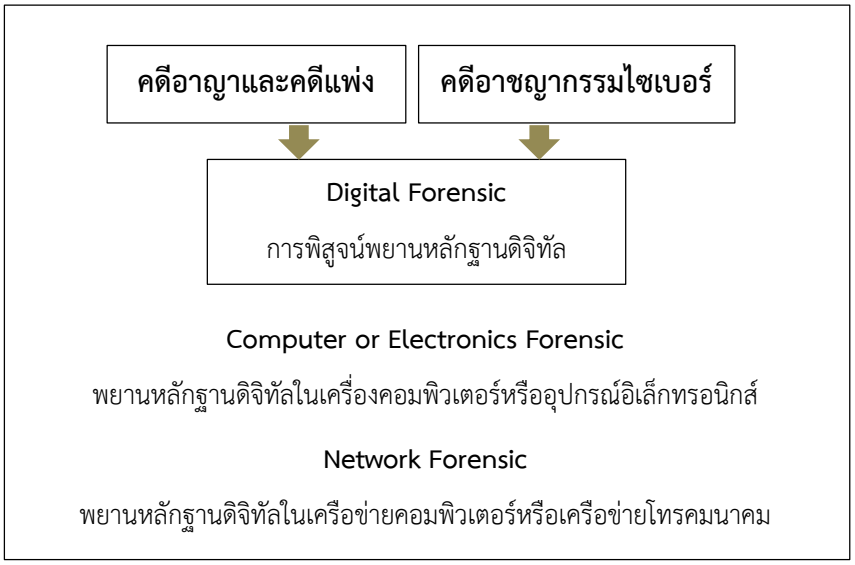
3. การตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล (Digital Evidence)

การศึกษาเรื่องพยานหลักฐานดิจิทัล (Digital Evidence) ยังมีตำราหรือการเรียนการสอนน้อยมาก และพยานหลักฐานดิจิทัล ไม่ได้อยู่ในอาชญากรรมไซเบอร์เท่านั้น แต่อยู่ในทุกคดีปัจจุบัน ทั้งคดีอาญา และคดีแพ่ง เพราะปัจจุบันการรวบรวมพยานหลักฐานคดีต่างๆ ต้องมีพยานหลักฐานดิจิทัลรวมอยู่ด้วยแทบจะทุกคดี

พยานหลักฐานหมายถึงสิ่งที่ใช้พิสูจน์ข้อเท็จจริงตามกฎหมาย ส่วนพยานหลักฐานดิจิทัล “ข้อมูลคอมพิวเตอร์” ตาม พรบ. คอมพิวเตอร์ฯ และหมายถึงข้อมูลอิเล็กทรอนิกส์ ตาม พรบ. ธุรกรรมอิเล็กทรอนิกส์ฯ ที่นำมาใช้พิสูจน์ข้อเท็จจริง (ผู้วิจัย) เช่น ข้อมูลคอมพิวเตอร์หรือข้อมูลอิเล็กทรอนิกส์ที่ถูกบันทึกอยู่ในรูปแบบ ธุรกรรมการเงิน (Transaction) เอกสาร (Document) เสียง (Voice) ภาพนิ่ง (Photo) ภาพเคลื่อนไหว (Video) อักษร (Letter) และสื่อสังคมออนไลน์ (Social Media) เป็นต้น

Larry และ Lars E. Daniel. (2559) ได้ให้ความหมายของการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลในเครื่องคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ที่ยังไม่เชื่อมต่ออินเทอร์เน็ต เช่น ในกล้องถ่ายรูป ในโทรศัพท์มือถือ ไฟล์เสียง ไฟล์วิดีโอ หรือแม้แต่ในเครื่องเล่นเกม เรียกว่า Computer or Electronics

