แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด ด้านการอำนวยความยุติธรรมทางอาญาเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐

โดย

นายธีระวัฒน์ พุฒิบูรณวัฒน์
อัยการผู้เชี่ยวชาญพิเศษ
สำนักงานอัยการสูงสุด

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๙
ประจำปีการศึกษา พุทธศักราช ๒๕๕๙ – ๒๕๖๐

บทคัดย่อ

เรื่อง แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐

ลักษณะวิชา ยุทธศาสตร์

ผู้วิจัย นายธีระวัฒน์ พุฒิบูรณวัฒน์ หลักสูตร วปอ. รุ่นที่ ๕๙

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ แนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดให้เหมาะสมและมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐ โดยมีขอบเขตการวิจัยมุ่งเน้นศึกษาผลกระทบด้านคดีอาชญากรรมทางเศรษฐกิจที่มีการใช้คอมพิวเตอร์ในการกระทำความผิดและคดีที่มีการกระทำความผิดต่อระบบคอมพิวเตอร์ โดยการรวบรวมข้อมูลปฐมภูมิจากวิธีการสัมภาษณ์ข้อมูลเชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิ และข้อมูลทุติยภูมิจากการทบทวนวรรณกรรมและสถิติที่เกี่ยวข้อง ผลการวิจัยพบว่า ปริมาณคดีอาชญากรรมคอมพิวเตอร์มีแนวโน้มสูงขึ้นและมีความซับซ้อนมากขึ้นกว่าในอดีต พบปัญหาและอุปสรรคสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการจากปัจจัยภายในองค์กร เช่น การจัดเก็บสถิติคดีอาชญากรรมคอมพิวเตอร์ที่ยังไม่เหมาะสม การขาดการจัดสรรงบประมาณที่เพียงพอ และบุคลากรผู้ปฏิบัติงานขาดองค์ความรู้ที่เหมาะสม รวมถึงปัจจัยภายนอกองค์กร ได้แก่ เจ้าพนักงานสืบสวนและพนักงานสอบสวนขาดองค์ความรู้ที่เหมาะสม และขาดการประสานความร่วมมือกันระหว่างหน่วยงานที่เกี่ยวข้อง ดังนั้นผู้วิจัยจึงมีข้อเสนอแนะว่า สำนักงานอัยการสูงสุดควรจัดเก็บสถิติอาชญากรรมคอมพิวเตอร์ให้สอดคล้องกับฐานข้อมูลสถิติของหน่วยงานในกระบวนการยุติธรรมอื่น จัดสรรงบประมาณสำหรับแผนงานพัฒนาศักยภาพในการดำเนินคดีของสำนักงานคดีทั้งหมดภายในสำนักงานอัยการสูงสุดอย่างบูรณาการเพื่อเป็นการประหยัดในเชิงงบประมาณ โดยการจัดอบรมให้ความรู้แก่ผู้ปฏิบัติงานควรส่งเสริมให้มีการประสานงานความร่วมมือกับหน่วยงานภายนอก ควบคู่ไปกับการพัฒนาเครื่องมือในการปฏิบัติงานอย่างยั่งยืน เช่น การจัดตั้งศูนย์รวบรวม วิเคราะห์ และเผยแพร่องค์ความรู้ให้แก่พนักงานอัยการ และการปรับปรุงคู่มือสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ให้เป็นปัจจุบัน และประการสำคัญคือ การสร้างแนวทางประสานความร่วมมือในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับหน่วยงานในกระบวนการยุติธรรมอื่น

คำนำ

ระบบคอมพิวเตอร์และอินเทอร์เน็ตมีผลกระทบเปลี่ยนแปลงของสภาพเศรษฐกิจและสังคมของโลกในยุคปัจจุบันให้แตกต่างไปจากในอดีตอย่างมาก การประกอบธุรกิจทางการค้าแบบดั้งเดิมถูกแทนที่โดยธุรกรรมทางอิเล็กทรอนิกส์ และเมื่อภาครัฐส่งเสริมนโยบายประเทศไทย ๔.๐ ในการขับเคลื่อนเศรษฐกิจและสังคมด้วยดิจิทัล ปริมาณการใช้งานระบบคอมพิวเตอร์และอุปกรณ์ดิจิทัลย่อมมีแนวโน้มเพิ่มมากขึ้น ซึ่งการขับเคลื่อนนโยบายประเทศไทย ๔.๐ อย่างมั่นคงและยั่งยืนนั้น ภาครัฐจำเป็นต้องสร้างกลไกในการคุ้มครองความมั่นคงปลอดภัยทางไซเบอร์เพื่อให้ผู้ที่ทำธุรกรรมทางอิเล็กทรอนิกส์เกิดความมั่นใจ ซึ่งยังรวมไปถึงกลไกในการดำเนินมาตรการทางกฎหมายกับผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ด้วย โดยสำนักงานอัยการสูงสุดเป็นองค์กรในกระบวนการยุติธรรมทางอาญาที่มีบทบาทสำคัญในการพิจารณามีความสั่งฟ้องผู้กระทำความผิดแล้วนำผู้กระทำความผิดเข้าสู่กระบวนการพิจารณาในศาลเพื่อพิสูจน์ความผิดและรับโทษ

อย่างไรก็ดี จากการที่ลักษณะของการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความพิเศษแตกต่างไปจากการดำเนินคดีอาญาทั่วไปบางประการ อาทิเช่น รูปแบบการรวบรวมพยานหลักฐาน การพิจารณาพยานหลักฐาน และการนำสืบคดีในชั้นศาล พนักงานอัยการผู้ดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์จึงจำเป็นต้องมีองค์ความรู้ด้านระบบคอมพิวเตอร์และองค์ความรู้ด้านพยานหลักฐานทางดิจิทัลอย่างเหมาะสม

การวิจัยนี้จึงมุ่งศึกษาสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ แนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด และแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการ เพื่อประโยชน์โดยรวมในการสร้างความมั่นคงปลอดภัยทางเศรษฐกิจและสังคมโดยรวมของชาติ

.

(นายธีระวัฒน์ พุฒิบูรณวัฒน์)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๕๙
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

การกำหนดยุทธศาสตร์และแผนปฏิบัติราชการของหน่วยงานภาครัฐจำเป็นต้องสอดคล้องกับแผนยุทธศาสตร์ชาติซึ่งเป็นกรอบภาพรวมของการจัดทำนโยบายและการจัดสรรงบประมาณของรัฐบาล รวมไปถึงต้องสอดคล้องกับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติด้วย เพื่อให้การปฏิบัติราชการของหน่วยราชการต่างๆเป็นไปในทิศทางเดียวกันและสอดคล้องกัน ทั้งนี้ เมื่อประมาณกลางปีพ.ศ. ๒๕๕๙ พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) ได้กล่าวมอบนโยบายและปาฐกถาพิเศษในงานวาระต่างๆ เกี่ยวกับการนำพาประเทศไทยก้าวสู่โมเดล “ประเทศไทย ๔.๐” หรือ “ไทยแลนด์ ๔.๐” อันเป็นกลไกขับเคลื่อนการปฏิรูปเศรษฐกิจและความมั่นคงในศตวรรษที่ ๒๑ ไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม (Value-based Economy) โดยการเติมเต็มด้วยวิทยาการ ความคิดสร้างสรรค์ นวัตกรรม วิทยาศาสตร์ เทคโนโลยี และการวิจัยและการพัฒนา โดยมีกลุ่มดิจิทัล เทคโนโลยีอินเทอร์เน็ตที่เชื่อมต่อและบังคับอุปกรณ์ต่างๆ เป็นหนึ่งในกลุ่มเทคโนโลยีและอุตสาหกรรมเป้าหมาย แนวนโยบายนี้ได้ถูกผนวกรวมอยู่ในยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ – ๒๕๗๙) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ซึ่งเป็นแผนที่สอดรับกับยุทธศาสตร์ชาติระยะ ๒๐ ปี ในลักษณะของการถ่ายทอดยุทธศาสตร์ระยะยาวลงสู่การปฏิบัติในช่วงเวลา ๕ ปี ซึ่งได้ให้ความสำคัญกับการพัฒนาเศรษฐกิจและสังคมดิจิทัล (ปรเมธี วิมลศิริ, ออนไลน์, ๒๕๖๐)

ในส่วนของสำนักงานอัยการสูงสุดซึ่งเป็นหน่วยงานสำคัญในกระบวนการยุติธรรมทางอาญา ได้ประกาศใช้ยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ อันเป็นแผนแม่บทยุทธศาสตร์เฉพาะขององค์กรอัยการ โดยในส่วนของแผนงานด้านการอำนวยความยุติธรรมทางอาญา แม้ว่าสำนักงานอัยการสูงสุดได้มีการกำหนดกลยุทธ์เพื่อเพิ่มประสิทธิภาพในการดำเนินคดีอาญาของพนักงานอัยการ เพิ่มขีดความสามารถของพนักงานอัยการด้านการสอบสวน และเพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญาสำหรับคดีที่มีลักษณะของอาชญากรรมข้ามชาติไว้แล้วก็ตาม แต่ยุทธศาสตร์สำนักงานอัยการสูงสุดฉบับดังกล่าว มีการจัดทำและประกาศใช้ก่อนที่ยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ – ๒๕๗๙) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ซึ่งผนวกรวมแนวนโยบายประเทศไทย ๔.๐ ไว้ จะบังคับใช้

เนื่องจากสภาพเศรษฐกิจและสังคมของโลกในยุคปัจจุบันได้เปลี่ยนแปลงไปจากอดีตอย่างมาก จนมีคำพูดว่า “The whole world has gone digital” หรือ “โลกทั้งใบได้เปลี่ยนเป็นดิจิทัลแล้ว” ดังจะเห็นได้จากอัตราการเติบโตในแต่ละปีของจำนวนผู้ใช้งานอินเทอร์เน็ตผ่านอุปกรณ์ในการสื่อสาร โทรศัพท์เคลื่อนที่ Smart Phone หรือแม้แต่บรรดาสิ่งอำนวยความสะดวกในครัวเรือน

เช่น ทีวี ระบบไฟฟ้า หรือระบบรักษาความปลอดภัย ก็ล้วนมีการนำเอาระบบคอมพิวเตอร์มาใช้ในการประมวลผลและควบคุมการใช้งาน นอกจากนี้ ในด้านของธุรกรรมทางอิเล็กทรอนิกส์ซึ่งได้รับความนิยมจากผู้บริโภคเพิ่มมากขึ้นทุกปี ระบบคอมพิวเตอร์ได้ถูกนำมาใช้เป็นช่องทางในการขับเคลื่อนเศรษฐกิจเพื่อการซื้อ การขาย และการชำระราคาสินค้า ดังจะเห็นได้จากธุรกรรมทางอิเล็กทรอนิกส์ที่ถูกนำมาแทนที่รูปแบบการประกอบธุรกิจทางการค้าแบบดั้งเดิม โดยในปัจจุบันผู้ซื้อและผู้ขายไม่จำต้องพบหน้ากัน ไม่ต้องส่งมอบเงินสดในการชำระค่าราคาสินค้า แต่สามารถซื้อขายสินค้าและชำระราคาผ่านวิธีการทางอิเล็กทรอนิกส์ได้อย่างรวดเร็ว หรือแม้แต่ในเรื่องของการจัดการทางการเงิน ผู้บริโภคไม่จำต้องเสียเวลาและสิ้นเปลืองค่าใช้จ่ายในการเดินทางไปยังธนาคารเพื่อทำธุรกรรม แต่ผู้บริโภคสามารถเลือกใช้วิธีจัดการทางการเงินผ่านระบบธนาคารทางอินเทอร์เน็ต (I-Banking) หรือระบบธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking) แต่ทว่า เมื่อธุรกรรมต่างๆ สามารถเกิดขึ้นได้ในเวลาอันรวดเร็วและไร้ข้อจำกัด ในทางกลับกัน ธุรกรรมดังกล่าวก็อาจตกเป็นเป้าหมายของกลุ่มมิจฉาชีพที่ใช้คอมพิวเตอร์เป็นเครื่องมือในกระทำความผิด หรือมิจฉาชีพซึ่งประสงค์กระทำความผิดต่อระบบคอมพิวเตอร์โดยตรงไม่ว่าเพื่อแสวงหาประโยชน์ในทางมิชอบหรือเพื่อทำให้บุคคลหนึ่งบุคคลใดเสียหาย ซึ่งความเสียหายของอาชญากรรมเกี่ยวกับคอมพิวเตอร์มักเกิดเป็นความเสียหายในวงกว้างและมีมูลค่าความเสียหายจำนวนสูงมาก (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ออนไลน์, ๒๕๕๙) ดังนั้น การขับเคลื่อนและการพัฒนาเศรษฐกิจซึ่งอาศัยเทคโนโลยีในกลุ่มดิจิทัลเป็นพื้นฐานจึงต้องมีโครงสร้างความมั่นคงปลอดภัยทางไซเบอร์เพื่อการสร้างความเชื่อมั่นกับผู้กระทำธุรกรรม

อย่างไรก็ดี เมื่อมีการกระทำความผิดอาญาเกี่ยวกับคอมพิวเตอร์เกิดขึ้น เช่น การฉ้อโกงหรือฉ้อโกงประชาชนด้วยวิธีการนำเข้าซึ่งข้อมูลปลอมหรือข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ การปลอมแปลงข้อมูลในระบบคอมพิวเตอร์ของผู้อื่น หรือการกระทำใดๆเพื่อให้เกิดผลกระทบต่อการใช้งานระบบคอมพิวเตอร์โดยปกติของบุคคลอื่น บุคลากรในหน่วยงานด้านการยุติธรรมตามทฤษฎีการดำเนินคดีอาญาโดยรัฐที่มีอำนาจหน้าที่พิจารณามีคำสั่งฟ้องหรือไม่ฟ้องผู้ต้องหาในคดีอาญาและดำเนินคดีอาญาชั้นพิจารณาในศาล คือ พนักงานอัยการ ซึ่งพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ มาตรา ๑๑ และมาตรา ๑๔(๒) ได้กำหนดให้พนักงานอัยการมีฐานะเป็นทนายแผ่นดิน มีอำนาจหน้าที่ในคดีอาญาตามที่ประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นซึ่งบัญญัติว่าเป็นอำนาจหน้าที่ของสำนักงานอัยการสูงสุด แต่ทว่าลักษณะของการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความพิเศษแตกต่างไปจากการดำเนินคดีอาญาทั่วไปบางประการ อาทิเช่น รูปแบบการรวบรวมพยานหลักฐาน การพิจารณาพยานหลักฐาน และการนำสืบคดีในชั้นศาล พนักงานอัยการผู้ดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์จึงจำเป็นต้องมีองค์ความรู้ด้านระบบคอมพิวเตอร์และองค์ความรู้ด้านพยานหลักฐานทางดิจิทัลอย่างเหมาะสม

เมื่อปริมาณงานด้านคดีอาชญากรรมคอมพิวเตอร์ภายหลังการดำเนินการภายใต้นโยบายประเทศไทย ๔.๐ มีแนวโน้มสูงขึ้นตามการใช้งานระบบคอมพิวเตอร์ และการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ หากสำนักงานอัยการสูงสุดซึ่งมีบทบาทหน้าที่ด้านงานคดีอาชญากรรมคอมพิวเตอร์ยังไม่มีแผนงานที่ชัดเจนเพื่อเตรียมความพร้อมในด้านต่างๆเพื่อการตอบโต้อาชญากรรมคอมพิวเตอร์ย่อมส่งผลทำให้เกิดปัญหาในประสิทธิภาพในการอำนวยความยุติธรรมทางอาญาในคดีอาชญากรรม

คอมพิวเตอร์ และส่งผลกระทบในภาพรวมถึงความมั่นคงทางเศรษฐกิจและสังคมของชาติ ดังนั้น ข้อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด และแนวทาง การกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ ให้สอดคล้องกับการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ จึงมีความจำเป็นและสำคัญอย่างยิ่งยวด เพื่อให้กระบวนการบังคับใช้กฎหมายอาญาในชั้นของพนักงานอัยการเป็นไปโดยมีประสิทธิภาพ สามารถอำนวยความยุติธรรมให้กับผู้มีส่วนได้เสียในคดี รวมทั้งสร้างความมั่นใจให้กับประชาชนซึ่งทำธุรกรรมต่างๆในโลกดิจิทัล เพื่อประโยชน์โดยรวมในการสร้างความมั่นคงปลอดภัยทางเศรษฐกิจและสังคมโดยรวมของชาติ

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐

๒. เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐

ขอบเขตของการวิจัย

๑. ขอบเขตด้านเนื้อหา มุ่งเน้นศึกษาผลกระทบด้านคดีอาชญากรรมทางเศรษฐกิจที่มีการใช้คอมพิวเตอร์ในการกระทำความผิด และคดีที่มีการกระทำความผิดต่อระบบคอมพิวเตอร์ จากการพัฒนากลุ่มดิจิทัล และเทคโนโลยีด้านพาณิชย์ทางอิเล็กทรอนิกส์ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ โดยเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเฉพาะงานด้านการอำนวยความยุติธรรมซึ่งเกี่ยวข้องกับแผนงานในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการ นอกจากนี้ เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ มีผลใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษา (๒๔ มกราคม ๒๕๖๐) ซึ่งตรงกับวันที่ ๒๔ พฤษภาคม ๒๕๖๐ ดังนั้น ข้อมูลที่อ้างอิงในเอกสารวิจัยนี้ส่วนใหญ่จึงยังคงเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒. ขอบเขตด้านประชากร มุ่งเน้นศึกษาแนวคิดของผู้ทรงคุณวุฒิโดยใช้วิธีการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านการคดีอาชญากรรมคอมพิวเตอร์ รวม ๑๐ คน

๓. ขอบเขตด้านพื้นที่ มุ่งเน้นศึกษาแนวทางการกำหนดยุทธศาสตร์และแผนแม่บทด้านความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ ซึ่งเป็นประเทศต้นแบบด้านการตอบโต้ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์

๔. ขอบเขตด้านเวลา มุ่งเน้นศึกษาสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทยย้อนหลังไม่เกิน ๕ ปี

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

๑. การรวบรวมข้อมูล

๑.๑ ข้อมูลทุติยภูมิ (Secondary Data) เป็นการศึกษาบทบัญญัติกฎหมาย ระเบียบ คำสั่ง คู่มือ แนวทางปฏิบัติของหน่วยงาน รวมถึงเอกสารทางวิชาการต่างๆ ที่มีผู้ศึกษาเอาไว้แล้ว ทั้งจากสื่ออิเล็กทรอนิกส์ วารสาร บทความ หนังสือพิมพ์ หนังสือทั่วไป วิทยานิพนธ์ และงานวิจัยที่มีเนื้อหาเกี่ยวกับนโยบายประเทศไทย ๔.๐ ตามยุทธศาสตร์ชาติ ๒๐ ปี และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ แนวคิดเกี่ยวกับการพัฒนาเศรษฐกิจและสังคมดิจิทัลของไทย สถิติเกี่ยวกับการใช้งานระบบคอมพิวเตอร์และสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มประเทศผู้นำด้านเทคโนโลยีดิจิทัล ได้แก่ สหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ แนวความคิดและทฤษฎีการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยพนักงานอัยการ และแนวความคิดและทฤษฎีการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์สำนักงานอัยการสูงสุด

๑.๒ ข้อมูลปฐมภูมิ (Primary Data) ดำเนินการศึกษาและเก็บรวบรวมข้อมูลภาคสนาม โดยใช้วิธีการสัมภาษณ์และแลกเปลี่ยนเรียนรู้กับกลุ่มผู้ให้ข้อมูลสำคัญที่ได้กำหนดเอาไว้ในหัวข้อขอบเขตของการวิจัย ข้อ ๒ เพื่อสำรวจความคิดเห็นและข้อเสนอแนะจากพนักงานอัยการผู้ทรงคุณวุฒิด้านการคดีอาชญากรรมทางเศรษฐกิจ โดยใช้วิธีการสัมภาษณ์ข้อมูลเชิงลึก (In-depth Interview) จากกลุ่มตัวอย่างในหลากหลายสำนักงานคดีของสำนักงานอัยการสูงสุด

๒. การวิเคราะห์ข้อมูล

ดำเนินการโดยการนำเอาข้อมูลสถิติเกี่ยวกับการใช้งานระบบคอมพิวเตอร์และสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของหน่วยงานต่างๆ ที่รวบรวมได้ในห้วงเวลาย้อนหลังไม่เกิน ๕ ปี มาวิเคราะห์และสังเคราะห์แนวโน้มสภาพปัญหาอาชญากรรมคอมพิวเตอร์ในประเทศไทยภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ เพื่อทราบแนวโน้มโอกาสเกิดอาชญากรรมคอมพิวเตอร์ตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) จากนั้นทำการวิเคราะห์ข้อมูลเกี่ยวกับแนวคิดในการกำหนดยุทธศาสตร์สำนักงานอัยการสูงสุดในการตอบโต้อาชญากรรมคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์ เปรียบเทียบกับแนวคิดแผนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของรัฐบาลและหน่วยงานของต่างประเทศซึ่งเป็นต้นแบบด้านการตอบโต้ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ ได้แก่ สหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ พิจารณาร่วมกับข้อมูลผลการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านคดีอาชญากรรมทางเศรษฐกิจ (ข้อมูลปฐมภูมิ) โดยใช้วิธีการประสมประสานข้อมูล

เข้าด้วยกัน แล้วนำข้อมูลที่ได้จากการวิเคราะห์ดังที่ได้กล่าวมาทั้งหมดมาใช้วิเคราะห์สภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการ และเสนอแนะแนวทางในการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาให้เหมาะสมและมีประสิทธิภาพในการตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐

๒. ทำให้สามารถเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐

คำจำกัดความ (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ผ ๑ – ผ ๒๑; สำนักงานอัยการสูงสุด, ๒๕๕๙)

การกระทำความผิดเกี่ยวกับคอมพิวเตอร์	หมายถึง	การกระทำด้วยประการใดๆให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดหรือทำงานผิดพลาดจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เพื่อให้ล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลอันเป็นเท็จทำให้เกิดความเสียหาย
ความมั่นคงปลอดภัยทางไซเบอร์	หมายถึง	ความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงการรักษาความมั่นคงปลอดภัยในโลกดิจิทัล ซึ่งมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อการสื่อสาร การรักษาข้อมูลความลับของข้อมูลที่ต้องคำนึงถึงการป้องกันภัย และควบคุมการทำรายการผ่านระบบออนไลน์ การป้องกัน การละเมิดข้อมูล มาตรฐานที่เกี่ยวข้องและวิธีการจัดการความปลอดภัย ความเชื่อมั่นของผู้ใช้

ไซเบอร์	หมายถึง	สิ่งที่เกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต โดยเป็นคำที่ลดรูปมาจากคำว่า ไซเบอร์เนติกส์ (cybernetics)
ยุทธศาสตร์	หมายถึง	แผนและนโยบายในการปฏิบัติงานให้เป็นไปตามวัตถุประสงค์ที่กำหนดไว้
ยุทธศาสตร์สำนักงานอัยการสูงสุด	หมายถึง	แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒
ธุรกรรมอิเล็กทรอนิกส์	หมายถึง	ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน การทำธุรกรรมผ่านสื่ออิเล็กทรอนิกส์ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต และระบบโทรศัพท์เคลื่อนที่ ครอบคลุมการทำธุรกรรมตั้งแต่การซื้อขายสินค้าและบริการทางอิเล็กทรอนิกส์ และการชำระเงินทางอิเล็กทรอนิกส์ เป็นต้น
ประเทศไทย ๔.๐	หมายถึง	วิสัยทัศน์เชิงนโยบายการพัฒนาเศรษกิจของประเทศไทย ด้วยความมุ่งมั่นปรับเปลี่ยนโครงสร้างทางเศรษฐกิจไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม (Value-Based Economy) โดยมีฐานคิดหลัก คือ เปลี่ยนจากการผลิตสินค้าโภคภัณฑ์ไปสู่สินค้าเชิงนวัตกรรม เปลี่ยนจากการขับเคลื่อนประเทศด้วยอุตสาหกรรมไปสู่การขับเคลื่อนด้วยเทคโนโลยี ความคิดสร้างสรรค์และนวัตกรรม
พาณิชย์ทางอิเล็กทรอนิกส์	หมายถึง	การประกอบธุรกิจ ดังต่อไปนี้ ๑. การเสนอซื้อหรือขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต ๒. การให้บริการอินเทอร์เน็ต ๓. การให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์ผ่านแม่ข่าย ๔. การบริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต ๕. การทำธุรกรรมโดยวิธีใช้สื่ออิเล็กทรอนิกส์อื่นตามที่กรมพัฒนาธุรกิจการค้าประกาศกำหนด

ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
เศรษฐกิจและสังคมดิจิทัล	หมายถึง	เศรษฐกิจและสังคมที่ใช้เทคโนโลยีดิจิทัล (คอมพิวเตอร์) เป็นกลไกสำคัญในการขับเคลื่อนการปฏิรูปกระบวนการผลิต การดำเนินธุรกิจ การค้า การบริการ การศึกษาการสาธารณสุข การบริหารราชการแผ่นดิน รวมทั้งกิจกรรมทางเศรษฐกิจและสังคมอื่นๆ
สังคมออนไลน์	หมายถึง	สังคมออนไลน์ที่มีผู้ใช้เป็นผู้สื่อสาร หรือเขียนเล่าเนื้อหา เรื่องราว ประสบการณ์ บทความ รูปภาพ และวีดีโอ ที่ผู้ใช้เขียนขึ้นเอง ทำขึ้นเอง หรือพบเจอจากสื่ออื่นๆ แล้วนำมาแบ่งปันให้กับผู้อื่นที่อยู่ในเครือข่ายของตน ผ่านทางเว็บไซต์ เครือข่ายสังคม (Social Network) ที่ให้บริการบนอินเทอร์เน็ต
อาชญากรรมคอมพิวเตอร์	หมายถึง	อาชญากรรมซึ่งมีลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
อาชญากรรมทางเศรษฐกิจ	หมายถึง	อาชญากรรมซึ่งมีลักษณะของการกระทำความผิดโดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งกำไรหรือผลประโยชน์ทางเศรษฐกิจ โดยเป็นการกระทำความผิดต่อกฎหมายที่เกี่ยวกับเศรษฐกิจและการพาณิชย์ที่มีผลกระทบต่อระบบเศรษฐกิจและความมั่นคงของประเทศ

บทที่ ๒
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การศึกษาในบทที่ ๒ นี้ เป็นการทบทวนวรรณกรรมที่เกี่ยวข้อง โดยจะศึกษาครอบคลุมเนื้อหาเกี่ยวกับแนวความคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องกับการอำนวยความยุติธรรมทางอาญาโดยพนักงานอัยการ ในการตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐ โดยมีลำดับการศึกษาดังนี้

๑. แนวความคิดเกี่ยวกับนโยบายประเทศไทย ๔.๐ กับการพัฒนาเศรษฐกิจและสังคมดิจิทัล
๒. แนวความคิดและทฤษฎีการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยพนักงานอัยการ
๓. แนวความคิดและทฤษฎีการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์สำนักงานอัยการสูงสุด
๔. วรรณกรรมที่เกี่ยวข้อง และแนวคิดของผู้ทรงคุณวุฒิ
๕. กรอบความคิดของการวิจัย
๖. สรุป

แนวความคิดเกี่ยวกับนโยบายประเทศไทย ๔.๐ กับการพัฒนาเศรษฐกิจและสังคมดิจิทัล

๑. แนวความคิดนโยบายประเทศไทย ๔.๐

เมื่อประมาณกลางปีพ.ศ. ๒๕๕๙ พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) ได้กล่าวมอบนโยบายและปาฐกถาพิเศษในงานวาระต่างๆ เกี่ยวกับการนำพาประเทศไทยก้าวสู่โมเดล “ประเทศไทย ๔.๐” หรือ “ไทยแลนด์ ๔.๐”

ในเรื่องนี้ สุวิทย์ เมษินทรีย์ (ออนไลน์, ๒๕๕๙) รัฐมนตรีช่วยว่าการกระทรวงพาณิชย์ ได้กล่าวอธิบายเกี่ยวกับโมเดลประเทศไทย ๔.๐ ไว้ค่อนข้างละเอียด ดังนี้

“ประเทศไทย ๔.๐” หรือ “ไทยแลนด์ ๔.๐” เป็นเรื่องเกี่ยวกับโมเดลเศรษฐกิจใหม่ ซึ่งต่างชาติหลายประเทศก็ได้กำหนดโมเดลเศรษฐกิจรูปแบบใหม่เพื่อสร้างความมั่งคั่งในศตวรรษที่ ๒๑ อาทิเช่น “A Nation of Makers” ของสหรัฐอเมริกา “Design of Innovation” ของสหราชอาณาจักร“Made in China 2025” ของสาธารณรัฐประชาชนจีน “Made in India” ของอินเดีย หรือ “Creative Economy” ของสาธารณรัฐเกาหลี (เกาหลีใต้) เป็นต้น

ในช่วง ๕๐ ปีที่ผ่านมา ประเทศไทยยังติดอยู่ใน “กับดักประเทศรายได้ปานกลาง” กล่าวคือ ในช่วงระยะแรก (พ.ศ.๒๕๐๐ – ๒๕๓๖) เศรษฐกิจไทยมีการเติบโตอย่างต่อเนื่องอยู่ที่ร้อย

ละ ๗-๘ ต่อปี อย่างไรก็ตาม ในช่วงระยะถัดมา (พ.ศ.๒๕๓๗-ปัจจุบัน) เศรษฐกิจไทยเริ่มมีการเติบโตในระดับเพียงร้อยละ ๓-๔ ต่อปีเท่านั้น

ในอดีต โมเดลเศรษฐกิจเริ่มต้นจาก “โมเดลประเทศไทย ๑.๐” ที่เน้นภาคการเกษตร ไปสู่ “โมเดลประเทศไทย ๒.๐” ที่เน้นอุตสาหกรรมเบา และก้าวสู่ “โมเดลประเทศไทย ๓.๐” ในปัจจุบันที่เน้นอุตสาหกรรมหนัก ซึ่งนอกจากต้องเผชิญกับกับดักประเทศรายได้ปานกลางแล้ว ประเทศไทยยังต้องเผชิญกับ “กับดักความเหลื่อมล้ำของความมั่งคั่ง” และ “กับดักความไม่สมดุลในการพัฒนา” กับดักเหล่านี้เป็นประเด็นที่ท้าทายรัฐบาล ในการปฏิรูปโครงสร้างเศรษฐกิจ เพื่อก้าวข้าม “ประเทศไทย ๓.๐” ไปสู่ “ประเทศไทย ๔.๐” โมเดลเศรษฐกิจใหม่นี้จึงเป็นความมุ่งมั่นของรัฐที่ต้องการปรับเปลี่ยนโครงสร้างเศรษฐกิจไปสู่ “Value–Based Economy” หรือ “เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม” โดยปรับเปลี่ยนโมเดลเศรษฐกิจเป็น “ทำน้อย ได้มาก” ด้วยการขับเคลื่อนให้เกิดการเปลี่ยนแปลงอย่างน้อยใน ๓ มิติสำคัญ คือ

๑. เปลี่ยนจากการผลิตสินค้า “โภคภัณฑ์” ไปสู่สินค้าเชิง “นวัตกรรม”

๒. เปลี่ยนจากการขับเคลื่อนประเทศด้วยภาคอุตสาหกรรม ไปสู่การขับเคลื่อนด้วยเทคโนโลยี ความคิดสร้างสรรค์ และนวัตกรรม

๓. เปลี่ยนจากการเน้นภาคการผลิตสินค้า ไปสู่การเน้นภาคบริการมากขึ้น

ประเทศไทย ๔.๐ จึงเป็นการเปลี่ยนผ่านทั้งระบบใน ๔ องค์ประกอบสำคัญ คือ

๑. เปลี่ยนจากการเกษตรแบบดั้งเดิม (Traditional Farming) ในปัจจุบัน ไปสู่การเกษตรสมัยใหม่ที่เน้นการบริหารจัดการและเทคโนโลยี (Smart Farming) โดยเกษตรกรต้องร่ำรวยขึ้น และเป็นเกษตรกรแบบเป็นผู้ประกอบการ (Entrepreneur)

๒. เปลี่ยนจาก Traditional SMEs หรือ SMEs ที่รัฐต้องให้ความช่วยเหลืออยู่ตลอดเวลา ไปสู่การเป็น Smart Enterprises และ Startups ที่มีศักยภาพสูง

๓. เปลี่ยนจาก Traditional Services ซึ่งมีการสร้างมูลค่าค่อนข้างต่ำ ไปสู่ High Value Services

๔. เปลี่ยนจากแรงงานทักษะต่ำไปสู่แรงงานที่มีความรู้ ความเชี่ยวชาญ และทักษะสูงขับเคลื่อนเศรษฐกิจด้วยนวัตกรรม

ทั้งนี้ ด้วยการเติมเต็มด้วยวิทยาการ ความคิดสร้างสรรค์ นวัตกรรม วิทยาศาสตร์ เทคโนโลยี และการวิจัยและพัฒนา แล้วต่อยอดความได้เปรียบเชิงเปรียบเทียบเป็น ๕ กลุ่มเทคโนโลยีและอุตสาหกรรมเป้าหมาย ประกอบด้วย

๑. กลุ่มอาหาร เกษตร และเทคโนโลยีชีวภาพ (Food, Agriculture & Bio -Tech)

๒. กลุ่มสาธารณสุข สุขภาพ และเทคโนโลยีทางการแพทย์ (Health, Wellness & Bio - Med)

๓. กลุ่มเครื่องมืออุปกรณ์อัจฉริยะ หุ่นยนต์ และระบบเครื่องกลที่ใช้ระบบอิเล็กทรอนิกส์ควบคุม (Smart Devices, Robotics & Mechatronics)

๔. กลุ่มดิจิทัลเทคโนโลยีอินเทอร์เน็ตที่เชื่อมต่อและบังคับอุปกรณ์ต่างๆ ปัญญาประดิษฐ์และเทคโนโลยีสมองกลฝังตัว (Digital, IoT, Artificial Intelligence & Embedded Technology) ในการสร้างเทคโนโลยีด้านการเงิน (Fintech) อุปกรณ์เชื่อมต่อออนไลน์โดย

ไม่ต้องใช้คน (IoT) เทคโนโลยีการศึกษา (Edtech) อี–มาร์เก็ตเพลส (E–Marketplace) อี–คอมเมิร์ซ (E–Commerce)

๕. กลุ่มอุตสาหกรรมสร้างสรรค์ วัฒนธรรม และบริการที่มีมูลค่าสูง (Creative, Culture & High Value Services)

สุวิทย์ เมษินทรีย์ (ออนไลน์, ๒๕๕๙) ยังได้กล่าวสรุปด้วยว่า กระบวนทัศน์ในการพัฒนาประเทศภายใต้ “ประเทศไทย ๔.๐” มี ๓ ประเด็นที่สำคัญ คือ

๑. เป็นจุดเริ่มต้นของยุทธศาสตร์ชาติ ๒๐ ปี ในการขับเคลื่อนไปสู่การเป็นประเทศที่มั่นคง มั่งคั่ง และยั่งยืน อย่างเป็นรูปธรรม

๒. เป็น “Reform in Action” ที่มีการผลักดันการปฏิรูปโครงสร้างเศรษฐกิจ การปฏิรูปการวิจัยและการพัฒนา และการปฏิรูปการศึกษาไปพร้อมๆ กัน

๓. เป็นการผนึกกำลังของทุกภาคส่วนภายใต้แนวคิด “ประชารัฐ” โดยเป็นประชารัฐที่ผนึกกำลังกับเครือข่ายพันธมิตรทางธุรกิจ การวิจัยพัฒนา และบุคลากรระดับโลก ภายใต้หลักปรัชญาเศรษฐกิจพอเพียงของการ “รู้จักเติม รู้จักพอ และรู้จักปัน”

ซึ่งแนวนโยบายประเทศไทย ๔.๐ ได้ถูกผนวกรวมอยู่ในยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ – ๒๕๗๙) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ซึ่งเป็นแผนที่สอดรับกับยุทธศาสตร์ชาติระยะ ๒๐ ปี ในลักษณะของการถ่ายทอดยุทธศาสตร์ระยะยาวลงสู่การปฏิบัติในช่วงเวลา ๕ ปี ซึ่งได้ให้ความสำคัญกับการพัฒนาเศรษฐกิจและสังคมดิจิทัล (ปรเมธี วิมลศิริ, ออนไลน์, ๒๕๖๐)

ยุทธศาสตร์ชาติ ๒๐ ปี เป็นกรอบการพัฒนาระยะยาวของประเทศที่จัดทำโดยคณะกรรมการจัดทำยุทธศาสตร์ชาติ เพื่อใช้เป็นกรอบในการดำเนินงานระยะที่ ๒ ของรัฐบาล (พ.ศ. ๒๕๕๘ – ๒๕๕๙) และกรอบการปฏิรูปในระยะที่ ๓ (พ.ศ. ๒๕๖๐ เป็นต้นไป) ยุทธศาสตร์ชาตินี้เป็นยุทธศาสตร์ในการพัฒนาประเทศในระยะยาว เพื่อเป็นการกำหนดให้ฝ่ายบริหารมีความรับผิดชอบที่จะต้องขับเคลื่อนประเทศไปสู่เป้าหมายที่เป็นที่ยอมรับร่วมกันและเป็นเอกภาพ ซึ่งยุทธศาสตร์ชาติที่ใช้เป็นกรอบแนวทางพัฒนาในระยะ ๒๐ ปี ต่อไปจากนี้ (พ.ศ. ๒๕๖๐ – ๒๕๗๙) จะประกอบด้วย ๖ ยุทธศาสตร์ได้แก่ ๑. ยุทธศาสตร์ด้านความมั่นคง ๒. ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน ๓. ยุทธศาสตร์ด้านการพัฒนาและเสริมสร้างศักยภาพคน ๔. ยุทธศาสตร์ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมทางสังคม ๕. ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม และ ๖. ยุทธศาสตร์ด้านการปรับสมดุลและการพัฒนาระบบการบริหารการจัดการภาครัฐ

ในส่วนของแผนพัฒนาเศรษฐกิจและสังคมแห่งชาตินั้น สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคมแห่งชาติ (สศช.) ได้จัดทำแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) บนพื้นฐานของยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๐ – ๒๕๗๙) ซึ่งเป็นแผนแม่บทหลักของการพัฒนาประเทศและเป้าหมายการพัฒนาที่ยั่งยืน (Sustainable Development Goals: SDGs) รวมทั้งการปรับโครงสร้างประเทศไปสู่ประเทศไทย ๔.๐ ในลักษณะการแปลงยุทธศาสตร์ระยะยาวไปสู่การปฏิบัติ โดยในแต่ละยุทธศาสตร์ของแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ ได้กำหนดประเด็นการพัฒนา พร้อมทั้งแผนงาน/โครงการสำคัญที่ต้องดำเนินการ

ให้เห็นผลเป็นรูปธรรมในช่วง ๕ ปีแรกของการขับเคลื่อนยุทธศาสตร์ชาติ ยุทธศาสตร์การพัฒนาประเทศตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) ประกอบด้วย ๑๐ ยุทธศาสตร์ ดังนี้

ยุทธศาสตร์ที่ ๑ การเสริมสร้างและพัฒนาศักยภาพทุนมนุษย์
ยุทธศาสตร์ที่ ๒ การสร้างความเป็นธรรมและลดความเหลื่อมล้ำในสังคม
ยุทธศาสตร์ที่ ๓ การสร้างความเข้มแข็งทางเศรษฐกิจและแข่งขันได้อย่างยั่งยืน
ยุทธศาสตร์ที่ ๔ การเติบโตที่เป็นมิตรกับสิ่งแวดล้อมเพื่อการพัฒนาอย่างยั่งยืน
ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน
ยุทธศาสตร์ที่ ๖ การบริหารจัดการในภาครัฐ การป้องกันการทุจริตประพฤติมิชอบและธรรมาภิบาลในสังคมไทย
ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์
ยุทธศาสตร์ที่ ๘ การพัฒนาวิทยาศาสตร์ เทคโนโลยี วิจัยและนวัตกรรม
ยุทธศาสตร์ที่ ๙ การพัฒนาภาค เมือง และพื้นที่เศรษฐกิจ
ยุทธศาสตร์ที่ ๑๐ ความร่วมมือระหว่างประเทศเพื่อการพัฒนา

แนวคิดโมเดลประเทศไทย ๔.๐ ดังที่กล่าวมาตอนต้นปรากฏอยู่ในยุทธศาสตร์การพัฒนาประเทศตามแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) (ราชกิจจานุเบกษา, ๒๕๕๙ : ๘๒-๘๗) ซึ่งในส่วนของ**ยุทธศาสตร์ที่ ๓ การสร้างความเข้มแข็งทางเศรษฐกิจและแข่งขันได้อย่างยั่งยืน** กำหนดให้การขับเคลื่อนให้เศรษฐกิจเจริญเติบโตในช่วงแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) เน้นการพัฒนาและการใช้วิทยาศาสตร์ เทคโนโลยี และนวัตกรรมขั้นก้าวหน้าที่เข้มข้นมากขึ้น การพัฒนาเศรษฐกิจดิจิทัล การพัฒนาและยกระดับคุณภาพของกำลังคน และความคิดสร้างสรรค์ในการขยายฐานเศรษฐกิจและฐานรายได้ใหม่ควบคู่กับการเพิ่มผลิตผลของฐานการผลิตและบริการเดิม รวมทั้งการต่อยอดการผลิตและบริการเดิมโดยใช้ดิจิทัลและเทคโนโลยีอัจฉริยะ นอกจากนี้ ในส่วนภาคการเงิน มีแนวทางการพัฒนาโดยส่งเสริมการใช้บริการทางการเงินและระบบการชำระเงินทางอิเล็กทรอนิกส์ (E-Money หรือ E-Payment) และบริการทางการเงินที่เป็นนวัตกรรมและเทคโนโลยีสมัยใหม่ (FinTech) ตลอดจนสนับสนุนมาตรการต่างๆภายใต้แผนยุทธศาสตร์พัฒนาโครงสร้างพื้นฐานระบบการชำระเงินทางอิเล็กทรอนิกส์แห่งชาติ และแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และในส่วนของการสร้างความมั่นคงเพื่อรองรับการเปลี่ยนแปลงทางเศรษฐกิจและสังคม อันเกิดจากกระแสโลกาภิวัฒน์และความก้าวหน้าทางเทคโนโลยี ทั้งในลักษณะภัยคุกคามจากอาชญากรรมข้ามชาติและภัยคุกคามจากภายในประเทศ อันได้แก่ การคุกคามทางเศรษฐกิจโดยอาชญากรรมคอมพิวเตอร์ ทั้งนี้ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) ได้กำหนดไว้ใน **ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน** หมวดแผนงานและโครงการสำคัญ ข้อ ๕.๕ ให้มีแนวทางการป้องกันและการแก้ไขภัยคุกคามทางเทคโนโลยีสารสนเทศและไซเบอร์ มีสาระสำคัญว่า ภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรงและมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการก่ออาชญากรรมและ

การโจมตีทางไซเบอร์จะมีผลอย่างร้ายแรง ซึ่งรัฐต้องให้ความสำคัญและมีมาตรการป้องกันภัยคุกคามทางไซเบอร์ให้สอดรับกับความเปลี่ยนแปลงทางสภาพแวดล้อม โดยเฉพาะการกำหนดกฎหมายและมาตรการที่เกี่ยวกับความปลอดภัยในโลกไซเบอร์ให้รัดกุมมากยิ่งขึ้นตั้งแต่ระดับชาติถึงระดับบุคคล โดยมีการกำหนดหน่วยงานหลักในการดำเนินการ คือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และสำนักงานตำรวจแห่งชาติ

๒. แนวความคิดการพัฒนาเศรษฐกิจและสังคมดิจิทัล

แผนภาพที่ ๒-๑ แผนภูมิความเชื่อมโยงของยุทธศาสตร์ชาติกับแผนในระดับต่างๆ

ที่มา : ปรเมธี วิมลศิริ, ออนไลน์, ๒๕๖๐

แผนภาพที่ ๒-๒ ภาพสรุปความเชื่อมโยงระหว่างยุทธศาสตร์ชาติ ๒๐ ปี กับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ที่มา : ปรเมธี วิมลศิริ, ออนไลน์, ๒๕๖๐

ดังที่ได้กล่าวมาในหัวข้อ “แนวคิดเกี่ยวกับนโยบายประเทศไทย ๔.๐” ข้างต้นว่า แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) ซึ่งจัดทำภายในกรอบยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ.๒๕๖๐ – ๒๕๗๙) ได้ผนวกโมเดลเศรษฐกิจ “ประเทศไทย ๔.๐” ไว้ในยุทธศาสตร์การพัฒนาประเทศ ยุทธศาสตร์ที่ ๓ การสร้างความเข้มแข็งทางเศรษฐกิจและแข่งขันได้อย่างยั่งยืน ซึ่งการขับเคลื่อนประเทศด้วยโมเดลประเทศไทย ๔.๐ ถือได้ว่าเป็นเรื่องที่ค่อนข้างใหม่และก้าวกระโดด ดังนั้น ประเทศไทยจึงจำเป็นต้องมีโครงสร้างรองรับการเปลี่ยนแปลงเทคโนโลยีในยุคดิจิทัลโดยเฉพาะอย่างยิ่งในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสร้างความเชื่อมั่นในการพัฒนาเศรษฐกิจดิจิทัล ซึ่งยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน ได้กำหนดให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (หรือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เดิม) เป็นหนึ่งในหน่วยงานหลักในการดำเนินการ

เมื่อวันที่ ๕ เมษายน ๒๕๕๙ คณะรัฐมนตรีได้เห็นชอบ**แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม**ที่เสนอโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ปัจจุบัน คือ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) โดยแผนฉบับนี้มีการกำหนดวิสัยทัศน์ว่า “ปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์” คำว่า “ดิจิทัลไทยแลนด์ (Digital Thailand)” หมายถึงประเทศไทยที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้อย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อการขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน โดยแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ได้กำหนดกรอบยุทธศาสตร์การพัฒนา ๖ ด้าน คือ

ยุทธศาสตร์ที่ ๑ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ
ยุทธศาสตร์ที่ ๒ ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล
ยุทธศาสตร์ที่ ๓ สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล
ยุทธศาสตร์ที่ ๔ ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล
ยุทธศาสตร์ที่ ๕ พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล
ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

จากยุทธศาสตร์ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมข้างต้น จะเห็นได้ว่าการขับเคลื่อนตามนโยบายประเทศไทย ๔.๐ ผ่านการพัฒนาเศรษฐกิจและสังคมดิจิทัล มีทั้งส่วนที่เป็นการมุ่งขับเคลื่อนการพัฒนาระบบดิจิทัล และส่วนที่เป็นการสร้างความพร้อมเพื่อรองรับการเปลี่ยนแปลง ทั้งในด้านกำลังคนและด้านการสร้างความเชื่อมั่นแก่ผู้เกี่ยวข้อง

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ๑๔-๑๖) ได้เผยความท้าทายจากพลวัตของเทคโนโลยีดิจิทัลในช่วง ๕ ปีข้างหน้า ไว้หลายประการ เช่น การเปลี่ยนแปลงทางเทคโนโลยีแบบก้าวกระโดด เกิดการหลอมรวมระหว่างกิจกรรมทางเศรษฐกิจสังคมของโลกออนไลน์และออฟไลน์ (Convergence of Online and Offline Activities) ด้วยเทคโนโลยีใหม่ โดยกิจกรรมของประชาชน ธุรกิจ หรือรัฐ จะถูกย้ายมาอยู่ในระบบออนไลน์มากขึ้น เช่น การสื่อสาร การซื้อขายสินค้า การทำธุรกรรมทางการเงิน การเรียนรู้ การดูแลสุขภาพ และการบริการของภาครัฐ อย่างไรก็ดี การแพร่ระบาดของภัยไซเบอร์ก็ถือเป็นความท้าทายในอนาคตด้วย โดยจะเกิดความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ตามมาอีกหลายรูปแบบ เช่น การก่อกวน สร้างความรำคาญแก่ผู้ใช้ระบบ การเข้าถึงข้อมูลและระบบโดยไม่ได้รับอนุญาต การยับยั้งข้อมูลและระบบ การสร้างความเสียหายแก่ระบบ การจารกรรมข้อมูลบนระบบคอมพิวเตอร์ (ข้อมูลการค้า การเงิน หรือข้อมูลส่วนตัว) หรือแม้แต่การโจมตีโครงสร้างพื้นฐานที่มีความสำคัญอย่างยิ่งยวดที่สามารถทำให้ระบบเศรษฐกิจหยุดชะงักและได้รับความเสียหายหรือเกิดอันตรายต่อชีวิตและทรัพย์สินของผู้คน โดยที่ภัยไซเบอร์เหล่านี้ล้วนแล้วแต่พัฒนาอย่างรวดเร็วตามความก้าวหน้าของเทคโนโลยี และบ่อยครั้งยังเป็นเรื่องทำจากนอกประเทศ ทำให้การป้องกันหรือติดตามจับกุมการกระทำผิดเป็นเรื่องที่ยากและสลับซับซ้อนมากขึ้นด้วย

ดังนั้น จากความจำเป็นในการสร้างบุคคลากรของรัฐเพื่อรองรับมาตรการสร้างความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งบุคลากรในกระบวนการยุติธรรมทางอาญาในการดำเนินคดีกับผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ ยุทธศาสตร์ที่ ๕ “พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล” ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม จึงมุ่งเน้นการ

พัฒนากำลังคนดิจิทัล (Digital Workforce) ขึ้นมารองรับการทำงานในระบบเศรษฐกิจดิจิทัล โดยมีแผนงานในข้อ ๑.๔ ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ๕๑) ระบุว่า “พัฒนาบุคลากรที่เกี่ยวข้องกับการบัญญัติและบังคับใช้กฎหมาย กฎ ระเบียบ ข้อบังคับต่างๆ ให้มีความรอบรู้ และเท่าทันต่อเทคโนโลยีสมัยใหม่ เช่น บุคลากรวิชาชีพด้านนิติศาสตร์มีความเข้าใจและเชี่ยวชาญทางด้านเทคโนโลยีดิจิทัลในกระบวนการยุติธรรม”นอกจากนี้ ยุทธศาสตร์ที่ ๖ “สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล” ได้กำหนดแผนงานในข้อ ๓.๓ ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ๕๖) โดยกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากล โดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เพื่อให้มีความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงานรับแจ้งเหตุและสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันและปราบปรามการกระทำความผิดที่มีผลกระทบต่อความมั่นคงปลอดภัยดิจิทัล การส่งเสริมให้เกิดความตระหนักและรู้เท่าทันภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ต้องดำเนินการอย่างต่อเนื่อง

๓. แนวความคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ในต่างประเทศ

ขณะที่ประเทศไทยกำลังมุ่งพัฒนาเศรษฐกิจดิจิทัลตามนโยบายประเทศไทย ๔.๐ การสร้างความเชื่อมั่นในความมั่นคงปลอดภัยทางไซเบอร์ถือได้ว่าเป็นวาระที่สำคัญซึ่งไม่อาจมองข้าม เพื่อให้การเติบโตของระบบเศรษฐกิจดิจิทัลเป็นไปโดยมั่นคงและยั่งยืน เมื่อศึกษาแนวคิดในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มประเทศซึ่งใช้ระบบดิจิทัลเข้ามาเป็นกลไกสำคัญในการขับเคลื่อนทางเศรษฐกิจ ได้แก่ สหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ พบข้อมูลโดยสรุปดังนี้

๓.๑ สหรัฐอเมริกา (Homeland Security, Online, 2016)

เมื่อกล่าวถึงประเทศผู้นำทางด้านเทคโนโลยีในโลกไซเบอร์ สหรัฐอเมริกาเป็นประเทศลำดับต้นๆที่หลายท่านนึกถึง เดิมสหรัฐอเมริกามีคำสั่งประธานาธิบดีที่ ๔๑ (Presidential Policy Directive 41 หรือ PPD-41) ในชื่อ “United States Cyber Incident Coordination” ซึ่งวางหลักการในระดับรัฐบาลสหพันธรัฐเพื่อตอบโต้เหตุการณ์ด้านไซเบอร์ที่เกี่ยวข้องกับภาครัฐและภาคเอกชน ซึ่งต่อมาได้มีการพัฒนาเป็นแผนระดับชาติในการตอบโต้เหตุการณ์ด้านไซเบอร์ (National Cyber Incident Response Plan-NCIRP) โดยแผนที่ว่านี้ไม่มีลักษณะเป็นแผนเชิงปฏิบัติการ แต่มีลักษณะเป็นการกำหนดกรอบยุทธศาสตร์เบื้องต้นเพื่อสร้างความเข้าใจให้กับผู้มีส่วนได้เสียที่เกี่ยวข้องในเรื่องเกี่ยวกับบทบาทของหน่วยงานระดับสหพันธรัฐที่มีการจัดให้มีปฏิบัติการสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ เช่น การกำหนดให้กระทรวงยุติธรรม (The Department of Justice) เป็นหน่วยงานหลักที่มีบทบาทในการตอบโต้ภัยคุกคามด้านไซเบอร์ โดยดำเนินงานผ่านสำนักสืบสวนระดับสหพันธรัฐและหน่วยงานสืบสวนทางไซเบอร์ระดับชาติ (The Federal Bureau of Investigations and National Cyber Investigative Joint Task Force) ซึ่งมีอำนาจหน้าที่สืบสวน เก็บรวบรวมพยานหลักฐาน จำแนกประเภทภัยคุกคาม บังคับใช้แผนงานในการลดภัยคุกคาม อำนวยการแลกเปลี่ยนข้อมูลและความร่วมมือที่เกี่ยวข้อง โดยหน่วยงานสำคัญที่

สังกัดอยู่ในกระทรวงยุติธรรมของสหรัฐอเมริกาซึ่งมีบทบาทในการตอบโต้อาชญากรรมคอมพิวเตอร์ ได้แก่ หน่วยงานสืบสวนกลางระดับสหพันธรัฐ หรือ FBI และสำนักงานอัยการ เป็นต้น

๓.๒ เครือรัฐออสเตรเลีย (Attorney-General's Department, Online, 2016)

เมื่อปีพ.ศ. ๒๕๕๖ รัฐบาลของเครือรัฐออสเตรเลียได้ประกาศใช้แผนระดับชาติในการต่อสู้กับอาชญากรรมคอมพิวเตอร์ (National Plan to Combat Cybercrime) ซึ่งกำหนดทิศทางยุทธศาสตร์สำหรับหน่วยงานที่เกี่ยวข้องทั้งในระดับรัฐบาลท้องถิ่น รัฐ และเครือรัฐ โดยมีการกำหนดเครือข่ายออนไลน์เพื่อการรายงานอาชญากรรมคอมพิวเตอร์ (The Australian Cybercrime Online Reporting Network – ACORN) ซึ่งฐานข้อมูลของ ACORN จะมีส่วนช่วยในการกำหนดมาตรการเชิงนโยบายและเชิงปฏิบัติการเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ด้วย แผนระดับชาติดังกล่าวได้กำหนดหลักการสำคัญและเรื่องที่มีความสำคัญเร่งด่วนที่จะต้องดำเนินการในระยะสั้นถึงระยะกลาง อาทิเช่น การให้ความรู้แก่สังคมในการป้องกันตนเอง การส่งเสริมการมีส่วนร่วมของภาคอุตสาหกรรมในการต่อสู้กับปัญหาอาชญากรรมคอมพิวเตอร์ การปรับปรุงความสามารถของหน่วยงานรัฐโดยเฉพาะอย่างยิ่งหน่วยงานผู้บังคับใช้กฎหมายในการดำเนินการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ การสร้างความมั่นใจในกรอบงานยุติธรรมทางอาญาที่มีประสิทธิภาพโดยให้ความสำคัญกับการให้ความรู้แก่พนักงานอัยการและเจ้าพนักงานในกระบวนการยุติธรรมในงานด้านพยานหลักฐานดิจิทัล และการปรับปรุงบทบัญญัติแห่งกฎหมายและกำหนดบทลงโทษให้เหมาะสมกับการตอบโต้อาชญากรรมคอมพิวเตอร์

๓.๓ สาธารณรัฐสิงคโปร์ (Cyber Security Agency, Online, 2016)

สาธารณรัฐสิงคโปร์เป็นประเทศที่นำระบบคอมพิวเตอร์มาขับเคลื่อนระบบเศรษฐกิจและสังคมในประเทศอย่างเข้มข้น โดยนายลีเซียงลุง นายกรัฐมนตรี ได้ให้ความสำคัญต่อการสร้างความมั่นคงปลอดภัยทางไซเบอร์อย่างมาก กล่าวคือ ในปี พ.ศ. ๒๕๕๙ ที่ผ่านมา สาธารณรัฐสิงคโปร์ได้ประกาศใช้ยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Singapore's Cybersecurity Strategy) และจัดตั้งหน่วยงานเฉพาะในชื่อ "หน่วยงานด้านความมั่นคงทางไซเบอร์แห่งสิงคโปร์" (Cyber Security Agency of Singapore) เป็นหน่วยงานผู้รับผิดชอบโดยตรง นอกจากนี้ ในเดือนกรกฎาคม ๒๕๕๙ Ministry of Home Affairs (เทียบเคียงได้กับกระทรวงมหาดไทย) ได้ออกแผนปฏิบัติการด้านอาชญากรรมคอมพิวเตอร์ระดับชาติ หรือ National Cybercrime Action Plan - NCAP ซึ่งกำหนดแผนปฏิบัติการรวม ๔ ด้าน ได้แก่ ๑. Educating and empowering the public to stay safe in cyberspace คือ การให้ความรู้แก่ประชาชนเกี่ยวกับความเสี่ยงของอาชญากรรมคอมพิวเตอร์พร้อมบังคับใช้มาตรการอย่างง่ายในการป้องกันอาชญากรรมคอมพิวเตอร์เพื่อรักษาความปลอดภัยของข้อมูลของประชาชนในโลกไซเบอร์ โดยสาธารณรัฐสิงคโปร์มีหน่วยงานตำรวจ (Singapore Police Force) ซึ่งจะแบ่งปันข้อมูลเกี่ยวกับการป้องกันอาชญากรรมคอมพิวเตอร์ให้แก่ประชาชนผ่านสื่อหลากหลายช่องทาง ทั้งทีวี หนังสือพิมพ์ โปสเตอร์ และช่องทางสังคมออนไลน์ รวมไปถึงการแจ้งเตือนการหลอกลวงผ่านระบบคอมพิวเตอร์ (Scam) ๒. Enhancing government's capacity and capability to combat cybercrime ได้แก่ การพัฒนากลไกความสามารถในการตอบโต้อาชญากรรมคอมพิวเตอร์ ด้วยการสร้างความร่วมมือระหว่างหน่วยงานตำรวจ (Singapore Police Force) กับหน่วยงานภาครัฐอื่น โดยหลายปีที่

ผ่านมา หน่วยงานตำรวจ (Singapore Police Force) และสำนักงานอัยการสูงสุดของสาธารณรัฐสิงคโปร์ได้ทำงานร่วมกันอย่างใกล้ชิดในคดีอาชญากรรมคอมพิวเตอร์ที่สำคัญตั้งแต่ในชั้นสืบสวน โดยสำนักงานอัยการสูงสุดจะเป็นหน่วยงานที่มีความเชี่ยวชาญในการให้คำแนะนำในเรื่องของความครบถ้วนเพียงพอของพยานหลักฐานสำคัญที่ตำรวจจะต้องทำการสืบสวนสอบสวนเพื่อใช้พิสูจน์การกระทำความผิดในคดีอาชญากรรมคอมพิวเตอร์ ๓. Strengthening legislation and the criminal justice framework คือ การสร้างความเข้มแข็งด้านกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ โดยการสืบสวนและการฟ้องคดีอาชญากรรมคอมพิวเตอร์จะต้องได้รับการสนับสนุนจากกรอบงานยุติธรรมทางอาญาที่เข้มแข็งจริงจัง และจะต้องมีการปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้องเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ประเภทใหม่ๆ ในปัจจุบัน และ ๔. Stepping up partnerships and international engagement คือ การสร้างหุ้นส่วนความร่วมมือเพื่อการตอบโต้อาชญากรรมคอมพิวเตอร์ทั้งในระดับภายในและระหว่างประเทศ

แนวความคิดและทฤษฎีการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยพนักงานอัยการ

๑. ทฤษฎีการดำเนินคดีอาญาโดยรัฐ

(ปิยฉัตร ผังสุวรรณดำรง, ๒๕๕๔ : ๑๕-๑๗)

ทฤษฎีการดำเนินคดีอาญาโดยรัฐ (Theory of Public Prosecution) มีที่มาจากแนวความคิดการฟ้องคดีตามระบบฝรั่งเศส ภายใต้ประมวลกฎหมายวิธีพิจารณาความอาญา ฉบับ ค.ศ. ๑๘๐๘ ของสาธารณรัฐฝรั่งเศส ซึ่งเห็นว่า เมื่อมีการการทำความผิดอาญาเกิดขึ้น รัฐย่อมมีหน้าที่อำนวยความยุติธรรมทางอาญาด้วยการเข้าไปจัดการกับการกระทำผิดอาญานั้นผ่านองค์กรที่มีอำนาจในการดำเนินคดีอาญาของรัฐ ซึ่งได้แก่ สำนักงานตำรวจแห่งชาติ องค์กรอัยการ และองค์กรศาล ผ่านกระบวนการในชั้นสอบสวน การสั่งคดี การพิจารณาคดีในชั้นศาล และการบังคับคดี สำหรับองค์กรที่มีอำนาจในการฟ้องคดีอาญาแทนรัฐภายใต้ทฤษฎีนี้ คือ องค์กรอัยการ โดยพนักงานอัยการเป็นผู้มีอำนาจหน้าที่ในการฟ้องคดีและดำเนินคดีในชั้นศาลเพื่อพิสูจน์การกระทำความผิดของผู้ถูกกล่าวหา (จำเลย) ไปจนกว่าคดีจะถึงที่สุดตามกฎหมาย

สำหรับประเทศไทยได้บัญญัติเกี่ยวกับทฤษฎีการดำเนินคดีอาญาโดยรัฐไว้ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ หมวด ๑๓ ว่าด้วย “องค์กรอัยการ” มาตรา ๒๔๘ ประกอบกับ พระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ มาตรา ๑๑ และมาตรา ๑๔(๒) ซึ่งกำหนดให้พนักงานอัยการมีฐานะเป็นทนายแผ่นดิน มีอำนาจหน้าที่ในคดีอาญาตามที่ประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นซึ่งบัญญัติว่าเป็นอำนาจหน้าที่ของสำนักงานอัยการสูงสุดหรือพนักงานอัยการ ซึ่งอำนาจหน้าที่สำคัญประการหนึ่งตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๘(๑) และมาตรา ๑๔๓ คือ การทำคำสั่งทางคดีทั้งคำสั่งฟ้องคดีหรือคำสั่งไม่ฟ้องคดี เว้นแต่ความผิดต่อส่วนตัวที่ขึ้นอยู่กับความประสงค์ของผู้เสียหาย หากผู้เสียหายประสงค์ดำเนินคดีในความผิดต่อส่วนตัวแล้ว ผู้เสียหายจะต้องดำเนินการแจ้งความร้องทุกข์ตามกฎหมายด้วย ในการฟ้องคดีแต่ละเรื่องพนักงานอัยการจะต้องคำนึงถึงความเป็นธรรมในการรักษา

กฎหมายและความสงบเรียบร้อยของสังคมเป็นหลัก ควบคู่ไปกับการคำนึงถึงสิทธิและเสรีภาพของประชาชนด้วย

๒. ทฤษฎีการฟ้องคดีตามดุลพินิจ (ปิยฉัตร ผังสุวรรณดำรง, ๒๕๕๔ : ๑๙-๒๑

ทฤษฎีการฟ้องคดีตามดุลพินิจ (Theory of Prosecutorial Discretion) หมายถึง ในการฟ้องคดีแทนรัฐโดยพนักงานอัยการนั้นไม่มีกฎหมายบัญญัติบังคับว่า เมื่อพนักงานอัยการมีเหตุอันควรเชื่อว่าผู้ต้องหาได้กระทำผิดตามกฎหมาย พนักงานอัยการจะต้องยื่นฟ้องผู้ต้องหาต่อศาล กล่าวคือ พนักงานอัยการมีดุลพินิจสั่งไม่ฟ้องคดีได้หากมีเหตุผลตามสมควร ซึ่งหลักการดำเนินคดีอาญาตามดุลพินิจนี้ เป็นหลักที่ใช้ผ่อนคลายความเข้มงวดในการบังคับใช้กฎหมายอาญาลงเพื่อให้สอดคล้องกับทฤษฎีการดำเนินคดีอาญาโดยรัฐตามที่กล่าวมาข้างต้น ซึ่งพนักงานอัยการจะต้องคำนึงถึงความเป็นธรรมในการรักษากฎหมายและความสงบเรียบร้อยของสังคมเป็นหลัก มิใช่คำนึงแต่เพียงการลงโทษผู้กระทำความผิดในเชิงการแก้แค้น โดยดุลพินิจในการฟ้องคดีของพนักงานอัยการนี้ต้องคำนึงถึงภูมิหลังอาชญากร สิ่งแวดล้อม รัฐศาสนโยบายความสัมพันธ์อันดีระหว่างประเทศ ประกอบกัน ทั้งนี้ สามารถสังเกตจากบทบัญญัติกฎหมายของประเทศที่ใช้ระบบนี้ได้ว่า จะไม่มีการบัญญัติกฎหมายใดบังคับให้พนักงานอัยการต้องมีคำสั่งฟ้องคดีเท่านั้นเมื่อพบว่าคดีมีพยานหลักฐานพอฟ้อง ประเทศที่ใช้ระบบนี้ได้แก่ สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฝรั่งเศส และประเทศญี่ปุ่น เป็นต้น

สำหรับประเทศไทยนั้น พนักงานอัยการมีอิสระในการพิจารณาสั่งคดีและการปฏิบัติหน้าที่ให้เป็นไปตามรัฐธรรมนูญและตามกฎหมายโดยสุจริตและเที่ยงธรรมตามที่บัญญัติไว้ในมาตรา ๒๑ วรรคแรก โดยดุลพินิจของพนักงานอัยการในการพิจารณาสั่งคดีและการปฏิบัติหน้าที่ซึ่งได้แสดงเหตุผลอันสมควรประกอบแล้วย่อมได้รับความคุ้มครองตามมาตรา ๒๒ ของพระราชบัญญัติดังกล่าว นอกจากนี้ ทฤษฎีการฟ้องคดีตามดุลพินิจโดยพนักงานอัยการยังปรากฏอยู่ในพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ มาตรา ๒๑ ด้วย ซึ่งบัญญัติว่า หากพนักงานอัยการเห็นว่าการฟ้องคดีอาญาจะไม่เป็นประโยชน์แก่สาธารณชน หรือมีผลกระทบต่อความปลอดภัยหรือความมั่นคงของชาติ หรือต่อผลประโยชน์อันสำคัญของประเทศ สามารถเสนออัยการสูงสุดเพื่อมีคำสั่งไม่ฟ้องคดีได้

การใช้ดุลพินิจในการฟ้องคดีหรือไม่ฟ้องคดี พนักงานอัยการจะต้องปฏิบัติให้ถูกต้องตามระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ.๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ด้วย โดยหากข้อเท็จจริงที่ได้จากการสอบสวนของพนักงานสอบสวนไม่สิ้นกระแสความเพียงพอที่จะใช้ดุลพินิจมีคำสั่งในทางคดี พนักงานอัยการมีอำนาจสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมหรือส่งพยานคนใดมาให้ซักถามเพื่อมีคำสั่งต่อไปได้ ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๑๔๓ วรรคสอง (ก) ประกอบกับ ระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ.๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ข้อ ๖๙ นอกจากนี้ ในการพิจารณาฐานความผิดของผู้ต้องหา พนักงานอัยการจะต้องพิจารณาจากการกระทำที่ผู้ต้องหาถูกกล่าวหา พนักงานอัยการจะพิจารณาแต่เฉพาะฐานความผิดที่พนักงานสอบสวนได้แจ้งให้ผู้ต้องหาทราบและมีความเห็นเท่านั้นไม่ได้ โดยหากการกระทำที่กล่าวหาเป็นความผิดฐานอื่นด้วย พนักงานอัยการจะต้องพิจารณาสั่งคดีในความผิดฐานอื่นนั้นด้วย แต่ก่อนสั่งคดี พนักงานอัยการจะต้องสั่งให้

พนักงานสอบสวนดำเนินการในเรื่องการแจ้งข้อหาให้ครบถ้วนเสียก่อน ตามนัยระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ.๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ข้อ ๖๗

๓. อำนาจหน้าที่ตามกฎหมายของพนักงานอัยการ

๓.๑ อำนาจหน้าที่ของสำนักงานอัยการสูงสุดและพนักงานอัยการ

สำนักงานอัยการสูงสุดเป็นหน่วยงานของรัฐที่มีบทบาทสำคัญในกระบวนการยุติธรรมทางอาญา โดยรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐ หมวด ๑๓ ว่าด้วย “องค์กรอัยการ” มาตรา ๒๔๘ ได้บัญญัติให้องค์กรอัยการมีหน้าที่และอำนาจตามที่บัญญัติไว้ในรัฐธรรมนูญและกฎหมาย โดยพนักงานอัยการมีอิสระในการพิจารณาสั่งคดีและการปฏิบัติหน้าที่ให้เป็นไปโดยรวดเร็ว เที่ยงธรรม และปราศจากอคติทั้งปวง และไม่ให้ถือว่าเป็นคำสั่งทางปกครอง

กฎหมายหลักที่บัญญัติอำนาจหน้าที่ของสำนักงานอัยการสูงสุด ได้แก่ พระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ และพระราชบัญญัติระเบียบข้าราชการฝ่ายอัยการ พ.ศ.๒๕๕๓ รวมทั้งประกาศคณะรักษาความสงบแห่งชาติ (คสช.) ในส่วนที่เกี่ยวข้องกับกระบวนการยุติธรรม (สำนักงานอัยการสูงสุด, ๒๕๕๙ : ๒-๓) ซึ่งตามพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ มาตรา ๑๑ กำหนดให้พนักงานอัยการมีฐานะเป็นทนายแผ่นดิน และมาตรา ๑๔(๒) พนักงานอัยการมีอำนาจหน้าที่ในคดีอาญาตามที่ประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นซึ่งบัญญัติว่าเป็นอำนาจหน้าที่ของสำนักงานอัยการสูงสุดสอดคล้องกับประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๘(๑) ซึ่งบัญญัติให้พนักงานอัยการมีอำนาจฟ้องคดีอาญาต่อศาลด้วย

ในกรณีทั่วไป เมื่อเกิดการกระทำความผิดอาญา เจ้าพนักงานตำรวจจะมีอำนาจหน้าที่ในการสืบสวนสอบสวนคดีอาญา รวบรวมพยานหลักฐาน ทั้งคำให้การของพยานบุคคล พยานวัตถุ และพยานเอกสารเพื่อพิสูจน์ว่าผู้ต้องหาเป็นผู้กระทำความผิดตามประมวลกฎหมายอาญาหรือตามกฎหมายอื่นซึ่งมีบัญญัติโทษทางอาญา จากนั้นเมื่อเจ้าพนักงานตำรวจซึ่งเป็นพนักงานสอบสวนผู้รับผิดชอบเห็นว่าการสอบสวนแล้วเสร็จ พนักงานสอบสวนผู้รับผิดชอบจะทำความเห็นว่าควรสั่งฟ้องหรือควรสั่งไม่ฟ้องผู้ต้องหาส่งไปยังพนักงานอัยการพร้อมกับสำนวนการสอบสวน ตามประมวลกฎหมายวิธีพิจารณาความอาญามาตรา ๑๔๑ เมื่อพนักงานอัยการได้รับสำนวนการสอบสวนคดีอาญาพร้อมความเห็นทางคดีจากพนักงานสอบสวนแล้ว พนักงานอัยการจะดำเนินการตรวจพิจารณาสำนวนและมีคำสั่งในทางคดีตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๑๔๓ โดยการปฏิบัติหน้าที่ดังกล่าวของพนักงานอัยการ มีระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) หมวดที่ ๓ บัญญัติให้แนวทางไว้ว่า พนักงานอัยการต้องพิจารณาข้อเท็จจริงและพยานหลักฐานในสำนวนซึ่งพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา รวมถึงแนวทางการดำเนินคดีจากพยานหลักฐาน และข้อกฎหมายว่าจะทำให้ศาลลงโทษผู้ต้องหาได้หรือไม่ ทั้งนี้ ตามข้อ ๖๙ ของระเบียบดังกล่าว ได้บัญญัติให้พนักงานอัยการพิจารณาพยานหลักฐานในคดีให้ได้ความแน่ชัดว่าผู้ต้องหาได้กระทำความผิดหรือไม่ก่อนจะมีความเห็นและคำสั่ง หากยังไม่แน่ชัดก็ให้สั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมหรือสั่งให้ส่งพยานมาเพื่อซักถามตามรูปคดีก็ได้ จากนั้น เมื่อพนักงานอัยการเห็นว่าข้อเท็จจริงในคดีสิ้นกระแสความและคดีมี

พยานหลักฐานเพียงพอในการทำความเห็นและคำสั่งแล้ว พนักงานอัยการจะมีคำสั่งทางคดี ซึ่งหากพนักงานอัยการมีคำสั่งฟ้องผู้ต้องหาในคดีอาญา พนักงานอัยการมีอำนาจหน้าที่เป็นโจทก์ฟ้องผู้ต้องหาเป็นจำเลยในคดีอาญา และต้องเป็นผู้ดำเนินกระบวนพิจารณาเป็นโจทก์ในศาลชั้นต้น ศาลอุทธรณ์ และศาลฎีกา จนกว่าคดีนั้นจะถึงที่สุดตามกฎหมาย

พนักงานอัยการมีอิสระในการพิจารณาสั่งคดีและการปฏิบัติหน้าที่ให้เป็นไปตามรัฐธรรมนูญและตามกฎหมายโดยสุจริตและเที่ยงธรรมตามที่บัญญัติไว้ในพระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓ มาตรา ๒๑ วรรคแรก โดยดุลพินิจของพนักงานอัยการในการพิจารณาสั่งคดีและการปฏิบัติหน้าที่ซึ่งได้แสดงเหตุผลอันสมควรประกอบแล้วย่อมได้รับความคุ้มครองตามมาตรา ๒๒ ของพระราชบัญญัติดังกล่าว

๓.๒ ลักษณะคดีอาชญากรรมคอมพิวเตอร์ในความรับผิดชอบของพนักงานอัยการ (สำนักงานอัยการสูงสุด, ๒๕๕๔ ก : ๑-๑๓)

อาชญากรรมคอมพิวเตอร์หรืออาชญากรรมซึ่งมีลักษณะของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ทั้งนี้ไม่รวมถึงการใช้คอมพิวเตอร์ในลักษณะที่เป็นเพียงการเก็บข้อมูลหลักฐานของการกระทำความผิดอื่น) สามารถจำแนกลักษณะที่คอมพิวเตอร์มีส่วนเกี่ยวข้องกับการกระทำความผิดได้ ดังนี้

๓.๒.๑ คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets)

หมายถึง การกระทำความผิดเกี่ยวกับคอมพิวเตอร์โดยตรง ซึ่งผู้กระทำมีเจตนาที่จะกระทำต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์โดยตรง มุ่งก่อให้เกิดความเสียหายแก่ผู้เป็นเจ้าของ ผู้ให้บริการ ผู้ใช้บริการ หรือประชาชนทั่วไป โดยมีบทบัญญัติกำหนดลักษณะของฐานความผิดไว้ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ตัวอย่างเช่น ความผิดฐานเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะโดยมิชอบ ความผิดฐานดักรับข้อมูลคอมพิวเตอร์โดยมิชอบ (Illegal Interception หรือ Sniffing) ความผิดฐานเปลี่ยนแปลงหน้าเว็บไซต์โดยใช้การเข้าถึงโดยมิชอบ (Web Defacement) ความผิดฐานรบกวนหรือขัดขวางระบบคอมพิวเตอร์ (System Inference) หรือทำให้ระบบไม่สามารถทำงานได้ตามปกติ (Denial of Service) หรือความผิดฐานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข (Spam Mail) เป็นต้น

๓.๒.๒ คอมพิวเตอร์ถูกใช้เป็นเครื่องมือประกอบอาชญากรรม (Computer as Tools)

หมายถึง การกระทำความผิดที่ผู้กระทำมีเจตนาที่จะกระทำความผิดฐานอื่น แต่ได้นำเอาคอมพิวเตอร์มาใช้เป็นเครื่องมือในการกระทำความผิด การกระทำลักษณะนี้ นอกจากเป็นการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ แล้ว หากเข้าองค์ประกอบความผิดตามประมวลกฎหมายอาญาหรือกฎหมายอื่น ก็

ถือเป็นความผิดตามประมวลกฎหมายอาญาหรือกฎหมายอื่นด้วย โดยการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดถือได้ว่าเป็นคดีอาชญากรรมคอมพิวเตอร์ประเภทที่พบมากที่สุด ตัวอย่างเช่น การนำเข้าสู่ระบบคอมพิวเตอร์ที่มีลักษณะเป็นการข่มขู่ หรือทำให้อับอาย อาจจะเกิดจากการโฆษณาทางเว็บไซต์หรือโดยใช้จดหมายอิเล็กทรอนิกส์ก็ได้ เช่น การส่งภาพลามกอนาจารของผู้เสียหายไปยังบุคคลอื่นเพื่อต้องการให้ผู้เสียหายได้รับความอับอาย และหากเป็นการกระทำที่ประสงค์ต่อทรัพย์ด้วย ก็ถือเป็นความผิดฐานกรรโชกทรัพย์ตามประมวลกฎหมายอาญาด้วย นอกจากนั้น ยังมีกรณีการปลอมแปลงเกี่ยวกับข้อมูลคอมพิวเตอร์โดยมิชอบ (Computer-related Forgery) ซึ่งหากเป็นการกระทำโดยประสงค์ต่อทรัพย์ ก็อาจเป็นความผิดฐานฉ้อโกงหรือฉ้อโกงประชาชน ตามประมวลกฎหมายอาญาด้วย ปัจจุบันมีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดฐานฉ้อโกง (Computer-related Fraud) ในหลากหลายรูปแบบ เช่น กรณีที่คนร้ายโฆษณาขายสินค้าหลอกลวงทางเว็บไซต์ โดยแท้จริงแล้ว ไม่มีเจตนาจะขายและหรือส่งมอบสินค้าดังกล่าว กรณีที่คนร้ายสั่งซื้อสินค้าทางอินเทอร์เน็ตโดยหลอกลวงใช้ข้อมูลอันเป็นเท็จในการซื้อสินค้า โดยแท้จริงแล้วผู้กระทำไม่มีเจตนาที่จะชำระเงินค่าสินค้าให้แก่ผู้ขายสินค้า กรณี Phishing ซึ่งคนร้ายปลอมแปลงจดหมายอิเล็กทรอนิกส์ (Email Spoofing) หรือโดยสร้างเว็บไซต์ปลอมเพื่อหลอกลวงเหยื่อให้กรอกข้อมูลส่วนตัวของเหยื่อ เช่น ชื่อ ที่อยู่ หมายเลขบัตรเครดิต แล้วนำข้อมูลดังกล่าวไปให้กระทำความผิด กรณีการนำเข้าข้อมูลสู่ระบบคอมพิวเตอร์ในการกระทำความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรตามประมวลกฎหมายอาญา กรณีการใช้คอมพิวเตอร์เป็นเครื่องมือในการทำซ้ำดัดแปลง เผยแพร่ต่อสาธารณชนซึ่งงานอันมีลิขสิทธิ์ของผู้อื่นอันเป็นความผิดเกี่ยวกับการละเมิดลิขสิทธิ์ หรือกรณีการจัดทำเว็บไซต์ลามกอนาจารเพื่อแสวงหาผลประโยชน์ตอบแทนอันมิชอบ เป็นต้น

๓.๓ กฎหมายที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์

บทบัญญัติกฎหมายหลักเกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ได้แก่

๓.๓.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๓.๓.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

๓.๓.๓ ประมวลกฎหมายอาญา

๓.๓.๔ พระราชบัญญัติลิขสิทธิ์ พ.ศ.๒๕๓๗ (ที่แก้ไขเพิ่มเติม)

๓.๓.๕ พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ และพระราชบัญญัติการสอบสวนคดีพิเศษ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

๓.๔ โครงสร้างสำนักงานคดีที่เกี่ยวข้องกับคดีอาชญากรรมคอมพิวเตอร์

๓.๔.๑ สำนักงานคดีอาญา

สำนักงานคดีอาญามีอำนาจหน้าที่ตามประกาศคณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจและหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๔ รับผิดชอบการดำเนินคดีอาญาทั้งปวงตามที่กฎหมายกำหนดให้เป็นอำนาจและหน้าที่ของพนักงานอัยการหรือสำนักงานอัยการสูงสุด ซึ่งไม่อยู่ในอำนาจหน้าที่เฉพาะของสำนักงานคดีอื่น

๓.๔.๒ สำนักงานคดีเศรษฐกิจและทรัพยากร

สำนักงานคดีเศรษฐกิจและทรัพยากรมีอำนาจหน้าที่ในส่วนที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามประกาศคณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจและหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๔ ประกอบคำสั่งกรมอัยการที่ ๑๙/๒๕๓๔ เรื่อง กำหนดอำนาจหน้าที่ของกองคดีเศรษฐกิจและทรัพยากร และความผิดเกี่ยวกับเศรษฐกิจและทรัพยากรแนบท้ายคำสั่งกรมอัยการที่ ๑๙/๒๕๓๔ ลงวันที่ ๑๘ กุมภาพันธ์ ๒๕๓๔ ข้อ ๒.๖ ซึ่งได้กำหนดให้ “การฉ้อโกงโดยใช้เทคโนโลยีแผนใหม่ เช่น การใช้เครื่องคอมพิวเตอร์ หรือเทเลกซ์ปลอม” เป็นคดีที่อยู่ในอำนาจหน้าที่ของสำนักงานคดีเศรษฐกิจและทรัพยากร

๓.๔.๓ สำนักงานคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ

สำนักงานคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศมีอำนาจหน้าที่ตามประกาศคณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจและหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๔ รับผิดชอบการดำเนินคดีทั้งปวงตามที่กฎหมายกำหนดให้เป็นอำนาจและหน้าที่ของพนักงานอัยการหรือสำนักงานอัยการสูงสุด ซึ่งอยู่ในอำนาจพิจารณาพิพากษาของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศกลาง

๓.๔.๔ สำนักงานคดีพิเศษ

สำนักงานคดีพิเศษมีอำนาจหน้าที่ในส่วนที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามประกาศคณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจและหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๔ รับผิดชอบการสอบสวนและการดำเนินคดีอาญาทั้งปวงที่กฎหมายกำหนดให้เป็นอำนาจและหน้าที่ของกรมสอบสวนคดีพิเศษ (DSI) กระทรวงยุติธรรม ทั้งนี้ ในส่วนที่เกี่ยวข้องกับคดีอาชญากรรมคอมพิวเตอร์ มีกฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติม ตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕ กำหนดให้คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗

๓.๔.๕ สำนักงานการสอบสวน

สำนักงานการสอบสวนมีอำนาจหน้าที่ในส่วนที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามประกาศคณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจและหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด (ฉบับที่ ๖) พ.ศ. ๒๕๕๖ ได้แก่ ความรับผิดชอบในการสอบสวนและการดำเนินการอื่นตามกฎหมายว่าด้วยการป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติที่กำหนดให้เป็นอำนาจและหน้าที่ของอัยการสูงสุดหรือผู้รักษาการแทน การสอบสวนในความผิดที่มีโทษตามกฎหมายไทยซึ่งได้กระทำลงนอกราชอาณาจักร ตามประมวลกฎหมายวิธีพิจารณาความอาญาที่กำหนดให้เป็นอำนาจและหน้าที่ของอัยการสูงสุดหรือผู้รักษาการแทน และรับผิดชอบการร่วมสอบสวนตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ

แนวความคิดและทฤษฎีการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์สำนักงานอัยการสูงสุด

๑. ทฤษฎีสามเหลี่ยมอาชญากรรม (กองบังคับการปราบปราม, ออนไลน์, ๒๕๖๐)

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) เป็นทฤษฎีที่อธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรม ซึ่งประกอบด้วย

๑.๑ ผู้กระทำผิดหรือคนร้าย หมายถึง ผู้ที่มีความต้องการจะก่อเหตุหรือลงมือกระทำความผิด

๑.๒ เหยื่อหรือเป้าหมาย หมายถึง บุคคล สถานที่ หรือวัตถุสิ่งของ ที่ผู้กระทำผิดหรือคนร้าย มุ่งกระทำต่อหรือเป็นเป้าหมายที่ต้องการ

๑.๓ โอกาส หมายถึง ช่วงเวลาและสถานที่ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม

เมื่อสถานการณ์ครบทั้ง ๓ องค์ประกอบดังกล่าวย่อมจะเกิดอาชญากรรมขึ้น ตามทฤษฎีดังกล่าวได้สะท้อนแนวคิดในการแก้ไขปัญหาอาชญากรรมหรือการป้องกันไม่ให้เกิดอาชญากรรม โดยต้องพยายามทำให้องค์ประกอบของสามเหลี่ยมอาชญากรรมด้านใดด้านหนึ่งหายไป เพื่อจะทำให้อาชญากรรมไม่เกิดขึ้น นอกจากนี้ ทฤษฎีสามเหลี่ยมอาชญากรรมนี้ยังสามารถนำมาปรับใช้ในการพิจารณาเหตุปัจจัยของการเกิดอาชญากรรม เพื่อประโยชน์ในการวิเคราะห์และสร้างมาตรการเชิงรุกเพื่อป้องกันและปราบปรามอาชญากรรมในสังคม โดยปัจจัยด้านเหยื่อหรือเป้าหมายและด้านโอกาสนั้นอาจมีความแตกต่างกันไปตามลักษณะประเภทของอาชญากรรม ซึ่งในส่วนของอาชญากรรมคอมพิวเตอร์นั้น เหยื่อหรือเป้าหมายในการกระทำความผิด คือ ผู้ที่เข้าถึงการเชื่อมต่อข้อมูลคอมพิวเตอร์ ผู้ใช้บริการทางอินเทอร์เน็ต และผู้ที่ครอบครองหรือเก็บรักษาข้อมูลสำคัญไว้ในระบบคอมพิวเตอร์ เป็นต้น ส่วนปัจจัยด้านโอกาสในการก่ออาชญากรรมคอมพิวเตอร์นั้นค่อนข้างกว้างขวางกว่าอาชญากรรมประเภทอื่น เนื่องจากอาชญากรรมคอมพิวเตอร์เกิดขึ้นได้ทุกที่ทุกเวลาที่มีการเชื่อมต่อระบบคอมพิวเตอร์และอินเทอร์เน็ต แม้ว่าผู้กระทำผิดและเหยื่อจะมิได้พบหน้ากันก็ตาม โดยนัยนี้ ข้อมูลด้านสถิติที่เกี่ยวข้องจึงมีความสำคัญในการสะท้อนถึงปัจจัยด้านโอกาสในการเกิดอาชญากรรม และสามารถใช้วิเคราะห์แนวโน้มสภาพความรุนแรงและจำนวนอาชญากรรมในอนาคตได้ด้วย

๒. ข้อมูลด้านสถิติ

แผนภาพที่ ๒-๓ สถิติประชากรผู้ใช้อินเทอร์เน็ต โซเชียลมีเดีย และโทรศัพท์เคลื่อนที่ ณ เดือนมกราคม ๒๕๕๙

ที่มา : Veedvil, Online, 2016

แผนภาพที่ ๒-๓ แสดงสถิติประชากรผู้ใช้อินเทอร์เน็ต โซเชียลมีเดีย และโทรศัพท์เคลื่อนที่ ณ เดือนมกราคม ๒๕๕๙ โดยจากการสำรวจข้อมูลของเว็บไซต์ www.veedvil.com พบสถิติที่สำคัญว่า มีประชากรประมาณ ๓๘ ล้านคน จากจำนวนประชากรรวมทั้งประเทศประมาณ ๖๘.๐๕ ล้านคน เป็นผู้ใช้อินเทอร์เน็ต และพบว่า มีการเชื่อมต่ออินเทอร์เน็ตจากอุปกรณ์ประเภทโทรศัพท์เคลื่อนที่มากถึง ๘๒.๗๘ ล้านอุปกรณ์ หรือเท่ากับร้อยละ ๑๒๒ ของจำนวนประชากรรวมของประเทศ (๑ คน มากกว่า ๑ เครื่อง)

แผนภาพที่ ๒-๔ สถิติกิจกรรมที่กระทำผ่านโทรศัพท์เคลื่อนที่ ณ เดือนมกราคม ๒๕๕๙

ที่มา : Veedvil, Online, 2016

แผนภาพที่ ๒-๔ แสดงสถิติกิจกรรมที่กระทำผ่านโทรศัพท์เคลื่อนที่ ณ เดือนมกราคม ๒๕๕๙ โดยจากการสำรวจข้อมูลของเว็บไซต์ www.veedvil.com พบสถิติพฤติกรรมของผู้ใช้โทรศัพท์เคลื่อนที่ว่า มีผู้ใช้โทรศัพท์เคลื่อนที่ในการติดต่อสื่อสารผ่านข้อความคิดเป็นจำนวนร้อยละ ๔๐ ใช้ดูวีดีโอคิดเป็นจำนวนร้อยละ ๓๓ ใช้เล่นเกมส์คิดเป็นจำนวนร้อยละ ๓๓ ใช้ทำธุรกรรมทางธนาคารคิดเป็นจำนวนร้อยละ ๓๐ และใช้บริการด้านแผนที่คิดเป็นจำนวนร้อยละ ๓๒