Forensic ส่วนการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลในเครือข่ายคอมพิวเตอร์หรือเครือข่ายโทรคมนาคม เรียกว่า Network Forensic ซึ่งข้อมูลดิจิทัลที่ส่งผ่านในเครือข่ายการสื่อสารนั้น คือการทำ “สำเนา” ไปเรื่อยๆ ไม่ได้ส่งไฟล์แล้วไฟล์ต้นฉบับจะหายไปด้วย ต่างจากการส่งจดหมายทางไปรษณีย์เป็นการส่งต้นฉบับไปถึงผู้รับ ซึ่งการส่งจดหมายทางอีเมลล์ ไฟล์ต้นฉบับยังอยู่กับเจ้าของ แล้วทำการสำเนาส่งต่อกันเรื่อยๆ ผ่าน Server ผ่านโครงข่ายโทรคมนาคมไปยังอุปกรณ์ปลายทาง การรู้ข้อมูลต้นทางหรือระหว่างทางนั่นก็สามารถพิสูจน์ได้ว่าข้อมูลปลายทางคืออะไร



ภาพที่ 2 ผังการศึกษาการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล

ที่มา: โดยผู้เขียนปรับปรุงจาก Larry และ Lars E. Daniel., (2559)

4. หลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล

นักศึกษาด้านอาชญาวิทยาหรือนิติวิทยาศาสตร์หรือนิติศาสตร์ และนักเรียนนายร้อยตำรวจหรือพนักงานสอบสวนควรทราบหลักการพื้นฐานในการตรวจพิสูจน์พยานหลักฐานดิจิทัล 4 ข้อ (Larry และ Lars E. Daniel., 2559) ในการตรวจพิสูจน์พยานหลักฐานดิจิทัล ประกอบไปด้วย

4.1 การรวบรวมพยานหลักฐานดิจิทัล (Acquisition)

เป็นจุดเริ่มต้นที่พนักงานสอบสวนหรือพิสูจน์หลักฐานได้สัมผัสพยานหลักฐานดิจิทัลครั้งแรก สิ่งสำคัญที่สุดคือสร้างความเชื่อมั่นเรื่องความสมบูรณ์ของพยานหลักฐาน และการรวบรวมพยานหลักฐานทั้งหมด (ยึด) หรือทำสำเนา ฮาร์ด ไดรฟ์ เป็นไปอย่างสมบูรณ์ขณะเกิดเหตุไม่ได้ถูกเปลี่ยนแปลงแก้ไขใดๆ ทั้งสิ้น

4.2 การเก็บรักษาพยานหลักฐานดิจิทัล (Preservation)

จะต้องเก็บรักษาไว้ในสภาพรับฟังได้ในชั้นศาล การเก็บรักษาเป็นไปตามกระบวนการสร้างห่วงโซ่คุ้มครองพยานหลักฐาน (Chain of Custody) และ Hash value กล่าวได้ว่าในหลักสากลมีมาตรฐานการเก็บรักษาพยานหลักฐานดิจิทัลที่ทุกฝ่ายยอมรับ มีบันทึกขั้นตอนการคุ้มครองพยานหลักฐานและวิธีการเก็บรักษา ให้มั่นใจได้ว่าข้อมูลไม่ได้ถูกแก้ไขเปลี่ยนแปลงนับจากที่ได้รับอุปกรณ์มาจากผู้ต้องหา กระบวนการ Hash จะเป็นฮาร์ดดิสก์ทั้งลูกหรือเป็นหน่วยความจำทำการเข้ารหัสข้อมูลแบบ SHA (Secure Hash Algorithm) และเก็บกุญแจไว้ ซึ่งมีเพียงเจ้าหน้าที่เท่านั้นที่มีกุญแจไขเข้าไปตรวจสอบข้อมูลได้

4.3 การวิเคราะห์พยานหลักฐานดิจิทัล (Analysis)