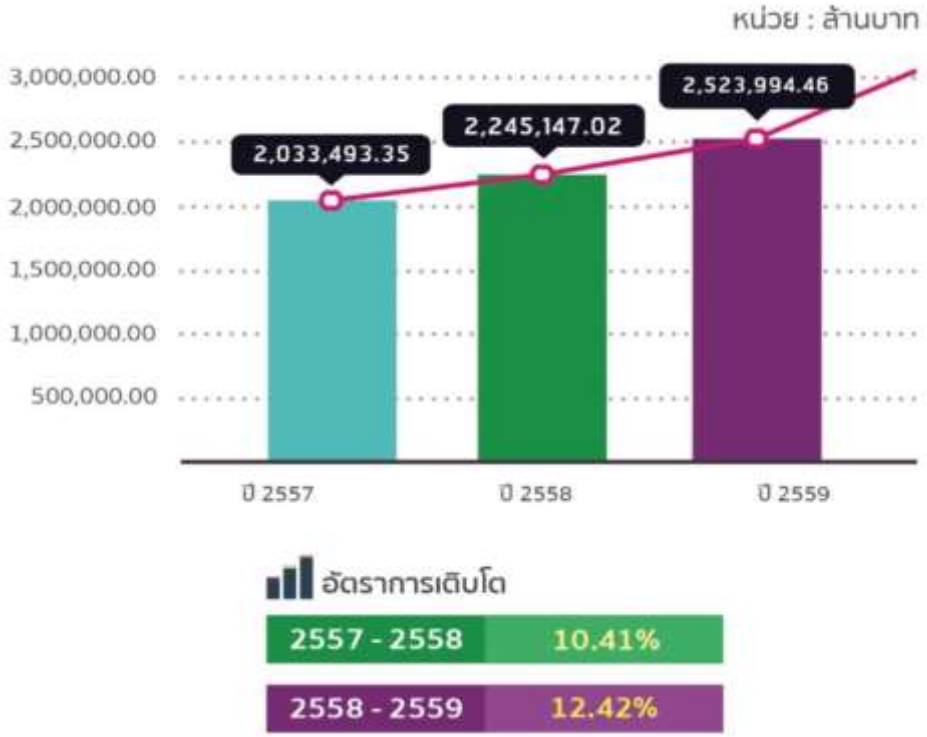
แผนภาพที่ ๒-๕ สถิติพาณิชย์ทางอิเล็กทรอนิกส์ที่กระทำผ่านอุปกรณ์อินเทอร์เน็ต ณ เดือนมกราคม ๒๕๕๙

ที่มา : Veedvil, Online, 2016

แผนภาพที่ ๒-๕ แสดงสถิติพาณิชย์ทางอิเล็กทรอนิกส์ (E-Commerce) ที่กระทำผ่านอุปกรณ์อินเทอร์เน็ต ณ เดือนมกราคม ๒๕๕๙ โดยจากการสำรวจข้อมูลของเว็บไซต์ www.veedvil.com พบว่า ในช่วงรอบ ๓๐ วันก่อนการสำรวจ มีจำนวนประชากรมากถึงร้อยละ ๔๔ ที่เพิ่งทำธุรกรรมซื้อสินค้าหรือบริการออนไลน์ จำนวนร้อยละ ๔๘ เข้าดูอินเทอร์เน็ตเพื่อหาข้อมูลเกี่ยวกับสินค้าที่จะซื้อ จำนวนร้อยละ ๔๐ เข้าดูเว็บไซต์ของผู้ประกอบการรายย่อย (ค้าปลีก) จำนวนร้อยละ ๓๙ ซื้อสินค้าออนไลน์ผ่านเครื่องคอมพิวเตอร์แบบ Laptop/ Desktop และจำนวนร้อยละ ๓๑ ซื้อสินค้าออนไลน์ผ่านการเชื่อมต่ออินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่

แผนภาพที่ ๒-๖ กราฟแสดงมูลค่าพาณิชย์ทางอิเล็กทรอนิกส์ (E-Commerce)

ปีพ.ศ. **๒๕๕๗ – ๒๕๕๙**



ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ออนไลน์, ๒๕๖๐

จากแผนภาพที่ ๒-๖ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ทำการวิจัยข้อมูลพบว่า ในปีพ.ศ. ๒๕๕๘ ประเทศไทยมีมูลค่าพาณิชย์ทางอิเล็กทรอนิกส์ หรือ E-Commerce ที่นับรวมมูลค่าการประมูลทางอิเล็กทรอนิกส์ (E-Auction) จำนวนทั้งสิ้น ๒,๒๔๕,๑๔๗.๐๒ ล้านบาท ซึ่งเติบโตเพิ่มขึ้นจากปี ๒๕๕๗ สูงถึงร้อยละ ๑๐.๔๐ ในขณะที่การคาดการณ์มูลค่า E-Commerce ปีพ.ศ. ๒๕๕๙ นั้น สามารถประมาณการได้เป็นจำนวนทั้งสิ้น ๒,๕๒๓,๙๙๔.๔๖ ล้านบาท และจะมีอัตราการเติบโตเพิ่มขึ้นจากปีพ.ศ. ๒๕๕๘ คิดเป็นร้อยละ ๑๒.๔๒

แผนภาพที่ ๒–๗ กราฟแสดงมูลค่าพาณิชย์ทางอิเล็กทรอนิกส์ (E-Commerce) ปีพ.ศ. ๒๕๕๘ และคาดการณ์ปีพ.ศ. ๒๕๕๙ ของอุตสาหกรรมการค้าปลีกและการค้าส่ง จำแนกตามประเภทสินค้าและบริการ (ไม่รวม E-Auction)

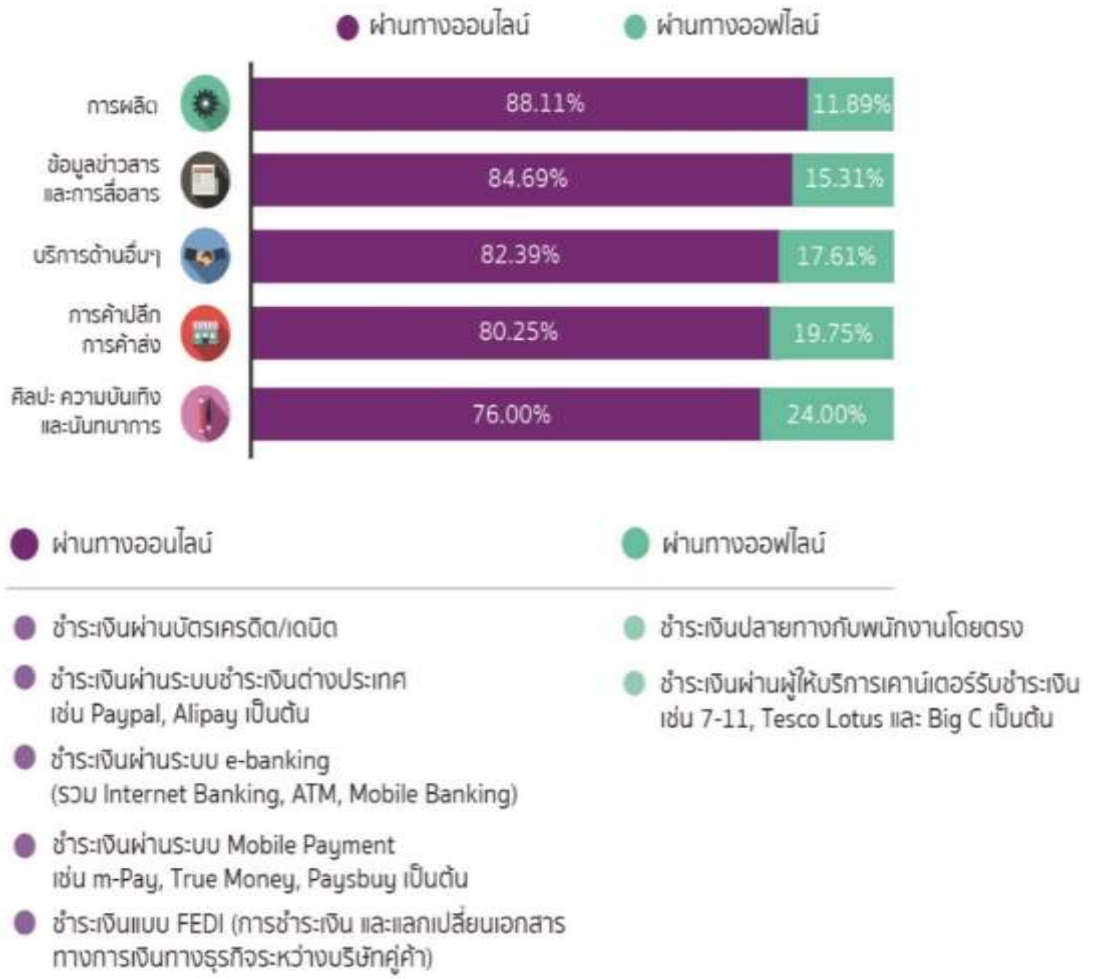
ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ออนไลน์, ๒๕๖๐

จากแผนภาพที่ ๒-๗ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ทำการวิจัยข้อมูล พบว่า สินค้า/บริการของอุตสาหกรรมการค้าปลีกและการค้าส่งที่มีมูลค่าพาณิชย์ทางอิเล็กทรอนิกส์ หรือ E-Commerce ปีพ.ศ. ๒๕๕๘ (ไม่รวมการประมูลทางอิเล็กทรอนิกส์ (E-Auction)) สูงที่สุด ๓ อันดับแรก ได้แก่ อันดับที่ ๑ ธุรกิจห้างสรรพสินค้าออนไลน์ มีมูลค่า E-Commerce ทั้งสิ้น ๑๖๗,๓๖๔.๔๙ ล้านบาท อันดับที่ ๒ การจำหน่ายเครื่องสำอาง อาหารเสริม น้ำหอม และอุปกรณ์เสริมความงาม มีมูลค่า E-Commerce ทั้งสิ้น ๑๑๕,๘๓๑.๔๗ ล้านบาท และอันดับที่ ๓ การจำหน่ายอาหาร อาหารแปรรูป และเครื่องดื่ม ผลิตผลทางการเกษตรและประมง มีมูลค่า E-Commerce ทั้งสิ้น ๑๐๒,๑๘๖.๘๘ ล้านบาท

ในขณะที่สินค้า/บริการของอุตสาหกรรมการค้าปลีกและการค้าส่ง ที่คาดว่าจะมีมูลค่า E-Commerce ในปีพ.ศ. ๒๕๕๙ (ไม่รวม E-Auction) สูงที่สุด ๓ อันดับแรก ได้แก่ อันดับที่ ๑ ธุรกิจห้าง สรรพสินค้าออนไลน์ มีมูลค่า E-Commerce ทั้งสิ้น ๒๓๑,๑๗๗.๖๖ ล้านบาท อันดับที่ ๒ การจำหน่ายอาหาร อาหารแปรรูป และเครื่องดื่ม ผลิตผลทางการเกษตรและประมง มีมูลค่า E-Commerce ทั้งสิ้น ๑๖๕,๕๐๖.๒๗ ล้านบาท และอันดับที่ ๓ การจำหน่าย เครื่องสำอาง อาหารเสริม น้ำหอม และอุปกรณ์เสริมความงาม มีมูลค่า E-Commerce ทั้งสิ้น ๑๔๓,๒๐๖.๖๘ ล้านบาท

เมื่อพิจารณาอัตราการเติบโตของมูลค่า E-Commerce ในแต่ละกลุ่มสินค้า/บริการ ในช่วงปีพ.ศ. ๒๕๕๘ – ๒๕๕๙ พบว่า สินค้า/บริการที่มีอัตราการเติบโตของมูลค่า E-Commerce สูงที่สุด ได้แก่ ผลิตภัณฑ์อาหาร อาหารแปรรูปและเครื่องดื่ม ผลิตผล ทางการเกษตรและประมง มีอัตราการเติบโตสูงถึงร้อยละ ๖๑.๙๖ รองลงมาคือ ธุรกิจห้างสรรพสินค้าออนไลน์ ด้วยอัตราการเติบโตร้อยละ ๓๘.๑๓ และการจำหน่ายยานยนต์และผลิตภัณฑ์ มีอัตราการเติบโตสูงเป็นอันดับที่ ๓ โดยคิดเป็นร้อยละ ๓๖.๕๓

แผนภาพที่ ๒–๘ การให้บริการช่องทางการชำระเงินของผู้ประกอบการกลุ่ม SMEs ในยุคเศรษฐกิจดิจิทัล



ที่มา : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ออนไลน์, ๒๕๖๐

จากแผนภาพที่ ๒-๘ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ทำการวิจัยข้อมูล พบว่า ผู้ประกอบการในเกือบทุกอุตสาหกรรมนั้นเน้นให้ความสำคัญในการเปิดให้บริการช่องทางการชำระเงินทางออนไลน์ ในอัตราส่วนที่มากกว่าออฟไลน์

ตารางที่ ๒-๑ สถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่าน ThaiCERT ปีพ.ศ. ๒๕๕๗

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	1	1	0	0	0	0	3	1	1	1	0	0	**8**
Availability	0	0	2	2	0	0	1	3	0	0	0	0	**8**
Fraud	59	68	69	72	145	85	94	66	98	88	101	62	**1007**
Information Gathering	1	2	6	8	7	0	1	1	3	0	0	0	**29**
Information Security	0	1	0	0	0	2	0	0	1	0	0	0	**4**
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	75	**504**
Intrusion	9	150	77	33	55	50	69	47	86	32	35	66	**709**
Malicious Code	3	7	129	125	102	226	304	161	263	98	132	188	**1738**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**112**	**257**	**315**	**291**	**352**	**393**	**514**	**319**	**482**	**265**	**316**	**391**	**4007**

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ออนไลน์, ๒๕๕๙

ตารางที่ ๒-๒ สถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่าน ThaiCERT ปีพ.ศ. ๒๕๕๘

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	2	0	0	0	0	2	0	0	0	2	1	1	**8**
Availability	0	0	0	0	0	0	0	0	0	0	1	5	**6**
Fraud	75	83	100	90	155	134	113	99	70	67	80	75	**1141**
Information Gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information Security	0	0	1	0	0	0	0	0	0	0	0	0	**1**
Intrusion Attempts	83	89	65	27	60	44	63	51	52	59	43	28	**664**
Intrusions	69	76	88	12	78	187	159	83	51	105	42	55	**1005**
Malicious Code	104	83	174	143	140	209	192	97	143	119	92	50	**1546**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**333**	**331**	**428**	**272**	**433**	**576**	**527**	**330**	**316**	**352**	**259**	**214**	**4371**

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ออนไลน์, ๒๕๕๙

ตารางที่ ๒-๓ สถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่าน ThaiCERT ปีพ.ศ. ๒๕๕๙

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Availability	0	0	0	0	0	0	0	0	0	0	0	29	**29**
Fraud	98	95	66	73	164	125	104	52	57	55	43	70	1002
Information Gathering	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Information Security	0	0	0	0	0	0	0	0	0	0	2	18	**20**
Intrusion Attempts	35	39	36	62	69	70	59	82	42	35	66	111	**706**
Intrusions	175	51	122	96	53	44	158	60	95	37	40	89	1020
Malicious Code	97	123	80	104	168	167	49	14	78	30	89	21	1020
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**405**	**308**	**304**	**335**	**454**	**406**	**370**	**208**	**272**	**157**	**240**	**338**	**3797**

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ออนไลน์, ๒๕๕๙

ตารางที่ ๒-๑, ๒-๒ และ ๒-๓ แสดงข้อมูลสถิติภัยคุกคามทางไซเบอร์ (Cyber Threats) แยกตามประเภทของภัยคุกคามที่มีการรายงานผ่านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ในปีพ.ศ. ๒๕๕๗, ๒๕๕๘ และ ๒๕๕๙ ตามลำดับ ซึ่งพบว่าประเภทภัยคุกคามทางไซเบอร์สูงสุด ๓ อันดับแรกที่มีการรายงานไปยังไทยเซิร์ต ได้แก่ อันดับที่ ๑ Malicious Code คือ การฝังโค้ดอันตรายลงใน BIOS ที่สามารถขโมยข้อมูลต่างๆ ที่อยู่ในแรม (Ram) ของคอมพิวเตอร์ อันดับที่ ๒ Fraud คือ การฉ้อโกงทางคอมพิวเตอร์ เช่น การนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์เพื่อหลอกลวงเหยื่อให้ส่งมอบทรัพย์สินให้ผู้กระทำความผิดในลักษณะที่เป็นการฉ้อโกงทรัพย์ และอันดับที่ ๓ Intrusion คือ การโจมตีระบบที่มีช่องโหว่ เพื่อเข้าควบคุมและสั่งการทำงานในเครื่องคอมพิวเตอร์เหยื่อ

๓. แนวความคิดด้านการอำนวยความยุติธรรมทางอาญาตามยุทธศาสตร์สำนักงานอัยการสูงสุด

๓.๑ การอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ภารกิจสำคัญด้านการอำนวยความยุติธรรมทางอาญาของสำนักงานอัยการสูงสุดอย่างหนึ่งคือ การเป็นโจทก์ฟ้องคดีอาญา โดยพนักงานอัยการมีหน้าที่ต้องทำความเห็นและคำสั่งในทางคดีตามอำนาจหน้าที่ที่กฎหมายบัญญัติดังกล่าวมาข้างต้น ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ซึ่งถือว่าเป็นคดีอาญาอย่างหนึ่ง พนักงานอัยการต้องปฏิบัติตามระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ซึ่งเป็นหลักเกณฑ์ในการดำเนินคดีอาญาตั้งแต่ในชั้นรับสำนวนการสอบสวนจากพนักงานสอบสวน การสั่งสอบสวน

เพิ่มเติม การพิจารณาทำความเห็นและคำสั่งในทางคดี การดำเนินคดีในศาลชั้นต้น การดำเนินคดีในศาลอุทธรณ์ และการดำเนินคดีในศาลฎีกา ทั้งนี้นอกจากระเบียบดังกล่าวแล้ว เมื่อปีพ.ศ. ๒๕๕๔ สำนักงานอัยการสูงสุดได้จัดทำคู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ ๒๕๕๔ เพื่อเป็นแนวทางให้แก่พนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยมีเนื้อหาครอบคลุมเกี่ยวกับกฎหมายว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พนักงานอัยการกับการสอบสวนคดีความผิดเกี่ยวกับคอมพิวเตอร์ (กรณีพนักงานอัยการเป็นพนักงานสอบสวนร่วมกับพนักงานสอบสวนอื่นในคดีความผิดนอกราชอาณาจักร ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๐ และกรณีร่วมสอบสวนกับพนักงานสอบสวนในคดีที่มีการกระทำความผิดเป็นองค์กรอาชญากรรมข้ามชาติ ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.๒๕๕๖) การรับและการพิจารณาสั่งสำนวนคดีความผิดเกี่ยวกับคอมพิวเตอร์ และการดำเนินคดีในชั้นศาล (สำนักงานอัยการสูงสุด, ๒๕๕๔ ก)

๓.๒ ยุทธศาสตร์สำนักงานอัยการสูงสุด (สำนักงานอัยการสูงสุด, ๒๕๕๙ ข : ๑๒-๑๘)

ปัจจุบัน สำนักงานอัยการสูงสุดได้ประกาศใช้แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี พ.ศ. ๒๕๕๙ – ๒๕๖๒ ซึ่งจัดทำบนพื้นฐานของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๕๘ พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๗ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการจัดทำแผนบริหารราชการแผ่นดิน พ.ศ.๒๕๔๗ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการจัดทำแผนบริการราชการแผ่นดิน (ฉบับที่ ๒) พ.ศ. ๒๕๔๘ และแนวคิดการจัดการภาครัฐแนวใหม่ (New Public Management) โดยการจัดทำแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ มีคณะที่ปรึกษาจากศูนย์บริการวิชาการ สถาบันบัณฑิตพัฒนบริหารศาสตร์ เป็นผู้ดำเนินการศึกษาวิจัย โดยมีศาสตราจารย์ ดร. บรรเจิด สิงคะเนติ เป็นหัวหน้าโครงการวิจัย ซึ่งกรอบแนวคิดพื้นฐานด้านเนื้อหาในการจัดทำแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙–๒๕๖๒ ได้แก่

๓.๒.๑ มุ่งเน้นพัฒนาการทำงานเพื่อประชาชน และรักษาผลประโยชน์ของประเทศชาติ โดยยึดมั่นในอุดมการณ์เพื่อรับสนองต่อพระบรมราชปณิธานแห่งองค์พระบาทสมเด็จพระเจ้าอยู่หัว (รัชการที่ ๙) ในการครองแผ่นดินโดยธรรมเพื่อประโยชน์สุขแห่งมหาชนชาวสยาม

๓.๒.๒ น้อมนำหลักปรัชญาของเศรษฐกิจพอเพียงเป็นปรัชญานำทางในการพัฒนาสำนักงานอัยการสูงสุดและแนวทางการดำรงชีวิตและการปฏิบัติตนของบุคลากร เพื่อเสริมสร้างภูมิคุ้มกันและบริหารจัดการความเสี่ยง

๓.๒.๓ สอดคล้องกับแนวคิดและทิศทางการพัฒนาประเทศ ตามรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๕๗ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๑ นโยบายรัฐบาล แผนการบริหารราชการแผ่นดิน แผนยุทธศาสตร์การพัฒนาระบบราชการไทย แผนแม่บทการบริหารงานยุติธรรมแห่งชาติ และยุทธศาสตร์ของหน่วยงานในกระบวนการยุติธรรมอื่น ๆ รวมทั้งนโยบายและยุทธศาสตร์ของสานักงานอัยการสูงสุดของประเทศอื่นที่ได้มาตรฐานเป็นที่ยอมรับระดับสากล ข้อตกลง อนุสัญญาฯ และความร่วมมือระหว่างประเทศที่เกี่ยวข้อง

๓.๒.๔ สอดคล้องกับสถานการณ์ของประเทศ การรักษาความมั่นคงเกี่ยวกับสถานการณ์อาชญากรรมของประเทศ แนวทางการปฏิรูปด้านกฎหมายและกระบวนการยุติธรรมของประเทศไทย รวมทั้งสภาพแวดล้อมที่เปลี่ยนแปลงไปทั้งภายนอกและภายในประเทศ เช่น การปฏิรูปประเทศ การก่อการร้าย การค้ายาเสพติด การค้ามนุษย์ อาชญากรรมข้ามชาติ การแก้ไขปัญหาการใช้ความรุนแรงในจังหวัดชายแดนภาคใต้ และการจัดตั้งประชาคมอาเซียนในปี พ.ศ. ๒๕๕๘ เป็นต้น

๓.๒.๕ เน้นการพัฒนาประสิทธิภาพการบริหารงานยุติธรรมที่เข้าถึงได้ง่าย มีมาตรฐานตามหลักสากล ทันสมัย รวดเร็ว โปร่งใส เสมอภาคและเป็นธรรม กำหนดมาตรฐานการปฏิบัติงานให้ชัดเจน ตั้งแต่แนวทางปฏิบัติ วิธีการและขั้นตอนการดำเนินงาน ระยะเวลาแล้วเสร็จ รวมทั้งลดขั้นตอนการปฏิบัติงานให้รวดเร็ว กระชับ แน่นอน สะดวกในการเข้าใช้บริการ ส่งเสริมการพัฒนาองค์กรและสร้างองค์ความรู้ในงานยุติธรรม พัฒนาบุคลากรให้มีความรู้ ทักษะ ความเชี่ยวชาญเป็นมืออาชีพ ปลูกฝังค่านิยมประชาธิปไตย หลักธรรมาภิบาล คุณธรรม จริยธรรม จิตสานึกในการรักษาศักดิ์ศรีของความเป็นข้าราชการและความซื่อสัตย์สุจริต และมีจิตสานึกที่ดีในการให้บริการ สนับสนุนการศึกษาวิจัย การนำเทคโนโลยีที่ทันสมัยและความรู้ทางนิติวิทยาศาสตร์มาใช้ในการปฏิบัติงานและเชื่อมโยงข้อมูลกระบวนการยุติธรรมร่วมกัน

๓.๒.๖ ปรับปรุงระบบการให้ความช่วยเหลือทางกฎหมายด้วยมาตรการเชิงรุกให้เข้าถึงความเป็นธรรมได้ง่าย รวดเร็ว ขยายการให้บริการและให้ความรู้ทางกฎหมายแก่ประชาชน รวมทั้งส่งเสริมกระบวนการยุติธรรมทางเลือกและการมีส่วนร่วมในงานยุติธรรม ลดปริมาณคดีขึ้นสู่ศาล และสร้างความปรองดองสมานฉันท์ในสังคม

๓.๒.๗ เน้นการพัฒนาและบังคับใช้กฎหมายอย่างเสมอภาคและเป็นธรรม สร้างความเชื่อมั่นในกระบวนการยุติธรรมตามหลักนิติธรรม หลักคุณธรรมและจริยธรรม และหลักผลประโยชน์ส่วนรวมของประเทศ และหลักสิทธิมนุษยชนโดยไม่เลือกปฏิบัติ

๓.๒.๘ สร้างระบบบริหารจัดการภาครัฐ ยึดหลักการบริหารกิจการบ้านเมืองที่ดี การบริหารจัดการภาครัฐแบบใหม่ การตอบสนองความต้องการของประชาชนในฐานะที่เป็นศูนย์กลาง ยึดประโยชน์ส่วนรวม และความสมานฉันท์ในทุกภาคส่วนและทุกระดับ รวมทั้งปรับปรุงระบบการบริหารงานบุคคลให้มีหลักเกณฑ์ที่ชัดเจน แน่นอน มีความโปร่งใส ถูกต้องและเป็นธรรม พัฒนาระบบและกลไกการป้องกันและปราบปรามการทุจริตและประพฤติมิชอบอย่างมีส่วนร่วม เพื่อให้เกิดความร่วมมือระหว่างหน่วยงานในกระบวนการยุติธรรมและภาคส่วนต่างๆ ที่เกี่ยวข้อง และป้องกันการทุจริตประพฤติมิชอบและเพื่อความโปร่งใสในการบังคับใช้กฎหมาย

๓.๒.๙ สร้างกระบวนการพัฒนาโดยให้ความสำคัญกับความคิดเห็นและความต้องการของประชาชน ส่งเสริมให้ประชาชนทุกระดับมีโอกาสเข้าถึงกระบวนการยุติธรรมอย่างเท่าเทียมและสร้างความเป็นธรรมในการเข้าถึงระบบยุติธรรมที่เป็นมาตรฐานสากล ให้ความรู้เกี่ยวกับการใช้กฎหมายและขั้นตอนระบบงานยุติธรรมแก่ประชาชนทุกกลุ่ม เสริมสร้างการมีส่วนร่วมและบทบาทของภาคีการพัฒนาต่างๆ ได้แก่ ภาคประชาชน องค์กรปกครองท้องถิ่น ภาคเอกชน องค์กรเอกชน สถาบันการศึกษาและสื่อมวลชน ได้เข้ามามีส่วนร่วมในการพัฒนา เพื่อให้ประชาชนได้รับบริการที่สะดวก รวดเร็ว เข้าถึงง่าย เสมอภาค เป็นธรรม และสามารถดำรงชีวิตอยู่ได้อย่างมีศักดิ์ศรี

ในการจัดทำแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ ใช้วิธีการศึกษาในเชิงคุณภาพอาศัยวิธีการศึกษาวิจัยผสมผสาน ประกอบด้วย

๓.๒.๙.๑ การทบทวนวรรณกรรมที่เกี่ยวข้อง ได้แก่ พระบรมราโชวาทและพระราชดำรัสพระบาทสมเด็จพระเจ้าอยู่หัว (รัชกาลที่ ๙) รายงานเอกสารเกี่ยวกับบทบาท ภารกิจ การดำเนินงาน โครงสร้างองค์กร วัฒนธรรมองค์กร และนโยบายของสำนักงานอัยการสูงสุดที่ผ่านมา และรัฐธรรมนูญแห่งราชอาณาจักรไทย กฎหมาย ระเบียบที่เกี่ยวข้อง นโยบายรัฐบาล แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ แผนบริการราชการแผ่นดิน แผนยุทธศาสตร์การพัฒนาระบบราชการไทย แผนแม่บทการบริหารงานยุติธรรมแห่งชาติ และยุทธศาสตร์ของหน่วยงานในกระบวนการยุติธรรมอื่นๆ

๓.๒.๙.๒ การสัมภาษณ์เชิงลึก ผู้บริหารระดับสูงของสำนักงานอัยการสูงสุด อัยการสูงสุด และรองอัยการสูงสุด ผู้บริหารองค์กรตามรัฐธรรมนูญอื่นๆ รวม ๑๑ คน

๓.๒.๙.๓ สอบถามความคิดเห็น ของบุคคลากรในสำนักงานอัยการสูงสุดด้วยแบบสอบถามและแบบสอบถามออนไลน์

๓.๒.๙.๔ จัดประชุม และสัมมนาองค์ความรู้และประชุมเชิงปฏิบัติการ รวม ๗ ครั้ง

๓.๒.๙.๕ สัมมนาเพื่อรับฟังความคิดเห็น รวม ๒ ครั้ง

๓.๓ ยุทธศาสตร์ด้านการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด (สำนักงานอัยการสูงสุด, ๒๕๕๙ ข : ๒๑-๒๒)

แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ ได้กำหนดพันธกิจที่สำนักงานอัยการสูงสุดมุ่งที่จะบรรลุไว้ ๕ ประการ คือ

๓.๓.๑ อำนวยความยุติธรรมทางอาญาและบังคับใช้กฎหมายตามหลักนิติธรรม

๓.๓.๒ รักษาผลประโยชน์ของรัฐและประชาชน

๓.๓.๓ พัฒนางานด้านสิทธิมนุษยชน คุ้มครองสิทธิและเสรีภาพของประชาชนทั้งในและนอกประเทศตามหลักมาตรฐานสากล

๓.๓.๔ พัฒนาเครือข่ายความร่วมมือทางกฎหมายกับองค์กรหรือหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

๓.๓.๕ พัฒนาองค์กรสู่ความเป็นเลิศ

ในการปฏิบัติพันธกิจของสำนักงานอัยการสูงสุดให้บรรลุประสิทธิผล สำนักงานอัยการสูงสุดได้กำหนดเป้าประสงค์ซึ่งจะเป็นสิ่งที่กำหนดทิศทางในการปฏิบัติตามแผนยุทธศาสตร์สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ จำนวน ๔ ข้อ ดังนี้

๑. สามารถอำนวยความยุติธรรมทางอาญาตามหลักนิติธรรม

๒. สามารถรักษาผลประโยชน์ของรัฐและประชาชน

๓. สามารถรักษาและคุ้มครองสิทธิมนุษยชนและเสรีภาพของประชาชนตามหลักมาตรฐานสากล

๔. สามารถพัฒนาเครือข่ายความร่วมมือทางกฎหมายกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

จากนั้น เพื่อให้บรรลุภารกิจตามเป้าประสงค์ ประเด็นยุทธศาสตร์ (Strategies) จำนวน ๖ ข้อ ได้ถูกกำหนดขึ้นโดยมีความสอดคล้องกับพันธกิจและเป้าประสงค์ โดยใช้แนวทางการพัฒนาองค์กรอัยการสู่ความเป็นเลิศเป็นกรอบในการพัฒนาองค์กร ประกอบด้วย

ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา
ยุทธศาสตร์ที่ ๒ การรักษาผลประโยชน์ของรัฐและประชาชน
ยุทธศาสตร์ที่ ๓ การคุ้มครองสิทธิมนุษยชนและช่วยเหลือทางกฎหมาย
ยุทธศาสตร์ที่ ๔ การสร้างความเชื่อมั่นแก่ประชาชนและหน่วยงานผู้มีส่วนได้ส่วนเสียต่อการปฏิบัติราชการของสำนักงานอัยการสูงสุด
ยุทธศาสตร์ที่ ๕ การพัฒนาเครือข่ายความร่วมมือกับหน่วยงานทางกฎหมายทั้งในและต่างประเทศ
ยุทธศาสตร์ที่ ๖ การพัฒนาองค์กรสู่ความเป็นเลิศ

สำหรับกรอบเนื้อหาที่จะศึกษาในเอกสารวิจัยนี้ เน้นเฉพาะประเด็นการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา ซึ่งยุทธศาสตร์ในส่วนนี้มีการกำหนดกลยุทธ์เพื่อเป็นกรอบและแนวทางในการดำเนินงาน รวมทั้งกิจกรรมที่อยู่ภายในวัตถุประสงค์ของกลยุทธ์ ดังนี้

ตารางที่ ๒-๔ ตารางแสดงกลยุทธ์ วัตถุประสงค์ และโครงการ ภายใต้ยุทธศาสตร์การอำนวยความยุติธรรมทางอาญา

ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา		
กลยุทธ์	**วัตถุประสงค์**	**โครงการ**
กลยุทธ์ที่ ๑.๑ สร้างมาตรฐานและศักยภาพในการอำนวยความยุติธรรม	เพื่อเพิ่มประสิทธิภาพในการดำเนินคดีอาญาของพนักงานอัยการ และการให้บริการประชาชน	๑. โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญา ๒. โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญาในพื้นที่สำนักงานอัยการสูงสุด ภาค ๑-๙ ๓. โครงการสร้างมาตรฐานกระบวนงานผ่านสื่ออิเล็กทรอนิกส์ ๔. โครงการเพิ่มประสิทธิภาพการดำเนินคดียาเสพติด ๕. โครงการสร้างมาตรฐานในการดำเนินคดีทรัพย์สินทางปัญญาในรูปแบบอิเล็กทรอนิกส์ ๖. โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมทางเทคโนโลยี ๗. โครงการจัดตั้งศูนย์วิชาการด้านคดีเศรษฐกิจและทรัพยากร
กลยุทธ์ที่ ๑.๒ พัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน	เพื่อเพิ่มขีดความสามารถของพนักงานอัยการในด้านการสอบสวนคดีอาญา	๑. โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน ๒. โครงการพัฒนาศักยภาพของพนักงานอัยการด้านการสอบสวนเด็กและเยาวชนที่เกี่ยวข้องในกระบวนการยุติธรรม
กลยุทธ์ที่ ๑.๓ พัฒนาบทบาทหน้าที่ของพนักงานอัยการในกระบวนการยุติธรรมทางเลือก	เพื่อลดปริมาณคดีอาญาขึ้นสู่ศาลด้วยกระบวนการยุติธรรมทางเลือก	๑. โครงการเสริมสร้างศักยภาพพนักงานอัยการในการใช้กระบวนการยุติธรรมทางเลือก ๒. โครงการรองรับมาตรการแทนการฟ้องคดีอาญา
กลยุทธ์ที่ ๑.๔ เพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญา	เพื่อเพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในทางอาญา	โครงการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา
		รวม ๑๒ โครงการ

ที่มา : สำนักงานอัยการสูงสุด, ๒๕๕๙ ข : ๒๙-๓๐

ทั้งนี้ ในปีงบประมาณ ๒๕๖๐ อัยการสูงสุดได้เห็นชอบแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปีงบประมาณ ๒๕๖๐ (Action Plan) โครงการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ รวมทั้งสิ้น ๑๖ โครงการเป็นเงินจำนวน ๑๒,๐๐๐,๐๐๐ บาท โดยในส่วนของโครงการที่มีความเกี่ยวข้องกับการส่งเสริมการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์ที่ ๑ “อำนวยความยุติธรรมทางอาญา” ที่ได้รับการอนุมัติงบประมาณ จำนวน ๒ โครงการ (สำนักงานอัยการสูงสุด, ๒๕๕๙ ก : ๑๔-๑๖) คือ

๑. โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน ตามกลยุทธ์ที่ ๑.๒ มีวัตถุประสงค์เพื่อเพิ่มขีดความสามารถของพนักงานอัยการในด้านการสอบสวนคดีอาญา จำนวนเงินงบประมาณ ๗๕๐,๐๐๐ บาท ระยะเวลาดำเนินงาน ๑ ตุลาคม ๒๕๕๙ ถึง ๓๐ กันยายน ๒๕๖๐ หน่วยงานรับผิดชอบคือ สำนักงานการสอบสวน

๒. โครงการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา ตามกลยุทธ์ที่ ๑.๔ มีวัตถุประสงค์เพื่อเพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในทางคดีอาญา จำนวนเงินงบประมาณ ๒๐๐,๐๐๐ บาท ระยะเวลาดำเนินงาน ๑ ตุลาคม ๒๕๕๙ ถึง ๓๐ กันยายน ๒๕๖๐ หน่วยงานรับผิดชอบคือ สำนักงานต่างประเทศ

อนึ่ง สำหรับ “โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมทางเทคโนโลยี” ตามกลยุทธ์ที่ ๑.๑ (วงเงินงบประมาณ ๗๒๐,๐๐๐ บาท) ซึ่งอยู่ภายใต้แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ มีสำนักงานคดีเศรษฐกิจและทรัพยากรธรรมชาติ สถาบันพัฒนาข้าราชการฝ่ายอัยการ และสำนักงานวิชาการ เป็นหน่วยงานรับผิดชอบ ยังไม่มีการจัดสรรงบประมาณในปี ๒๕๖๐

วรรณกรรมที่เกี่ยวข้อง และแนวคิดของผู้ทรงคุณวุฒิ

ในเบื้องต้น จากการทบทวนตำรา งานเขียน วิทยานิพนธ์ และงานวิจัย ผ่านการสืบค้นฐานข้อมูลของงานกองเอกสารวิจัยวิจัยและห้องสมุดวิทยาลัยป้องกันราชอาณาจักร ห้องสมุดจุฬาลงกรณ์มหาวิทยาลัย และห้องสมุดมหาวิทยาลัยธรรมศาสตร์ ยังไม่พบวรรณกรรมหรืองานวิจัยในเรื่องยุทธศาสตร์ของสำนักงานอัยการสูงสุดในการตอบโต้อาชญากรรมคอมพิวเตอร์โดยตรง แต่พบวรรณกรรมทางวิชาการทั่วไปในภาพรวมเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ (วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต, ๒๕๕๗) หรือในบางครั้งเรียกว่า “อาชญากรรมบนสื่อออนไลน์” รวมถึงวรรณกรรมเกี่ยวกับแนวทางป้องกันและแก้ปัญหาอาชญากรรมของหน่วยงานภาครัฐในภาพรวม และวรรณกรรมเกี่ยวกับปัญหาการรับฟังพยานหรือการรวบรวมพยานหลักฐานอิเล็กทรอนิกส์หรือพยานหลักฐานดิจิทัล (นัทธ์ ธเนศวาณิชย์, ๒๕๕๕ : ๖๓. ; สุนีย์ สกาวรัตน์, ๒๕๕๙ : ๗๒.)

ผลงานวิจัยที่สำคัญ และแนวความคิดของผู้ทรงคุณวุฒิที่เกี่ยวข้องกับงานวิจัยนี้ ได้แก่

เฉลิมชนม์ แน่นหนา และคณะ (๒๕๕๕ : ๙๐-๙๐) ซึ่งทำการวิจัยในหลักสูตรการป้องกันราชอาณาจักร (วปอ.) รุ่นที่ ๕๕ เรื่อง “อาชญากรรมบนสื่อออนไลน์ (Cybercrime)” เน้นวิเคราะห์แนวทางการป้องกันและแก้ปัญหาอาชญากรรมออนไลน์ โดยมีพื้นฐานความคิดว่าทุกคนต้องตระหนักถึงความสำคัญ และภัยที่มาควบคู่กับสื่อออนไลน์ให้มากขึ้น และต้องมีการป้องกันภัยคุกคามออนไลน์

อย่างรู้เท่าทัน โดยทำการศึกษาอาชญากรรมบนสื่อออนไลน์ในบริบทของการให้การประสานความร่วมมือกันทั้งภาครัฐและภาคเอกชน เพื่อชี้แนะแนวทางในการป้องกันและแก้ไขปัญหาอาชญากรรมบนสื่อออนไลน์อย่างเป็นระบบ โดยเฉลิมชนม์ แน่นหนา และคณะ (๒๕๕๕ : ๙๐-๙๑) ได้เสนอแนะแนวทางในการป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์อย่างเป็นระบบ ดังนี้

๑. การแก้กฎหมายต้องมีความชัดเจนระหว่างการกระทำความผิดอาญาตามประมวลกฎหมายอาญาหรือกฎหมายอื่นที่มีโทษทางอาญาโดยผ่านช่องทางคอมพิวเตอร์หรือสื่อออนไลน์กับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ รวมทั้งเสนอให้มีการจัดตั้งศาลชำนัญการพิเศษและบัญญัติกฎหมายลักษณะพยาน และวิธีพิจารณาคดีอาชญากรรมคอมพิวเตอร์และอาชญากรรมออนไลน์บัญญัติขึ้นโดยเฉพาะเพื่อให้สอดคล้องกับสภาพปัญหาที่เกิดขึ้น

๒. การนำนโยบายไปสู่การปฏิบัติไม่ควรมองปัญหาแบบแยกส่วนในลักษณะต่างคนต่างทำ การดำเนินงานต้องมีเอกภาพในการดำเนินการ และให้มีหน่วยงานหลักในการรวมหรือบูรณาการแผนรวม เพื่อเดินไปสู่เป้าหมายและทิศทางเดียวกัน ซึ่งคดีที่เกี่ยวกับความผิดทางคอมพิวเตอร์บนสื่อออนไลน์ ส่วนใหญ่เป็นคดีที่ต้องอาศัยความรู้ความชำนาญและมีลักษณะคดีที่เกิดขึ้นในหลายท้องที่ทั้งในและนอกราชอาณาจักร อีกทั้ง ในแต่ละหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามก็ยังขาดแคลนบุคลากรที่มีความรู้ความเชี่ยวชาญอยู่เป็นจำนวนมาก จึงเห็นควรให้มีการยุบรวมหน่วยงานในการป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์ โดยให้มีกฎหมายพิเศษระบุอำนาจหน้าที่เจ้าหน้าที่ผู้ปฏิบัติให้มีความคล่องตัวและสะดวกรวดเร็วทันต่ออาชญากรรมต่างๆที่ก่อตัวอย่างรวดเร็วผ่านสื่อออนไลน์ ในอีกด้านหนึ่งก็ต้องจัดให้มีระบบตรวจสอบและถ่วงดุลอำนาจที่มีความน่าเชื่อถือมิให้เป็นข้อกังขาได้ว่าเจ้าหน้าที่ปฏิบัติหน้าที่โดยมิชอบด้วย

๓. จัดสรรอำนาจหน้าที่ งบประมาณ และวางกรอบแนวทางการประสานงานระหว่างหน่วยงานที่ทำหน้าที่ป้องกันและปราบปรามอาชญากรรมบนสื่อออนไลน์โดยตรง กับหน่วยงานที่มีหน้าที่ให้การสนับสนุนให้ชัดเจน โดยเฉพาะการจัดวางแผนอัตรากำลังเจ้าหน้าที่มีความรู้ความชำนาญให้เพียงพอต่อความต้องการ ซึ่งในเบื้องต้นอาจใช้การประสานความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน เช่น การแต่งตั้งเจ้าหน้าที่หรือพนักงานของหน่วยงานภาครัฐหรือเอกชนที่มีความรู้ความเชี่ยวชาญในลักษณะงานที่มีประโยชน์ต่อการสืบสวนสอบสวนคดีเป็นผู้ช่วยพนักงานสอบสวน

๔. จัดทำคู่มือปฏิบัติงานและหลักนิยมสำหรับผู้ทำหน้าที่ปราบปรามอาชญากรรมบนสื่อออนไลน์ รวมทั้งศึกษารวบรวมสถิติคดีความที่เกิดขึ้นเพื่อนำมาปรับปรุงพัฒนาคู่มือปฏิบัติให้ทันต่อความเปลี่ยนแปลงและความซับซ้อนของการก่ออาชญากรรมบนสื่อสื่อออนไลน์

เฉลิมชนม์ แน่นหนา และคณะ (๒๕๕๕ : ๘๘) ได้ตั้งข้อสังเกตว่า ปัจจุบัน แม้ว่าหน่วยงานภาครัฐได้มีการบูรณาการความร่วมมือกับหน่วยงานต่าง ๆ ทั้งในและต่างประเทศเพื่อสืบสวนสอบสวนพิสูจน์หลักฐานและปราบปรามผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ก็ตาม แต่การใช้กลยุทธ์ต่างๆ ในการจัดการกับอาชญากรรมคอมพิวเตอร์ยังคงเป็นไปโดยขาดเอกภาพ อีกทั้งหน่วยงานภาครัฐมีข้อจำกัดด้านอัตรากำลังคน บุคลากรที่มีความรู้ความชำนาญด้านคอมพิวเตอร์ และงบประมาณ ประกอบกับยังมีข้อจำกัดทางกฎหมาย หลักเกณฑ์และวิธีการปฏิบัติทางราชการต่างๆ ที่ไม่เอื้ออำนวยต่อการปรับเปลี่ยนกลยุทธ์หรือยุทธวิธีต่างๆให้ทันต่ออาชญากรรมคอมพิวเตอร์

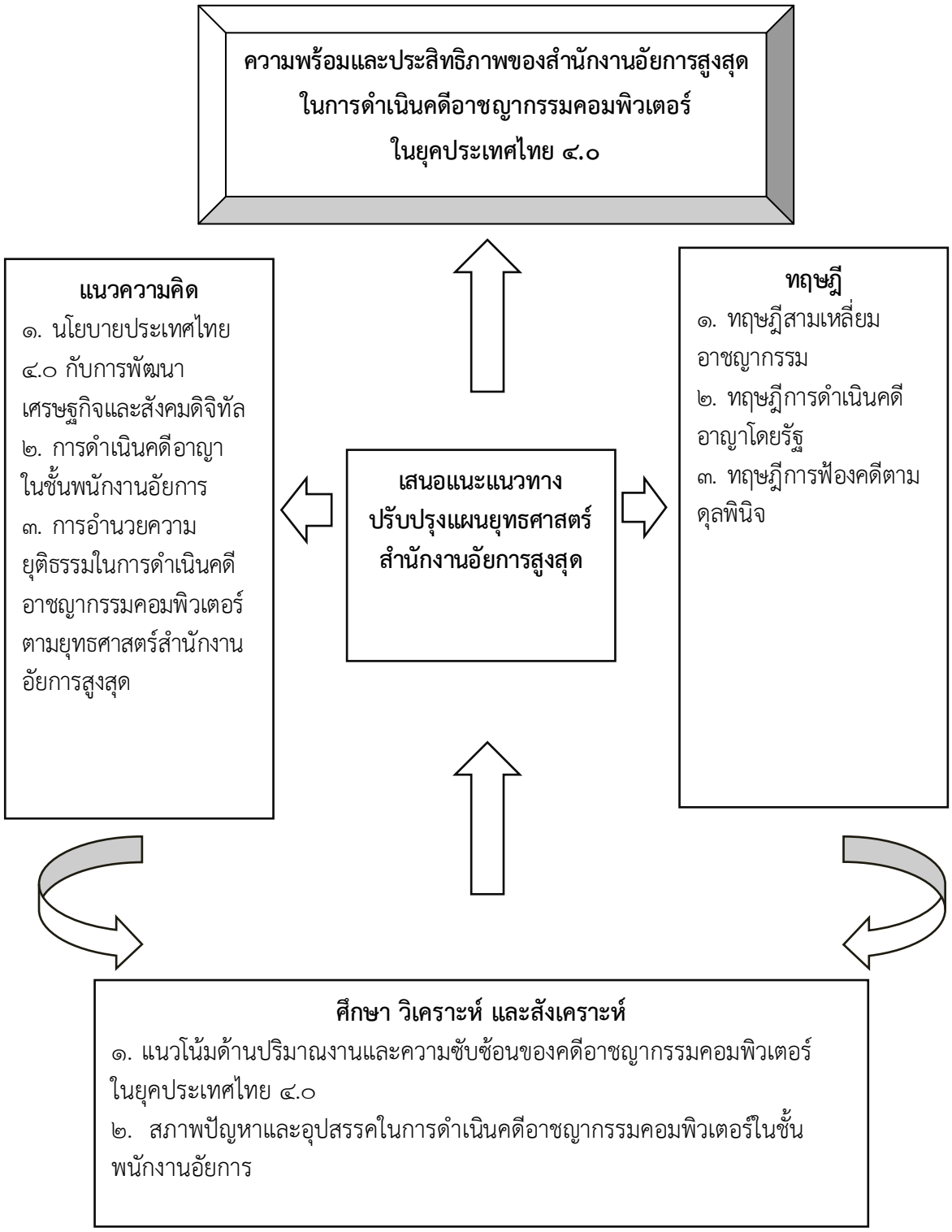
วิทยา สุริยวงค์ (๒๕๕๒ : ๖๘-๗๔) ได้ทำการวิจัยในหลักสูตรการป้องกันราชอาณาจักร (วปอ.) รุ่นที่ ๕๒ เรื่อง “ยุทธศาสตร์การต่อสู้ปัญหาอาชญากรรม : ศึกษากรณีการจัดทำรายงานอาชญากรรมข้ามชาติ โดยศึกษาสภาพปัญหาและข้อจำกัดในการจัดทำรายงานอาชญากรรมที่ใช้อยู่ในประเทศไทย แนวคิดหลักเกณฑ์และระบบคำนวณอัตราอาชญากรรมที่ใช้อยู่จริง รวมถึงการจัดทำรายงานอาชญากรรมของประเทศต่างๆ แนวทางเกณฑ์มาตรฐานและความเป็นไปได้ในการจัดทำรายงานอาชญากรรมระดับชาติและนำเสนอรูปแบบที่ควรจะเป็น เนื่องจากเห็นว่า สถิติทางอาญาและรายงานอาชญากรรมเป็นเรื่องที่มีความสำคัญต่อการพัฒนาประเทศ โดยข้อมูลที่ได้จะสามารถนำไปใช้วิเคราะห์ในเชิงวิชาการและการกำหนดนโยบายการป้องกันและปราบปรามอาชญากรรมที่ถูกต้องเหมาะสม โดยวิทยา สุริยะวงค์ (๒๕๕๒ : ๖๘-๗๔) ได้ศึกษาสภาพปัญหาของการจัดทำรายงานอาชญากรรมระดับชาติผ่านการวิเคราะห์ข้อมูลรูปแบบการจัดเก็บสถิติอาชญากรรมที่รวบรวมโดยหน่วยงานในกระบวนการยุติธรรมทางอาญา ได้แก่ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด สำนักงานศาลยุติธรรม และกรมราชทัณฑ์ โดยได้วิเคราะห์รูปแบบการเก็บข้อมูลสถิติคดีอาญาของสำนักงานอัยการสูงสุดไว้ว่า ข้อมูลสถิติคดีอาญาที่มีการรวบรวมโดยสำนักงานอัยการสูงสุดมีลักษณะเป็นการแสดงถึงปริมาณคดีที่มีการส่งมายังพนักงานอัยการเพื่อดำเนินการในการนำคดีเข้าสู่ศาล และการติดตามการดำเนินคดี โดยแยกแยะข้อมูลสถิติตามวัตถุประสงค์การนำไปใช้ แต่มิได้มีการนำมาคิดคำนวณอัตราคดีต่อประชากรเพื่อแสดงอัตราอาชญากรรม

ในด้านการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ **ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ (๒๕๕๗ : ๓๓-๓๕)** ได้ทำการศึกษาวิจัยการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม ซึ่งเป็นการศึกษาวิจัยเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ในเชิงการตอบโต้ภัยคุกคามด้านความมั่นคงของประเทศ เพื่อเป็นข้อมูลประกอบการพิจารณากำหนดนโยบายยุทธศาสตร์ และระเบียบวิธีในการปฏิบัติของหน่วยงานด้านความมั่นคงของประเทศไทย นอกจากนี้ การพัฒนามาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ในเชิงการสร้างความมั่นใจให้แก่ผู้ใช้งานระบบอินเทอร์เน็ตในยุคเศรษฐกิจและสังคมดิจิทัลปรากฏอยู่ในแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

จากสถิติที่เกี่ยวข้องตามที่ได้กล่าวมาในหัวข้อ “สถิติที่เกี่ยวข้อง” คาดการณ์ได้ว่าปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันมีแนวโน้มเพิ่มมากขึ้นและทวีความซับซ้อนของรูปแบบของการกระทำความผิดมากขึ้น ทำให้การรวบรวมพยานหลักฐานและการพิสูจน์การกระทำความผิดของผู้กระทำความผิดทำได้ยากลำบากขึ้น เนื่องจากการเก็บและพิสูจน์พยานหลักฐานทางดิจิทัลมีหลักเกณฑ์และเงื่อนไขที่แตกต่างจากการรับฟังพยานหลักฐานในคดีอาญาทั่วไป ดังนั้น หากผู้บังคับใช้กฎหมายขาดความรู้ความเข้าใจในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ย่อมทำให้เกิดปัญหาในการบังคับใช้กฎหมายซึ่งจะส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจ ดังที่ **วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต (๒๕๕๗, ๑๘๙-๑๙๐)** ได้วิเคราะห์ปัญหาการกำหนดขอบเขตที่แท้จริงของการกระทำความผิดทางอาญาเกี่ยวกับคอมพิวเตอร์ไว้ว่า “(ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์)...พนักงานอัยการก็ลังเลที่จะดำเนินคดีและศาลก็คงไม่แน่ใจ ที่จะพิพากษาตัดสิน

เนื่องจากทั้ง ๒ กลุ่มต่างก็ไม่เข้าใจถึงเทคโนโลยีและยังมีความลำบากที่จะค้นหาความเสียหายต่อสาธารณชนอันเกิดจากการกระทำดังกล่าว”

กรอบความคิดของการวิจัย



สรุป

การทบทวนวรรณกรรมของผู้วิจัยใช้การทบทวนแนวความคิด ทฤษฎี และข้อมูลจากงานเขียน เอกสารราชการ กฎหมาย บทความทางวิชาการ วิทยานิพนธ์ งานวิจัย สถิติที่เกี่ยวข้องกับผลกระทบของประเทศไทย ๔.๐ ที่คาดว่าจะเกิดกับปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ซึ่งอยู่ในอำนาจหน้าที่ความรับผิดชอบของสำนักงานอัยการสูงสุด เพื่อใช้เป็นข้อมูลพื้นฐานสำคัญในการวิเคราะห์แนวโน้มของคดีอาชญากรรมคอมพิวเตอร์ในอนาคต แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นการต่อยอดประเด็นการวิจัยเกี่ยวกับแนวทางแก้ไขปัญหาอาชญากรรมออนไลน์ ของ เฉลิมชนม์ แน่นหนา และคณะ (๒๕๕๕) และประเด็นการปรับปรุงการเก็บรวบรวมสถิติคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดเพื่อประโยชน์ในการจัดทำรายงานอาชญากรรมระดับชาติ ซึ่งกล่าวไว้ในงานวิจัยของ วิทยา สุริยะวงค์ (๒๕๕๒) พิจารณาประกอบกับผลการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิในด้านงานคดีของสำนักงานอัยการสูงสุด เพื่อเสนอแนะแนวทางในการปรับปรุงแผนยุทธศาสตร์ของสำนักงานอัยการสูงสุดในด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ในบทต่อๆ ไปของงานวิจัยนี้

บทที่ ๓
การดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการตามยุทธศาสตร์สำนักงานอัยการสูงสุด

การศึกษาในบทที่ ๓ มีความมุ่งหมายเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ ๑. เพื่อศึกษาแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ โดยมีลำดับการศึกษา ดังนี้

๑. แนวโน้มปริมาณงานคดีอาชญากรรมคอมพิวเตอร์
๒. ลักษณะและความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์
๓. แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด
๔. ตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ผ่านมา
๕. ปัญหาและอุปสรรคที่พบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์
๖. สรุป

แนวโน้มปริมาณงานคดีอาชญากรรมคอมพิวเตอร์

ด้วยเหตุที่การก่ออาชญากรรมคอมพิวเตอร์ต้องอาศัยโอกาสในการกระทำต่อตัวระบบคอมพิวเตอร์หรือผ่านระบบคอมพิวเตอร์ ดังนั้น ตัวแปรสำคัญประการหนึ่งของปริมาณงานคดีอาชญากรรมคอมพิวเตอร์จึงได้แก่จำนวนผู้ใช้งานระบบคอมพิวเตอร์และอินเทอร์เน็ต อาทิเช่น กลุ่มผู้เสียหายจากการฉ้อโกงธุรกรรมการซื้อขายสินค้าและบริการทางอินเทอร์เน็ต ย่อมได้แก่ ผู้ซื้อสินค้าหรือบริการทางอินเทอร์เน็ตซึ่งหลงเชื่อกลฉ้อฉลหลอกลวงของคนร้าย หรือกรณีของการเจาะเข้าสู่ระบบธุรกรรมทางการเงินอิเล็กทรอนิกส์เพื่อขโมยเงินในบัญชีเงินฝากธนาคารของเจ้าของบัญชีหรือเปลี่ยนแปลงข้อมูลส่วนบุคคลของเจ้าของบัญชีเพื่อแสวงหาผลประโยชน์โดยมิชอบประการอื่น กลุ่มผู้เสียหาย คือ เจ้าของบัญชีเงินฝากธนาคารและธนาคารพาณิชย์ซึ่งมีข้อมูลของลูกค้าที่จัดเก็บอยู่ในระบบคอมพิวเตอร์และสามารถเรียกดูหรือใช้ข้อมูลดังกล่าวผ่านระบบคอมพิวเตอร์ไม่ว่าจากอุปกรณ์คอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ซึ่งสามารถเชื่อมต่ออินเทอร์เน็ต ดังนั้น จึงอาจกล่าวได้ว่า เมื่อบุคคลเข้าถึงระบบคอมพิวเตอร์ได้มากขึ้นเท่าใด ย่อมมีโอกาสเกิดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้มากขึ้นเท่านั้น โดยผู้ที่ทำธุรกรรมทางอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์แต่ขาดความรู้ ความเข้าใจ ความรอบคอบระมัดระวัง ย่อมมีแนวโน้มตกเป็นเหยื่อของมิจฉาชีพได้ง่าย

จากข้อมูลสถิติประชากรผู้ใช้อินเทอร์เน็ต โซเชียลมีเดีย และโทรศัพท์เคลื่อนที่ ณ เดือนมกราคม ๒๕๕๙ ตามแผนภาพที่ ๒-๓ ในบทที่ ๒ แสดงให้เห็นว่า ณ เดือนมกราคม ๒๕๕๙ มีประชากรมากถึง ๓๘ ล้านคน จากจำนวนประชากรรวมทั้งประเทศประมาณ ๖๘.๐๕ ล้านคน เป็นผู้ใช้งานในระบบอินเทอร์เน็ต และแผนภาพที่ ๒-๔ แสดงสถิติกิจกรรมที่กระทำผ่านโทรศัพท์เคลื่อนที่

ณ เดือนมกราคม ๒๕๕๙ มีผู้ทำธุรกรรมทางธนาคารผ่านโทรศัพท์เคลื่อนที่คิดเป็นจำนวนร้อยละ ๓๐ ของประชากรรวมทั้งประเทศ ซึ่งในปัจจุบันการเข้าถึงระบบธุรกรรมการเงินของธนาคารแพร่หลายจากเดิมอย่างมาก โดยนอกเหนือจากการทำธุรกรรมผ่านอินเทอร์เน็ต (Internet Banking หรือ I-Banking) ที่เริ่มมีการใช้มาตั้งแต่สิบปีที่แล้ว ปัจจุบันธนาคารพาณิชย์เกือบทุกธนาคารได้เพิ่มช่องทางในการทำธุรกรรมทางการเงินผ่านโปรแกรม หรือแอพพลิเคชั่น (Application) บนอุปกรณ์โทรศัพท์เคลื่อนที่ซึ่งสามารถเชื่อมต่ออินเทอร์เน็ตได้ หรือที่รู้จักกันในชื่อของ Mobile Banking โดยเมื่อผู้ใช้บริการอินเทอร์เน็ตนิยมใช้ช่องทางจัดการทางการเงินผ่านแอพพลิเคชั่นของธนาคารพาณิชย์ไทยบนอุปกรณ์โทรศัพท์เคลื่อนที่ มิจฉาชีพจึงได้เริ่มใช้ระบบคอมพิวเตอร์ในการกระทำความผิดในรูปแบบต่างๆ เช่น กรณีการโจรกรรมทางการเงินบนอินเทอร์เน็ตเว็บไซต์ของธนาคารไทยพาณิชย์ จำกัด (มหาชน) จนทางธนาคารต้องออกประกาศเตือนในทำนองว่า มีการโจรกรรมในรูปแบบของการส่งข้อความสั้น (SMS) โดยใช้หมายเลข ๐๒-๗๗๗-๗๗๗๗ ซึ่งเป็นหมายเลข Call Center ของธนาคารไทยพาณิชย์ จำกัด (มหาชน) เป็นผู้ส่งและมีลิ้งก์เพื่อให้ดาวโหลดหรือติดตั้งโปรแกรมทางการเงิน หมายเลขดังกล่าวถูกปลอมขึ้นเพื่อหวังหลอกลวงประชาชนโดยตรง โดยธนาคารไทยพาณิชย์ จำกัด (มหาชน) ไม่มีนโยบายในการส่งลิ้งก์เพื่อให้ดาวโหลดโปรแกรมใดๆผ่านโทรศัพท์เคลื่อนที่ เพื่อความปลอดภัยทางธนาคารจึงเตือนให้ลูกค้าใช้งาน Mobile banking application ที่ดาวโหลดจาก “Google Play” หรือ “App Store” เท่านั้น (ผู้จัดการ Online, ออนไลน์, ๒๕๕๖) และต่อมามิจฉาชีพได้พัฒนารูปแบบในการหลอกลวงให้แนบเนียนยิ่งขึ้นมากขึ้นด้วยการสร้างแอพพลิเคชั่นปลอม เผยแพร่ระบาดอยู่ใน “Play Store” ของระบบ Android โดยรายชื่อธนาคารที่มีการปลอมแอพพลิเคชั่น ได้แก่ ธนาคารกรุงไทย ธนาคารกรุงเทพ ธนาคารไทยพาณิชย์ ธนาคารกรุงศรีอยุธยา และธนาคารธนชาติ จนธนาคารพาณิชย์ดังกล่าวต้องออกประกาศทุกช่องทางเพื่อเตือนให้ลูกค้าของธนาคารระมัดระวังในการดาวโหลดแอพพลิเคชั่นของธนาคาร (ผู้จัดการ Online, ออนไลน์, ๒๕๕๗)

ในด้านสถิติพาณิชย์ทางอิเล็กทรอนิกส์ (E-Commerce) ที่กระทำผ่านอุปกรณ์อินเทอร์เน็ต ณ เดือนมกราคม ๒๕๕๙ แผนภาพที่ ๒-๕ ที่กล่าวไว้ในบทที่ ๒ แสดงผลการสำรวจข้อมูลของเว็บไซต์ www.veedvil.com ซึ่งพบว่า ในช่วงรอบ ๓๐ วันก่อนการสำรวจ มีจำนวนประชากรมากถึงร้อยละ ๔๔ ที่เพิ่งทำธุรกรรมซื้อสินค้าหรือบริการออนไลน์ จำนวนร้อยละ ๔๘ เข้าดูอินเทอร์เน็ตเพื่อหาข้อมูลเกี่ยวกับสินค้าที่จะซื้อ จำนวนร้อยละ ๔๐ เข้าดูเว็บไซต์ของผู้ประกอบการรายย่อย (ค้าปลีก) จำนวนร้อยละ ๓๙ ซื้อสินค้าออนไลน์ผ่านเครื่องคอมพิวเตอร์แบบ Laptop/ Desktop และจำนวนร้อยละ ๓๑ ซื้อสินค้าออนไลน์ผ่านการเชื่อมต่ออินเทอร์เน็ตด้วยโทรศัพท์เคลื่อนที่

สถิติเหล่านี้สอดคล้องกับการวิจัยข้อมูลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (๒๕๖๐ : ๓๗-๓๘) ซึ่งพบว่า ในปีพ.ศ. ๒๕๕๘ ประเทศไทยมีมูลค่าพาณิชย์ทางอิเล็กทรอนิกส์ หรือ E-Commerce ที่นับรวมมูลค่าการประมูลทางอิเล็กทรอนิกส์ (E-Auction) จำนวนทั้งสิ้น ๒,๒๔๕,๑๔๗.๐๒ ล้านบาท เติบโตเพิ่มขึ้นจากปีพ.ศ. ๒๕๕๗ สูงถึงร้อยละ ๑๐.๔๐ ในขณะที่การคาดการณ์มูลค่า E-Commerce ปีพ.ศ. ๒๕๕๙ นั้น สามารถประมาณการได้เป็นจำนวนทั้งสิ้น ๒,๕๒๓,๙๙๔.๔๖ ล้านบาท และจะมีอัตราการเติบโตเพิ่มขึ้นจากปีพ.ศ. ๒๕๕๘ คิดเป็นร้อยละ ๑๒.๔๒ (แผนภาพที่ ๒-๖ ในบทที่ ๒) และพบว่า ผู้ประกอบการในเกือบทุกอุตสาหกรรมนั้นเน้นให้ความสำคัญในการเปิดให้บริการช่องทางการชำระเงินทางออนไลน์ ในอัตราส่วนที่มากกว่าออฟไลน์

(แผนภาพที่ ๒-๘ ในบทที่ ๒) ดังนั้น เมื่อจำนวนของผู้ใช้คอมพิวเตอร์ในการทำธุรกรรมซื้อขายสินค้าและบริการมีแนวโน้มเพิ่มมากขึ้นอย่างต่อเนื่อง โอกาสที่คนร้ายจะฉวยโอกาสจากการที่ผู้ใช้ระบบคอมพิวเตอร์ขาดความรู้ ความเข้าใจ และความระมัดระวังรักษาความปลอดภัยก็ย่อมมีมากขึ้นตามด้วย และหากกลไกในการสร้างความเชื่อมั่นในความมั่นคงปลอดภัยทางไซเบอร์ และการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับผู้กระทำความผิดยังไม่มีประสิทธิภาพ ย่อมจะทำให้ผู้บริโภคขาดความเชื่อมั่นที่จะเข้าทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งจะทำให้เกิดผลกระทบต่อภาพรวมการพัฒนาเศรษฐกิจผ่านพาณิชย์ทางอิเล็กทรอนิกส์ หรือ E-Commerce และผู้ลงทุนใหม่ย่อมขาดความมั่นใจในการสร้างธุรกิจใหม่ผ่านโลกออนไลน์อีกด้วย

สำหรับข้อมูลสถิติภัยคุกคามทางไซเบอร์ (Cyber Threats) แยกตามประเภทของภัยคุกคามที่มีการรายงานผ่านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ในปี พ.ศ. ๒๕๕๗, ๒๕๕๘ และ ๒๕๕๙ ตามลำดับ ตามที่เสนอไว้ในตารางที่ ๒-๑, ๒-๒ และ ๒-๓ ของบทที่ ๒ พบว่าประเภทภัยคุกคามทางไซเบอร์สูงสุด ๓ อันดับแรกที่มีการรายงานไปยังไทยเซิร์ต ได้แก่ อันดับที่ ๑ Malicious Code คือ การฝังโค้ดอันตรายลงใน BIOS ที่สามารถขโมยข้อมูลต่าง ๆ ที่อยู่ในแรม (Ram) ของคอมพิวเตอร์ อันดับที่ ๒ Fraud คือ การฉ้อโกงทางคอมพิวเตอร์ เช่น การนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์เพื่อหลอกลวงเหยื่อให้ส่งมอบทรัพย์สินให้ผู้กระทำความผิดในลักษณะที่เป็นการฉ้อโกงทรัพย์ และอันดับที่ ๓ Intrusion คือ การโจมตีระบบที่มีช่องโหว่เพื่อเข้าควบคุมและสั่งการทำงานในเครื่องคอมพิวเตอร์เหยื่อ ซึ่งเมื่อเปรียบเทียบแนวโน้มจำนวนกรณีที่มีการร้องเรียนเกี่ยวกับภัยคุกคามผ่านไทยเซิร์ตในช่วง ๓ ปีข้างต้น พบว่า มีแนวโน้มของจำนวนการร้องเรียนที่เพิ่มมากขึ้นทุกปี และจากการเปรียบเทียบกับสถิติข้อมูลสถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่านไทยเซิร์ต ในปีพ.ศ. ๒๕๕๔ (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ๒๕๕๙) ซึ่งเป็นข้อมูลย้อนหลังมากที่สุดที่มีการเก็บรวบรวมและเผยแพร่โดยไทยเซิร์ตในขณะนี้ พบว่า มีการเพิ่มขึ้นของภัยคุกคามที่มีการรายงานในช่วงปีพ.ศ. ๒๕๕๗, ๒๕๕๘ และ ๒๕๕๙ จากปีพ.ศ. ๒๕๕๔ อย่างมาก ดังกล่าวสรุปในตารางต่อไปนี้

ตารางที่ ๓-๑ สถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่าน ThaiCERT ปีพ.ศ. ๒๕๕๔ เปรียบเทียบกับปีพ.ศ.๒๕๕๗, ๒๕๕๘ และ ๒๕๕๙

ประเภทภัยคุกคาม / ปีพ.ศ.	๒๕๕๔	๒๕๕๗	๒๕๕๘	๒๕๕๙
Abusive Content	77	8	8	0
Availability	6	8	6	29
Fraud	309	1007	1141	1002
Information Gathering	93	29	0	0
Information Security	0	4	1	20
Intrusion Attempts	94	504	664	706
Intrusions	0	709	1005	1020
Malicious Code	63	1738	1546	1020
Other	4	0	0	0
รวม	646	4007	4071	3797

ที่มา : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), ออนไลน์, ๒๕๕๙

อย่างไรก็ดี สถิติข้อมูลสถิติภัยคุกคามทางไซเบอร์ (Cyber Threats) แยกตามประเภทของภัยคุกคามที่มีการรายงานผ่านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) ข้างต้น ยังคงมีข้อจำกัดด้านความครบถ้วนสมบูรณ์ เนื่องจากสถิติดังกล่าวมีการเก็บรวบรวมจากข้อมูลที่มีผู้ประสบเหตุ (ผู้ได้รับความเสียหาย) รายงานเหตุต่อไทยเซิร์ต จึงอาจเป็นไปได้ว่า จะมีผู้เสียหายจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มิได้รายงานเหตุต่อไทยเซิร์ต โดยอาจจะไม่มีการดำเนินคดีใดๆตามกฎหมายกับผู้กระทำความผิด หรืออาจจะมิได้รายงานเหตุต่อไทยเซิร์ต แต่ได้แจ้งความดำเนินคดีกับผู้กระทำความผิดผ่านหน่วยงานราชการอื่น

ในส่วนของสถิติการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ เมื่อพิจารณาจากรายงานประจำปี ๒๕๕๘ (สำนักงานอัยการสูงสุด, ๒๕๕๙ ค) พบว่า สำนักงานอัยการสูงสุดได้จัดเก็บสถิติข้อมูลคดีอาญาในศาลชั้นต้น โดยแยกตามประเภท เช่น

๑. คดีอาญาที่ปรากฏตัวผู้ต้องหาส่งมาพร้อมสำนวนการสอบสวน
๒. คดีอาญาชั้นฟ้องศาล (คดีที่มีการยื่นฟ้องต่อศาล)
๓. คดีอาญาที่ปรากฏตัวผู้ต้องหาที่ไม่ได้ส่งมา (เว้นแต่คดีเปรียบเทียบ) เช่น คดีที่ผู้ต้องหาหลบหนียังไม่ได้ตัวมา หรือคดีที่พนักงานสอบสวนมีความเห็นควรสั่งไม่ฟ้อง ผู้ต้องหา
๔. คดีอาญาที่ไม่ปรากฏผู้กระทำผิด

ทั้งนี้ สถิติคดีอาญาทั้ง ๔ ประเภทดังกล่าว ได้กำหนดฐานความผิดเพื่อประโยชน์ในการเก็บข้อมูลสถิติคดีไว้รวม ๖๓ ลำดับ ดังนี้

ตารางที่ ๓-๒ ลำดับสารบบฐานความผิดในการเก็บข้อมูลสถิติคดีอาญาของสำนักงานอัยการสูงสุด

ลำดับที่ ในสารบบคดี	ประเภทคดี แยกตามฐานความผิดตามบทบัญญัติกฎหมาย
๑ – ๔๑	ความผิดตามประมวลกฎหมายอาญา ตั้งแต่มาตรา ๑๐๗ ถึง มาตรา ๓๙๘
๔๒	ความผิดตามประมวลรัษฎากร
๔๓	ความผิดตามพระราชบัญญัติศุลกากร
๔๔	ความผิดตามพระราชบัญญัติสุรา
๔๕	ความผิดเกี่ยวกับกฎหมายภาษีอื่นๆ
๔๖	ความผิดตามพระราชบัญญัติยา
๔๗	ความผิดตามพระราชบัญญัติวิชาชีพเวชกรรม, ควบคุมการประกอบโรคศิลปะ
๔๘	ความผิดตามพระราชบัญญัติอาวุธปืนฯ (ที่ออกใบอนุญาตให้ได้)
๔๙	ความผิดตามพระราชบัญญัติอาวุธปืนฯ (ที่ออกใบอนุญาตให้ไม่ได้)
๕๐	ความผิดตามพระราชบัญญัติการพนัน (การพนันสลากกินรวบ)
๕๑	ความผิดตามพระราชบัญญัติการพนัน (การพนันอื่นๆ)
๕๒	ความผิดตามพระราชบัญญัติรับราชการทหาร
๕๓	ความผิดตามพระราชบัญญัติป่าไม้, ป่าสงวนแห่งชาติ, อุทยานแห่งชาติ
๕๔	ความผิดตามพระราชบัญญัติการประมง
๕๕	ความผิดตามพระราชบัญญัติคนเข้าเมือง
๕๖	ความผิดตามพระราชบัญญัติยาเสพติดให้โทษ
๕๗	ความผิดตามพระราชบัญญัติวัตถุที่ออกฤทธิ์ต่อจิตและประสาท
๕๘	ความผิดตามพระราชบัญญัติแร่
๕๙	ความผิดตามพระราชบัญญัติปราบปรามการค้าประเวณี
๖๐	ความผิดตามพระราชบัญญัติว่าด้วยความผิดอันเกิดจากการใช้เช็ค
๖๑	ความผิดตามพระราชบัญญัติโรงงาน
๖๒	ความผิดตามพระราชบัญญัติว่าด้วยราคาสินค้าและบริการ
๖๓	**ความผิดอื่นๆ**

ที่มา : สำนักงานอัยการสูงสุด, ๒๕๕๙ ค : ๙๒-๙๕

สำหรับวิธีการบันทึกข้อมูลสถิติในสารบบคดีของสำนักงานอัยการสูงสุดสำหรับคดีที่มีความเกี่ยวพันกับฐานความผิดหลายอย่าง เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดจะเลือกบันทึกรายการคดีโดยยึดฐานความผิดบทที่มีอัตราโทษสูงที่สุดเพียงรายการเดียวต่อ ๑ สำนวนคดี ตัวอย่างเช่น สำนวนคดีกรณีคนร้ายฉ้อโกงขายสินค้าประเภทรถจักรยานยนต์บนเว็บไซต์สื่อกลางซื้อขายสินค้าออนไลน์ที่ประชาชนทั่วไปสามารถเข้าดูและเห็น

ประกาศขายสินค้าได้ โดยผู้ต้องหาใช้อุบายทำปลอมขึ้นซึ่งสำเนาบัตรประชาชนและสำเนารายการจดทะเบียนรถยนต์ของผู้อื่น โดยใส่ชื่อ-สกุลของผู้ต้องหาแทนชื่อ-สกุลของผู้เป็นเจ้าของเอกสารที่แท้จริง เพื่อทำให้ประกาศขายรถจักรยานยนต์บนสื่อออนไลน์ดูน่าเชื่อถือ และทำให้ผู้พบเห็นประกาศขายรถจักรยานยนต์หลงเชื่อว่าผู้ต้องหาเป็นเจ้าของกรรมสิทธิ์ในรถจักรยานยนต์ และเข้าทำการซื้อขายโอนเงินค่าสินค้าให้แก่ผู้ต้องหาผ่านบัญชีธนาคารตามที่ผู้ต้องหากำหนด ทั้งที่ความจริงแล้วผู้ต้องหามิใช่ผู้ถือกรรมสิทธิ์ในรถจักรยานยนต์ที่ประกาศขายและไม่สามารถส่งมอบรถจักรยานยนต์ที่ประกาศขายให้แก่ผู้ซื้อ ครั้นเมื่อผู้ต้องหาได้รับเงินค่าสินค้าจากผู้เสียหายแล้ว ก็ไม่ยอมส่งมอบสินค้าหรือคืนเงินค่าสินค้า เมื่อผู้เสียหายทวงถามสินค้า ผู้ต้องหาก็ปิดการติดต่อกับผู้เสียหายทุกทาง การกระทำของผู้ต้องหาถือเป็นความผิดฐานปลอมเอกสารสิทธิอันเป็นเอกสารราชการและฉ้อโกงประชาชนตามประมวลกฎหมายอาญาและความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) กรณีเช่นว่านี้ เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดจะบันทึกสถิติคดีนี้เพียงในช่องรายการ “ประเภทคดี ๑๖ ความผิดเกี่ยวกับเอกสาร มาตรา ๒๖๔ – ๒๖๙” เนื่องจากความผิดที่มีอัตราโทษสูงสุดในสำนวนคดีนี้คือความผิดฐานปลอมเอกสารสิทธิอันเป็นเอกสารราชการตามประมวลกฎหมายอาญา จึงทำให้การลงบันทึกสถิติคดีอาญากรณีข้างต้นไม่ได้สะท้อนเห็นถึงข้อมูลสถิติคดีอาชญากรรมคอมพิวเตอร์ ประเภทคอมพิวเตอร์ถูกใช้เป็นเครื่องมือประกอบอาชญากรรม (Computer as Tools) โดยเฉพาะเจาะจง

ตัวอย่างอีกกรณี ได้แก่ การกระทำความผิดโดยมีคอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets) เช่น การฝัง Malicious Code ในระบบคอมพิวเตอร์ของผู้อื่นหรือการโจมตีระบบที่มีช่องโหว่เพื่อเข้าควบคุมและสั่งการทำงานในเครื่องคอมพิวเตอร์เหยื่อ (Intrusion) อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (และที่แก้ไขเพิ่มเติม) ซึ่งไม่ตรงกับรายการประเภทคดีลำดับที่ ๑ – ๖๒ เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดก็จะบันทึกสถิติคดีในช่องรายการ “ประเภทคดี ๖๓ ความผิดอื่นๆ” ซึ่งการลงบันทึกสถิติคดีอาญาเช่นว่านี้ก็ไม่ได้สะท้อนสถิติคดีอาชญากรรมคอมพิวเตอร์อย่างเฉพาะเจาะจงเช่นเดียวกัน เนื่องจากรายการ “ประเภทคดี ๖๓ ความผิดอื่นๆ” นอกจากหมายรวมถึงความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) แล้ว ยังรวมไปถึงความผิดตามพระราชบัญญัติอื่นๆ ซึ่งมีอยู่เป็นจำนวนมากในปัจจุบัน

ดังนั้น เพื่อสะท้อนปริมาณงานด้านคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการโดยเฉพาะเจาะจง ผู้วิจัยจึงใช้วิธีการสัมภาษณ์ผู้ทรงคุณวุฒิด้านงานคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ เพื่อทราบมุมมองของพนักงานอัยการผู้ปฏิบัติงานคดีทั้งในกรุงเทพมหานครและต่างจังหวัดที่มีต่อแนวโน้มปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ภายหลังการดำเนินนโยบายประเทศไทย ๔.๐ โดยผู้ทรงคุณวุฒิด้านงานคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ที่ตอบแบบสัมภาษณ์เชิงลึกทุกท่านมีความคิดเห็นเป็นไปในทำนองเดียวกันว่า ภายหลังจากการดำเนินนโยบายประเทศไทย ๔.๐ ปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดมีแนวโน้มเพิ่มมากขึ้น อาทิเช่น

ปกรณ์ ธรรมโรจน์ (สัมภาษณ์, ๘ มีนาคม ๒๕๖๐) เห็นว่า การปรับเปลี่ยนโครงสร้างเศรษฐกิจไปสู่ ระบบ “Value – Based Economy” หรือระบบเศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรมที่เน้นเทคโนโลยี ความคิดสร้างสรรค์ และการบริการ ย่อมมีผลให้การใช้เทคโนโลยีแพร่หลายมากขึ้น การประกอบอาชญากรรมโดยใช้เทคโนโลยีเป็นเครื่องมือ หรือคดีอาชญากรรมคอมพิวเตอร์ย่อมมีแนวโน้มเพิ่มมากขึ้นด้วย

เช่นเดียวกับ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) ซึ่งเห็นว่า นโยบายประเทศไทย ๔.๐ น่าจะมีผลกระทบทำให้จำนวนปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดเพิ่มมากขึ้น เนื่องจากเมื่อมีการส่งเสริมการใช้ระบบคอมพิวเตอร์ อินเทอร์เน็ต และระบบสื่อสารดิจิทัล ในการทำธุรกิจของภาคเอกชน ปริมาณการทำธุรกรรมด้านการค้าและบริการทางอิเล็กทรอนิกส์ (E-Commerce) ธุรกรรมการชำระราคา (E-Payment) และธุรกรรมการเงินทางอิเล็กทรอนิกส์ (E-Banking) รวมถึงการใช้งานระบบคอมพิวเตอร์ในสื่อสังคมออนไลน์ (Social Media) ย่อมมีมากขึ้น ดังนั้น ความเสี่ยงต่อการที่มิจฉาชีพจะแสวงหาผลประโยชน์โดยมิชอบย่อมอาจมีมากขึ้นด้วย

ในขณะที่ โชติกา ศรีนรเศรษฐ์ (สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐) คงยศ คุณจักร์ (สัมภาษณ์, ๑๒ มีนาคม ๒๕๖๐) และดวงพร เตชะกำธร (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) เห็นว่า นโยบายประเทศไทย ๔.๐ น่าจะมีผลกระทบทำให้ปริมาณคดีมากขึ้น เนื่องจากทุกภาคส่วนต่างถูกผลักดันให้ใช้เทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ตในการติดต่อสื่อสาร ทำให้ระบบคอมพิวเตอร์กลายเป็นองค์ประกอบหลักในการติดต่อสื่อสารระหว่างกัน ซึ่งจะเป็นช่องทางให้อาชญากรใช้เป็นเครื่องมือในการกระทำความผิดได้ง่ายขึ้น และแม้ว่าจะไม่มีนโยบายประเทศไทย ๔.๐ สมรัตน์ สุขคะ (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) ก็เชื่อว่าปริมาณคดีอาชญากรรมคอมพิวเตอร์จะสูงขึ้นกว่าในอดีต เนื่องจากประชาชนใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์ในชีวิตประจำวันและในการประกอบธุรกิจเพิ่มมากขึ้นกว่าในอดีต

จากข้อมูลสถิติที่เกี่ยวข้องและผลการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิจึงบ่งชี้ได้ว่า ปริมาณงานคดีอาชญากรรมคอมพิวเตอร์มีแนวโน้มเพิ่มสูงขึ้น อันเนื่องมาจากการใช้งานระบบคอมพิวเตอร์ในสื่อสังคมออนไลน์ที่มีปริมาณเพิ่มมากขึ้น อันเป็นปัจจัยด้านเหยื่อและด้านโอกาสในการเกิดคดีอาชญากรรมคอมพิวเตอร์มากขึ้น ตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory)

ลักษณะและความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (ออนไลน์, ๒๕๖๐) ได้รวบรวมการวิเคราะห์แนวโน้มของภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ในปีพ.ศ. ๒๕๕๗ ของบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ชื่อดัง เช่น FireEye, Kaspersky, Microsoft, Sophos, Symantec, Trend Micro และ InfoSec Institute นำเสนอโดยสรุปว่า มัลแวร์ (Malware) ที่ถูกใช้ในการก่ออาชญากรรมคอมพิวเตอร์จะมีความซับซ้อนมากขึ้น โดยจะมีความสามารถในการหลบหลีกการตรวจจับการติดต่อสื่อสารกับผู้ไม่หวังดีได้แยบยลขึ้น หรือมีความสามารถในการลบระบบปฏิบัติการเพื่อทำลายร่องรอยหลังปฏิบัติการสำเร็จ เช่น การลบตัวระบบปฏิบัติการวินโดวส์ (Windows) ทิ้งทั้งหมด ทำให้ไม่สามารถใช้งานคอมพิวเตอร์

ได้ นอกจากนี้ บริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ดังกล่าวเห็นพ้องว่าภัยคุกคามที่เกี่ยวข้องกับโทรศัพท์เคลื่อนที่มีแนวโน้มเพิ่มมากขึ้นตามจำนวนผู้ใช้งานโทรศัพท์เคลื่อนที่ที่เพิ่มขึ้น ด้วยการขโมย SMS ในโทรศัพท์เคลื่อนที่ที่ใช้การยืนยันตัวตน ๒ ชั้น (2-Step Verification) เช่น การขโมยรหัส OTP ที่เป็น SMS สำหรับใช้ลงทะเบียน (Log In) บัญชีธนาคารออนไลน์จะพบเห็นได้มากขึ้น Symantec ได้ยกตัวอย่างแอพพลิเคชั่นที่เพิ่ม Like ของโพสต์ในบัญชี Instagram ของผู้ใช้ โดยผู้ใช้ต้องระบุชื่อบัญชีผู้ใช้และรหัสผ่านของบัญชี Instagram ให้กับแอพพลิเคชั่น ซึ่งมีคนมากกว่าแสนคนตกเป็นเหยื่อแอพพลิเคชั่นหลอกลวงทางโทรศัพท์เคลื่อนที่ดังกล่าว ในขณะที่ Sophos ได้คาดการณ์ว่าการโจมตีระบบคลาวด์จะมีแนวโน้มเพิ่มมากขึ้น โดยอาจเป็นการโจมตีที่พุ่งเป้าหมายไปยังอุปกรณ์คอมพิวเตอร์ส่วนบุคคลต่างๆ เช่น โทรศัพท์เคลื่อนที่ของผู้ใช้ เพื่อเป็นช่องทางไปสู่การเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลขององค์กรบนระบบคลาวด์ (Cloud) หรืออาจเกิดจากการทำงานของมัลแวร์ประเภท Ransomware ที่มีเป้าหมายการโจมตีไปยังข้อมูลบนเครื่องคอมพิวเตอร์และข้อมูลบนระบบคลาวด์ที่สามารถเข้าถึงได้จากเครื่องคอมพิวเตอร์ของเหยื่อด้วย

นอกจากนี้ จากการที่ “บิทคอยน์” (Bitcoin) หรือสกุลเงินดิจิทัลซึ่งอยู่ภายใต้การดูแลของระบบเครือข่ายคอมพิวเตอร์เปรียบเสมือนธนบัตร โดยธนาคารบนระบบเครือข่ายคอมพิวเตอร์ที่บันทึกรายการธุรกรรมเกี่ยวกับ Bitcoin ผ่าน Bitcoin Mining Software บนคอมพิวเตอร์จะอยู่ในระบบที่ชื่อว่า “บล็อคเชน” (Block Chain) เริ่มมีการใช้งานอย่างแพร่หลายในปัจจุบัน บริษัท Kaspersky และ InfoSec Institute ได้ให้ความเห็นเป็นไปในทางเดียวกันว่า การเผยแพร่มัลแวร์ที่มีหน้าที่ในการคำนวณสำหรับการทำ Bitcoin Mining บนเครื่องคอมพิวเตอร์ของผู้ใช้ การขโมย Bitcoin โดยตรงไม่ว่าจะเป็นการเผยแพร่มัลแวร์ที่ทำการขโมย Bitcoin โดยเฉพาะบนเครื่องคอมพิวเตอร์ของผู้ใช้ หรือแม้กระทั่งการโจมตีผู้ให้บริการแลกเปลี่ยน Bitcoin กับสกุลเงินอื่นๆ จะพบเห็นได้มากขึ้นแทน เนื่องจากผู้ไม่หวังดีสามารถนำ Bitcoin ที่ขโมยได้ไปแลกเปลี่ยนเป็นเงินสกุลอื่นได้ทันที ในขณะที่การสืบหาตัวบุคคลที่แลกนั้นก็ยังเป็นเรื่องที่ทำได้ยาก จากบทวิเคราะห์แนวโน้มของภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ข้างต้นสะท้อนให้เห็นถึงพัฒนาการความซับซ้อนของการก่อคดีอาชญากรรมคอมพิวเตอร์เพื่อให้ยากต่อการติดตามตัวผู้กระทำความผิด