พยานหลักฐานแต่ละประเภทคดีแตกต่างกัน คดี Romance scam คดีฉ้อโกง คดีคอร์รัปชั่น คดีหมิ่นประมาท เป็นต้น วิธีวิเคราะห์จึงแตกต่างกัน เครื่องมือแตกต่างกัน ทักษะเจ้าหน้าที่แตกต่างกัน การฝึกอบรมเจ้าหน้าที่พิสูจน์หลักฐานจึงสำคัญที่สุด ผู้เชี่ยวชาญคอมพิวเตอร์ แตกต่างกับ เจ้าหน้าที่พิสูจน์หลักฐานดิจิทัล การวิเคราะห์พยานหลักฐานดิจิทัล จึงต้องใช้ผู้เชี่ยวชาญด้านพยานหลักฐานดิจิทัลมาวิเคราะห์

4.4 การนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล (Presentation)

การนำเสนอผลการตรวจพิสูจน์พยานหลักฐานดิจิทัล “เป็นรายงานรวมบันทึกคำให้การผู้เชี่ยวชาญ” ซึ่งอธิบายวิธีการตรวจสอบ เครื่องมือที่ใช้ตรวจสอบ ตรวจสอบสิ่งใดบ้าง วิธีเก็บพยานหลักฐาน สิ่งที่ค้นพบ และวิธีการยืนยันความแท้จริงของพยานหลักฐานดิจิทัล

ผู้เชี่ยวชาญ คือ กุญแจสำคัญของคดี โดยเฉพาะอย่างยิ่งการนำเสนอผลพิสูจน์พยานหลักฐานดิจิทัล ไม่ใช่เป็นผู้ที่มีความรู้เท่านั้น ต้องมีองค์ประกอบของความน่าเชื่อถือครบถ้วนด้วย ที่สำคัญที่สุดคือทักษะการสื่อสาร ทั้งการสื่อสารกับลูกความ และผู้ที่เกี่ยวข้องกับคดี ตลอดจนการให้การต่อศาล

5. มาตรฐานในการพิสูจน์พยานหลักฐานดิจิทัลต้องเป็นสากล

การพิสูจน์พยานหลักฐานดิจิทัล ต้องมีมาตรฐานสากลที่เป็นการยอมรับของทุกฝ่าย ทั้งเจ้าหน้าที่ตำรวจ ทั้งผู้เชี่ยวชาญ และเครื่องมือที่ใช้ในการศึกษาทดลอง และปฏิบัติจริง ข้อมูลคร่าวๆ ที่รวบรวมมาได้ดังนี้

5.1 ห้องทดลองหรือห้องทดสอบ (Laboratory)

ห้องทดลอง ทดสอบหรือ Laboratory ต้องมีการจัดเตรียมสภาพแวดล้อม และลักษณะทางกายภาพให้เหมาะสมได้มาตรฐาน ซึ่งมาตรฐานสากลทางด้านการตรวจสอบพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ (Computer Forensics) เช่น ISO 17020, ISO 17025 หรือ ISO 27001

5.2 หลักสูตรการฝึกอบรมและประกาศนียบัตรรับรอง

ที่ผ่านมามีหลายหน่วยงานได้พัฒนาองค์ความรู้และหลักสูตรการอบรม เช่น สถาบันฝึกอบรมและวิจัยการพิสูจน์หลักฐานตำรวจ เป็นหน่วยงานสังกัด สำนักงานพิสูจน์หลักฐานตำรวจ และศูนย์ดิจิทัลฟอเรนสิกส์ (Digital Forensics Center) ภายใต้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA เป็นต้น

โรงเรียนนายร้อยตำรวจควรเป็นศูนย์กลางด้านวิชาการด้านการอบรมการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล โดยบูรณาการหลักสูตรอบรมขึ้นมาใหม่เพื่อความสอดคล้องเป็นไปในทิศทางเดียวกัน และต้องจัดอบรมให้ตำรวจหรือพนักงานสอบสวนหมุนเวียนมาฝึกอบรมทั้งประเทศ รวมทั้งประชาชนภายนอกที่สนใจหรือผู้ประกอบวิชาชีพกฎหมายที่ต้องการประกาศนียบัตรรับรองเพื่อเป็นผู้เชี่ยวชาญด้านการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล

ปัจจุบันผู้เชี่ยวชาญการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลมีบทบาทสำคัญในการตัดสินพิจารณาคดีต่างๆ ซึ่งผู้เชี่ยวชาญขึ้นอยู่กับศาลและคู่ความเห็นชอบ แต่จำนวนผู้ที่ผ่านการฝึกอบรมหรือมีใบประกาศนียบัตรรับรองมีจำนวนน้อย เพราะการเข้าถึงหลักสูตรต่างๆ นั้นเป็นไปได้ยาก และมีค่าใช้จ่ายสูง

การบูรณาการหลักสูตรอบรมขึ้นมาใหม่ โรงเรียนนายร้อยตำรวจอาจสร้างความร่วมมือกับหน่วยต่างๆ และร่วมกับหลักสูตรต่างประเทศ เพื่อสร้างเป็นมาตรฐานสากล ขอยกตัวอย่างหลักสูตรการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลในสากลดังนี้

- EnCase Certified Examiner (EnCe) ประกาศนียบัตรโดย บริษัท Guidance Software ซึ่ง EnCase เป็นโปรแกรมตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลที่ได้รับความนิยมที่สุด
- Access Certified Examiner (ACE) ประกาศนียบัตรสำหรับซอฟต์แวร์ Forensic tool kit โดยบริษัท Access Data Corporation FTK เป็นซอฟแวร์ที่ถูกนำมาใช้แพร่หลายในสากล

- Certified Computer Examiner (CCE) ประกาศนียบัตรรับรองไม่เกี่ยวกับผู้ผลิต โดย The International Society of Forensic Computer Examiner
- GIAC Certified Forensic Examiner (GCFE) และ GIAC Certified Forensic Analyst (GCFA) ประกาศนียบัตรรับรองที่ไม่เกี่ยวข้องกับผู้ผลิตโดย SANS Institute
- ฯลฯ

5.3 เครื่องมือการตรวจสอบพิสูจน์หลักฐานดิจิทัลเป็นสากล

เมื่อมีห้องทดลองทดสอบที่เป็นสากลแล้ว เครื่องมือการตรวจสอบพิสูจน์หลักฐานดิจิทัลก็ต้องได้มาตรฐานสากล เครื่องมือส่วนใหญ่ก็คือคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่มีชุดโปรแกรมการตรวจสอบพิสูจน์หลักฐานดิจิทัลดังนี้

5.3.1 Software

ชุดโปรแกรมการตรวจสอบพิสูจน์หลักฐานดิจิทัลที่ได้รับความนิยมในสากล เช่น EnCase และ FTK ที่ถูกใช้ทั่วโลก และได้รับการยอมรับมากที่สุด

EnCase มีเครื่องมือสำเร็จรูปหลายอย่างที่ต้องใช้ในกระบวนการตรวจสอบพิสูจน์หลักฐานดิจิทัล ตั้งแต่การได้มาซึ่งพยานหลักฐาน การวิเคราะห์ และการรายงาน ซอฟต์แวร์ดังกล่าวยังรองรับการเขียนโปรแกรมสคริปต์ ชื่อว่า EnScript ซึ่งมี API หลายอย่างเตรียมไว้ให้เพื่ออ่านเขียนโต้ตอบกับตัวหลักฐาน

ส่วน FTK ของบริษัท AccessData สามารถดาวน์โหลดได้ฟรีจาก https://accessdata.com/product-download