ตัวอย่างของภัยคุกคามที่เกี่ยวข้องกับคอมพิวเตอร์กับประเทศไทยที่สำคัญในปี ๒๕๕๙ ที่ผ่านมา เริ่มต้นเมื่อวันที่ ๑๓ มกราคม ๒๕๕๙ มีการนำเสนอข่าวในโลกออนไลน์ (Anonymous แฮกเว็บศาลไทยล่ม 296 เว็บไซต์ ค้านคดีเกาะเต่า, ออนไลน์, ๒๕๕๙) ว่า “Anonymous” ซึ่งเป็นกลุ่มแฮกเกอร์ชื่อดังระดับโลกได้โจมตีเว็บไซต์ทางการของไทยเป็นระลอกที่ ๒ เหตุไม่พอใจคำตัดสินของศาลชั้นต้นที่พิพากษาให้ประหารชีวิตจำเลยชาวพม่าทั้งสองราย ในคดีฆาตกรรมนางสาวฮันนาห์ วิเทอริดจ์ และนายเดวิด มิลเลอร์ นักท่องเที่ยวชาวอังกฤษ ที่เกาะเต่า จังหวัดสุราษฎร์ธานี เมื่อช่วงเดือนกันยายน ๒๕๕๗ โดยพบว่าเว็บไซต์ทางการของไทยซึ่งมีส่วนเกี่ยวข้องกับเว็บไซต์ศาลยุติธรรมทั้งหมด ๓๐๕ แห่ง ถูกกลุ่ม Anonymous โจมตี ส่งผลให้ไม่สามารถเข้าใช้งานเว็บไซต์ได้ตามปกติ กล่าวคือ ในช่วงเช้าของวันที่ ๑๓ มกราคม ๒๕๕๙ กลุ่ม Anonymous ได้โพสต์รูปภาพและข้อความลงบน Facebook โดยระบุว่า “Anonymous กำลังเตรียมแฮกเว็บไซต์ทางการของรัฐบาลทุกเว็บที่มีส่วนเกี่ยวข้องกับการพิพากษาอันไม่เป็นธรรมในคดีเกาะเต่า เราพบว่าศาลยุติธรรมของไทยนั้นไม่ให้

ความเป็นธรรมกับชาวต่างด้าว ด้วยการจับแพะรับบาป และใช้กฎหมายของประเทศตนในการลงโทษ ทั้งหมดนี้ก็เพื่อสร้างภาพและกอบโกยผลประโยชน์ทางการเมือง” นอกจากนี้ กลุ่ม Anonymous ยังโพสต์ภาพคณะทำงานของศาลยุติธรรมของศาลจังหวัดเกาะสมุย พร้อมคาดตัวอักษรสีแดงตัวใหญ่ว่า “มีความผิด” พร้อมบรรยายว่า “เราขอตัดสินให้พวกคุณมีความผิด และความถูกต้องกำลังจะถูกเปิดเผยเร็วๆ นี้”

และนับจากที่รัฐบาลได้ประกาศใช้นโยบายประเทศไทย ๔.๐ ในช่วงประมาณกลางปีพ.ศ. ๒๕๕๙ ที่ผ่านมา รัฐบาลได้ส่งเสริมให้หน่วยงานราชการของรัฐรวมถึงภาคเอกชนนำเทคโนโลยีสารสนเทศทางดิจิทัลคอมพิวเตอร์ไปใช้ในการขับเคลื่อนเศรษฐกิจของประเทศรวมทั้งใช้เทคโนโลยีสารสนเทศทางดิจิทัลคอมพิวเตอร์ไปพัฒนาในการทำงานประจำของตน จากนั้น ช่วงประมาณปลายปี พ.ศ. ๒๕๕๙ ได้มีการพิจารณาประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ เพื่อปรับปรุงแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ให้ทันต่อสภาพการเปลี่ยนแปลงของสังคมในยุคปัจจุบัน เนื่องจากบทบัญญัติดังกล่าวมีผลใช้บังคับมาแล้วเป็นเวลานานถึง ๑๐ ปีแล้ว อย่างไรก็ดี เกิดกระแสวิพากษ์วิจารณ์จากกลุ่มบุคคลที่ไม่เห็นด้วยกับสาระบางประการที่มีการแก้ไขตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ โดยตามข่าวที่มีการนำเสนอในโลกออนไลน์ระบุว่ากลุ่มบุคคลที่มีบทบาทหลักในการต่อต้านการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ ใช้ชื่อว่า “กลุ่มพลเมืองต่อต้าน Single Gateway” โดยภายหลังจากที่โฆษกประจำสำนักนายกรัฐมนตรีได้ออกมาเตือนผู้ร่วมชุมนุมต่อต้านพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ ที่บริเวณหน้าหอศิลปะวัฒนธรรมแห่งกรุงเทพมหานครว่าการชุมนุมดังกล่าวอาจเข้าข่ายผิดกฎหมายเมื่อวันที่ ๑๘ ธันวาคม ๒๕๕๙ ต่อมาในวันที่ ๑๙ ธันวาคม ๒๕๕๙ ได้มีการเสนอข่าวว่า เว็บไซต์ของกระทรวงกลาโหมถูกแฮกในช่วงเช้า ตามมาด้วยการแฮกเว็บไซต์รัฐบาลอีก ๔ แห่ง ได้แก่ เว็บไซต์ทำเนียบรัฐบาล (www.thaigov.go.th) เว็บไซต์สำนักนายกรัฐมนตรี (www.opm.go.th) เว็บไซต์ราชกิจจานุเบกษา www.ratchakitcha.soc.go.th) และเว็บไซต์สำนักงานสภาความมั่นคงแห่งชาติ (www.nsc.go.th) และต่อเนื่องด้วยปฏิบัติการแฮกโจมตีเว็บไซต์หน่วยงานภาครัฐโดยมีเป้าหมายในการโจมตีเว็บไซต์ระบบบริหารการคลังภาครัฐและเว็บไซต์ระบบการจัดซื้อจัดจ้างภาครัฐ โดยเมื่อวันที่ ๒๐ ธันวาคม ๒๕๕๙ กลุ่มพลเมืองต่อต้าน Single Gateway ได้โพสต์ข้อความบน Facebook เผยแพร่คำแถลงการณ์ มีข้อความว่า

> ประกาศขยายเวลาปฏิบัติการเป็น จนถึง ๒๔.๐๐ น. ... ระบบการบริหารการคลังภาครัฐ (หมายถึงระบบการเบิกจ่ายเงินทั้งหมด) ทั้งประเทศทำงานไม่ได้ และรวมถึงการยื่นซองประกวดราคาทั่วประเทศทำงานไม่ได้ นี่คือการส่งสัญญาณเพียงครั้งแรกแบบแรงๆว่านี่คือยกระดับครั้งแรก แต่ถ้าพวกเราทำแค่ ๑ สัปดาห์ ระบบการบริหารภาครัฐจะจอดสนิท และถ้าทำต่อเนื่อง ๒ สัปดาห์เงินเดือนข้าราชการจะไม่ออกไม่สามารถเบิกจ่ายได้เลย พวกเราอยากจะรู้ว่ารัฐบาลนี้จะอยู่ได้อย่างไร รีบดำเนินการอย่างที่พวกเราร้องขอซะ ก่อนที่รัฐบาลนี้จะอยู่ไม่ได้ไปด้วย

(แฮกเกอร์เปิดฉากปฏิบัติการถล่มเว็บไซต์ระบบการบริหารการคลังภาครัฐ, ออนไลน์, ๒๕๕๙) จากนั้นเมื่อช่วงค่ำของวันที่ ๒๒ ธันวาคม ๒๕๕๙ กลุ่มพลเมืองต่อต้าน Single Gateway ได้เปิดเผยข้อมูลของตำรวจทางหลวง เช่น เอกสารทางการเงิน เลขบัญชีธนาคาร เลขประจำตัว เลขประจำตำแหน่ง ชื่อ

ชั้นยศ รวมถึง เงินเพิ่มพิเศษ เงินค่าเล่าเรียน เงินสวัสดิการต่างๆ เงินค่ารักษาพยาบาล ของตำรวจทางหลวงทุกกองบังคับการทั่วประเทศมาเผยแพร่ผ่าน Facebook โดยในช่วงเวลาเดียวกันเว็บไซต์หน่วยงานของรัฐบาลหลายแห่งล่มไม่สามารถใช้งานได้ตามปกติโดยเป้าหมายส่วนใหญ่เป็นเว็บไซต์หน่วยงานของกองทัพไทย เช่น ระบบการสื่อสารกองทัพภาคที่ ๒ หรือเว็บไซต์ของกองทัพเรือ (แฮกเกอร์ลุยแฮกข้อมูลกองทัพ พร้อมประกาศเผยข้อมูลงบประมาณกองทัพบก คืนนี้, ออนไลน์, ๒๕๕๙)

จากปรากฏการณ์ที่กล่าวมาข้างต้น ดร.ศักดิ์ เสกขุนทด ผู้อำนวยการสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สรอ. (แฮกเว็บประท้วง พ.ร.บ.คอมพ์ สัญญาเตือนติดอาวุธไอทีภาครัฐ, ออนไลน์, ๒๕๕๙) ได้กล่าวว่า สถานการณ์ที่เกิดขึ้น แบ่งได้เป็น ๒ กรณี คือ มีการเข้าไปแฮกระบบของเว็บไซต์โดยตรง กับเป็นการโจมตีด้วยการระดมคนกด “F5” เพื่อทำให้ระบบต้องทำงานหนักจนล่ม และใช้งานไม่ได้ ซึ่งการรับมือของแต่ละหน่วยงานทำได้มากน้อยแค่ไหนขึ้นกับความพร้อมของแต่ละแห่ง ซึ่งต้องยอมรับว่าเว็บไซต์หน่วยงานของรัฐหากนับไปถึงระดับหน่วยงานท้องถิ่น จะมี ๓,๐๐๐-๔,๐๐๐ เว็บไซต์ รวมสถาบันการศึกษาภาครัฐด้วยจะมีมากกว่า ๑๐,๐๐๐ แห่ง พบว่ายังขาดแคลนผู้ที่มีความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

การเคลื่อนไหวของกลุ่ม Anonymous หรือกลุ่มพลเมืองต่อต้าน Single Gateway สะท้อนให้เห็นถึงความร้ายแรงและความรวดเร็วโดยการก่อสงครามไซเบอร์ หรือ Cyber War โดยผู้กระทำความผิดไม่จำต้องมีกองกำลังหรืออาวุธยุทโธปกรณ์ใดๆ แต่ผู้ก่ออาชญากรรมคอมพิวเตอร์อาจเป็นบุคคลแค่คนเดียวหรือหลายคน ซึ่งสามารถกระทำความผิดจากที่หนึ่งที่ใดในโลกเพียงแค่สามารถเชื่อมต่อกับระบบคอมพิวเตอร์ได้เท่านั้น โดยการสืบหาร่องรอยเพื่อระบุตัวผู้กระทำความผิดทำได้ไม่ง่าย การดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงถือได้ว่ามีความซับซ้อนและยุ่งยากเป็นอย่างมาก เพราะการสืบหาร่องรอยของผู้กระทำความผิดจะต้องดำเนินการโดยผู้ที่มีความรู้ความเข้าใจเกี่ยวกับการทำงานของระบบคอมพิวเตอร์และระบบความปลอดภัยด้านคอมพิวเตอร์ (Computer Security) เป็นอย่างดี

ปกรณ์ ธรรมโรจน์ (สัมภาษณ์, ๘ มีนาคม ๒๕๖๐) และโชติกา ศรีนรเศรษฐ์ (สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐) มีความเห็นสอดคล้องกันว่า การดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะอย่างยิ่งภายหลังจากการดำเนินนโยบายประเทศไทย ๔.๐ จะมีความแตกต่างกับคดีอาญาทั่วไปในหลายแง่มุม เช่น พยานหลักฐานมีความซับซ้อน ง่ายแก่การใช้งานแต่ยากในการรวบรวม เข้าถึงข้อมูล และเข้าใจ อย่างแท้จริง ต้องใช้ผู้เชี่ยวชาญที่มีความรู้เฉพาะด้านการรวบรวมพยานหลักฐานเพื่อระบุตัวผู้กระทำความผิด การดำเนินคดีอาชญากรรมคอมพิวเตอร์กับผู้กระทำผิดยังมีความยุ่งยากซับซ้อนและมีอุปสรรคในหลายด้าน เช่น การขอความร่วมมือระหว่างประเทศในการรวบรวมพยานหลักฐาน การขาดแคลนผู้เชี่ยวชาญที่มีความเข้าใจ ทั้งการจัดการพยานหลักฐานคอมพิวเตอร์ก่อนที่พยานหลักฐานจะถูกทำลายก่อนที่จะเก็บรวบรวมได้ และความเข้าใจในการอธิบายข้อเท็จจริงเพื่อใช้พยานหลักฐานในการดำเนินคดีได้อย่างมีประสิทธิภาพสูงสุด โดยในประเด็นพยานหลักฐานทางอิเล็กทรอนิกส์ คงยศ คุณจักร์ (สัมภาษณ์, ๑๒ มีนาคม ๒๕๖๐) ได้กล่าวเพิ่มเติมว่า พยานหลักฐานที่เกี่ยวข้องจะมีข้อมูลอิเล็กทรอนิกส์เข้ามาเกี่ยวข้องจำนวนมากอันเป็นพยานหลักฐานที่มิใช่ตัวทรัพย์สินที่จับต้องได้เหมือนอย่างทรัพย์สินโดยทั่วไป จึงนำมาซึ่งความยากลำบากทั้งการได้มาซึ่งพยานหลักฐานและการนำไปสู่ตัวผู้กระทำความผิด อันแตกต่างจากความผิดคดีอาญาอื่นๆ

ส่วน เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) ได้อธิบายเพิ่มเติมถึงลักษณะการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความแตกต่างจากการดำเนินคดีอาญาทั่วไปในหลายด้าน เนื่องจากพยานหลักฐานสำคัญที่ใช้ในการพิสูจน์การกระทำความผิดของผู้ต้องหามักเป็นพยานหลักฐานทางดิจิทัล ผู้กระทำความผิดสามารถลงมือกระทำความผิดจากที่ใดก็ได้ เพียงแค่มีการเชื่อมต่ออุปกรณ์เข้าสู่ระบบอินเทอร์เน็ต เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (PC), เครื่องคอมพิวเตอร์ Laptop, Tablet, หรือโทรศัพท์ Smart Phone ผู้กระทำความผิดอาจมีเพียงบุคคลเดียว หรือหลายคนโดยแบ่งหน้าที่กัน ซึ่งคดีส่วนใหญ่มักไม่มีประจักษ์พยานเห็นเหตุการณ์ แตกต่างจากคดีอาญาทั่วไปซึ่งมักมีพยานบุคคลผู้พบเห็นเหตุการณ์ทั้งหมดหรือส่วนใดส่วนหนึ่ง นอกจากนั้น การดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการต้องอาศัยความรู้ความเข้าใจเกี่ยวกับการทำงานของคอมพิวเตอร์ รวมไปถึงลักษณะและความเชื่อมโยงของพยานหลักฐานทางดิจิทัลในการพิสูจน์การกระทำความผิดของผู้ต้องหา/จำเลย เพื่อให้ศาลรับฟังให้น้ำหนักกับพยานหลักฐานดิจิทัลในการพิสูจน์ว่าผู้ต้องหาเป็นผู้กระทำความผิดจริง การดำเนินคดีอาชญากรรมคอมพิวเตอร์จึงมีความยุ่งยากซับซ้อนมากกว่าคดีอาญาทั่วไปเพราะผู้กระทำความผิดมักใช้ความซับซ้อนของระบบคอมพิวเตอร์ปกปิดตัวตนของผู้กระทำความผิด การพิสูจน์ตัวบุคคลผู้กระทำความผิดจึงต้องมีการเชื่อมโยงหลายชั้น และแม้บางครั้งเมื่อไม่ปรากฏพยานหลักฐานโดยตรงที่ยืนยันตัวบุคคลผู้กระทำความผิด ก็จำต้องอาศัยพยานแวดล้อมอย่างอื่น เช่น พฤติกรรมที่เป็นเอกลักษณ์ในการกระทำความผิด (รูปแบบคำพูด กลุ่มบุคคลที่เกี่ยวข้อง หรือลักษณะการกระทำความผิด) รวมถึง เส้นทางการเงินที่ผู้กระทำความผิดได้รับ (บัญชีรับโอนเงินจากเหยื่อ) เพื่อใช้เพิ่มน้ำหนักในการพิสูจน์การกระทำความผิดของผู้ต้องหา

แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด

เมื่อพิจารณาแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙-๒๕๖๒ และแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปี (Action Plan) ในส่วนของยุทธศาสตร์ด้านการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ดังที่กล่าวไว้ในบทที่ ๒ (สำนักงานอัยการสูงสุด, ๒๕๕๙ ข : ๒๑-๒๒) พบว่า แผนยุทธศาสตร์และแผนปฏิบัติราชการดังกล่าวไม่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของผู้ปฏิบัติงานโดยตรง เนื่องจากมิได้มีการกำหนดแนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์สำหรับผู้ปฏิบัติงาน แต่แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปี (Action Plan) ที่ใช้บังคับในปัจจุบัน มีลักษณะเป็นยุทธศาสตร์ในเชิงเกี่ยวพันกับการจัดสรรและการบริหารเงินงบประมาณของสำนักงานคดีภายในสำนักงานอัยการสูงสุด โดยโครงการหรือกิจกรรมที่ได้รับการจัดสรรงบประมาณที่ระบุไว้ในเอกสารดังกล่าวยังมิได้มีลักษณะระบุรายละเอียดที่ชัดเจนของโครงการในระดับที่สะท้อนให้เห็นถึงทิศทางในการพัฒนางานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด

การดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน พนักงานอัยการต้องปฏิบัติให้เป็นไปตามบทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา และระเบียบสำนักงานอัยการสูงสุดว่าด้วย

การดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) โดยในส่วนของความรู้เกี่ยวกับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์นั้น ปัจจุบันมีคู่มือพนักงานอัยการสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ เผยแพร่โดยสถาบันพัฒนาข้าราชการฝ่ายอัยการเมื่อปี ๒๕๕๔ ใช้เป็นแนวทางในการทำความเข้าใจเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์เบื้องต้น แต่คู่มือดังกล่าวมีการเผยแพร่มาเป็นเวลานานแล้วและยังไม่มีการแก้ไขปรับปรุงเพิ่มเติม

การดำเนินคดีอาชญากรรมคอมพิวเตอร์จัดเป็นการดำเนินคดีอาญาประเภทหนึ่ง ซึ่งเริ่มต้นเมื่อพนักงานอัยการได้รับสำนวนการสอบสวนคดีอาญาพร้อมความเห็นทางคดีจากพนักงานสอบสวน จากนั้น พนักงานอัยการจะพิจารณาพยานหลักฐานในสำนวนการสอบสวนและมีคำสั่งทางคดีโดยการปฏิบัติหน้าที่ของพนักงานอัยการดังกล่าวมีระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) หมวดที่ ๓ บัญญัติให้แนวทางไว้ กล่าวคือ พนักงานอัยการต้องพิจารณาข้อเท็จจริงและพยานหลักฐานในสำนวนซึ่งพิสูจน์ความผิดหรือความบริสุทธิ์ของผู้ต้องหา แนวทางการดำเนินคดีจากพยานหลักฐานและข้อกฎหมายว่าจะทำให้ศาลลงโทษผู้ต้องหาได้หรือไม่ ทั้งนี้ ตามข้อ ๖๙ ของระเบียบดังกล่าว ได้บัญญัติให้พนักงานอัยการพิจารณาพยานหลักฐานในคดีให้ได้ความแน่ชัดว่าผู้ต้องหาได้กระทำความผิดหรือไม่ก่อนจะมีความเห็นและคำสั่ง หากยังไม่แน่ชัดก็ให้สั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมหรือสั่งให้ส่งพยานมาเพื่อซักถามตามรูปคดีก็ได้ จากนั้น เมื่อพนักงานอัยการเห็นว่าข้อเท็จจริงในคดีสิ้นกระแสความและคดีมีพยานหลักฐานเพียงพอในการทำความเห็นและคำสั่งแล้ว โดยทั่วไปพนักงานอัยการจะมีคำสั่งทางคดีอย่างหนึ่งอย่างใดใน ๓ ลักษณะ (สำนักงานอัยการสูงสุด, ๒๕๕๕ : ๓๘-๔๒) ดังต่อไปนี้

๑. มีคำสั่งฟ้อง

เมื่อพนักงานอัยการพิจารณาแล้วเห็นว่าข้อเท็จจริงจากการสอบสวนในคดีดังกล่าวมีพยานหลักฐานที่ชัดเจนพอเชื่อได้ว่าผู้ต้องหาเป็นผู้กระทำ การกระทำนั้นเป็นความผิด และไม่เข้ากรณีที่สิทธิฟ้องคดีอาญาระงับ โดยทั่วไปพนักงานอัยการจะสั่งฟ้องผู้ต้องหาตามบทกฎหมายและฐานความผิดที่เกี่ยวข้อง อันเป็นการพิจารณาทั้งในประเด็นข้อเท็จจริงและข้อกฎหมาย

๒. มีคำสั่งไม่ฟ้อง

๒.๑ กรณีที่ข้อเท็จจริงและพยานหลักฐานรับฟังได้ว่าผู้ต้องหาไม่ใช่ผู้กระทำความผิด โดยทั่วไปพนักงานอัยการจะสั่งไม่ฟ้องด้วยเหตุผลว่าผู้ต้องหาไม่ใช่ผู้กระทำความผิด อันเป็นการวินิจฉัยในข้อเท็จจริง

๒.๒ กรณีที่ข้อเท็จจริงและพยานหลักฐานรับฟังได้ว่าผู้ต้องหาเป็นผู้กระทำ แต่การกระทำนั้นไม่เป็นความผิด โดยทั่วไปพนักงานอัยการจะสั่งไม่ฟ้องด้วยเหตุผลว่าการกระทำของผู้ต้องหาไม่เป็นความผิด อันเป็นการวินิจฉัยในข้อกฎหมาย

๒.๓ กรณีที่ข้อเท็จจริงและพยานหลักฐานรับฟังได้ว่าผู้ต้องหาเป็นผู้กระทำแต่การกระทำนั้นข้อเท็จจริงไม่ชัดเจนพอ (แม้สอบสวนเพิ่มเติมแล้ว) ว่าเป็นผิดหรือไม่ (ข้อเท็จจริงไม่ครบองค์ประกอบ) โดยทั่วไปพนักงานอัยการมีดุลพินิจสั่งไม่ฟ้องด้วยเหตุผลว่าพยานหลักฐานไม่พอที่จะพิสูจน์ความผิดของผู้ต้องหา อันเป็นการวินิจฉัยในประเด็นปัญหาข้อเท็จจริง แต่บางกรณีจะมีประเด็นข้อกฎหมายที่ต้องวินิจฉัยรวมอยู่ด้วย (หากมีพยานหลักฐานใหม่ก็สั่งฟ้องได้)

๒.๔ กรณีที่ข้อเท็จจริงและพยานหลักฐานรับฟังไม่ได้ชัดเจนว่าผู้ต้องหาเป็นผู้กระทำผิดหรือไม่ (แม้สอบสวนเพิ่มเติมแล้ว) โดยทั่วไปพนักงานอัยการมีดุลพินิจสั่งไม่ฟ้องด้วยเหตุผลว่าคดีมีพยานหลักฐานเพียงพอที่จะพิสูจน์ความผิดของผู้ต้องหา อันเป็นการวินิจฉัยในประเด็นปัญหาข้อเท็จจริง (หากมีพยานหลักฐานใหม่ก็สั่งฟ้องได้)

๒.๕ กรณีมีกฎหมายบัญญัติไว้โดยชัดแจ้งว่า ผู้ต้องหาไม่ต้องรับโทษและกฎหมายไม่ได้บัญญัติเงื่อนไขให้ต้องดำเนินการอย่างหนึ่งอย่างใดต่อไปอีก เช่น เด็กอายุไม่เกินสิบปีทำผิด ตามประมวลกฎหมายอาญา มาตรา ๗๓ โดยพนักงานอัยการจะสั่งไม่ฟ้องด้วยเหตุผลว่าคดีดังกล่าวผู้ต้องหาไม่ต้องรับโทษตามกฎหมาย อันเป็นการวินิจฉัยทั้งในประเด็นปัญหาข้อเท็จจริงและปัญหาข้อกฎหมาย

๒.๖ กรณีที่เห็นว่าการฟ้องคดีใดจะไม่เป็นประโยชน์แก่สาธารณชนหรือจะขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน หรือจะมีผลกระทบต่อความปลอดภัยหรือความมั่นคงของชาติ หรือต่อผลประโยชน์อันสำคัญของประเทศ โดยทั่วไปพนักงานอัยการมีดุลพินิจสั่งไม่ฟ้องด้วยเหตุผลว่า ฟ้องคดีดังกล่าวจะไม่เป็นประโยชน์แก่สาธารณชนหรือจะขัดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน หรือจะมีผลกระทบต่อความปลอดภัยหรือความมั่นคงของชาติหรือต่อผลประโยชน์อันสำคัญของประเทศ อันเป็นการวินิจฉัยในประเด็นปัญหาข้อเท็จจริง

๓. มีคำสั่งกรณีสิทธิฟ้องคดีอาญาระงับ

โดยทั่วไป พนักงานอัยการจะพิจารณาสำนวนการสอบสวนในประเด็นเรื่องเงื่อนไขระงับคดีก่อนเป็นลำดับแรกและจะต้องระมัดระวังเรื่องเงื่อนไขระงับคดีตลอดเวลาการดำเนินคดีด้วย สำหรับเงื่อนไขระงับคดีตามกฎหมายปรากฏอยู่ในบทบัญญัติมาตรา ๓๙ แห่งประมวลกฎหมายวิธีพิจารณาความอาญา ทั้งนี้ระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ข้อ ๕๔ กำหนดให้พนักงานอัยการมีคำสั่งยุติการดำเนินคดีพร้อมระบุเหตุที่ทำให้สิทธิฟ้องคดีอาญาระงับไว้ในความเห็นและคำสั่งด้วย

เงื่อนไขระงับคดี หรือเหตุที่ทำให้สิทธิฟ้องคดีอาญาระงับลง มีดังนี้

๓.๑ โดยความตายของผู้กระทำความผิด

๓.๒ ในคดีความผิดต่อส่วนตัว เมื่อได้ถอนคำร้องทุกข์ ถอนฟ้อง หรือยอมความกันโดยถูกต้องตามกฎหมาย

๓.๓ เมื่อคดีเลิกกัน (คดีที่มีโทษปรับสถานเดียว เมื่อผู้กระทำความผิดยินยอมเสียค่าปรับในอัตราอย่างสูงสำหรับความผิดนั้นแก่พนักงานเจ้าหน้าที่ก่อน ศาลพิจารณา)

๓.๔ เมื่อมีคำพิพากษาเสร็จเด็ดขาดในความผิดซึ่งได้ฟ้อง

๓.๕ เมื่อมีกฎหมายออกใช้ภายหลังการกระทำผิดยกเลิกความผิดเช่นนั้น

๓.๖ เมื่อคดีขาดอายุความ

๓.๗ เมื่อมีกฎหมายยกเว้นโทษ

๓.๘ เมื่อคดีเป็นความผิดต่อส่วนตัวและมิได้ร้องทุกข์ตามระเบียบ

๓.๙ เมื่อคดีเป็นความผิดต่อส่วนตัวและผู้เสียหายได้ยื่นฟ้องแล้ว ไม่ว่าจะได้ยื่นฟ้องก่อนหรือหลังจากที่พนักงานอัยการได้รับสำนวนการสอบสวน และไม่ว่าคดี ที่ผู้เสียหายได้ยื่นฟ้องแล้วนั้นศาลจะพิพากษาแล้วหรือไม่

๓.๑๐ เมื่อมีคำสั่งเด็ดขาดไม่ฟ้องคดีนั้นแล้ว และไม่มีหลักฐานใหม่อันสำคัญแก่คดี ซึ่งน่าจะทำให้ศาลลงโทษผู้ต้องหานั้นได้

อย่างไรก็ดี คดีอาชญากรรมคอมพิวเตอร์มีลักษณะที่แตกต่างจากคดีอาญาทั่วไป เนื่องจากมีความสลับซับซ้อนในการกระทำความผิด ผู้กระทำความผิดเป็นผู้มีความรู้ความเชี่ยวชาญในการใช้คอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ต่างๆ แต่กลับนำไปใช้ในการกระทำผิดเพื่อให้เกิดความเสียหายแก่บุคคลอื่น ดังนั้น ในการสืบสวน สอบสวน ติดตามจับกุมผู้กระทำความผิด รวมทั้งการค้นหาพยานหลักฐานต่างๆ จำเป็นต้องกระทำโดยผู้ที่มีความรู้ความเชี่ยวชาญในเรื่องคอมพิวเตอร์และระบบอิเล็กทรอนิกส์ด้วยเช่นกัน นอกจากนั้น การกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ส่วนมากเกิดขึ้นในหลายท้องที่ต่อเนื่องเกี่ยวพันกัน รวมถึงการกระทำความผิดที่เกิดนอกราชอาณาจักรไทยที่จำเป็นต้องใช้ความร่วมมือระหว่างประเทศทางอาญา หรือในกรณีที่เป็นการกระทำความผิดที่เข้าลักษณะเป็นคดีพิเศษซึ่งพนักงานอัยการต้องคำนึงถึงความชอบด้วยกฎหมายของการสอบสวนเป็นพิเศษจากคดีอาญาอื่นๆ

ตามประมวลกฎหมายวิธีพิจารณาความอาญาได้กำหนดเป็นหลักการทั่วไปเกี่ยวกับอำนาจสอบสวน โดยให้พนักงานสอบสวนมีอำนาจสอบสวนแล้วส่งสำนวนการสอบสวนไปยังพนักงานอัยการเพื่อมีคำสั่งทางคดี ซึ่งกรณีทั่วไปนี้กฎหมายได้บัญญัติแยกอำนาจการสอบสวนของพนักงานสอบสวนออกต่างหากจากอำนาจสั่งคดีของพนักงานอัยการ ซึ่งหากพนักงานอัยการต้องการข้อเท็จจริงใดเพิ่มเติมเพื่อสั่งคดี ก็ต้องกระทำผ่านการสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติม คงมีเพียงบางกรณีที่กฎหมายกำหนดให้พนักงานอัยการมีอำนาจสอบสวนคดีบางประเภท (สำนักงานอัยการสูงสุด, ๒๕๕๔ ก : ๑๕-๑๘) ซึ่งอำนาจหน้าที่ของพนักงานอัยการในฐานะพนักงานสอบสวนในความผิดต่างๆ (รวมถึงคดีอาชญากรรมคอมพิวเตอร์) มี ๒ กรณี คือ

๑. การร่วมสอบสวนกับพนักงานสอบสวนอื่นตามที่กฎหมายกำหนด เช่น อัยการสูงสุดมอบหมายให้พนักงานอัยการเข้าร่วมสอบสวนคดีนอกราชอาณาจักรตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๐ วรรคสอง การร่วมสอบสวนคดีพิเศษตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ และการร่วมสืบสวนสอบสวนคดีที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. ๒๕๕๖

๒. การสอบสวนในฐานะที่เป็นพนักงานสอบสวนผู้รับผิดชอบตามที่อัยการสูงสุดมอบหมายในคดีความผิดที่เกิดนอกราชอาณาจักร ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา ๒๐ วรรคหนึ่ง

ตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ผ่านมา

๑. คดีฉ้อโกงขายสินค้าทางเว็บไซต์กลางขายสินค้า (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, ๙ มีนาคม ๒๕๖๐)

ข้อเท็จจริงโดยย่อ: ผู้เสียหายพบประกาศขายโทรศัพท์มือถือของร้านค้าแห่งหนึ่งบนเว็บไซต์ http://shopee.co.th ซึ่งเป็นเว็บไซต์สื่อกลางในการซื้อขายสินค้า โดยผู้เสียหายได้สนทนากับคนร้ายผ่านเว็บไซต์ดังกล่าวสั่งซื้อโทรศัพท์ยี่ห้อไอโฟนจำนวนหลายเครื่อง รวมราคา ๑๖,๒๐๐ บาท โดยผู้เสียหายโอนเงินค่าสินค้าให้กับคนร้ายผ่านทาง K-Mobile Banking PLUS เข้าไป

ยังบัญชีเงินฝากของผู้ต้องหาซึ่งคนร้ายได้แจ้งให้โอน รวม ๕ ครั้ง รวมเป็นเงินจำนวน ๑๖,๒๐๐ บาท แต่ต่อมาคนร้ายไม่ได้ส่งสินค้าให้แก่ผู้เสียหายตามนัด เมื่อผู้เสียหายทวงถามเงินคืน คนร้ายไม่คืนและปิดการติดต่อกับผู้เสียหาย พนักงานสอบสวนมีความเห็นควรสั่งฟ้องผู้ต้องหาในข้อหาฉ้อโกง ตามประมวลกฎหมายอาญาเพียงข้อหาเดียว

เนื่องจากคดีนี้ปรากฏว่ามีการกระทำความผิดในระบบคอมพิวเตอร์อินเทอร์เน็ต พนักงานอัยการจึงมีคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมในประเด็นว่าผู้ใดเป็นผู้นำเข้าสู่ข้อมูลประกาศขายสินค้าทางเว็บไซต์ดังกล่าวตั้งแต่เดือนกันยายน ๒๕๕๙ โดยให้พนักงานสอบสวนมีหนังสือแจ้งปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดำเนินการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ว่าเกี่ยวกับคดีนี้ผู้ใดเป็นผู้เข้าสู่ระบบคอมพิวเตอร์และเผยแพร่ประกาศขายสินค้าดังกล่าว ซึ่งกองป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ตรวจสอบพบว่า เว็บไซต์ http://shopee.co.th เป็นเว็บไซต์ที่มีผู้จดทะเบียนโดเมนและผู้ให้บริการอินเทอร์เน็ตในประเทศไทยและพบ IP address ของผู้เผยแพร่ประกาศดังกล่าว จึงได้สอบถามไปยังบริษัทผู้ให้บริการอินเทอร์เน็ตรายใหญ่ในประเทศไทยที่เกี่ยวข้องทั้งสองแห่งเพื่อสอบถามว่าตามวันเวลาเกิดเหตุบริษัทผู้ให้บริการดังกล่าวได้ให้บริการอินเทอร์เน็ต IP address ดังกล่าวให้ผู้รับบริการรายใด ผ่านทางหมายเลขโทรศัพท์ใดและมีสถานที่ติดตั้งอุปกรณ์เชื่อมต่ออินเทอร์เน็ตของผู้ให้บริการ ณ บริเวณสถานที่ใด แต่ปรากฏว่า พนักงานเจ้าหน้าที่ได้รับแจ้งจากบริษัทผู้ให้บริการอินเทอร์เน็ตที่เกี่ยวข้องสองแห่งข้างต้นว่า เนื่องจากข้อมูลจราจรทางคอมพิวเตอร์ที่ขอตรวจสอบเป็นข้อมูลที่ย้อนหลังเกินกว่า ๙๐ วัน ตามกำหนดระยะเวลาในมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ บริษัทฯ จึงมิได้จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่เกี่ยวข้องไว้แล้ว หลังจากนั้น พนักงานสอบสวนจัดส่งผลการสอบสวนเพิ่มเติมทั้งหมดให้แก่พนักงานอัยการเมื่อประมาณกลางเดือนมีนาคม ๒๕๖๐

อย่างไรก็ดี จากพยานหลักฐานตามทางการสอบสวนเพียงพอรับฟังได้ว่าผู้ต้องหาคือผู้ที่ได้รับประโยชน์ในทางทรัพย์สินจากการฉ้อโกงผู้เสียหายที่มีการกระทำผ่านการนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์ซึ่งประชาชนทั่วไปไม่จำกัดเพียงผู้เสียหายสามารถเห็นข้อความที่เป็นเท็จได้ เมื่อผู้ต้องหาคดีนี้อยู่ระหว่างหลบหนี พนักงานอัยการจึงมีความเห็นควรสั่งฟ้องผู้ต้องหาในข้อหาฉ้อโกงประชาชนและนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ

๒. คดีฉ้อโกงโดยแสดงตนเป็นผู้อื่น ผ่านเฟซบุ๊ก(Facebook)ปลอม (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, ๙ มีนาคม ๒๕๖๐)

ข้อเท็จจริงโดยย่อ: คนร้ายเปิดบัญชีเฟซบุ๊กโดยใช้ชื่อและภาพถ่ายของเจ้าของกิจการเครื่องดื่มชื่อดัง จากนั้นส่งข้อความผ่านทางโปรแกรมพูดคุยในห้องส่วนตัวของ Facebook Messenger ไปยัง Facebook ของผู้เสียหายหลอกลวงว่าผู้เสียหายคือผู้โชคดีจากการชิงโชคด้วยฝาเครื่องดื่มยี่ห้อดังกล่าว ได้รับรถยนต์เบนซ์จำนวน ๑ คัน แต่ก่อนที่จะได้รับรางวัลมีเงื่อนไขต้องแจ้งรหัสบัตรเงินสดทรูมันนี่ จำนวน ๒ ใบ รวมมูลค่า ๒,๐๐๐ บาท ให้แก่คนร้าย ผู้เสียหายหลงเชื่อเนื่องจากในช่วงเวลาดังกล่าวได้ส่งฝาเครื่องดื่มยี่ห้อดังกล่าวไปชิงโชคจริง จึงได้ซื้อบัตรเงินสดทรูมั่นนี่และบอกรหัสประจำบัตรให้แก่คนร้ายทราบทาง Facebook Messenger แต่เมื่อทราบรหัสบัตรเงินสดทรูมันนี่แล้ว

คนร้ายได้ปิดบล็อกการติดต่อทาง Facebook กับผู้เสียหาย ต่อมาผู้เสียหายตรวจสอบยอดเงินภายในบัตรเงินสดทรูมันนี่ พบว่ามีผู้ใช้มูลค่าตามบัตรเงินสดทรูมันนี่ จำนวน ๒ ใบดังกล่าวแล้ว

คดีนี้ได้รับความสนใจจากประชาชนเนื่องจากเกี่ยวข้องกับการฉ้อโกงโดยแสดงตนเป็นเจ้าของกิจการเครื่องดื่มชื่อดัง กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) จึงรับคดีไว้สอบสวน การสอบสวนจึงมีการรวบรวมค่อนข้างสมบูรณ์ พบพยานหลักฐานว่ามีผู้นำรหัสบัตรเงินสดทรูมันนี่ จำนวน ๒ ใบของผู้เสียหาย ไปขายในเว็บไซต์ที่เป็นสื่อกลางในการซื้อขายรหัสบัตรเงินสดทรูมันนี่ ซึ่งผู้ขายต้องมีการลงทะเบียนแสดงตนกับทางเว็บไซต์และแจ้งบัญชีธนาคารเพื่อใช้ในการโอนมูลค่าเงินสดตามบัตรเงินสดทรูมันนี่ (หลังหักค่าธรรมเนียมที่เว็บไซต์เรียกเก็บ) พบว่าผู้ต้องหาเป็นผู้เข้าทำธุรกรรมบนเว็บไซต์สื่อกลางในการซื้อขายรหัสบัตรเงินสดทรูมันนี่แล้วขายรหัสบัตรเงินสดทรูมันนี่ให้กับทางเว็บไซต์จากเครื่องคอมพิวเตอร์ซึ่งเชื่อมต่อระบบอินเทอร์เน็ตภายในห้องพักของผู้ต้องหาประกอบกับบัญชีที่รับเงินก็เป็นบัญชีของผู้ต้องหา

ประเด็นที่น่าสนใจจากคดีนี้คือ คดีนี้พยานหลักฐานทางดิจิทัลที่รวบรวมได้พิสูจน์ว่าผู้ต้องหาคือผู้ที่นำเข้าข้อมูลเพื่อขายรหัสบัตรเงินสดทรูมันนี่บนเว็บไซต์ที่เป็นสื่อกลางในการซื้อขายรหัสบัตรเงินสดทรูมันนี่ โดยพบว่าผู้ต้องหาเป็นผู้ลงทะเบียนแสดงตนด้วยหมายเลขโทรศัพท์และอีเมลล์กับทางเว็บไซต์และบัญชีธนาคารที่ใช้ในการรับเงินเป็นบัญชีของผู้ต้องหาและมีการกดเบิกถอนเงินสดออกจากบัญชีด้วยบัตรเอทีเอ็มภายหลังเกิดเหตุไม่นาน ในชั้นพิจารณาจำเลยต่อสู้ว่าได้ทำธุรกรรมขายสินค้าทางเฟซบุ๊ก และมีผู้ชำระค่าสินค้าด้วยรหัสบัตรทรูมันนี่แทนการชำระด้วยเงินสด แต่เมื่อจำเลยมิได้นำสืบให้เห็นว่าได้ชำระสินค้าอะไรให้แก่ผู้ใด ข้ออ้างของจำเลยจึงไม่มีน้ำหนักหักล้างพยานโจทก์ ศาลชั้นต้นจึงพิพากษาลงโทษจำคุกจำเลยมีกำหนด ๙ เดือน โดยไม่รอลงอาญา

๓. คดีหลอกลวงเหยื่อชายหญิงด้วยความรัก (Romance Scam)

(โชติกา ศรีนรเศรษฐ์, สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐)

ข้อเท็จจริงโดยย่อ: คนร้ายได้สร้างบัญชีผู้ใช้ (Account) ในเฟซบุ๊คว่า เป็นชาวต่างชาติ หน้าตาดี การศึกษาและหน้าที่การงานดี แล้วเข้ามาขอเป็นเพื่อนและพูดคุยกับหญิงไทยในลักษณะคนรัก และออกอุบายว่าจะส่งเงินจำนวนมากมาให้ แต่ขอให้หญิงผู้เสียหายช่วยออกค่าใช้จ่ายในการโอนเงินก่อน แล้วหญิงผู้เสียหายก็หลงเชื่อโอนเงินค่าใช้จ่ายต่างๆเป็นจำนวนมากเข้าบัญชีธนาคารตามที่คนร้ายแจ้ง แต่ในที่สุดคนร้ายก็ไม่ได้โอนเงินตามที่สัญญากับผู้เสียหายไว้มาให้

คดีทำนองนี้ พยานหลักฐานที่พนักงานสอบสวนมักรวบรวมมา คือ ข้อมูลทางบัญชีของผู้เปิดบัญชีรับโอนเงินจากผู้เสียหาย ซึ่งพนักงานสอบสวนมักจะมุ่งดำเนินคดีเพียงแค่เจ้าของบัญชีผู้รับโอนเงินจากผู้เสียหายเท่านั้น ในขณะที่ผู้ต้องหาซึ่งเป็นเจ้าของบัญชีมักจะปฏิเสธโดยให้เหตุผลว่าตนเองถูกบุคคลอื่นจ้างหรือขอร้องให้ช่วยเปิดบัญชีให้เท่านั้น แต่ไม่ได้รู้เห็นถึงการหลอกลวงผู้เสียหาย การสั่งคดีส่วนใหญ่ พนักงานอัยการมักมีคำสั่งฟ้องผู้ต้องหาซึ่งเป็นเจ้าของบัญชี ในลักษณะตัวการ ยกเว้นในบางคดีที่พนักงานสอบสวนได้กันเจ้าของบัญชีที่ให้ความร่วมมือในการให้ข้อมูลคนร้ายเอาไว้เป็นพยานในคดี การดำเนินคดีในชั้นศาลนั้นมีทั้งที่ศาลพิพากษาลงโทษและพิพากษายกฟ้อง

จากตัวอย่างคดีอาชญากรรมคอมพิวเตอร์ที่ได้กล่าวถึงตอนต้น จะเห็นได้อย่างชัดเจนว่า ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ พนักงานอัยการจะต้องมีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางอิเล็กทรอนิกส์ (พยานหลักฐานดิจิทัล หรือพยานหลักฐานทาง

คอมพิวเตอร์) อย่างเหมาะสม เนื่องจากบ่อยครั้งที่พนักงานสอบสวนยังทำการสอบสวนไม่สิ้นกระแสความทำให้พนักงานอัยการไม่สามารถมีความเห็นทางคดีในทันทีเมื่อได้รับสำนวนการสอบสวนจากพนักงานสอบสวน เช่น กรณีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดฐานฉ้อโกง พนักงานสอบสวนมักทำการสอบสวนแต่เพียงประเด็นข้อเท็จจริงเกี่ยวกับบุคคลที่ได้รับประโยชน์ทางทรัพย์สินจากผู้เสียหาย เช่น ผู้ที่เป็นเจ้าของบัญชีรับโอนเงินที่ได้จากการหลอกลวงผู้เสียหาย ซึ่งการสอบสวนจะไม่ซับซ้อนและกระทำได้ง่าย จากการขอทราบข้อมูลการเปิดบัญชี รายการเดินบัญชี และภาพถ่ายกล้องวงจรปิดบริเวณที่คนร้ายเบิกถอนเงินสดที่ผู้เสียหายหลงเชื่อโอนไปให้ออกจากบัญชีที่เกี่ยวข้อง แต่พนักงานสอบสวนมักมิได้ทำการสอบสวนหาพยานหลักฐานเพื่อพิสูจน์ความผิดของผู้ต้องหาในความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จหรือข้อมูลปลอม เนื่องจากต้องใช้การตรวจสอบพยานหลักฐานทางดิจิทัลของผู้เชี่ยวชาญ และหากข้อมูลหลักฐานเช่น IP Address ที่คนร้ายใช้ขณะนำเข้าข้อมูลคอมพิวเตอร์เท็จหรือปลอม อยู่ในความครอบครองของผู้ให้บริการอินเทอร์เน็ต การเรียกพยานหลักฐานดังกล่าวก็จะต้องกระทำผ่านพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ (ที่แก้ไขเพิ่มเติม) และอาจต้องใช้ระยะเวลาในการได้มาซึ่งข้อมูลที่เกี่ยวข้องโดยขึ้นอยู่กับความรวดเร็วในการให้ความร่วมมือของผู้ให้บริการอินเทอร์เน็ต ในกรณีที่พนักงานสอบสวนสรุปสำนวนการสอบสวนส่งมายังพนักงานอัยการโดยมิได้มีการสอบสวนพยานหลักฐานเพื่อพิสูจน์ความผิดของผู้ต้องหาในความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จหรือข้อมูลปลอม ในกรณีเช่นว่านี้ พนักงานอัยการมีอำนาจสั่งให้พนักงานสอบสวนดำเนินการสอบสวนเพิ่มเติมเพื่อให้ได้ข้อเท็จจริงที่เพียงพอในการทำความเห็นและคำสั่งทางคดี ดังนั้น พนักงานอัยการที่รับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์จึงมีความจำเป็นต้องมีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางดิจิทัล เพื่อออกคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมในประเด็นที่เกี่ยวข้องอย่างครบถ้วนสมบูรณ์ และแม้ว่าจะมีการฟ้องคดีต่อศาลแล้ว พนักงานอัยการซึ่งมีหน้าที่ในการดำเนินกระบวนพิจารณาว่าต่างคดีในชั้นศาล ก็จำต้องมีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางดิจิทัล เพียงพอที่จะนำเสนอพยานหลักฐานในการพิจารณาเพื่อโน้มน้าวให้ศาลรับฟังแล้วเชื่อว่าผู้ต้องหาเป็นผู้กระทำความผิดตามข้อกล่าวหาจริง ดังนั้น แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการจึงจำเป็นต้องมีองค์ความรู้เกี่ยวกับการจัดการกับพยานหลักฐานทางดิจิทัลที่เหมาะสม ดังต่อไปนี้ด้วย (สุนีย์ สกาวรัตน์, ๒๕๕๙ : ๖๗-๖๙)

๑. ความรู้ความเข้าใจเกี่ยวกับการรวบรวมพยานหลักฐาน (Acquisition) โดยพนักงานอัยการควรเข้าใจว่า พยานหลักฐานที่สามารถจัดเก็บจากระบบคอมพิวเตอร์มีอะไรบ้าง สามารถจัดเก็บด้วยวิธีใด และพยานหลักฐานที่ประสงค์จะจัดเก็บมีความสำคัญต่อการพิสูจน์การกระทำความผิดของผู้ต้องหาอย่างไร

๒. ความรู้ความเข้าใจเกี่ยวกับการเก็บรักษาพยานหลักฐาน (Preservation) โดยพนักงานอัยการควรมีความเข้าใจว่า เมื่อพยานหลักฐานถูกรวบรวมแล้ว จะต้องมีการเก็บรักษาไว้ในสภาพที่ใช้รับฟังโดยศาลได้อย่างไร กล่าวคือ โดยหลักแล้วพยานหลักฐานดิจิทัลจะต้องมีการเก็บรักษาผ่านกระบวนการสร้างห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of Custody) ซึ่งเริ่มต้นก่อนที่จะมีการเก็บรวบรวมและสิ้นสุดลงเมื่อพยานหลักฐานถูกส่งคืนให้เจ้าของหรือถูกทำลายไป การขาดขั้นตอนใดอาจนำไปสู่การตั้งคำถามความสงสัยเรื่องสภาพสมบูรณ์ของพยานหลักฐานทางดิจิทัล

๓. ความรู้ความเข้าใจเกี่ยวกับการวิเคราะห์พยานหลักฐาน (Analysis) โดยพนักงานอัยการควรมีความเข้าใจว่า ความแตกต่างของรูปแบบและประเภทของพยานหลักฐานเพื่อมุ่งพิสูจน์การกระทำความผิดของผู้ต้องหาในแต่ละคดี เพื่อทราบเป้าหมายการตรวจสอบพยานหลักฐานแต่ละรายการว่าจะสามารถพิสูจน์พฤติการณ์กระทำผิดของผู้ต้องหาได้มากน้อยเพียงใด

๔. ความรู้ความเข้าใจเกี่ยวกับการนำเสนอผลการตรวจพิสูจน์พยานหลักฐาน (Presentation) โดยพนักงานอัยการควรมีความเข้าใจว่า ในคดีความผิดอาญากรรมคอมพิวเตอร์ควรมีการนำเสนอผลการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลในรูปแบบใด ซึ่งบางกรณีมีความจำเป็นต้องมีรายงานผลการตรวจพิสูจน์ที่ออกโดยเจ้าพนักงานผู้มีอำนาจหน้าที่ตรวจพิสูจน์พยานหลักฐานทางคดี ประกอบบันทึกคำให้การเป็นหนังสือของผู้ตรวจพิสูจน์ หรือในบางคดีจำต้องนำรายงานสืบสวนของเจ้าพนักงานสืบสวน มาประกอบเพื่อสนับสนุนความเชื่อมโยงและพฤติการณ์ในการกระทำความผิดของผู้ต้องหา

ปัญหาและอุปสรรคที่พบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

จากตัวอย่างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ได้กล่าวถึงข้างต้น เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) และโชติกา ศรีนรเศรษฐ์ (สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐) กล่าวถึงปัญหาและอุปสรรคสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในฐานความผิดเกี่ยวกับการฉ้อโกงในกรณีที่พนักงานสอบสวนสรุปสำนวนการสอบสวนโดยเห็นว่าการสอบสวนเสร็จสิ้นแล้วและทำความเห็นควรสั่งฟ้องผู้ต้องหาในความผิดฐานฉ้อโกง แต่มักมิได้ทำการสอบสวนข้อเท็จจริงและรวบรวมพยานหลักฐานเพื่อพิสูจน์การกระทำความผิดในเรื่องการนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์ โดยจะรวบรวมพยานหลักฐานเพียงจากการตรวจสอบข้อมูลของบัญชีเงินฝากธนาคารของผู้ได้รับประโยชน์จากการฉ้อโกงเพียงอย่างเดียวแล้วดำเนินคดีกับผู้ที่เป็นเจ้าของบัญชีเงินฝากดังกล่าวเท่านั้น ซึ่งบ่อยครั้งผู้ต้องหาหรือจำเลยมักต่อสู้คดีในทำนองว่าตนเองถูกว่าจ้างให้เปิดบัญชีเงินฝากให้กับคนร้ายเท่านั้น เช่นเดียวกับ ดวงพร เตชะกำธร (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) เคยพบอุปสรรคในการดำเนินคดีอาญาด้านทรัพย์สินทางปัญญาว่า การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในคดีที่ผู้ต้องหามีชื่อเป็นเจ้าของบัญชีธนาคารซึ่งปรากฏบนเว็บไซต์ขายภาพยนตร์ละเมิดลิขสิทธิ์ขนาดใหญ่เพื่อให้ลูกค้าโอนเงินชำระค่าแผ่นดีวีดีละเมิดลิขสิทธิ์ให้ผู้ขาย ชั้นสอบสวนพบข้อเท็จจริงว่า ผู้ต้องหาเป็นหญิงอายุ ๗๐ ปี อ่านเขียนแทบไม่ได้ ไม่มีเครื่องคอมพิวเตอร์และไม่รู้ว่าอินเทอร์เน็ตคืออะไร ผู้ต้องหายอมรับว่าได้รับจ้างจากชายผู้หนึ่งให้ทำการเปิดบัญชีธนาคารในคดีดังกล่าวโดยได้รับค่าจ้างเป็นเงินจำนวน ๒,๐๐๐ บาท จะเห็นได้ว่า พยานหลักฐานอื่นที่จะนำมาพิสูจน์ว่าเจ้าของบัญชีคือบุคคลเดียวกันกับผู้กระทำความผิดในระบบคอมพิวเตอร์ อาทิเช่น การตรวจพิสูจน์ยืนยันว่าผู้ต้องหาเป็นเจ้าของอีเมล์หรือเจ้าของเว็บไซต์ที่มีการละเมิดลิขสิทธิ์ อันเป็นพยานหลักฐานสำคัญยิ่งในการพิสูจน์ตัวผู้กระทำความผิดในระบบคอมพิวเตอร์ เป็นเรื่องที่กระทำได้ยากยิ่ง เนื่องจากอาชญากรรมคอมพิวเตอร์มักเป็นความผิดข้ามชาติ การตรวจสอบเพื่อยืนยันบุคคลผู้กระทำผิดจากประเทศต้องอาศัยความร่วมมือระหว่างประเทศอย่างเป็นทางการเพื่อให้ได้มาซึ่งพยานหลักฐานอันเป็นที่ยอมรับในชั้นศาล ดังนั้น พนักงานสอบสวนมีทางเลือกที่จะระบุตัวผู้ต้องหาค่อนข้างจำกัดเพื่อมิให้ล่วงเลยกำหนดเวลาในการควบคุมตัวผู้ต้องหาตามกฎหมาย พนักงานสอบสวนจึงมักเลือกใช้เฉพาะข้อเท็จจริง

เรื่องชื่อบัญชีธนาคารที่ปรากฏในเว็บไซต์ ซึ่งเป็นพยานหลักฐานที่ยังคงมีข้อโต้เถียงต่อสู้เรื่องการพิสูจน์การกระทำความผิดของผู้ต้องหาตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อันสะท้อนถึงข้อขัดข้องอย่างยิ่งสำหรับผู้บังคับใช้กฎหมายในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

นอกจากนี้ เมื่อหน่วยงานในกระบวนการยุติธรรมซึ่งมีบทบาทในการดำเนินการกับอาชญากรรมคอมพิวเตอร์ยังไม่มีการบูรณาการความร่วมมือและแบ่งปันองค์ความรู้ซึ่งกันและกัน ย่อมทำให้การดำเนินการตามอำนาจหน้าที่ของผู้ใช้บังคับกฎหมายต้องเป็นไปตามกฎ ระเบียบ คู่มือหรือแนวทางปฏิบัติซึ่งใช้บังคับเฉพาะกับบุคลากรในแต่ละหน่วยงานเท่านั้น โดยในส่วนของสำนักงานอัยการสูงสุด การดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการจะต้องปฏิบัติให้เป็นไปตามบทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา และระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) โดยมีคู่มือพนักงานอัยการสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๔ ซึ่งวางแนวปฏิบัติเบื้องต้นเกี่ยวกับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์สำหรับการดำเนินคดีในชั้นพนักงานอัยการ

สรุป

การศึกษาในบทที่ ๓ เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ ๑. เพื่อศึกษาแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๑. สรุปได้ดังนี้

จากข้อมูลสถิติที่นำเสนอไว้ในบทที่ ๒ และจากการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิ ย่อมคาดการณ์ได้ว่า เมื่อภาครัฐและภาคเอกชนมีการพัฒนาและส่งเสริมการใช้ระบบคอมพิวเตอร์ อินเทอร์เน็ต และระบบสื่อสารดิจิทัลในการทำธุรกิจมากขึ้น อาทิเช่น การทำธุรกรรมด้านการค้าและบริการทางอิเล็กทรอนิกส์ ธุรกรรมการชำระราคาทางอิเล็กทรอนิกส์ และธุรกรรมการเงินทางอิเล็กทรอนิกส์ รวมไปถึงจำนวนการใช้งานระบบคอมพิวเตอร์ในสื่อสังคมออนไลน์ที่มีปริมาณเพิ่มมากขึ้น ประกอบกับการที่ตัวแปรสำคัญประการหนึ่งของปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ คือ จำนวนผู้ใช้งานระบบคอมพิวเตอร์และจำนวนธุรกรรมที่มีการกระทำผ่านระบบคอมพิวเตอร์ ซึ่งเป็นปัจจัยด้านเหยื่อและด้านโอกาสในการเกิดคดีอาชญากรรมคอมพิวเตอร์ ตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) กล่าวคือ เมื่ออาชญากรรมคอมพิวเตอร์เกิดขึ้นได้ทุกที่ทุกเวลาที่มีการเชื่อมต่อระบบคอมพิวเตอร์และอินเทอร์เน็ต แม้ว่าผู้กระทำผิดและเหยื่อจะมิได้พบหน้ากันก็ตาม ผู้กระทำความผิดผ่านระบบคอมพิวเตอร์ย่อมมีโอกาสกระทำความผิดเกี่ยวกับคอมพิวเตอร์ต่อผู้เสียหายซึ่งเป็นผู้ใช้งานระบบคอมพิวเตอร์ได้อย่างกว้างขวางมากขึ้นด้วย ซึ่งในช่วงปีที่ผ่านมา ได้มีตัวอย่างการกระทำความผิดต่อระบบคอมพิวเตอร์และการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรมจำนวนคดีมากขึ้น ในขณะที่การรวบรวมพยานหลักฐานเพื่อหาตัวผู้กระทำความผิดและพิสูจน์การกระทำความผิดของผู้กระทำมีความซับซ้อนมากกว่าในอดีต เนื่องจากผู้กระทำความผิดย่อมต้องใช้ความรู้ความเข้าใจด้านคอมพิวเตอร์ในการเจาะ

ระบบคอมพิวเตอร์ผ่านระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดูแลตัวระบบคอมพิวเตอร์ หรือแม้แต่กรณีที่ผู้กระทำความผิดที่ไม่มีความรู้ความเข้าใจด้านคอมพิวเตอร์ในระดับที่ดีมาก แต่เลือกใช้วิธีปกปิดตัวตนด้วยการกระทำความผิดผ่านการเชื่อมต่อระบบคอมพิวเตอร์ซึ่งมีที่ตั้ง Server ที่จัดเก็บข้อมูลผู้ใช้บริการอยู่ในต่างประเทศ เพื่อทำให้การได้มาซึ่งพยานหลักฐานทางดิจิทัลของพนักงานเจ้าหน้าที่ทำได้ยากขึ้น ดังนั้น เมื่ออาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่กระทำโดยผู้ที่มีความรู้หรือมีความเชี่ยวชาญด้านคอมพิวเตอร์ แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการซึ่งเป็นผู้บังคับใช้กฎหมายในกระบวนการยุติธรรมทางอาญาจึงจำต้องมีความรู้ความเข้าใจในการทำงานของคอมพิวเตอร์และพยานหลักฐานทางดิจิทัลอย่างเหมาะสมด้วย แต่จากการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านงานคดีอาชญากรรมคอมพิวเตอร์จากหลากหลายสำนักงานคดีกลับพบว่า ในปัจจุบันพนักงานอัยการประสบปัญหาในการดำเนินคดีอาชญากรรมคอมพิวเตอร์อย่างมากจากปัญหาการรวบรวมพยานหลักฐานในชั้นสอบสวนเพื่อพิสูจน์การกระทำความผิดในเรื่องการนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์ที่ยังไม่สิ้นกระแสความ และปัญหาการบูรณาการความร่วมมือและแบ่งปันองค์ความรู้ซึ่งกันและกันระหว่างหน่วยงานในกระบวนการยุติธรรมซึ่งมีบทบาทในการดำเนินการกับอาชญากรรมคอมพิวเตอร์

บทที่ ๔
วิเคราะห์ปัญหาและกำหนดแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด

การศึกษาในบทที่ ๔ มีความมุ่งหมายเพื่อตอบวัตถุประสงค์การวิจัยข้อที่ ๒. เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ โดยมีลำดับการศึกษา ดังนี้

๑. วิเคราะห์ปัญหาและอุปสรรคที่พนักงานอัยการพบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

๒. แนวทางตามยุทธศาสตร์การตอบโต้อาชญากรรมคอมพิวเตอร์ในต่างประเทศ

๓. กำหนดแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด

๔. สรุป

วิเคราะห์ปัญหาและอุปสรรคที่พนักงานอัยการพบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

แนวคิดประเทศไทย ๔.๐ ได้ถูกผนวกไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ โดยเฉพาะอย่างยิ่งในยุทธศาสตร์ที่ ๕ ของแผนดังกล่าว ซึ่งว่าด้วยการเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน หมวดแผนงานและโครงการข้อ ๕.๕ มีแนวทางการป้องกันและการแก้ไขภัยคุกคามทางเทคโนโลยีสารสนเทศและไซเบอร์เพราะเหตุที่ภาครัฐเล็งเห็นว่าภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรงและมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมคอมพิวเตอร์และการโจมตีทางไซเบอร์จะมีผลกระทบต่อประเทศอย่างร้ายแรง จึงต้องให้ความสำคัญในการมีมาตรการป้องกันภัยคุกคามทางไซเบอร์ให้สอดรับกับความเปลี่ยนแปลงทางสภาพแวดล้อมของสังคมในปัจจุบัน โดยกำหนดหน่วยงานหลักในการดำเนินการ คือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และสำนักงานตำรวจแห่งชาติ โดยในเวลาต่อมากระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เสนอแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งคณะรัฐมนตรีได้เห็นชอบแล้ว แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมดังกล่าวได้กำหนดยุทธศาสตร์เพื่อขับเคลื่อนการพัฒนาระบบดิจิทัล และสร้างความพร้อมเพื่อรองรับการเปลี่ยนแปลง ทั้งในด้านกำลังคนและด้านการสร้างความเชื่อมั่นแก่ผู้เกี่ยวข้อง โดยแผนงานในข้อ ๑.๔ ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ๕๑) ระบุว่า

“พัฒนาบุคลากรที่เกี่ยวข้องกับการบัญญัติและบังคับใช้กฎหมาย กฎ ระเบียบ ข้อบังคับต่างๆ ให้มีความรอบรู้ และเท่าทันต่อเทคโนโลยีสมัยใหม่ เช่น บุคลากรวิชาชีพด้านนิติศาสตร์มีความเข้าใจและเชี่ยวชาญทางด้านเทคโนโลยีดิจิทัลในกระบวนการยุติธรรม”และยุทธศาสตร์ที่ ๖ “สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล” ได้กำหนดแผนงานในข้อ ๓.๓ ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, ๒๕๕๙ : ๕๖) กำหนดให้มีมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากล โดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (Critical Infrastructure) เพื่อให้มีความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ พร้อมกำหนดหน่วยงานรับแจ้งเหตุและสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันและปราบปรามการกระทำความผิดที่มีผลกระทบต่อความมั่นคงปลอดภัยดิจิทัล อย่างไรก็ดี แผนดังกล่าวยังคงมีลักษณะเป็นการกำหนดแผนการดำเนินงานในส่วนของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหลัก ไม่ครอบคลุมแผนงานในลักษณะการเป็นหน่วยงานศูนย์กลางประสานความร่วมมืออย่างบูรณาการระหว่างหน่วยงานผู้บังคับใช้กฎหมายที่มีบทบาทในการต่อต้านอาชญากรรมคอมพิวเตอร์โดยรวมทั้งกระบวนการ อันได้แก่ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการสูงสุด และศาลยุติธรรม ด้วยเหตุนี้ จึงอาจทำให้แนวทางในการบังคับใช้กฎหมายเกี่ยวกับการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์และคดีที่มีผลกระทบต่อความมั่นคงปลอดภัยดิจิทัลในชั้นของเจ้าพนักงานตำรวจ (เจ้าหน้าที่สืบสวน และพนักงานสอบสวน) พนักงานอัยการ และศาล ไม่สอดคล้องกัน

เมื่อหน่วยงานในกระบวนการยุติธรรมซึ่งมีบทบาทในการดำเนินการกับอาชญากรรมคอมพิวเตอร์ยังไม่มีการบูรณาการความร่วมมือและแบ่งปันองค์ความรู้ซึ่งกันและกัน ย่อมทำให้การดำเนินการตามอำนาจหน้าที่ของผู้ใช้บังคับกฎหมายต้องเป็นไปตามกฎ ระเบียบ คู่มือ หรือแนวทางปฏิบัติซึ่งใช้บังคับเฉพาะกับบุคลากรในแต่ละหน่วยงานเท่านั้น โดยในส่วนของพนักงานอัยการ การดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบัน พนักงานอัยการต้องปฏิบัติให้เป็นไปตามบทบัญญัติประมวลกฎหมายวิธีพิจารณาความอาญา และระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (ที่แก้ไขเพิ่มเติม) ประกอบกับคู่มือพนักงานอัยการสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๔ ซึ่งวางแนวทางเบื้องต้นเกี่ยวกับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ในชั้นพนักงานอัยการ

จากสภาพปัญหาและอุปสรรคที่พนักงานอัยการพบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ดังที่ได้กล่าวมาในบทที่ ๓ สามารถจำแนกตามลักษณะของปัจจัยได้ดังนี้

๑. สภาพปัญหาและอุปสรรคจากปัจจัยภายในองค์กรอัยการ

๑.๑ ปัจจัยด้านโครงสร้างอำนาจหน้าที่ของสำนักงานคดีภายในสำนักงานอัยการสูงสุดที่ดำเนินคดีอาชญากรรมคอมพิวเตอร์

เนื่องจากอาชญากรรมคอมพิวเตอร์มักแฝงอยู่กับการกระทำความผิดตามกฎหมายในฐานอื่นๆ โดยมีลักษณะของการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดฐานอื่นๆ (Computers as Tools) จึงเป็นการยากที่จะแบ่งโครงสร้างความรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด โดยเฉพาะอย่างยิ่งโครงสร้างของสำนักงานคดีในส่วนกลาง

ซึ่งแตกต่างจากสำนักงานคดีในส่วนภูมิภาคที่ยังไม่พบปัญหาในเรื่องนี้มากนัก เนื่องจากในส่วนภูมิภาคมีการแบ่งอำนาจหน้าที่ของสำนักงานอัยการในลักษณะที่ยึดตามพื้นที่ทางภูมิศาสตร์เป็นหลัก และแยกการดำเนินคดีบางประเภทให้เป็นอำนาจของสำนักงานชำนัญพิเศษเฉพาะ เช่น คดีปกครอง คดีแรงงาน และคดีปราบทุจริต เท่านั้น ส่วนบรรดาคดีอาญาอื่นๆ ซึ่งรวมถึงคดีอาชญากรรมคอมพิวเตอร์อยู่ในความรับผิดชอบของสำนักงานอัยการจังหวัดในแต่ละจังหวัด

ปัจจุบัน สำนักงานคดีส่วนกลางภายในสำนักงานอัยการสูงสุดที่รับผิดชอบงานที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์มีหลายสำนักงาน ได้แก่ สำนักงานคดีอาญา สำนักงานคดีเศรษฐกิจและทรัพยากร สำนักงานคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ สำนักงานคดีพิเศษ และสำนักงานการสอบสวน จึงทำให้การพัฒนาศักยภาพบุคลากรในแต่ละสำนักงานแยกต่างหากออกจากกันทั้งโครงการและงบประมาณที่ได้รับจัดสรร โดยในมุมมองของพนักงานอัยการผู้ปฏิบัติงานคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์หลายท่านมีความเห็นว่า โครงสร้างอำนาจหน้าที่ของสำนักงานด้านคดีภายในสำนักงานอัยการสูงสุดยังขาดความชัดเจนหรือมีความซ้ำซ้อนในความรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ อาทิเช่น

ดวงพร เตชะกำธร (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) ซึ่งเป็นพนักงานอัยการที่มีประสบการณ์ในงานด้านคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ เห็นว่า ในคดีทรัพย์สินทางปัญญา หากการซื้อขายสินค้าละเมิดทรัพย์สินทางปัญญาถูกนำมาวางจำหน่ายผ่านทางอินเทอร์เน็ต การกระทำดังกล่าวก็เป็นอาชญากรรมคอมพิวเตอร์แล้ว อย่างไรก็ดี หากมีลักษณะของการล่อลวงผ่านคอมพิวเตอร์ให้ผู้เสียหายโอนเงินให้ ความผิดดังกล่าวก็อยู่ในความรับผิดชอบของสำนักงานคดีเศรษฐกิจและทรัพยากร ดังนั้น ในบางครั้งหากเป็นการกระทำความผิดหลายฐานความผิดตามกฎหมายแตกต่างกันในคดีเดียวกัน อาจเกิดความซ้ำซ้อนในเรื่องอำนาจหน้าที่ โดยดวงพร เตชะกำธร (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) เสนอแนวทางแก้ไข โดยยกตัวอย่าง พนักงานอัยการของประเทศสหรัฐอเมริกาที่มีชื่อว่า Computer Crime and Intellectual Property Section (CCIPS) เป็นผู้รับผิดชอบคดีอาชญากรรมคอมพิวเตอร์และทรัพย์สินทางปัญญาทั้งหมด

สำหรับงานคดีเศรษฐกิจและทรัพยากร โชติกา ศรีนรเศรษฐ์ (สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐) เห็นว่า โครงสร้างอำนาจหน้าที่ของสำนักงานคดีของสำนักงานอัยการสูงสุดค่อนข้างซ้ำซ้อนกันในบางกรณี เช่น คดีหมิ่นประมาทผ่านระบบคอมพิวเตอร์ จะอยู่ในความรับผิดชอบของสำนักงานคดีอาญา แต่หากเป็นการฉ้อโกงผ่านระบบคอมพิวเตอร์ (เช่น Facebook, LINE, Instagram หรือเว็บไซต์ต่างๆ) จะอยู่ในความรับผิดชอบของสำนักงานคดีเศรษฐกิจและทรัพยากร ซึ่งบางครั้งอาจสร้างความสับสนให้กับพนักงานสอบสวน นิติกร และผู้ปฏิบัติงานอื่นๆ อีกทั้ง สำนักงานคดีเศรษฐกิจและทรัพยากรไม่ได้รับผิดชอบเฉพาะคดีอาชญากรรมคอมพิวเตอร์เพียงอย่างเดียว แต่ยังรับผิดชอบคดีอื่นที่มีการฉ้อโกงโดยใช้เทคโนโลยีแผนใหม่ ซึ่งบางครั้งก็ยังเกิดการถกเถียงกันว่าเทคโนโลยีแผนใหม่ครอบคลุมถึงอะไรบ้าง

เช่นเดียวกับ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) ยกตัวอย่างความซ้ำซ้อนของโครงสร้างอำนาจหน้าที่ของสำนักงานคดีเศรษฐกิจและทรัพยากร กับสำนักงานคดีพิเศษ เช่น คดีฉ้อโกงประชาชนทางเฟซบุ๊ก หากการสอบสวนคดีดังกล่าวกระทำโดยเจ้าหน้าที่กรมสอบสวนคดีพิเศษ (DSI) คดีดังกล่าวจะอยู่ในความรับผิดชอบของสำนักงานคดีพิเศษ แต่

หากสอบสวนโดยพนักงานสอบสวนทั่วไป คดีดังกล่าวจะอยู่ในความรับผิดชอบของสำนักงานคดีเศรษฐกิจและทรัพยากร ซึ่งเบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) เห็นว่า การแบ่งโครงสร้างความรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ดังกล่าวยังไม่เหมาะสม เนื่องจากเป็นการแบ่งแยกความรับผิดชอบตามประเภทของพนักงานสอบสวนซึ่งไม่มีความจำเป็น เพราะคดีประเภทดังกล่าวแม้จะได้รับการสอบสวนโดยเจ้าหน้าที่กรมสอบสวนคดีพิเศษก็ยังคงอยู่ภายใต้อำนาจพิจารณาคดีของศาลอาญาไม่แตกต่างจากคดีที่ผ่านการสอบสวนโดยพนักงานสอบสวนทั่วไป ดังนั้น สำนักงานอัยการสูงสุดควรแบ่งโครงสร้างความรับผิดชอบสำนวนคดีให้เหมาะสมตามความเชี่ยวชาญเฉพาะทางของพนักงานอัยการมากกว่า โดยเฉพาะอย่างยิ่งงานคดีอาชญากรรมคอมพิวเตอร์ที่เป็นคดีที่มีผลกระทบต่อระบบเศรษฐกิจโดยรวมและมีความเกี่ยวข้องกับฐานความผิดอื่นๆที่อยู่ในอำนาจความรับผิดชอบของสำนักงานคดีเศรษฐกิจและทรัพยากร ควรมอบหมายให้พนักงานอัยการของสำนักงานคดีเศรษฐกิจและทรัพยากรเป็นผู้รับผิดชอบ เพื่อจะได้เกิดความเชี่ยวชาญและชำนาญเฉพาะทางเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ที่เป็นอาชญากรรมทางเศรษฐกิจโดยตรง

๑.๒ ปัจจัยด้านบทบัญญัติที่เป็นแนวทางปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์

ปัจจัยของปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในประการต่อมา คือ การได้รับทราบแนวทางปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์ จากการทบทวนวรรณกรรมในบทที่ ๒ พบว่า นอกจากบทกฎหมายหลักในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ อันได้แก่ ประมวลกฎหมายอาญา ประมวลกฎหมายวิธีพิจารณาความอาญา ระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการแล้ว ยังมีคู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๔ ที่ระบุแนวทางการดำเนินคดีที่มีคอมพิวเตอร์เกี่ยวข้องกับการกระทำความผิด และรวบรวมตัวอย่างคำฟ้องคดีอาชญากรรมคอมพิวเตอร์หลากหลายประเภทคดี แต่จากการสัมภาษณ์เชิงลึกผู้ทรงคุณวุฒิด้านคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ พบว่า มีจำนวนมากถึงร้อยละ ๕๐ ของจำนวนผู้ตอบแบบสอบถาม ยังขาดความรู้และความเข้าใจในคู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๔ กล่าวคือ บางส่วนทราบเพียงว่ามีคู่มือดังกล่าวแต่ไม่ทราบรายละเอียดเพราะยังคงยึดถือเพียงบทกฎหมายหลักเท่านั้น และบางส่วนไม่ค่อยใช้ประโยชน์จากคู่มือดังกล่าวโดยเห็นว่าคู่มือดังกล่าวมีเนื้อหาไม่เป็นปัจจุบัน จึงเป็นการสะท้อนให้เห็นว่า แม้ว่าคู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๔ จะถูกจัดพิมพ์เผยแพร่มานานกว่า ๖ ปี แต่สำนักงานอัยการสูงสุดยังขาดการประชาสัมพันธ์ที่ทั่วถึง อีกทั้งยังขาดการปรับปรุงคู่มือดังกล่าวให้ทันสมัย

๑.๓ ปัจจัยด้านการจัดสรรงบประมาณเพื่อรองรับ และพัฒนางานคดีอาชญากรรมคอมพิวเตอร์

ดังที่กล่าวไว้ในหัวข้อ “ยุทธศาสตร์ด้านการอำนวยความยุติธรรมทางอาญาในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด” และตารางที่ ๒-๔ ในบทที่ ๒ ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา โครงการภายใต้กลยุทธ์ที่ ๑.๑ สร้างมาตรฐานและศักยภาพในการอำนวยความยุติธรรม มีโครงการที่น่าจะสอดคล้องกับการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ๓ โครงการ คือ

โครงการที่ ๕ “โครงการสร้างมาตรฐานในการดำเนินคดีทรัพย์สินทางปัญญาในรูปแบบอิเล็กทรอนิกส์”

โครงการที่ ๖ “โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมทางเทคโนโลยี”

โครงการที่ ๗ “โครงการจัดตั้งศูนย์วิชาการด้านคดีเศรษฐกิจและทรัพยากร”

แต่ทว่าทั้ง ๓ โครงการข้างต้น ยังไม่ได้รับการจัดสรรงบประมาณในปี ๒๕๖๐ ซึ่งเป็นปีที่เริ่มดำเนินการและคาดว่าจะได้รับผลกระทบในเชิงปริมาณงานและความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ จากการดำเนินนโยบายประเทศไทย ๔.๐ ดังที่กล่าวมาในบทที่ ๓

ส่วนโครงการภายใต้กลยุทธ์ที่ ๑.๒ “พัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน” และกลยุทธ์ที่ ๑.๓ “เพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญา” มีโครงการที่อาจมีความเกี่ยวข้องกับการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ๓ โครงการ คือ

โครงการที่ ๑ กลยุทธ์ที่ ๑.๒ “โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน”

โครงการที่ ๑ กลยุทธ์ที่ ๑.๔ “โครงการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา”

พบว่า แม้ว่าทั้งสองโครงการจะได้รับการอนุมัติงบประมาณในปีงบประมาณ ๒๕๖๐ แต่กรอบของโครงการทั้งสองก็ค่อนข้างกว้าง มิได้เน้นเฉพาะเรื่องที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์โดยตรง และเนื่องจากโครงการทั้งสองมีสำนักงานคดีที่รับผิดชอบหลัก คือ สำนักงานการสอบสวน และสำนักงานต่างประเทศ ซึ่งมีภาระความรับผิดชอบ และอำนาจหน้าที่ในคดีประเภทอื่นๆ ด้วย จึงเป็นไปได้ว่าโครงการดังกล่าวอาจไม่ครอบคลุมการพัฒนาความรู้ของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยตรง

๑.๔ ปัญหาด้านองค์ความรู้ของบุคลากร

ในคดีอาชญากรรมคอมพิวเตอร์บางคดี ต้องอาศัยพยานหลักฐานดิจิทัลหลายชั้นในการพิสูจน์เชื่อมโยงบ่งบอกตัวคนร้าย โดยพนักงานอัยการตองมีองค์ความรู้เกี่ยวกับการจัดการกับพยานหลักฐานทางดิจิทัลอย่างเหมาะสม (สุนีย์ สกาวรัตน์, ๒๕๕๙ : ๖๗-๖๙) เช่นเดียวกับผู้มีวิชาชีพทางกฎหมายทั่วไป พนักงานอัยการมีความรู้ความเชี่ยวชาญในประเด็นข้อกฎหมาย แต่มีข้อจำกัดด้านความรู้เกี่ยวกับพยานหลักฐานทางดิจิทัล ทำให้พนักงานอัยการบางท่านที่ไม่คุ้นเคยกับระบบการทำงานของคอมพิวเตอร์ เกิดอุปสรรคในการกำหนดประเด็นคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติม รวมทั้งขาดความเข้าใจในการเชื่อมโยงพยานหลักฐานต่างๆในคดีอาชญากรรมคอมพิวเตอร์ซึ่งมักต้องอาศัยพยานหลักฐานหลายอย่างพิจารณาร่วมกันเพื่อย้อนรอยบ่งบอกระบุตัวของผู้กระทำความผิดและสถานที่กระทำความผิดอันเกี่ยวข้องกับอำนาจการสอบสวนของพนักงานสอบสวนด้วย จึงอาจทำให้พนักงานอัยการพบปัญหาในการนำเสนอพยานหลักฐานในชั้นศาล (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, ๙ มีนาคม ๒๕๖๐)

๒. สภาพปัญหาและอุปสรรคจากปัจจัยภายนอกองค์กรอัยการ

๒.๑ ปัญหาด้านองค์ความรู้ของบุคลากรในกระบวนการสืบสวนสอบสวน

เนื่องจากผู้ที่มีบทบาทสำคัญเป็นต้นทางของการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในการรวบรวมข้อเท็จจริงและพยานหลักฐานในทางคดีเพื่อตั้งรูปคดีและเชื่อมโยงพฤติการณ์ในคดีให้เพียงพอที่จะระบุการกระทำที่เป็นความผิดและผู้ที่น่าเชื่อว่าคือผู้กระทำผิดก่อนส่งสำนวนการสอบสวนพร้อมความเห็นไปยังพนักงานอัยการ คือ เจ้าหน้าที่สืบสวนและพนักงานสอบสวน ซึ่งหากสำนวนคดีที่มีการรวบรวมข้อเท็จจริงและพยานหลักฐานที่สมบูรณ์เพียงพอที่พนักงานอัยการจะมีความเห็นและคำสั่งทางคดี การพิจารณามีความเห็นสั่งฟ้องและดำเนินคดีกับผู้กระทำความผิดก็ย่อมเป็นไปด้วยความรวดเร็วมากขึ้น แต่ในปัจจุบัน พบว่า เจ้าหน้าที่สืบสวนและพนักงานสอบสวนบางส่วนยังขาดความรู้ความเข้าใจในการรวบรวมพยานหลักฐานทางดิจิทัลในคดีอาชญากรรมคอมพิวเตอร์

ในประเด็นนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) ชี้ให้เห็นถึงลักษณะปัญหาในชั้นสอบสวนของคดีอาชญากรรมทางเศรษฐกิจ จากกรณีตัวอย่างคดีฉ้อโกงขายสินค้าทางเว็บไซต์กลางขายสินค้าซึ่งความรู้ความเข้าใจของพนักงานสอบสวนในการรวบรวมพยานหลักฐานในชั้นสอบสวนเพื่อพิสูจน์ความผิดของผู้ต้องหามีความสำคัญอย่างยิ่งในการทำให้สำนวนการสอบสวนสมบูรณ์ เนื่องจากพยานหลักฐานดิจิทัล เช่น ข้อมูลจราจรทางคอมพิวเตอร์ ต้องมีการดำเนินการรวบรวมจัดเก็บอย่างรวดเร็วและถูกต้องตามกฎหมาย ก่อนที่จะถูกทำลายหรือได้รับความเสียหาย พนักงานสอบสวนที่ขาดความรู้ความเข้าใจในการรวบรวมพยานหลักฐานทางดิจิทัลจึงเลือกส่งสำนวนการสอบสวนมายังพนักงานอัยการเพื่อใช้ดุลพินิจในการสั่งสอบสวนเพิ่มเติมจะทำให้คดีเกิดความล่าช้าและได้รับความเสียหาย นอกจากนั้น ด้วยเหตุที่พนักงานสอบสวนมิใช่พนักงานเจ้าหน้าที่ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ในการสอบสวนหาผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พนักงานสอบสวนจึงต้องส่งหนังสือขอความร่วมมืออย่างเป็นทางการพร้อมส่งข้อมูลเบื้องต้นในคดีไปขอให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นผู้ดำเนินการตรวจสอบ ดังนั้น หากพนักงานสอบสวนขาดความรู้ความเข้าใจเบื้องต้นเกี่ยวกับการทำงานของระบบคอมพิวเตอร์หรือขาดความรู้ความเข้าใจเบื้องต้นเกี่ยวกับลักษณะของพยานหลักฐานที่จะต้องใช้ในการพิสูจน์การกระทำความผิดของผู้ต้องหา ก็อาจมิได้แจ้งข้อเท็จจริงที่เกี่ยวข้องให้กับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ทราบอย่างครบถ้วน อาทิเช่น URL ของเว็บไซต์ที่พบข้อความฉ้อโกง รวมถึงวิธีในการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้เสียหายจนพบเว็บไซต์ที่พบข้อความ เป็นเหตุให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มิอาจดำเนินการตรวจสอบได้ในทันที

๒.๒ ปัญหาด้านการสืบสวนสอบสวน

จากผลการวิจัยของกองวิจัย สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ (เอกสารวิจัย, ๒๕๕๙ : ข) ที่ทำการวิจัยกลุ่มตัวอย่างพนักงานสอบสวนจำนวน ๔๐๐ นาย และกลุ่มตัวอย่างเจ้าหน้าที่สืบสวน จำนวน ๔๐๐ นาย พบข้อมูลสำคัญดังนี้

๒.๒.๑ ในเรื่องความรู้ด้านเทคนิคการสืบสวนสอบสวนของผู้ปฏิบัติงาน

พบว่า ด้านสอบสวน โดยรวมอยู่ในระดับน้อย โดยในประเด็นเข้าใจความหมายของสิ่งต่าง ๆ และสิ่งที่ควรรู้เกี่ยวกับคอมพิวเตอร์ เช่น Hosting, ISP, Protocal, Log File, FTP มีค่าเฉลี่ยน้อยที่สุด ถือว่าเป็นปัญหาสำคัญ เพราะคำเหล่านี้ล้วนแต่เป็นหลักฐานทางอิเล็กทรอนิกส์เป็นข้อเท็จจริง ในมุมมองของการสอบสวนสามารถหาร่องรอยย้อนกลับได้ ถ้าไม่เข้าใจความหมายแล้วจะไม่สามารถนำมาวิเคราะห์ ตีความเป็นประโยชน์ต่อรูปคดีได้เลยและส่งผลให้กระบวนการสืบสวนสอบสวนด้อยประสิทธิภาพลงไป

ด้านสืบสวน โดยรวมอยู่ในระดับน้อย โดยในประเด็นเข้าใจความหมาย ของสิ่งต่าง ๆ และสิ่งที่ควรรู้เกี่ยวกับคอมพิวเตอร์ เช่น Hosting, ISP, Protocal, Log File, FTP มีค่าเฉลี่ยน้อยที่สุด ถือว่าเป็นปัญหาสำคัญ เช่นเดียวกับการสอบสวน เพราะคำเหล่านี้ เป็นพยานหลักฐานว่าใคร ทำอะไร ที่ไหน ในทางอาชญากรรมคอมพิวเตอร์ถ้าไม่เข้าใจจะไม่สามารถหาร่องรอยย้อนกลับได้

๒.๒.๒ ในเรื่องการรวบรวมพยานหลักฐาน พบว่า

ด้านสอบสวน ในส่วนของพยานหลักฐานทางอิเล็กทรอนิกส์มีค่าเฉลี่ยน้อยที่สุด ซึ่งถ้าพนักงานสอบสวนไม่เข้าใจและกระทำไปทั้งที่ไม่รู้ จะทำให้เกิดความเสียหายต่อรูปคดีได้

ด้านสืบสวน โดยรวมอยู่ในระดับน้อย โดยเฉพาะในประเด็น “การรักษาห่วงโซ่ของพยานหลักฐาน (Chain of Custody) ทางอิเล็กทรอนิกส์ว่า ณ เวลานั้นๆ พยานหลักฐานชิ้นนั้นอยู่ภายใต้ความครอบครองของใครมีค่าเฉลี่ยน้อยที่สุด เป็นปัญหาเพราะถ้าเจ้าหน้าที่สายสืบสวนไม่เข้าใจหลักการนี้ทำให้กระบวนการสืบสวนสอบสวนขาดความน่าเชื่อถือได้

๒.๒.๓ ในเรื่องการตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์ พบว่า

ทั้งด้านสอบสวน และด้านสืบสวน ประเด็นการกู้ข้อมูลที่ถูกลบออกไปแล้ว มีค่าเฉลี่ยน้อยที่สุดเป็นเพราะการกู้ข้อมูลที่ถูกลบออกไปแล้ว จำเป็นต้องใช้ผู้เชี่ยวชาญ พนักงานสอบสวนและเจ้าหน้าที่สายสืบอาจจะไม่สามารถกระทำได้ แต่บุคลากรทั้งสองกลุ่มควรจะต้องทราบว่าข้อมูลสามารถกู้ได้โดยผู้เชี่ยวชาญและเครื่องมือ

๒.๒.๔ ในเรื่องการปรับใช้กฎหมาย พบว่า

ทั้งด้านสอบสวน และด้านสืบสวน ส่วนใหญ่เห็นว่าตนเองมีปัญหาในการตีความบทบัญญัติของ พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น คำว่าข้อมูลคอมพิวเตอร์หมายความถึง “ข้อความ” ด้วย ข้อมูล “ลามกอนาจาร” ลักษณะอย่างไรเพียงใดจึงจะถือว่าเป็นการลามกอนาจาร หรือคำว่า “ก่อให้เกิดความตื่นตระหนกแก่ประชาชน” นั้นต้องมีพฤติการณ์ถึงขั้นไหนโดยส่วนมากมีความคิดเห็นอยู่ในระดับปานกลาง เป็นเพราะบทบัญญัติของกฎหมายบางอย่างไม่สามารถเขียนให้ทุกคนเข้าใจได้ คนที่จะเข้าใจได้ต้องมีความรู้ขั้นพื้นฐานทางคอมพิวเตอร์พอสมควร พนักงานสอบสวนอ่านพระราชบัญญัติว่าด้วยการกระทำความผิดทาง

คอมพิวเตอร์ พ.ศ. ๒๕๕๐ ในภาพรวม อาจยังไม่เข้าใจสารบัญญัติของข้อกฎหมายซึ่งผู้ปฏิบัติต้องเข้าใจข้อเท็จจริงทางเทคโนโลยี ที่สำคัญคือบุคลากรทั้งสองกลุ่มต้องมีองค์ความรู้ด้านคอมพิวเตอร์ในระดับที่เป็นผู้ใช้ (Users) ได้

ปัญหาเกี่ยวกับองค์ความรู้ของเจ้าหน้าที่สืบสวนและพนักงานสอบสวนดังกล่าวส่งผลทำให้เกิดความล่าช้าในการดำเนินคดี ดังที่ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๒๕๖๐) ได้ยกตัวอย่างคดีฉ้อโกงขายสินค้าทางเว็บไซต์กลางขายสินค้า บนเว็บไซต์ http://shopee.co.th ซึ่งเป็นเว็บไซต์สื่อกลางในการซื้อขายสินค้า คดีดังกล่าวเหตุเกิดเมื่อประมาณกลางเดือนกรกฎาคม ๒๕๕๙ แต่พนักงานสอบสวนส่งสำนวนการสอบสวนไปยังพนักงานอัยการในเดือนกันยายน ๒๕๕๙ โดยมิได้มีการสอบสวนในประเด็นเกี่ยวกับความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ แม้ว่า พนักงานอัยการจะมีคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมทันทีภายหลังจากที่ได้รับสำนวนการสอบสวนจากพนักงานสอบสวนก็ตาม แต่การสอบสวนเพิ่มเติมยังคงใช้เวลานานถึง ๖ เดือน ซึ่งเป็นระยะเวลาที่ล่าช้าอย่างมาก และเป็นสาเหตุโดยตรงที่ผู้ให้บริการอินเทอร์เน็ตไม่สามารถให้ข้อมูลที่เกี่ยวข้องได้ เนื่องจากผู้ให้บริการอินเทอร์เน็ตมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามกฎหมายเป็นระยะเวลาเพียง ๙๐ วัน