5.3.2 Hardware

ฮาร์ดแวร์ที่ได้รับความนิยมในการใช้ตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลจากโทรศัพท์เคลื่อนที่ก็คือ Cellebrite ของบริษัท Cellebrite Mobile Synchronization ที่โด่งดังจากการที่ FBI ร้องขอให้ Apple ช่วยถอดรหัส iPhone แต่ไม่ต้องรอความช่วยเหลือจาก Apple เมื่อได้รับความร่วมมือจาก Cellebrite ซึ่งเป็นผู้เชี่ยวชาญด้านการตรวจหาหลักฐานดิจิทัลในอิสราเอล เป็นบริษัทลูกของ Sun Corporation ในญี่ปุ่น นอกจากอุปกรณ์นี้ ยังมีอุปกรณ์อื่นๆ ที่ทันสมัยอีกหลายชนิด

บทสรุปและข้อคิดเห็นทางวิชาการ

ปัญหาอาชญากรรมไซเบอร์ในไทยได้ให้ความสำคัญอย่างสูงต่อเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) หากจะสังเกตเห็นได้จากตำรา สถานศึกษา และหน่วยงานภาครัฐ รวมทั้งความพยายามตรากฎหมายเรื่องความมั่นคงปลอดภัยทางไซเบอร์ แต่จากการย่อเรื่องราวปรากฏการณ์อาชญากรรมที่ผ่านมาในต้นบทความนั้น อาชญากรรมไซเบอร์ไม่ได้หยุดอยู่กับที่กลับมีพลวัตทวีความรุนแรงเติบกว้างขวางไปมากมายหลายรูปแบบ ทั้งการนำเทคโนโลยีการสื่อสารไปประกอบอาชญากรรม และอาชญากรรมรูปแบบใหม่ที่เกิดจากเทคโนโลยีการสื่อสาร เช่น การฉ้อโกงสินทรัพย์ดิจิทัล การล่อลวงเด็กทางอินเทอร์เน็ตเพื่อค้ามนุษย์ การระดมทุนการก่อการร้ายด้วยเงินเสมือน การใช้โดรนติดปืนเคลื่อนที่อัตโนมัติโดยระบบระบุพิกัดสังหารเหยื่อ การลักพาตัวคนมาทรมานให้ชมผ่านดาร์คเว็บ (Dark web) และจ่ายค่าเข้าชมด้วย บิตคอยน์ (Bitcoin) เป็นต้น สิ่งเหล่านี้ยังไม่ได้รับความสนใจในวงกว้างหรือรัฐยังไม่มีมาตรการที่จะป้องกันก่อนภัยคุกคามมาถึงไทย

การรวบรวมพยานหลักฐานดิจิทัลในปัจจุบัน ผู้สนใจศึกษาเพื่อเป็นผู้เชี่ยวชาญการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลยังมีน้อย ซึ่งไม่จำเป็นต้องเป็นวิศวกรหรือโปรแกรมเมอร์ จะเป็นผู้ใดก็ได้ที่รู้จักกระบวนการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัล และใช้เครื่องมือเป็น โดยผ่านการอบรมหลักสูตรที่มีมาตรฐานสากลก็สามารถเป็นได้ แต่ทั้งหลักสูตรการศึกษาและสถาบันการศึกษาในไทยยังให้ความสนใจน้อย อาจทำให้กระบวนการยุติธรรมไทยมีปัญหามากมายในภายภาคหน้า เช่น คำพิพากษาศาลฎีกาคดี หมายเลขดำ อ.4857/2554 พนักงานอัยการฝ่ายคดีอาญา 6 เป็นโจทก์ยื่นฟ้องโปรแกรมเมอร์อิสระนายหนึ่งใช้ E-mail กระทำความผิดในฐานหมิ่นประมาท ดูหมิ่น หรือแสดงความอาฆาตมาดร้ายพระมหากษัตริย์ พระราชินี ตามประมวลกฎหมายกฎหมายอาญา มาตรา 112 และนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ และ พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3, 14, 17 แต่ในการพิจารณาคดีนั้น จำเลยไม่ได้ยกข้อต่อสู้ว่าได้กระทำความผิดหรือไม่ แต่มุ่งไปที่การตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลว่าเป็นไปตามกระบวนการหรือไม่ โดยทนายความได้แสดงให้เห็นว่าคอมพิวเตอร์ที่ถูกยึดตั้งแต่ช่วงที่มีการจับกุมพบ timestamp ที่แสดงถึงการเปิดเครื่องใช้งานก่อนจะมีการส่งตรวจพิสูจน์หลักฐาน ดังนั้นจึงยกฟ้องจำเลยทั้ง 3 ศาลจนถึงชั้นฎีกา