๒.๓ ปัญหาด้านการดำเนินคดีที่มีองค์ประกอบข้ามชาติ

ปัญหาเรื่องข้อจำกัดของพนักงานสอบสวนในการแสวงหาพยานหลักฐานสำคัญอีกประการหนึ่ง พบในคดีที่มีการกระทำความผิดข้ามพรมแดนหรืออีกนัยหนึ่งคือการกระทำผิดนอกราชอาณาจักร ซึ่งในกรณีทั่วไปการแสวงหาพยานหลักฐานซึ่งอยู่ภายนอกประเทศ ย่อมทำได้ยากและต้องอาศัยความร่วมมือระหว่างประเทศทางอาญาซึ่งมักมีขั้นตอนและกระบวนการซึ่งใช้ระยะเวลานานพอสมควรอาจมีข้อติดขัด อีกทั้งในเรื่องการติดต่อสื่อสารกับหน่วยงานในต่างประเทศในขณะที่ลำพังแต่เพียงการแสวงหาพยานหลักฐานภายในประเทศอาจทำให้ได้พยานหลักฐานแห่งคดีไม่สมบูรณ์ ในหลายกรณีพบว่าพนักงานสอบสวนไม่สามารถนำหมายเลขไอพีแอดเดรส (IP address) ของคนร้ายไปตรวจสอบข้อมูลได้ เนื่องจากการกระทำผิดส่วนใหญ่มักกระทำผ่านเฟซบุ๊ก แอพพลิเคชั่นไลน์ หรืออีเมล ซึ่งมีสถานที่ตั้งของ Server ที่ใช้จัดเก็บและเรียกประมวลผลข้อมูลอยู่ในต่างประเทศ ทำให้เกิดข้อขัดข้องไม่อาจขอข้อมูลผู้ใช้บริการได้ ทำให้ผู้ต้องหาที่พนักงานสอบสวนสามารถหาหลักฐานเอาผิดและนำตัวมาดำเนินคดีได้มีเพียงเจ้าของบัญชีผู้รับโอนเงินซึ่งเป็นปลายทางของขบวนการผู้กระทำความผิดหรือบางครั้งเป็นเพียงผู้รับจ้างเปิดบัญชีเท่านั้น ส่วนผู้กระทำผิดหลักที่เป็นผู้โพสต์ข้อความหลอกลวงผู้เสียหายในกรณีการฉ้อโกง พนักงานสอบสวนมักไม่สามารถติดตามหาหลักฐานเชื่อมโยงถึงผู้กระทำผิดได้ เนื่องจากหลักฐานดังกล่าวมักต้องอาศัยความร่วมมือจากผู้ให้บริการอินเทอร์เน็ตเกี่ยวกับข้อมูลผู้ใช้งาน รวมทั้งเมื่อได้ข้อมูลผู้ใช้งานแล้ว ก็มักไม่มีหลักฐานในลักษณะประจักษ์พยานที่จะยืนยันได้ว่า ผู้มีชื่อเป็นผู้ใช้บริการอินเทอร์เน็ตคนดังกล่าวเป็นผู้โพสต์ข้อความหลอกลวงผู้เสียหายเองหรือไม่ ปัญหาในการรวบรวมพยานหลักฐานในกรณีที่มีองค์ประกอบข้ามชาติ พนักงานสอบสวนอาจไม่ทราบว่าจะประสานการตรวจสอบต่อไปอย่างไร สามารถติดต่อได้เองหรือต้องผ่านผู้ประสานงานกลาง (อัยการสูงสุด) โดยพนักงานสอบสวนอาจขาดความเข้าใจเกี่ยวกับขั้นตอนการขอความร่วมมือทางอาญาระหว่างประเทศ (MLAT)

ในเรื่องนี้ เบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) ได้ยกตัวอย่างกรณีปัญหาและอุปสรรคสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นจริง ในกรณีคดีอาญาที่มีการกระทำความผิดผ่านเว็บไซต์เฟซบุ๊ก (www.facebook.com) ซึ่งมีผู้จดทะเบียนเว็บไซต์ และที่ตั้งของ Server อยู่ต่างประเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเคยมีหนังสือแจ้งตอบว่า เฟซบุ๊กเปิดตัวสำนักงาน Facebook ในประเทศไทย แต่ไม่ปรากฏข้อมูลการเปิดตัวว่าใครเป็น Head of Thailand และไม่ปรากฏข้อมูลที่ตั้งของสำนักงาน นอกจากนี้ Facebook Inc. ซึ่งเป็นผู้ให้บริการของบริการเฟซบุ๊ก มีถิ่นฐานอยู่ที่สหรัฐอเมริกา นอกราชอาณาจักรไทย อันเป็นข้อจำกัดในการสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บ หรือข้อมูลที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จึงไม่สามารถดำเนินการขอตรวจสอบข้อมูลจราจรคอมพิวเตอร์จากผู้ให้บริการได้

๒.๔ ปัญหาด้านการบูรณาการความร่วมมือและการประสานงานระหว่างหน่วยงาน

ด้วยเหตุที่ประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ขึ้นอยู่กับประสิทธิภาพของผู้บังคับใช้กฎหมายตั้งแต่ต้นทางถึงปลายทาง จากพนักงานสอบสวน ถึงพนักงานอัยการ ไปยังศาล ดังนั้น การแก้ไขปัญหาการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในแต่ละคดีจึงต้องอาศัยการบูรณาการความร่วมมือและการประสานงานระหว่างหน่วยงานและบุคคลากรด้านการสอบสวนและด้านการดำเนินคดี แต่ทว่า ในการดำเนินคดีอาญาทั่วไป (ยกเว้นแต่กรณีที่มีบทบัญญัติแห่งกฎหมายกำหนดไว้เป็นการเฉพาะ) อยู่ภายใต้โครงสร้างการถ่วงดุลอำนาจในกระบวนการยุติธรรมทางอาญาตามประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งกำหนดแยกอำนาจความรับผิดชอบในการสอบสวนออกจากการฟ้องและการดำเนินคดี จึงส่งผลให้การดำเนินคดีอาชญากรรมคอมพิวเตอร์อาจเกิดความล่าช้า กล่าวคือ ในบางกรณีมุมมองของพนักงานอัยการและของพนักงานสอบสวนอาจไม่ตรงกันในการพิจารณาว่าคดีมีพยานหลักฐานเพียงพอที่จะดำเนินคดีกับผู้ต้องหาหรือไม่ ทำให้พนักงานอัยการมีความจำเป็นต้องสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมเพื่อให้คดีมีพยานหลักฐานเพียงพอที่จะดำเนินคดีให้ศาลลงโทษจำเลยได้ ซึ่งระยะเวลาในการดำเนินการยิ่งมากเท่าใด ก็ย่อมส่งผลกระทบต่อความสมบูรณ์ของพยานหลักฐานทางดิจิทัลที่จะสามารถจัดเก็บได้มากเท่านั้น ซึ่งโครงสร้างการดำเนินคดีอาญาของไทยดังกล่าวจะแตกต่างจากโครงสร้างการดำเนินคดีอาญาในต่างประเทศ ดังที่จะได้กล่าวในหัวข้อต่อไป ทั้งนี้ เมื่อเปรียบเทียบกับในหลายประเทศที่พนักงานอัยการมีบทบาทใกล้ชิดในการเสนอแนะแนวทางการสอบสวนและการตั้งรูปคดีให้แก่พนักงานสอบสวนได้ตั้งแต่ในชั้นสืบสวนสอบสวน

แนวทางตามยุทธศาสตร์การตอบโต้อาชญากรรมคอมพิวเตอร์ในต่างประเทศ

๑ **สหรัฐอเมริกา** (Homeland Security, Online, 2016)

สหรัฐอเมริกาเป็นประเทศผู้นำทางด้านเทคโนโลยีในโลกไซเบอร์ มีแผนระดับชาติในการตอบโต้เหตุการณ์ด้านไซเบอร์ (National Cyber Incident Response Plan-NCIRP) ซึ่งแผน

ดังกล่าวแม้จะไม่มีลักษณะเป็นแผนเชิงปฏิบัติการ แต่มีการกำหนดกรอบยุทธศาสตร์เบื้องต้นเพื่อสร้างความเข้าใจให้กับผู้มีส่วนได้เสียเกี่ยวข้อง เกี่ยวกับบทบาทของหน่วยงานระดับสหพันธรัฐที่มีการจัดให้มีปฏิบัติการสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ เช่น การกำหนดให้กระทรวงยุติธรรม (The Department of Justice) เป็นหน่วยงานหลักที่มีบทบาทในการตอบโต้ภัยคุกคามด้านไซเบอร์ โดยดำเนินงานผ่านสำนักสืบสวนระดับสหพันธรัฐและหน่วยงานสืบสวนทางไซเบอร์ระดับชาติ (The Federal Bureau of Investigations and National Cyber Investigative Joint Task Force) ซึ่งมีอำนาจหน้าที่สืบสวน เก็บรวบรวมพยานหลักฐาน จำแนกประเภทภัยคุกคาม บังคับใช้แผนงานในการลดภัยคุกคาม อำนวยการแลกเปลี่ยนข้อมูลและความร่วมมือที่เกี่ยวข้อง โดยกำหนดให้สำนักงานอัยการสูงสุดซึ่งสังกัดอยู่ในกระทรวงยุติธรรมของสหรัฐอเมริกาเป็นหน่วยงานสำคัญที่มีบทบาทในการตอบโต้อาชญากรรมคอมพิวเตอร์ ร่วมกับหน่วยงานสืบสวนกลางระดับสหพันธรัฐ หรือ FBI โดยพนักงานอัยการสหรัฐอเมริกาจะมีการทำงานในเชิงรุกควบคู่ไปกับการทำงานของเจ้าพนักงานสืบสวนและพนักงานสอบสวน โดยเริ่มตั้งแต่การให้คำปรึกษาเกี่ยวกับการรวบรวมพยานหลักฐานในชั้นสอบสวนอย่างใกล้ชิดเพื่อให้รูปคดีในชั้นสอบสวนครบถ้วนสมบูรณ์และมีพยานหลักฐานเพียงพอที่พนักงานอัยการจะดำเนินคดีกับผู้ต้องหา

๒ เครือรัฐออสเตรเลีย (Attorney-General's Department, Online, 2016)

ในส่วนของเครือรัฐออสเตรเลียที่มีการประกาศใช้แผนระดับชาติในการต่อสู้กับอาชญากรรมคอมพิวเตอร์ (National Plan to Combat Cybercrime) กำหนดทิศทางยุทธศาสตร์สำหรับหน่วยงานที่เกี่ยวข้องทั้งในระดับรัฐบาลท้องถิ่น รัฐ และเครือรัฐ โดยมีการกำหนดเครือข่ายออนไลน์เพื่อการรายงานอาชญากรรมคอมพิวเตอร์ (The Australian Cybercrime Online Reporting Network – ACORN) ซึ่งฐานข้อมูลของ ACORN จะมีส่วนช่วยในการกำหนดมาตรการเชิงนโยบายและเชิงปฏิบัติการเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ด้วย แผนระดับชาติดังกล่าวได้กำหนดหลักการสำคัญและเรื่องที่มีความสำคัญเร่งด่วนที่จะต้องดำเนินการในระยะสั้นถึงระยะกลาง อาทิเช่น การให้ความรู้แก่สังคมในการป้องกันตนเอง การส่งเสริมการมีส่วนร่วมของภาคอุตสาหกรรมในการต่อสู้ปัญหาอาชญากรรมคอมพิวเตอร์ การปรับปรุงความสามารถของหน่วยงานรัฐโดยเฉพาะอย่างยิ่งหน่วยงานผู้บังคับใช้กฎหมายในการดำเนินการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ การสร้างความมั่นใจในกรอบงานยุติธรรมทางอาญาที่มีประสิทธิภาพโดยให้ความสำคัญกับการให้ความรู้แก่พนักงานอัยการและเจ้าพนักงานในกระบวนการยุติธรรมในงานด้านพยานหลักฐานดิจิทัล และการปรับปรุงบทบัญญัติแห่งกฎหมายและกำหนดบทลงโทษให้เหมาะสมกับการตอบโต้อาชญากรรมคอมพิวเตอร์ โดยจะเห็นได้ว่า ความโดดเด่นของแผนงานตอบโต้อาชญากรรมคอมพิวเตอร์ของเครือรัฐออสเตรเลียนั้น คือ การจัดทำแผนงานระดับชาติซึ่งมีการกำหนดทิศทางยุทธศาสตร์สำหรับหน่วยงานที่เกี่ยวข้องกับกระบวนการยุติธรรมอย่างชัดเจน ในเชิงบูรณาการระหว่างหน่วยงานของรัฐและการส่งเสริมการมีส่วนร่วมของภาคเอกชน และที่สำคัญคือ มีแผนงานที่ชัดเจนเพื่อสร้างองค์ความรู้ด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์ให้แก่พนักงานอัยการและเจ้าพนักงานอื่นๆ ในกระบวนการยุติธรรมไปพร้อมๆ กัน

๓ สาธารณรัฐสิงคโปร์ (Cyber Security Agency, Online, 2016)

สาธารณรัฐสิงคโปร์เป็นประเทศที่นำระบบคอมพิวเตอร์มาขับเคลื่อนระบบเศรษฐกิจและสังคมในประเทศอย่างเข้มข้น ตามที่รู้จักกันในชื่อของ “Smart City” หรือ “Smart Nation” โดยนายลีเซียงลุง นายกรัฐมนตรีสิงคโปร์ ได้ให้ความสำคัญต่อการสร้างความมั่นคงปลอดภัยทางไซเบอร์อย่างมาก กล่าวคือ ในปี ๒๕๕๙ ที่ผ่านมา สาธารณรัฐสิงคโปร์ได้ประกาศใช้ยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Singapore’s Cybersecurity Strategy) และจัดตั้งหน่วยงานเฉพาะในชื่อ “หน่วยงานด้านความมั่นคงทางไซเบอร์แห่งสิงคโปร์” (Cyber Security Agency of Singapore) เป็นหน่วยงานผู้รับผิดชอบโดยตรง นอกจากนี้ ในเดือนกรกฎาคม ๒๕๕๙ Ministry of Home Affairs (เทียบเคียงได้กับกระทรวงมหาดไทย) ได้ออกแผนปฏิบัติการด้านอาชญากรรมคอมพิวเตอร์ระดับชาติ หรือ National Cybercrime Action Plan - NCAP ซึ่งกำหนดแผนปฏิบัติการรวม ๔ ด้าน ได้แก่ ๑. Educating and empowering the public to stay safe in cyberspace คือ การให้ความรู้แก่ประชาชนเกี่ยวกับความเสี่ยงของอาชญากรรมคอมพิวเตอร์พร้อมบังคับใช้มาตรการอย่างง่ายในการป้องกันอาชญากรรมคอมพิวเตอร์เพื่อรักษาความปลอดภัยของข้อมูลของประชาชนในโลกไซเบอร์ โดยสาธารณรัฐสิงคโปร์มีหน่วยงานตำรวจ (Singapore Police Force) ซึ่งจะแบ่งปันข้อมูลเกี่ยวกับการป้องกันอาชญากรรมคอมพิวเตอร์ให้แก่ประชาชนผ่านสื่อหลากหลายช่องทาง ทั้งทีวี หนังสือพิมพ์ โปสเตอร์ และช่องทางสังคมออนไลน์ รวมไปถึงการแจ้งเตือนการหลอกลวงผ่านระบบคอมพิวเตอร์ (Scam) ๒. Enhancing Government’s capacity and capability to combat cybercrime ได้แก่ การพัฒนากลไกความสามารถในการตอบโต้อาชญากรรมคอมพิวเตอร์ ด้วยการสร้างความร่วมมือระหว่างหน่วยงานตำรวจ (Singapore Police Force) กับหน่วยงานภาครัฐอื่น โดยหลายปีที่ผ่านมา หน่วยงานตำรวจ (Singapore Police Force) และสำนักงานอัยการสูงสุดของสาธารณรัฐสิงคโปร์ได้ทำงานร่วมกันอย่างใกล้ชิดในคดีอาชญากรรมคอมพิวเตอร์ที่สำคัญตั้งแต่ในชั้นสืบสวน โดยสำนักงานอัยการสูงสุดจะเป็นหน่วยงานที่มีความเชี่ยวชาญในการให้คำแนะนำในเรื่องของความเพียงพอของพยานหลักฐานสำคัญที่ตำรวจจะต้องทำการสืบสวนสอบสวนเพื่อใช้พิสูจน์การกระทำความผิดในคดีอาชญากรรมคอมพิวเตอร์ ๓. Strengthening legislation and the criminal justice framework คือ การสร้างความเข้มแข็งด้านกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ โดยการสืบสวนและการฟ้องคดีอาชญากรรมคอมพิวเตอร์จะต้องได้รับการสนับสนุนจากกรอบงานยุติธรรมทางอาญาที่เข้มแข็งจริงจัง และจะต้องมีการปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้องเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ประเภทใหม่ๆ ในปัจจุบัน และ ๔. Stepping up partnerships and international engagement คือ การสร้างหุ้นส่วนความร่วมมือเพื่อการตอบโต้อาชญากรรมคอมพิวเตอร์ทั้งในระดับภายในและระหว่างประเทศ และบูรณาการระหว่างหน่วยงานบังคับใช้กฎหมาย ซึ่งเมื่อประมาณเดือนตุลาคม ๒๕๕๙ สำนักงานอัยการสูงสุดแห่งสาธารณรัฐสิงคโปร์ได้จัดการประชุมโต๊ะกลม (Roundtable Meeting) ซึ่งจัดควบคู่กับงานสัปดาห์ไซเบอร์ซึ่งมีรัฐบาลสาธารณรัฐสิงคโปร์เป็นเจ้าภาพ (Singapore International Cyber Week 2016) โดยเชิญผู้แทนสำนักงานอัยการจากกลุ่มประเทศอาเซียนซึ่งรวมถึงผู้แทนสำนักงานอัยการไทย เพื่อแลกเปลี่ยนข้อมูล สถิติ สถานการณ์และรูปแบบของอาชญากรรมคอมพิวเตอร์ รวมถึงตัวอย่างคดีที่ประสบความสำเร็จและอุปสรรคในการดำเนินคดีในชั้นศาล ซึ่งสะท้อนให้เห็นถึง

ยุทธศาสตร์การสร้างความร่วมมือและแลกเปลี่ยนข้อมูลระหว่างสำนักงานอัยการสูงสุดในภูมิภาคอาเซียนเพื่อตอบโต้ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ ซึ่งมีลักษณะเป็นอาชญากรรมข้ามชาติหรืออาชญากรรมที่มีผลกระทบต่อสภาพเศรษฐกิจโดยรวมของภูมิภาคอาเซียน

ข้อสังเกตประการหนึ่งเมื่อเปรียบเทียบยุทธศาสตร์ในการตอบโต้อาชญากรรมข้ามชาติของไทยกับของต่างประเทศ คือ ความแตกต่างของระบบกฎหมายของไทยซึ่งใช้ระบบกฎหมาย Civil Law ในขณะที่ระบบกฎหมายของประเทศตัวอย่างข้างต้นใช้ระบบกฎหมาย Common Law โดยหนึ่งในความแตกต่างคืออำนาจการสอบสวนของพนักงานอัยการ ซึ่งระบบกฎหมายของไทยในคดีอาญาทั่วไปเป็นระบบกล่าวหา แยกอำนาจหน้าที่ในการสอบสวนให้เป็นของพนักงานสอบสวน ส่วนพนักงานอัยการมีอำนาจในชั้นของการพิจารณาพยานหลักฐานเมื่อพนักงานสอบสวนรวบรวมมาแล้ว โดยพนักงานอัยการจะพิจารณามีคำสั่งฟ้อง คำสั่งไม่ฟ้อง หรือคำสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติม คงมีเพียงคดีบางลักษณะที่มีบทกฎหมายเฉพาะที่บัญญัติให้อำนาจพนักงานอัยการเป็นพนักงานสอบสวนร่วมกับเจ้าพนักงานตำรวจ เช่น คดีความผิดที่ได้กระทำลงนอกราชอาณาจักร และคดีที่มีการกระทำผิดโดยองค์กรอาชญากรรมข้ามชาติ เป็นต้น ซึ่งเป็นแนวคิดที่แยกการทำงานของเจ้าพนักงานในชั้นสอบสวนออกจากเจ้าพนักงานในชั้นฟ้องคดี เพื่อให้เกิดการถ่วงดุลและดำเนินคดีอย่างรอบคอบ แต่ในลักษณะของการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีลักษณะพิเศษจากคดีอาชญากรรมทั่วไปดังที่กล่าวไว้ในบทที่ ๓ ซึ่งคดีอาชญากรรมคอมพิวเตอร์ต้องอาศัยพยานหลักฐานทางดิจิทัลเป็นพยานหลักฐานสำคัญในการพิสูจน์หาผู้กระทำความผิด โดยพยานหลักฐานทางดิจิทัลนี้มีความเสี่ยงตามกาลเวลาที่จะสูญหาย หรือถูกทำให้ปนเปื้อนจนมิอาจรับฟังได้ ซึ่งมีความจำเป็นต้องรวบรวมพยานหลักฐานทางดิจิทัลให้ครบถ้วนเพียงพอในการดำเนินคดีกับผู้กระทำความผิดโดยเร็วที่สุด ดังนั้น จุดอ่อนซึ่งถือเป็นปัญหาในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามที่พนักงานอัยการผู้ทรงคุณวุฒิในด้านงานคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์ได้ให้ความเห็นไว้ในแบบสัมภาษณ์เชิงลึกของเอกสารวิจัยนี้ว่า เมื่อพนักงานสอบสวนเห็นว่าการสอบสวนของตนเสร็จสิ้นแล้วก็จะส่งสำนวนการสอบสวนพร้อมความเห็นทางคดีมายังพนักงานอัยการ แต่เมื่อพนักงานอัยการพิจารณาแล้วเห็นว่า พนักงานสอบสวนยังสอบสวนไม่ครบถ้วนสมบูรณ์และส่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมให้ได้พยานหลักฐานทางดิจิทัลสำคัญบางประการ แต่ปรากฏว่าระยะเวลาล่วงเลยกว่าที่ผู้ให้บริการทางอินเทอร์เน็ตมีหน้าที่จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามที่กฎหมายกำหนดจึงไม่สามารถทำการสอบสวนเพิ่มเติมต่อได้

ดังนั้นแล้ว เมื่อประเทศไทยกำลังมุ่งพัฒนาเศรษฐกิจดิจิทัลตามนโยบายประเทศไทย ๔.๐ การสร้างความเชื่อมั่นในความมั่นคงปลอดภัยทางไซเบอร์ถือได้ว่าเป็นวาระที่สำคัญซึ่งไม่อาจมองข้าม เพื่อให้การเติบโตของระบบเศรษฐกิจดิจิทัลเป็นไปโดยมั่นคงและยั่งยืน ตัวอย่างแนวทางยุทธศาสตร์การตอบโต้อาชญากรรมคอมพิวเตอร์ในกลุ่มประเทศชั้นนำทางเทคโนโลยีข้างต้นที่สำนักงานอัยการไทยอาจนำมาปรับใช้เป็นแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด คือ การพัฒนาองค์ความรู้ของพนักงานอัยการผู้ปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์ให้ทันต่อสภาพการณ์ปัจจุบัน และการสร้างความร่วมมืออย่างบูรณาการกับหน่วยงานผู้บังคับใช้กฎหมายอื่นๆ เพื่อให้สอดคล้องกับทิศทางแผนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับชาติ

กำหนดแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด

แผนยุทธศาสตร์ในระดับสำนักงานอัยการสูงสุดซึ่งเผยแพร่ในเว็บไซต์ของสำนักงานอัยการพิเศษฝ่ายนโยบายและยุทธศาสตร์ ประกอบด้วย

๑. แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒

๒. แผนปฏิบัติการสำนักงานอัยการสูงสุด ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ (Action Plan)

๓. แผนแม่บทด้านการส่งเสริมความเสมอภาคระหว่างหญิงชาย สำนักงานอัยการสูงสุด

๔. แผนปฏิบัติการด้านการส่งเสริมความเสมอภาคระหว่างหญิงชาย สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๘

๕. แผนปฏิบัติการป้องกันและปราบปรามการทุจริต สำนักงานอัยการสูงสุด ประจำปีงบประมาณ พ.ศ. ๒๕๖๐

โดยแผนยุทธศาสตร์หลักซึ่งสะท้อนทิศทางในบริหารงานคดีของสำนักงานอัยการสูงสุด คือ แผนตาม ข้อ ๑. และข้อ ๒. ข้างต้น

จากการที่การกำหนดยุทธศาสตร์และแผนปฏิบัติราชการของหน่วยงานภาครัฐจำเป็นต้องสอดคล้องกับแผนยุทธศาสตร์ชาติซึ่งเป็นกรอบภาพรวมของการจัดทำนโยบายและการจัดสรรงบประมาณของรัฐบาล รวมไปถึงต้องสอดคล้องกับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ โดยแผนยุทธศาสตร์ของหน่วยงานภาครัฐเป็นสิ่งที่สะท้อนให้เห็นถึงทิศทางหรือแนวทางปฏิบัติตามพันธกิจและภารกิจ (Mission) ให้สัมฤทธิผลตามวิสัยทัศน์ (Vision) และเป้าประสงค์ขององค์กร (Goal) แผนยุทธศาสตร์ที่ดีนั้นจึงควรต้องถูกกำหนดขึ้นตามวิสัยทัศน์ขององค์กร อันเป็นผลผลิตทางความคิดร่วมกันของสมาชิกในองค์กรที่ได้ทำงานร่วมกันหรือจะทำงานร่วมกัน โดยวิสัยทัศน์นี้เป็นความเห็นพ้องต้องกันว่าเป็นจุดหมายปลายทางที่องค์กรประสงค์จะไปให้ถึง และวิสัยทัศน์นี้มีการแปลงออกมาเป็นวัตถุประสงค์ (Objective) ที่เป็นรูปธรรม และสามารถวัดได้ ทั้งนี้ องค์กรสามารถใช้แผนยุทธศาสตร์เป็นกรอบในการประเมินผลงานประจำปีงบประมาณ ยิ่งไปกว่านั้นองค์กรยังสามารถใช้แผนยุทธศาสตร์เป็นกรอบในการจัดทำแผนปฏิบัติการ (Action Plan) เพื่อการจัดทำงบประมาณรายจ่ายประจำปีได้อีกด้วย (จักษวัชร ศิริวรรณ, ออนไลน์, ๒๕๖๐) ดังนั้น โดยสภาพและลักษณะของการกำหนดแผนยุทธศาสตร์และแผนปฏิบัติราชการของสำนักงานอัยการสูงสุดดังกล่าวมาข้างต้น ประกอบกับลักษณะของคดีอาชญากรรมคอมพิวเตอร์ซึ่งมิได้ถูกกำหนดให้อยู่ในอำนาจหน้าที่ของสำนักงานคดีใดสำนักงานคดีหนึ่งของสำนักงานอัยการสูงสุดโดยเฉพาะ โดยโครงสร้างอำนาจหน้าที่ของสำนักงานคดีภายในสำนักงานอัยการสูงสุดแบ่งแยกความรับผิดชอบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามลักษณะความผิดฐานหลักที่เกี่ยวข้องหรือตามอำนาจการสอบสวนของพนักงานสอบสวนในคดี จึงทำให้แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุดมิได้ระบุถึงแผนงานในการตอบโต้อาชญากรรมคอมพิวเตอร์ในรายละเอียดเพื่อเป็นแนวทางการปฏิบัติงานของพนักงานอัยการระดับผู้ปฏิบัติงานคดี แต่แผนงานในการตอบโต้อาชญากรรมคอมพิวเตอร์จะแฝงอยู่ในกรอบโครงการประเภทของโครงการเพิ่มศักยภาพในการดำเนินคดีของพนักงานอัยการของสำนักงานคดีที่เกี่ยวข้อง โดยแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปี (Action Plan) ในปัจจุบัน ไม่เกี่ยวข้องกับ

การดำเนินคดีอาชญากรรมคอมพิวเตอร์ของผู้ปฏิบัติงานโดยตรง เพราะมิได้มีการกำหนดแนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์สำหรับผู้ปฏิบัติงาน แต่แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปี (Action Plan) ในปัจจุบัน มีลักษณะเกี่ยวพันกับการจัดสรรงบประมาณของสำนักงานคดีภายในสำนักงานอัยการสูงสุดเท่านั้น โดยโครงการหรือกิจกรรมที่ได้รับการจัดสรรงบประมาณที่ระบุไว้ในเอกสารดังกล่าวยังมิได้ลงรายละเอียดให้เห็นถึงทิศทางในการพัฒนางานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด

สุดเขต เพิ่มผล (สัมภาษณ์, ๒๑ มีนาคม ๒๕๖๐) ผู้ช่วยเลขานุการรองอัยการสูงสุด (นายนิตสิต ระเบียบธรรม) ซึ่งดูแลงานของสำนักงานนโยบาย ยุทธศาสตร์ และงบประมาณ ของสำนักงานอัยการสูงสุด และวัฒนพงศ์ วงศ์ใหญ่ (สัมภาษณ์, ๒๒ เมษายน ๒๕๖๐) เลขานุการผู้ตรวจการอัยการ (นายวัฒนชัย คุ้มวงศ์ดี) เห็นสอดคล้องกันว่า สำนักงานอัยการสูงสุดยังไม่มีโครงการที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ไว้เป็นการเฉพาะ แต่เห็นว่าในแผนปฏิบัติการสำนักงานอัยการสูงสุด ประจำปี ๒๕๖๐ โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญาที่มีกิจกรรมเพิ่มศักยภาพในการปฏิบัติงานด้านคดี (เน้นเฉพาะการเปิดเสรีด้านการเงิน) เมื่อเข้าสู่ประชาคมเศรษฐกิจอาเซียน (AEC) ที่มีสำนักงานคดีพิเศษเป็นหน่วยงานรับผิดชอบนั้น เป็นโครงการที่น่าจะมีเนื้อหาที่เกี่ยวข้องกับการกระทำความผิดทางการเงิน ซึ่งในปัจจุบันนี้การทำธุรกรรมทางการเงินนั้นได้ทำโดยใช้คอมพิวเตอร์ อินเทอร์เน็ตในการดำเนินการแทบทั้งสิ้น ซึ่งสุดเขต เพิ่มผล (สัมภาษณ์, ๒๑ มีนาคม ๒๕๖๐) เห็นว่า ควรจะมีโครงการเพิ่มศักยภาพเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ไว้เป็นการเฉพาะด้วย โดยแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา ในโครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญา ที่มีกิจกรรมเพิ่มศักยภาพในการปฏิบัติงานด้านคดี (เน้นเฉพาะการเปิดเสรีด้านการเงิน) เมื่อเข้าสู่ประชาคมเศรษฐกิจอาเซียน (AEC) นั้น น่าจะเป็นองค์ความรู้ส่วนหนึ่งที่เป็นประโยชน์ต่องานคดีอาชญากรรมคอมพิวเตอร์ได้ แต่องค์ความรู้ในโครงการดังกล่าวที่เน้นแต่เฉพาะในด้านการเปิดเสรีด้านการเงินน่าจะยังไม่เพียงพอที่จะใช้ในการปฏิบัติงานเกี่ยวกับคดีอาชญากรรมทางคอมพิวเตอร์ เนื่องจากคดีอาชญากรรมทางคอมพิวเตอร์ไม่ได้มีแต่เฉพาะเรื่องที่เกี่ยวกับการเงินเท่านั้น เพราะยังมีเรื่องของการกระทำผิดเกี่ยวกับการนำเข้าข้อมูลคอมพิวเตอร์ในการกระทำละเมิดลิขสิทธิ์ การแพร่ภาพข้อมูลที่มีลักษณะลามกอนาจารซึ่งโครงการดังกล่าวไม่มีเนื้อหาครอบคลุมถึงที่จะรองรับต่อคดีอาชญากรรมคอมพิวเตอร์ทุกเรื่องได้

การปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ภายหลังจากที่รัฐบาลได้ส่งเสริมนโยบายประเทศไทย ๔.๐ มีความจำเป็นต้องปรับปรุงกลไกขับเคลื่อนในรูปแบบยุทธศาสตร์หลักตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ และรูปแบบยุทธศาสตร์คู่ขนาน ด้วยมาตรการอื่นๆเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ที่คาดว่าจะเกิดขึ้น โดยมีแนวทางดังนี้

๑. แนวทางการปรับปรุงแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด

๑.๑ ด้านความพร้อมด้านข้อมูลสนับสนุนการจัดทำยุทธศาสตร์

การเก็บสถิติอาชญากรรมของหน่วยงานย่อมมีประโยชน์ในการเป็นตัวบ่งชี้ระดับความรุนแรงและจำนวนอาชญากรรมแต่ละประเภทในแต่ละพื้นที่ นอกจากนี้ ข้อมูลสถิติอาชญากรรมยังมีประโยชน์ในภาพรวมเพื่อวัดระดับประสิทธิภาพในการบังคับใช้กฎหมาย เพื่อการวางแผนและจัดลำดับความสำคัญในการแก้ปัญหาอาชญากรรมรวมถึงการประเมินสถานการณ์และแนวโน้มของการเกิดอาชญากรรมที่คาดว่าจะเกิดขึ้นในอนาคต โดยวิเคราะห์จากข้อมูลสถิติคดีที่เกิดขึ้นตั้งแต่อดีตถึงปัจจุบัน เพื่อประโยชน์ในการจัดเตรียมงบประมาณของหน่วยงาน และเพื่อเป็นแหล่งข้อมูลที่เป็นประโยชน์แก่หน่วยงานในการกำหนดแนวทางเพื่อเตรียมพร้อมในการจัดการกับอาชญากรรมที่เกิดขึ้น (วิทยา สุริยะวงค์, ๒๕๕๒) ปัจจุบันสภาพสังคมมีการเปลี่ยนแปลงอย่างรวดเร็ว การใช้สถิติคดีมาพิจารณาประกอบการวางแผนบริหารจัดการองค์กร จึงมีความสำคัญสำหรับผู้บริหารองค์กรทำให้สามารถคาดการณ์ประเภทและปริมาณคดีในอนาคตได้ นอกจากนี้ ในกระบวนการจัดเก็บสถิติอาชญากรรมควรมีการสังเคราะห์ข้อมูลทางสถิติให้มีความเหมาะสมต่อการนำไปใช้พิจารณาประกอบการวางแผนบริหารจัดการองค์กรด้วย โดยสถิติคดีแต่ละประเภทที่อยู่ในความรับผิดชอบของสำนักงานอัยการสูงสุดมีความเกี่ยวข้องหรือมีความสำคัญในการจัดทำแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปีโดยตรง กล่าวคือ ในการจัดทำโครงการหรือกิจกรรมภายในกรอบเงินงบประมาณขององค์กรที่มีอยู่อย่างจำกัดให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดนั้นย่อมสมควรต้องพิจารณาถึงสถิติคดีประกอบด้วย โดยหากปริมาณคดีประเภทใดมีแนวโน้มที่จะเพิ่มมากขึ้นอย่างต่อเนื่อง ก็เป็นเรื่องที่สำนักงานอัยการสูงสุดควรจะต้องให้ความสำคัญ เพราะเป็นผลกระทบต่อสังคมโดยส่วนรวม เป็นต้น

อย่างไรก็ดี ทั้งที่สถิติเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการมีความเกี่ยวข้องหรือมีความสำคัญในการกำหนดแนวนโยบายผู้บริหาร แผนยุทธศาสตร์ และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุดอย่างมาก แต่จากการทบทวนวรรณกรรมข้อมูลการจัดทำยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ ในบทที่ ๒ หัวข้อแนวคิดและทฤษฎีการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด พบว่า ในการจัดทำยุทธศาสตร์สำนักงานอัยการสูงสุดดังกล่าวใช้วิธีการศึกษาในเชิงคุณภาพแบบผสมผสาน ประกอบด้วย การทบทวนวรรณกรรมที่เกี่ยวข้อง การสัมภาษณ์เชิงลึกผู้บริหารระดับสูงของสำนักงานอัยการสูงสุด สอบถามความคิดเห็นของบุคคลากรในสำนักงานอัยการสูงสุดด้วยแบบสอบถามและแบบสอบถามออนไลน์ การจัดประชุมและสัมมนาองค์ความรู้และประชุมเชิงปฏิบัติการ และการสัมมนาเพื่อรับฟังความคิดเห็น โดยในส่วนของข้อมูลด้านสถิติคดีอาญา (โดยเฉพาะอาชญากรรมคอมพิวเตอร์) พบว่า ยังมิใช่เครื่องมือสำคัญที่ถูกนำไปใช้บ่งบอกแนวโน้มสถานการณ์ของคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันเพื่อประยุกต์ใช้ในการจัดทำแผนงานเพื่อรับมือกับภัยอาชญากรรมคอมพิวเตอร์โดยตรง โดยการรวบรวมสถิติเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการของสำนักงานอัยการสูงสุดควรมีการรวบรวมที่รอบด้านมิใช่เป็นการรวบรวมที่มีจุดประสงค์เพียงเพื่อทราบปริมาณงานคดีในแต่ละปี แต่ควรมีการจัดเก็บข้อมูลเชิงคุณภาพด้วย เช่น สถิติดังกล่าวควรมีการแยกประเภทของอาชญากรรมคอมพิวเตอร์ (กระทำต่อระบบคอมพิวเตอร์ หรือใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด), ผลคดี (สั่งฟ้อง-สั่งไม่ฟ้อง, ลงโทษ-ยกฟ้อง) เพื่อใช้เป็นข้อมูลประกอบในการจัดทำยุทธศาสตร์เฉพาะ

เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในโอกาสข้างหน้า (เบญจพร วัชระวุฒิชัย, สัมภาษณ์ , ๙ มีนาคม ๒๕๖๐ ; สมรัตน์ สุขคะ, สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐)

นอกจากนี้ สุภกิตต์ โสตถิทัต (สัมภาษณ์, ๒๒ เมษายน ๒๕๖๐) ซึ่งเป็นผู้ช่วยเลขานุการผู้ตรวจการอัยการ (นายวัฒนชัย คุ้มวงศ์ดี) และเป็นคณะทำงานตามคำสั่งสำนักงานอัยการสูงสุดที่ ๑๗๐/๒๕๕๓ ร่วมสอบสวนคดีความผิดที่มีโทษตามกฎหมายไทยที่ได้กระทำลงนอกราชอาณาจักรกับพนักงานสอบสวนกรณีเว็บไซต์หมิ่นสถาบัน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประมวลกฎหมายอาญา มาตรา ๑๑๒ ได้เสนอความเห็นเพิ่มเติมว่า ในปัจจุบันคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะคดีเว็บไซต์หมิ่นสถาบัน เป็นคดีนโยบายที่มีความสำคัญกระทบต่อความมั่นคงของประเทศซึ่งรัฐบาลและคณะรักษาความสงบแห่งชาติติดตามตรวจสอบคดีประเภทดังกล่าวมาโดยตลอด ดังนั้น สำนักงานอัยการสูงสุดจึงมีความจำเป็นต้องจัดเก็บข้อมูลสถิติคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการไว้เพื่อเป็นส่วนหนึ่งของแผนยุทธศาสตร์ เนื่องจากในอนาคตย่อมมีความจำเป็นในการใช้ข้อมูลสถิติดังกล่าวบูรณาการความร่วมมือกับหน่วยงานราชการที่เกี่ยวข้องแห่งอื่นด้วย

ทั้งนี้ จากการศึกษาแนวทางการจัดเก็บสถิติข้อมูลคดีอาชญากรรมคอมพิวเตอร์ผ่านการบันทึกสารบบคดีของสำนักงานอัยการสูงสุดสำหรับคดีที่มีความเกี่ยวพันกับฐานความผิดหลายอย่าง ตามตารางที่ ๓-๒ ดังที่กล่าวไว้ในบทที่ ๓ พบปัญหาว่า เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดจะเลือกบันทึกรายการคดีโดยยึดฐานความผิดบทที่มีอัตราโทษสูงที่สุดเพียงรายการเดียวต่อ ๑ สำนวนคดี ตัวอย่างเช่น คดีที่ผู้ต้องหากระทำความผิดฐานปลอมเอกสารสิทธิอันเป็นเอกสารราชการและฉ้อโกงประชาชน ตามประมวลกฎหมายอาญาและความผิดฐานนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลอันเป็นเท็จ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) กรณีเช่นว่านี้ เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดจะบันทึกสถิติคดีนี้เพียงในช่องรายการ “ประเภทคดี ๑๖ ความผิดเกี่ยวกับเอกสาร มาตรา ๒๖๔ – ๒๖๙” เนื่องจากความผิดที่มีอัตราโทษสูงสุดในสำนวนคดีนี้คือ ความผิดฐานปลอมเอกสารสิทธิอันเป็นเอกสารราชการตามประมวลกฎหมายอาญา จึงทำให้การลงบันทึกสถิติคดีอาญากรณีข้างต้นไม่ได้สะท้อนเห็นถึงข้อมูลสถิติคดีอาชญากรรมคอมพิวเตอร์ประเภทคอมพิวเตอร์ถูกใช้เป็นเครื่องมือประกอบอาชญากรรม (Computer as Tools) โดยเฉพาะเจาะจง หรือกรณีการกระทำความผิดโดยมีคอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets) อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) ซึ่งไม่ตรงกับรายการประเภทคดีลำดับที่ ๑ – ๖๒ ของตารางที่ ๓-๒ เจ้าหน้าที่ธุรการผู้บันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดก็จะบันทึกสถิติคดีในช่องรายการ “ประเภทคดี ๖๓ ความผิดอื่นๆ” การลงบันทึกสถิติคดีอาญาเช่นว่านี้จึงอาจไม่ได้สะท้อนสถิติคดีอาชญากรรมคอมพิวเตอร์อย่างเฉพาะเจาะจงเช่นเดียวกัน เนื่องจากรายการ “ประเภทคดี ๖๓ ความผิดอื่นๆ” นอกจากหมายรวมถึงความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) แล้ว ยังรวมไปถึงความผิดตามพระราชบัญญัติอื่นๆ ซึ่งมีอยู่เป็นจำนวนมากในปัจจุบัน

ดังนั้น ผู้วิจัยจึงเห็นว่าแนวทางเพื่อสร้างความพร้อมด้านข้อมูลสนับสนุนการจัดทำยุทธศาสตร์ ได้แก่ การปรับปรุงแนวทางการปรับปรุงการจัดเก็บสถิติข้อมูลงานคดีที่เกี่ยวพันกับอาชญากรรมคอมพิวเตอร์ เพื่อสร้างความพร้อมด้านข้อมูลสนับสนุนการจัดทำยุทธศาสตร์และประมาณการงบประมาณให้เหมาะสม และตรงตามสภาพของสังคมภายหลังจากที่รัฐบาลมีการส่งเสริมนโยบายประเทศไทย ๔.๐ ซึ่งพบว่า แนวโน้มความรุนแรงของอาชญากรรมคอมพิวเตอร์จะเพิ่มสูงขึ้นตามปริมาณการใช้งานระบบคอมพิวเตอร์ อีกทั้งเพื่อเป็นการบูรณาการด้านความร่วมมือทางข้อมูลกับหน่วยงานรัฐแห่งอื่น โดยสำนักงานอัยการสูงสุดควรมีการทบทวนปรับปรุงเพิ่มเติมฐานความผิดสารบบคดีให้ครอบคลุมความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ (และที่แก้ไขเพิ่มเติม) ซึ่งมีปริมาณคดีมากขึ้นเมื่อเทียบกับปริมาณงานคดีความผิดฐานอื่นๆ ประกอบกับควรมีการรวบรวมสถิติงานของสำนักงานคดีที่เกี่ยวข้อง โดยแยกประเภทของการใช้คอมพิวเตอร์ในการกระทำความผิด อาทิเช่น กรณีอาชญากรรมคอมพิวเตอร์ประเภทคอมพิวเตอร์ถูกใช้เป็นเครื่องมือประกอบอาชญากรรม (Computer as Tools) หรือกรณีการกระทำความผิดโดยมีคอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets) ซึ่งผู้วิจัยเห็นว่า การจัดเก็บข้อมูลคดีอาชญากรรมคอมพิวเตอร์ดังกล่าวควรเป็นฐานข้อมูลที่สอดคล้องกับฐานข้อมูลสถิติของหน่วยงานในกระบวนการยุติธรรมอื่นด้วย โดยเริ่มต้นจากการเชื่อมโยงกับฐานข้อมูลของพนักงานสอบสวน ตลอดถึงผลการพิจารณามีคำสั่งฟ้องหรือไม่ฟ้องของพนักงานอัยการไปถึงผลทางคดีท้ายที่สุดตามคำพิพากษาของศาล ในลักษณะเชื่อมโยงให้เห็นถึงประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในแต่ละคดี ตั้งแต่ต้นสายของกระบวนการยุติธรรมไปจนถึงปลายทางในกระบวนการยุติธรรม เพื่อประโยชน์ในการจัดทำรายงานอาชญากรรมระดับชาติตามแนวทางที่ วิทยา สุริยะวงค์ (๒๕๕๒) ได้เสนอแนะไว้ โดยข้อมูลสถิติคดีอาชญากรรมคอมพิวเตอร์ในรูปแบบที่มีความละเอียดดังที่กล่าวมาข้างต้นยังสามารถนำไปใช้ประโยชน์เพื่อกำหนดทิศทางการวางแผนจัดการงบประมาณ และแผนการพัฒนาบุคลากรในองค์กรของสำนักงานอัยการสูงสุดให้เหมาะสมต่อไปด้วย