ดังนั้น ในการเสนอความเห็นทางวิชาการ เห็นว่าสมควรแก่เวลาแล้วที่จะต้องปฏิรูปงานวิชาการด้านอาชญากรรมไซเบอร์ให้มีความเป็นวิชาการ มีตำรา มีบทความวิชาการ มีหลักสูตรที่เป็นรูปธรรม มีสถาบันอบรมการตรวจสอบพิสูจน์พยานหลักฐานดิจิทัลที่ได้มาตรฐานสากลหรือรัฐกำหนดมาตรฐานขึ้น

และผู้สนใจเข้าศึกษาสามารถเข้าถึงโอกาสได้โดยง่าย ซึ่งหากรัฐหรือสถานศึกษาปรับองค์ความรู้ทางวิชาการหรือหลักสูตรเพื่อผลิตบุคลากรมารองรับเข้ากับยุคสมัยมากขึ้นแล้ว ยังแสดงให้เห็นถึงวิสัยทัศน์ในการวางแผนยุทธศาสตร์รับมือภัยคุกคามรูปแบบใหม่ๆ จากโลกอนาคตในระดับชาติได้อย่างดี

เอกสารอ้างอิง

คณะทำงานจัดทำร่างมาตรฐานการปฏิบัติงานตรวจพิสูจน์พยานหลักฐานดิจิทัล (2559). **ข้อเสนอแนะมาตรฐานการจัดการอุปกรณ์ดิจิทัลในงานตรวจพิสูจน์พยานหลักฐาน Version 1.0**. ศูนย์ดิจิทัลฟอเรนสิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน).

พรชัย ขันตี. (2558). **ทฤษฎีอาชญาวิทยา: หลักการ งานวิจัย และนโยบายประยุกต์.** กรุงเทพมหานคร: ส.การพิมพ์.

พรศักดิ์ ผ่องแผ้ว. (2529). **ศาสตร์แห่งการวิจัย.** กรุงเทพมหานคร: สำนักพิมพ์ไทยวัฒนาพานิช.

รัตนะ บัวสนธ์. (2560). **ปรัชญาวิจัย**. (พิมพ์ครั้งที่ 4). กรุงเทพมหานคร: จุฬาลงกรณ์มหาวิทยาลัย.

Financial Action Task Force (FATF). (2015). **Guidance for a RISK-BASED approach**. VIRTUAL CURRENCIES. France: Paris Cedex.

Kabay M. E. (2008). **A Brief History of Computer Crime: An Introduction for Students**. School of Graduate Studies, Norwich University.

Larry E. Daniel, Lars E. Daniel. (2559). **การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย.** สุนีย์ สกาวรัตน์, ผู้แปล. กรุงเทพฯ: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง.

Petter Gotschalk. (2010). **Policing Cyber Crime**. Retrieved June 22, 2018. from https://bookboon.com/en/policing-cyber-crime-ebook.

ผู้เขียน

คำนำหน้า ชื่อ-สกุล	**นายปรเมศวร์ กุมารบุญ**
หน่วยงาน/สังกัด	หลักสูตรอาชญาวิชาและการยุติธรรมภาควิชาสังคมวิทยาและมานุษยวิทยา
ที่อยู่ของหน่วยงาน	คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ถนนอังรีดูนังต์ แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330
E-mail:	poramez@live.com