๑.๒ ด้านโครงสร้างหน่วยงานผู้รับผิดชอบตามแผนยุทธศาสตร์

ปัญหาประการหนึ่งที่กล่าวมาในตอนต้นของบทนี้คือ โครงสร้างหน่วยงานผู้รับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ในส่วนกลาง (ท้องที่กรุงเทพมหานคร) ซึ่งพบว่ายังมีความซ้ำซ้อนกันอยู่ เนื่องจากลักษณะของการกระทำผิดด้วยคอมพิวเตอร์มักเกี่ยวพันกับความผิดฐานหลักซึ่งอยู่ในอำนาจการพิจารณาดำเนินคดีของสำนักงานคดีที่แตกต่างกันโดยเฉพาะอย่างยิ่งในท้องที่กรุงเทพมหานคร ซึ่งมีสำนักงานคดีในส่วนกลาง (ท้องที่กรุงเทพมหานคร) ที่เกี่ยวข้องกับคดีอาชญากรรมคอมพิวเตอร์หลายสำนักงาน เช่น คดีที่เกี่ยวข้องกับการหมิ่นประมาทหรือหมิ่นสถาบันเผยแพร่ในระบบคอมพิวเตอร์ รวมถึงการเข้าถึงข้อมูลและเปลี่ยนแปลงข้อมูลในระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ จะอยู่ในอำนาจดำเนินคดีของสำนักงานคดีอาญาในเขตท้องที่ที่เกี่ยวข้อง เช่น สำนักงานคดีอาญา สำนักงานคดีอาญากรุงเทพใต้ สำนักงานคดีอาญาธนบุรี สำนักงานอัยการจังหวัดพระโขนง สำนักงานอัยการจังหวัดมีนบุรี และสำนักงานอัยการจังหวัดตลิ่งชัน เป็นต้น แต่หากเป็นคดีอาชญากรรมคอมพิวเตอร์ที่มีความเกี่ยวพันกับความผิดฐานหลักซึ่งมีผลกระทบต่อระบบเศรษฐกิจการเงินและการธนาคาร เช่น การฉ้อโกงหรือการฉ้อโกงประชาชน หรือการลักลอบเข้ารหัสผ่านระบบ

คอมพิวเตอร์เพื่อแก้ไขหรือใช้โดยมิชอบซึ่งข้อมูลบัญชีลูกค้าธนาคาร คดีดังกล่าวจะอยู่ในอำนาจดำเนินคดีของสำนักงานคดีเศรษฐกิจและทรัพยากร ในขณะที่คดีที่มีความเกี่ยวพันกับความผิดฐานหลักเกี่ยวกับทรัพย์สินทางปัญญา คดีจะอยู่ในอำนาจดำเนินคดีของสำนักงานคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ แต่หากคดีใดดังที่ว่ามาทั้งหมดเป็นคดีที่กรมสอบสวนคดีพิเศษ (DSI) รับไว้สอบสวนเป็นคดีพิเศษแล้ว คดีดังกล่าวก็จะตกอยู่ในความรับผิดชอบของสำนักงานคดีพิเศษ สำนักงานอัยการสูงสุด ทุกคดี เว้นเฉพาะแต่คดีค้ามนุษย์ซึ่งอยู่ในความผิดชอบของสำนักงานคดีค้ามนุษย์ โดยในประเด็นความซ้ำซ้อนเชิงโครงสร้างความรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ระหว่างสำนักงานคดีพิเศษ และสำนักงานคดีอื่นๆ มีความเห็นจากพนักงานอัยการที่แตกต่างกันดังนี้

ดวงพร เตชะกำธร (สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐) เห็นว่า ทางแก้ไขอาจทำได้ดังเช่นอัยการแห่งประเทศสหรัฐอเมริกาที่มีชื่อว่า Computer Crime and Intellectual Property Section (CCIPS) เป็นผู้รับผิดชอบคดีอาชญากรรมคอมพิวเตอร์และทรัพย์สินทางปัญญาทั้งหมด แตกต่างจาก ปกรณ์ ธรรมโรจน์ (สัมภาษณ์, ๘ มีนาคม ๒๕๖๐) ซึ่งเห็นว่า คดีอาชญากรรมคอมพิวเตอร์ มีหลายลักษณะ แต่การแบ่งความรับผิดชอบของหน่วยงานในสำนักงานอัยการสูงสุด มีหลายลักษณะ ทั้งประเภทคดีและท้องที่ซึ่งยังมีความซ้ำซ้อนกันอยู่ อย่างไรก็ตาม การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด หรือเป็นหลักฐานในการพิสูจน์ความผิด จะเป็นเรื่องปกติในอนาคต ทำให้พนักงานอัยการทั้งหมดต้องปรับตัวและเรียนรู้การดำเนินคดีดังกล่าว ดังนั้น การกระจายคดีคอมพิวเตอร์ไปยังหลายหน่วยงานตามประเภทคดีจึงมีความเหมาะสมแล้ว

ในขณะที่ โชติกา ศรีนรเศรษฐ์ (สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐) และเบญจพร วัชระวุฒิชัย (สัมภาษณ์, ๙ มีนาคม ๒๕๖๐) เสนอแนะแนวทางแก้ไขความซ้ำซ้อนของอำนาจหน้าที่เกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานคดีเศรษฐกิจและทรัพยากรและสำนักงานคดีพิเศษ โดยเห็นพ้องกันว่า ควรมีการจัดประชุมเพื่อพูดคุยทำความเข้าใจกันในระหว่างสำนักงานที่เกี่ยวข้องกับคดีอาชญากรรมทางคอมพิวเตอร์เพื่อกำหนดแนวทางให้ชัดเจนว่าอาชญากรรมทางคอมพิวเตอร์ประเภทใดอยู่ในความรับผิดชอบของสำนักงานใดและควรมีการออกคำสั่งจากผู้บริหารระดับสูงให้ชัดเจนเพื่อถือปฏิบัติเป็นแนวทางเดียวกัน เพื่อลดความซ้ำซ้อนของการดำเนินคดีในแต่ละสำนักงาน และเพื่อกำหนดกรอบการดำเนินคดีที่ชัดเจน หรือหากเห็นว่ามีความจำเป็นในการจัดตั้งสำนักงานคดีหรือกลุ่มงานที่มีความเชี่ยวชาญด้านอาชญากรรมทางคอมพิวเตอร์เพื่อรองรับงานคดีประเภทนี้ซึ่งมีแนวโน้มปริมาณคดีเพิ่มมากขึ้นเรื่อยๆ ไว้เป็นการเฉพาะ สำนักงานอัยการสูงสุดอาจพิจารณาทบทวนเหตุผลและความจำเป็นในการจัดตั้งสำนักงานที่มีความเชี่ยวชาญเฉพาะทางในงานคดีอาชญากรรมคอมพิวเตอร์ในอนาคตด้วย

ส่วนในแง่ของการกำหนดรายละเอียดแผนโครงการตามยุทธศาสตร์สำนักงานอัยการสูงสุด สุดเขต เพิ่มผล (สัมภาษณ์, ๒๑ มีนาคม ๒๕๖๐) เห็นว่า สำนักงานอัยการสูงสุดควรจะต้องมีการปรับปรุงยุทธศาสตร์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดเพื่อรองรับความเปลี่ยนแปลงภายหลังรัฐบาลดำเนินนโยบายประเทศไทย ๔.๐ โดยอย่างน้อยสำนักงานอัยการสูงสุดต้องให้ความสำคัญโดยกำหนดเป็นโครงการเพิ่มศักยภาพของพนักงานอัยการในเรื่องนี้ขึ้น โดยมีหน่วยงานที่ต้องรับผิดชอบ คือ ๑. สำนักงานนโยบาย ยุทธศาสตร์ และงบประมาณ เพราะเป็นเรื่องที่เกี่ยวกับนโยบายของสำนักงานอัยการสูงสุด ๒. สำนักงานคดีต่างๆที่

เกี่ยวข้องกับการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ เพราะเป็นหน่วยงานในการดำเนินคดีโดยตรง ๓. สถาบันพัฒนาข้าราชการฝ่ายอัยการ ซึ่งเป็นหน่วยงานที่เกี่ยวข้องกับการจัดฝึกอบรมตามโครงการ ๔. สำนักงานวิชาการ โดยเฉพาะสำนักงานอัยการพิเศษฝ่ายบริหารจัดการความรู้ ที่จะช่วยในการเก็บรวบรวมและกระจายองค์ความรู้ไปยังหน่วยงานต่างๆของสำนักงานอัยการสูงสุดได้ โดยอาจจัดทำแผนงานโครงการเสนอต่ออัยการสูงสุดเพื่อพิจารณาอนุมัติต่อไป

สำหรับความเห็นของผู้วิจัยเกี่ยวกับแนวทางการกำหนดโครงสร้างหน่วยงานผู้รับผิดชอบตามแผนยุทธศาสตร์ในส่วนกลาง (กรุงเทพมหานคร) ซึ่งเกิดปัญหาความซ้ำซ้อนดังที่กล่าวมาข้างต้นนั้น ผู้วิจัยเห็นว่า เนื่องจากลักษณะของคดีอาชญากรรมคอมพิวเตอร์ในชั้นของพนักงานอัยการมีลักษณะเป็นส่วนหนึ่งของการกระทำความผิดฐานหลักอื่นซึ่งมีลักษณะเฉพาะของรูปแบบการดำเนินคดีที่แตกต่างกัน เช่นความผิดฐานหลักซึ่งเกี่ยวกับอาชญากรรมทางเศรษฐกิจและระบบการเงินการธนาคาร ซึ่งอยู่ในอำนาจพิจารณาของศาลยุติธรรมในเขตท้องที่ที่เกิดเหตุ มีลักษณะแตกต่างจากความผิดฐานหลักซึ่งเกี่ยวกับอาชญากรรมเกี่ยวกับทรัพย์สินทางปัญญา ซึ่งอยู่ในอำนาจพิจารณาของศาลทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ การที่จะกำหนดให้มีสำนักงานคดีใดสำนักงานคดีหนึ่งรับผิดชอบเฉพาะความผิดเกี่ยวกับคอมพิวเตอร์ย่อมก่อให้เกิดปัญหาหลายประการ เนื่องจากข้อจำกัดในเรื่องเขตอำนาจศาลที่มีอำนาจพิจารณาความผิดซึ่งเป็นความผิดกรรมเดียวกัน อีกทั้งลักษณะของอาชญากรรมคอมพิวเตอร์ที่แฝงอยู่ในอาชญากรรมความผิดฐานหลัก อาทิเช่น การนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์เพื่อฉ้อโกงทรัพย์ ย่อมมีลักษณะการกระทำความผิดที่แตกต่างจากการเผยแพร่ ทำซ้ำ หรือดัดแปลง ซึ่งข้อมูลอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาซึ่งต้องอาศัยความเชี่ยวชาญเฉพาะทางของพนักงานอัยการที่ดำเนินคดีฐานหลักในการเชื่อมโยงรูปคดีทั้งคดี ดังนั้น การกำหนดโครงสร้างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในปัจจุบันที่แยกตามคดีฐานหลักซึ่งมีสำนักงานคดีที่รับผิดชอบโดยเฉพาะเป็นแนวทางที่เหมาะสมแล้ว อย่างไรก็ดี ในส่วนของความซ้ำซ้อนระหว่างสำนักงานคดีพิเศษและสำนักงานคดีเศรษฐกิจและทรัพยากรนั้น เห็นว่าสำนักงานอัยการสูงสุดควรมีการทบทวนและปรับปรุงการกำหนดลักษณะคดีที่อยู่ในเขตอำนาจของทั้งสองสำนักงานให้ชัดเจนขึ้น โดยยึดเจตนารมณ์ในการจัดตั้งสำนักงานคดีแต่ละแห่งประกอบกับแนวทางในการสร้างและพัฒนาความเชี่ยวชาญเฉพาะทางของพนักงานอัยการ พร้อมทั้งต้องรับฟังความคิดเห็นและข้อเสนอแนะจากทั้งสำนักงานคดีเศรษฐกิจและทรัพยากรและสำนักงานคดีพิเศษประกอบด้วย นอกจากนี้ ในเรื่องการกำหนดแผนงานพัฒนาศักยภาพในการดำเนินคดีที่มีความเกี่ยวข้องกับคอมพิวเตอร์หรือเทคโนโลยีแผนใหม่นั้น ผู้วิจัยเห็นว่า หากเป็นโครงการพัฒนาศักยภาพในการดำเนินคดีของพนักงานอัยการการที่ครอบคลุมการพัฒนาความรู้พื้นฐานที่จำเป็นเกี่ยวกับพยานหลักฐานดิจิทัล สำนักงานอัยการสูงสุดควรกำหนดยุทธศาสตร์และแผนงานโครงการ ดังกล่าวในลักษณะบูรณาการระหว่างสำนักงานคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ทั้งหมดเพื่อเป็นการประหยัดในเชิงงบประมาณ และเพื่อส่งเสริมให้มีการแลกเปลี่ยนความรู้ระหว่างผู้ปฏิบัติงานในแต่ละลักษณะคดี เนื่องจากปัจจุบันอาชญากรรมคอมพิวเตอร์แฝงอยู่ในอาชญากรรมเกือบทุกประเภท สำนักงานอัยการสูงสุดจึงต้องคำนึงถึงความสำคัญของคดีอาชญากรรมคอมพิวเตอร์ในการจัดทำยุทธศาสตร์สำนักงานอัยการสูงสุดในส่วนของยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญาด้วย

๒. แนวทางการจัดทำแผนยุทธศาสตร์คู่ขนานเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์

จากสภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายใต้ยุทธศาสตร์สำนักงานอัยการสูงสุดดังที่กล่าวมาในตอนต้นของบทนี้ ซึ่งพบว่ามีทั้งสภาพปัญหาและอุปสรรคที่เกิดจากปัจจัยภายในสำนักงานอัยการสูงสุดและที่เกิดจากปัจจัยภายนอก การปรับปรุงแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ รวมถึงแผนปฏิบัติราชการประจำปี (Action Plan) ซึ่งมีการประกาศใช้ก่อนที่รัฐบาลจะประกาศใช้แนวนโยบายประเทศไทย ๔.๐ การปรับปรุงแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ ซึ่งเป็นยุทธศาสตร์หลักของสำนักงานอัยการสูงสุด จำต้องมีแนวทางในการปรับปรุงความพร้อมด้านข้อมูลสนับสนุน (สถิติคดี) และการปรับปรุงโครงสร้างผู้ปฏิบัติงานตามแผนยุทธศาสตร์อันถือเป็นแนวทางการแก้ไขที่ต้องใช้เวลานานและต้องดำเนินการตามขั้นตอนของกฎหมายและกฎระเบียบที่เกี่ยวข้องอย่างเป็นทางการ อย่างไรก็ดี เพื่อให้ทันต่อแนวโน้มการเพิ่มขึ้นของอาชญากรรมคอมพิวเตอร์ ซึ่งสำนักงานอัยการสูงสุดมีความจำเป็นต้องมีแนวทางในการรับมือกับคดีอาชญากรรมคอมพิวเตอร์ในระยะสั้นและระยะกลางควบคู่กันไปด้วย

ผู้วิจัยเห็นว่า แนวทางการตอบโต้อาชญากรรมคอมพิวเตอร์ในระยะสั้นซึ่งจะไม่กระทบกับงบประมาณที่ได้รับอนุมัติจัดสรรไว้แล้วแต่เดิม สามารถทำได้หลากหลายประการ อาทิเช่น การกำหนดเป็นแนวนโยบายของสำนักงานอัยการสูงสุดเพื่อเป็นแนวทางในการบริหารงบประมาณที่ยังมิได้จัดสรรประจำปี ๒๕๖๑ และปี ๒๕๖๒ การจัดทำหนังสือเวียนซักซ้อมความเข้าใจแก่พนักงานอัยการผู้ปฏิบัติงาน การปรับปรุงกฎระเบียบแนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ และการจัดการองค์ความรู้ภายในองค์กร โดยผู้วิจัยเห็นว่า แนวทางการตอบโต้อาชญากรรมคอมพิวเตอร์ดังกล่าวควรมีลักษณะเป็นแนวทางการพัฒนาอย่างยั่งยืนและต่อเนื่อง ซึ่งแนวทางการแก้ไขปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ดังที่ได้กล่าวมาในตอนต้นของบทนี้ มีแนวทางครอบคลุม ๔ ด้านดังนี้

๒.๑ ด้านแนวนโยบายและโครงสร้างองค์กร

๒.๑.๑ สำนักงานอัยการสูงสุดควรมีแนวนโยบายการบริหารงานคดีอาชญากรรมคอมพิวเตอร์เพื่อเตรียมความพร้อมสำหรับพนักงานอัยการซึ่งรับผิดชอบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ โดยรับฟังความคิดเห็นจากพนักงานอัยการในสำนักงานคดีที่รับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ และพิจารณาถึงข้อดีและข้อเสียของรูปแบบโครงสร้างสำนักงานคดีที่เกี่ยวข้องในปัจจุบัน โดยในส่วนที่มีปัญหาความซ้ำซ้อนอันเกิดจากความไม่ชัดเจนของบทกฎหมายที่เกี่ยวกับโครงสร้างการแบ่งอำนาจหน้าที่ของแต่ละสำนกงาน สมควรมีการทบทวนและกำหนดแนวทางที่ชัดเจนเพื่อแจ้งเวียนให้พนักงานอัยการที่เกี่ยวข้องได้รับทราบ อันเป็นการแก้ไขข้อขัดข้องให้ทันต่อสภาวการณ์ในปัจจุบัน

๒.๑.๒ สำนักงานอัยการสูงสุดควรมีแนวนโยบายและวางแผนยุทธศาสตร์องค์กรเพื่อเตรียมความพร้อมพนักงานอัยการ และศึกษาหาแนวทางสร้างสำนักงานที่เชี่ยวชาญเฉพาะด้าน เนื่องจากคดีลักษณะดังกล่าวต้องการผู้มีความรู้ความเข้าใจในด้านนี้อย่างจริงจัง และพนักงานอัยการผู้ปฏิบัติงานด้านอาชญากรรมคอมพิวเตอร์จำเป็นต้องมีความสนใจในการเพิ่มพูน

ความรู้ด้านเทคโนโลยีใหม่ๆ ตลอดเวลา เพื่อให้สามารถรับมือกับรูปแบบอาชญากรรมคอมพิวเตอร์ที่มีแนวโน้มซับซ้อนขึ้นกว่าในอดีต อีกทั้งพนักงานอัยการยังจำเป็นต้องมีความรู้เกี่ยวกับเทคโนโลยีของประเทศอื่นทั่วโลกด้วยเนื่องจากอาชญากรรมคอมพิวเตอร์มักมีการเกิดขึ้นในลักษณะความผิดข้ามประเทศ (สมรัตน์ สุขคะ, สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐)

๒.๒ ด้านการพัฒนาบุคลากร

๒.๒.๑ สำนักงานอัยการสูงสุด ควรมีนโยบายอย่างเร่งด่วนในการฝึกอบรมภายใต้กรอบงบประมาณที่ได้รับอนุมัติแล้ว เพื่อให้องค์ความรู้ที่เกี่ยวกับกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่ปัจจุบันมีความซับซ้อนให้กับพนักงานอัยการที่รับผิดชอบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ทั้งในกรุงเทพมหานครและในต่างจังหวัด รวมไปถึงนิติกรผู้ปฏิบัติงานคดีที่เกี่ยวข้องด้วย โดยควรจัดให้มีการอบรมให้ความรู้โดยสม่ำเสมอเมื่อมีกรณีการกระทำผิดใหม่ๆเกิดขึ้น เนื่องจากคดีอาชญากรรมคอมพิวเตอร์จะมีการเปลี่ยนแปลงรูปแบบในการกระทำความผิดอยู่ตลอดเวลา รวมถึงต้องจัดให้มีคู่มือการปฏิบัติงาน การจัดให้มีข้อมูลแหล่งความรู้เพื่อการปฏิบัติงานด้วย (สุดเขต เพิ่มผล, สัมภาษณ์, ๒๑ มีนาคม ๒๕๖๐ ; ดวงพร เตชะกำธร, สัมภาษณ์, ๑๗ มีนาคม ๒๕๖๐)

๒.๒.๒ ในการจัดฝึกอบรมความรู้เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามโครงการที่แต่ละสำนักงานภายในสำนักงานอัยการสูงสุดได้รับอนุมัติงบประมาณจากสำนักงานอัยการสูงสุดแล้ว ไม่ควรมีเพียงวิทยากรที่เป็นพนักงานอัยการเท่านั้น แต่ควรมีองค์ประกอบของวิทยากรที่มาจากพนักงานสอบสวนและผู้ตรวจพิสูจน์ที่มีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางดิจิทัล (เบญจพร วัชระวุฒิชัย, สัมภาษณ์, ๙ มีนาคม ๒๕๖๐)

๒.๒.๓ สำนักงานอัยการสูงสุดควรชี้แจงทำความเข้าใจที่ถูกต้องตรงกันเกี่ยวกับทิศทางแผนงานการบริหารงานคดีอาชญากรรมคอมพิวเตอร์โดยรวม เพื่อให้พนักงานอัยการนิติกร และเจ้าหน้าที่ที่เกี่ยวข้องของสำนักงานอัยการสูงสุด รับทราบและเข้าใจเกี่ยวกับทิศทางที่องค์การกำลังจะมุ่งไป เพื่อให้การนำแผนยุทธศาสตร์ไปสู่การปฏิบัติประสบความสำเร็จ

๒.๓ ด้านการพัฒนาองค์ความรู้และข้อมูล

๒.๓.๑ สำนักงานอัยการสูงสุดควรเตรียมความพร้อมในการเผยแพร่ความรู้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ให้ทันกับสภาพสังคม โดยอาจจัดตั้งศูนย์รวบรวม วิเคราะห์และเผยแพร่องค์ความรู้ให้แก่พนักงานอัยการ เพื่อให้พนักงานอัยการสามารถได้รับการถ่ายทอดความรู้ต่างๆ ไปใช้ในการดำเนินคดีได้อย่างทันท่วงที (ปกรณ์ ธรรมโรจน์, สัมภาษณ์, ๘ มีนาคม ๒๕๖๐)

๒.๓.๒ สถาบันพัฒนาข้าราชการฝ่ายอัยการ ควรร่วมมือกับสำนักงานคดีต่างๆซึ่งมีความรับผิดชอบในงานด้านคดีอาชญากรรมคอมพิวเตอร์ เพื่อปรับปรุงคู่มือพนักงานอัยการสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๔ ให้มีเนื้อหาครบถ้วนและทันสมัยตามรูปแบบการใช้เทคโนโลยีที่เปลี่ยนไปในปัจจุบัน และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ที่เพิ่งประกาศใช้เมื่อไม่นานมานี้ (โชติกา ศรีนรเศรษฐ์, สัมภาษณ์, ๑๐ มีนาคม ๒๕๖๐ ; เบญจพร วัชระวุฒิชัย, สัมภาษณ์, ๙ มีนาคม ๒๕๖๐)

๒.๓.๓ สถาบันกฎหมายอาญา สำนักงานวิชาการ และสำนักงานพัฒนากฎหมาย ของสำนักงานอัยการสูงสุด ควรประสานงานร่วมมือกันจัดทำแผนการศึกษา วิจัย และ

รวบรวมองค์ความรู้สำหรับพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะ เนื่องจากการดำเนินคดีของพนักงานอัยการ มีหลายภาคส่วนที่ต้องใช้ความรู้เฉพาะด้านอย่างเหมาะสม เช่น การวิเคราะห์ปัญหาข้อกฎหมาย ทั้งในส่วนของสาระบัญญัติและวิธีสบัญญัติเกี่ยวกับพยานหลักฐานและการดำเนินคดีคอมพิวเตอร์ในศาล (วัฒนพงศ์ วงศ์ใหญ่, สัมภาษณ์, ๒๒ เมษายน ๒๕๖๐)

๒.๓.๔ สำนักงานอัยการสูงสุดควรจัดให้มีแหล่งข้อมูลศึกษาค้นคว้า เช่น ระบบสืบค้นข้อมูลสำคัญหรือห้องสมุดอิเล็กทรอนิกส์ โดยมีแหล่งความรู้ที่ทันสมัยทั้งกฎหมาย ตำรา บทความ คู่มือการปฏิบัติงาน คำพิพากษาของศาลที่น่าสนใจในรูปของสื่อทางอิเล็กทรอนิกส์ เพื่อให้พนักงานอัยการในท้องที่ต่างจังหวัดมีโอกาสและได้รับความสะดวกในการเข้าถึงข้อมูลความรู้เช่นเดียวกันกับพนักงานอัยการในส่วนกลาง เป็นต้น

๒.๔ ด้านการสร้างแนวทางประสานความร่วมมือกับหน่วยงานอื่น

๒.๔.๑ สำนักงานอัยการสูงสุดควรมีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น เจ้าพนักงานสืบสวน พนักงานสอบสวน พนักงานอัยการ และศาล เพื่อให้แนวนโยบายของหน่วยงานราชการในกระบวนการยุติธรรมเป็นไปในแนวทางที่สอดคล้องและมีประสิทธิภาพทั้งกระบวนการ โดยหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรมควรประสานงานร่วมกับสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเพื่อแสวงหาแนวทางการแก้ไขปัญหาความล่าช้าในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล และแก้ไขข้อจำกัดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๒๖ โดยควรกำหนดแนวทางที่จะสามารถกระทำได้เพื่อพิสูจน์หาตัวผู้กระทำความผิดในกรณีที่มีการกระทำความผิดผ่านสื่อสังคมออนไลน์ เช่น Facebook, LINE, Gmail, Hotmail, Yahoo, Instagram ซึ่งผู้ให้บริการมีถิ่นฐานอยู่นอกราชอาณาจักร เนื่องจากปัจจุบันมีจำนวนผู้ใช้ Facebook, LINE, Gmail, Hotmail, Yahoo, Instagram ในการติดต่อสื่อสารและทำธุรกรรมต่างๆ ซึ่งรวมถึงการซื้อขายสินค้าและบริการจำนวนมาก เมื่อมีการดำเนินแนวนโยบายประเทศไทย ๔.๐ ซึ่งส่งเสริมให้มีการทำธุรกรรมด้านสินค้าและบริการผ่านระบบคอมพิวเตอร์ หากยังไม่มีระบบในการตรวจสอบผู้ที่ทำธุรกรรมผ่านสื่อกลางดังกล่าวย่อมก็ให้เกิดปัญหาในการดำเนินคดีกับผู้กระทำความผิดผ่านสื่อกลางดังกล่าวอย่างแน่นอน

๒.๔.๒ สำนักงานอัยการสูงสุดควรมีแนวทางประสานความร่วมมือกับหน่วยงานต่างๆ ซึ่งมีองค์ความรู้ด้านพยานหลักฐานทางดิจิทัลเป็นอย่างดี เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กรมสอบสวนคดีพิเศษ สำนักงานนิติวิทยาศาสตร์ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) เป็นต้น เพื่อแลกเปลี่ยนองค์ความรู้ด้านดิจิทัล รวมทั้งเพื่อสร้างมาตรฐานในการดำเนินการเกี่ยวกับการรวบรวมพยานหลักฐานให้ครบถ้วนสมบูรณ์ รวดเร็ว และเพียงพอต่อการดำเนินคดีในชั้นศาล

๒.๔.๓ สำนักงานอัยการสูงสุดควรมีแนวทางประสานความร่วมมือกับสำนักงานอัยการและหน่วยงานราชการในต่างประเทศ ทั้งรูปแบบทางการและความร่วมร่วมมือที่ไม่เป็นทางการ เพื่อขอความร่วมมือในการรวบรวมพยานหลักฐานทางคอมพิวเตอร์อย่างรวดเร็วภายหลังเกิดเหตุ เพื่อมิให้พยานหลักฐานทางดิจิทัลสูญหายหรือถูกปนเปื้อน เนื่องจากเว็บไซต์ส่วนใหญ่ที่

คนร้ายใช้กระทำผิดมักมีถิ่นกำเนิด (สถานที่ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์)อยู่ต่างประเทศ รวมทั้งควรมีแนวทางประสานงานกับองค์กรต่างประเทศเพื่อการแลกเปลี่ยนองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์และพยานหลักฐานทางดิจิทัล เพื่อสร้างแผนงานในการรับมืออาชญากรรมรูปแบบใหม่ๆที่เริ่มเกิดขึ้นในต่างประเทศด้วย

สรุป

การศึกษาในบทที่ ๔ เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ ๒. เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ ผลการศึกษาที่ตอบวัตถุประสงค์การวิจัยข้อที่ ๒. สรุปได้ดังนี้

แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐ ที่ดีจะต้องมีความสอดรับกับการแก้ไขปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายใต้ยุทธศาสตร์สำนักงานอัยการสูงสุดในปัจจุบัน แต่จากการศึกษาวิเคราะห์พบว่า ภายใต้การดำเนินการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติราชการประจำปีในปัจจุบัน พบปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการหลายประการทั้งที่เกิดจากปัจจัยภายในองค์กรเอง อาทิเช่น โครงสร้างอำนาจหน้าที่ของสำนักงานภายในสำนักงานอัยการสูงสุดที่ดำเนินคดีอาชญากรรมคอมพิวเตอร์ บทบัญญัติที่ใช้เป็นแนวทางปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์สำหรับพนักงานอัยการ การจัดสรรงบประมาณในงานคดีอาชญากรรมคอมพิวเตอร์ และองค์ความรู้ของบุคลากรของสำนักงานอัยการสูงสุด และที่เกิดจากปัจจัยภายนอกองค์กร อาทิเช่น การขาดองค์ความรู้ที่เหมาะสมของบุคลากรในกระบวนการสืบสวนสอบสวนซึ่งเป็นต้นทางก่อนที่จะส่งสำนวนการสอบสวนไปยังพนักงานอัยการ ข้อจำกัดในการดำเนินคดีที่มีองค์ประกอบข้ามชาติ และการขาดการบูรณาการความร่วมมือและประสานงานระหว่างหน่วยงาน ซึ่งแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดควรมีทั้งแนวทางในการปรับปรุงแผนปฏิบัติราชการประจำปีในส่วนของการบริหารงบประมาณที่ยังมิได้จัดสรรประจำปี ๒๕๖๑ และปี ๒๕๖๒ ซึ่งต้องมีการเตรียมความพร้อมของข้อมูลสถิติเพื่อสะท้อนแนวทางการบริหารงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานคดีที่เกี่ยวข้องซึ่งจะสัมพันธ์กับการพิจารณาจัดสรรงบประมาณให้สอดคล้องกับสภาพการณ์ปัจจุบัน รวมไปถึงแนวทางการจัดทำแผนยุทธศาสตร์คู่ขนานเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ซึ่งจะไม่กระทบกับการจัดสรรงบประมาณ อาทิเช่น การพิจารณาทบทวนแนวนโยบายและโครงสร้างองค์กร การพัฒนาความรู้ของบุคลากรที่เกี่ยวข้อง และการแสวงหาแนวทางบูรณาการความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งควรดำเนินการคู่ขนานไปพร้อม

กันเพื่อให้ทันต่อปริมาณงานด้านอาชญากรรมคอมพิวเตอร์ที่มีแนวโน้มสูงมากขึ้นภายหลังการดำเนินนโยบายประเทศไทย ๔.๐

บทที่ ๕
สรุปและข้อเสนอแนะ

การศึกษาวิจัยเรื่องแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐ เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยได้รวบรวมข้อมูลทั้งข้อมูลทุติยภูมิและปฐมภูมิ มาจัดระเบียบแล้วดำเนินการในการวิเคราะห์ข้อมูลโดยการใช้การวิเคราะห์เนื้อหาเป็นหลัก หลังจากนั้นได้นำมาสังเคราะห์เพื่อหาแนวทางในการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุด โดยใช้ทฤษฎีที่เกี่ยวข้องมาประกอบการวิเคราะห์และสังเคราะห์ข้อมูล โดยผู้วิจัยได้ตั้งวัตถุประสงค์การวิจัยไว้จำนวน ๒ ข้อ ประกอบด้วย ๑. เพื่อศึกษาแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ และ ๒. เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙ – ๒๕๖๒ เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย ๔.๐ จนกระทั่งศึกษาวิจัยได้ข้อค้นพบใหม่สามารถตอบวัตถุประสงค์การวิจัยทั้ง ๒ ข้อ ดังกล่าวข้างต้น ในบทที่ ๕ จะได้นำเสนอสรุปผลการวิจัยที่ตอบวัตถุประสงค์การวิจัย ๒ ข้อดังกล่าวข้างต้น พร้อมกันนั้น จะนำเสนอข้อเสนอแนะเพิ่มเติมเพื่อที่จะทำให้ข้อค้นพบจากการวิจัยนี้สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรมต่อไป

สรุป

ตอบวัตถุประสงค์การวิจัยข้อที่ ๑. สรุปได้ว่า จากการวิเคราะห์และสังเคราะห์ข้อมูลสถิติที่เกี่ยวข้อง และผลการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิ ทำให้คาดการณ์ได้ว่า เมื่อภาครัฐและภาคเอกชนมีการพัฒนาและส่งเสริมการใช้ระบบคอมพิวเตอร์ อินเทอร์เน็ต และระบบสื่อสารดิจิทัลในการทำธุรกิจมากขึ้น อาทิเช่น การทำธุรกรรมด้านการค้าและบริการทางอิเล็กทรอนิกส์ ธุรกรรมการชำระราคาทางอิเล็กทรอนิกส์ และธุรกรรมการเงินทางอิเล็กทรอนิกส์ รวมไปถึงจำนวนการใช้งานระบบคอมพิวเตอร์ในสื่อสังคมออนไลน์ที่มีปริมาณเพิ่มมากขึ้น ประกอบกับการที่ตัวแปร

สำคัญประการหนึ่งของปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ คือ จำนวนผู้ใช้งานระบบคอมพิวเตอร์และจำนวนธุรกรรมที่มีการกระทำผ่านระบบคอมพิวเตอร์ ซึ่งเป็นปัจจัยด้านเหยื่อและด้านโอกาสในการเกิดคดีอาชญากรรมคอมพิวเตอร์ ตามทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) กล่าวคือ เมื่ออาชญากรรมคอมพิวเตอร์เกิดขึ้นได้ทุกที่ทุกเวลาที่มีการเชื่อมต่อระบบคอมพิวเตอร์และอินเทอร์เน็ต แม้ว่าผู้กระทำผิดและเหยื่อจะมิได้พบหน้ากันก็ตาม ผู้กระทำความผิดผ่านระบบคอมพิวเตอร์ย่อมมีโอกาสกระทำความผิดเกี่ยวกับคอมพิวเตอร์ต่อผู้เสียหายซึ่งเป็นผู้ใช้งานระบบคอมพิวเตอร์ได้อย่างกว้างขวางมากขึ้นด้วย ซึ่งในช่วงปีที่ผ่านมา ได้มีตัวอย่างการกระทำความผิดต่อระบบคอมพิวเตอร์และการกระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือประกอบอาชญากรรมจำนวนคดีมากขึ้น ในขณะที่การรวบรวมพยานหลักฐานเพื่อหาตัวผู้กระทำความผิดและพิสูจน์การกระทำความผิดของผู้กระทำมีความซับซ้อนมากกว่าในอดีต เนื่องจากผู้กระทำความผิดย่อมต้องใช้ความรู้ความเข้าใจด้านคอมพิวเตอร์ในการเจาะระบบคอมพิวเตอร์ผ่านระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ดูแลตัวระบบคอมพิวเตอร์ หรือแม้แต่กรณีที่ผู้กระทำความผิดที่ไม่มีความรู้ความเข้าใจด้านคอมพิวเตอร์ในระดับที่ดีมาก แต่เลือกใช้วิธีปกปิดตัวตนด้วยการกระทำความผิดผ่านการเชื่อมต่อระบบคอมพิวเตอร์ซึ่งมีที่ตั้ง Server ที่จัดเก็บข้อมูลผู้ใช้บริการอยู่ในต่างประเทศ เพื่อทำให้การได้มาซึ่งพยานหลักฐานทางดิจิทัลของพนักงานเจ้าหน้าที่ทำได้ยากขึ้น ดังนั้น เมื่ออาชญากรรมคอมพิวเตอร์เป็นอาชญากรรมที่กระทำโดยผู้ที่มีความรู้หรือมีความเชี่ยวชาญด้านคอมพิวเตอร์ แนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการซึ่งเป็นผู้บังคับใช้กฎหมายในกระบวนการยุติธรรมทางอาญาตามทฤษฎีการดำเนินคดีอาญาโดยรัฐจึงจำต้องมีความรู้ความเข้าใจในการทำงานของคอมพิวเตอร์และพยานหลักฐานทางดิจิทัลอย่างเหมาะสมด้วย แต่จากการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านงานคดีอาชญากรรมคอมพิวเตอร์จากหลายหลายสำนักงานคดีกลับพบว่า ในปัจจุบันพนักงานอัยการประสบปัญหาในการดำเนินคดีอาชญากรรมคอมพิวเตอร์อย่างมากจากปัญหาการรวบรวมพยานหลักฐานในชั้นสอบสวนเพื่อพิสูจน์การกระทำความผิดในเรื่องการนำเข้าข้อมูลเท็จสู่ระบบคอมพิวเตอร์ที่ยังไม่สิ้นกระแสความ ทำให้พนักงานอัยการจำเป็นต้องใช้ดุลพินิจสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมซึ่งการที่พนักงานสอบสวนมิได้รวบรวมพยานหลักฐานทางดิจิทัลมาตั้งแต่ต้นทำให้เสี่ยงต่อการสูญหายหรือเสียหายต่อพยานหลักฐานทางดิจิทัลได้ และปัญหาการบูรณาการความร่วมมือและแบ่งปันองค์ความรู้ซึ่งกันและกันระหว่างหน่วยงานในกระบวนการยุติธรรมซึ่งมีบทบาทในการดำเนินการกับอาชญากรรมคอมพิวเตอร์

ตอบวัตถุประสงค์การวิจัยข้อที่ ๒. สรุปได้ว่า แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐ ที่ดีจะต้องมีความสอดรับกับการแก้ไขปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายใต้ยุทธศาสตร์สำนักงานอัยการสูงสุดในปัจจุบัน แต่จากการศึกษาวิเคราะห์พบว่า ภายใต้การดำเนินการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติราชการประจำปีในปัจจุบัน พบปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการหลายประการทั้งที่เกิดจากปัจจัยภายในองค์กรเอง อาทิเช่น โครงสร้างอำนาจหน้าที่ของสำนักงานภายในสำนักงานอัยการสูงสุดที่ดำเนินคดีอาชญากรรมคอมพิวเตอร์ บทบัญญัติที่ใช้เป็นแนวทางปฏิบัติงานคดีอาชญากรรมคอมพิวเตอร์สำหรับพนักงานอัยการ การจัดสรรงบประมาณในงาน

คดีอาชญากรรมคอมพิวเตอร์ และองค์ความรู้ของบุคลากรของสำนักงานอัยการสูงสุด และที่เกิดจากปัจจัยภายนอกองค์กร อาทิเช่น การขาดองค์ความรู้ที่เหมาะสมของบุคลากรในกระบวนการสืบสวนสอบสวนซึ่งเป็นต้นทางก่อนที่จะส่งสำนวนการสอบสวนไปยังพนักงานอัยการ ข้อจำกัดในการดำเนินคดีที่มีองค์ประกอบข้ามชาติ และ การขาดการบูรณาการความร่วมมือและประสานงานระหว่างหน่วยงาน ซึ่งแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดควรมีทั้งแนวทางในการปรับปรุงแผนปฏิบัติราชการประจำปีในส่วนของการบริหารงบประมาณที่ยังมิได้จัดสรรประจำปี ๒๕๖๑ และปี ๒๕๖๒ ซึ่งต้องมีการเตรียมความพร้อมของข้อมูลสถิติเพื่อสะท้อนแนวทางการบริหารงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานคดีที่เกี่ยวข้องซึ่งจะสัมพันธ์กับการพิจารณาจัดสรรงบประมาณให้สอดคล้องกับสภาพการณ์ปัจจุบัน รวมไปถึงแนวทางการจัดทำแผนยุทธศาสตร์คู่ขนานเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ซึ่งจะไม่กระทบกับการจัดสรรงบประมาณ อาทิเช่น การพิจารณาทบทวนแนวนโยบายและโครงสร้างองค์กร การพัฒนาความรู้ของบุคลากรที่เกี่ยวข้อง และการแสวงหาแนวทางบูรณาการความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ซึ่งควรดำเนินการคู่ขนานไปพร้อมกันเพื่อให้ทันต่อปริมาณงานด้านอาชญากรรมคอมพิวเตอร์ที่มีแนวโน้มสูงมากขึ้นภายหลังการดำเนินนโยบายประเทศไทย ๔.๐

ข้อเสนอแนะ

๑. ข้อเสนอแนะระดับนโยบาย

๑.๑ แก้ไขปัญหาด้านโครงสร้างหน่วยงานผู้รับผิดชอบคดีอาชญากรรมคอมพิวเตอร์ กล่าวคือ สำนักงานอัยการสูงสุดควรมีการทบทวนและปรับปรุงการกำหนดลักษณะคดีที่อยู่ในเขตอำนาจของสำนักงานคดีอาญา สำนักงานคดีเศรษฐกิจและทรัพยากร สำนักงานคดีทรัพย์สินทางปัญญาและการค้าระหว่างประเทศ สำนักงานคดีพิเศษ และสำนักงานการสอบสวน ให้ชัดเจนขึ้น โดยยึดเจตนารมณ์ในการจัดตั้งสำนักงานคดีแต่ละแห่งประกอบกับแนวทางในการสร้างและพัฒนาความเชี่ยวชาญเฉพาะทางของพนักงานอัยการ พร้อมทั้งต้องรับฟังความคิดเห็นและข้อเสนอแนะจากทุกสำนักงานที่เกี่ยวข้องประกอบด้วย อย่างไรก็ดี ในเรื่องการกำหนดแผนงานพัฒนาศักยภาพในการดำเนินคดีที่มีความเกี่ยวข้องกับคอมพิวเตอร์หรือเทคโนโลยีแผนใหม่นั้น ผู้วิจัยเห็นว่า หากเป็นโครงการพัฒนาศักยภาพในการดำเนินคดีของพนักงานอัยการการที่ครอบคลุมการพัฒนาความรู้พื้นฐานที่จำเป็นเกี่ยวกับพยานหลักฐานดิจิทัล สำนักงานอัยการสูงสุดควรกำหนดยุทธศาสตร์และแผนงานโครงการดังกล่าวในลักษณะบูรณาการระหว่างสำนักงานคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ทั้งหมดโดยไม่ควรกำหนดแผนงานแยกจำกัดเพียงภายในแต่ละสำนักงาน เพื่อเป็นการประหยัดในเชิงงบประมาณ และเพื่อส่งเสริมให้มีการแลกเปลี่ยนองค์ความรู้และประสบการณ์ด้านงานคดีที่หลากหลายระหว่างผู้ปฏิบัติงานจากต่างสำนักงานคดี

๑.๒ สร้างแนวทางประสานความร่วมมือในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับหน่วยงานอื่น กล่าวคือ สำนักงานอัยการสูงสุดควรมีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรม เช่น เจ้าพนักงานสืบสวน พนักงานสอบสวน พนักงานอัยการและศาล เพื่อให้แนวนโยบายของหน่วยงานราชการในกระบวนการยุติธรรมเป็นไปในแนวทางที่สอดคล้องและมีประสิทธิภาพทั้งกระบวนการ โดยหน่วยงานที่เกี่ยวข้องในกระบวนการยุติธรรมควร

ประสานงานร่วมกับสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเพื่อแสวงหาแนวทางการแก้ไขปัญหาความล่าช้าในการตรวจพิสูจน์พยานหลักฐานทางดิจิทัลรวมทั้งควรมีแนวทางประสานความร่วมมือกับหน่วยงานต่างๆ ซึ่งมีองค์ความรู้ด้านพยานหลักฐานทางดิจิทัลเป็นอย่างดี เช่น กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กรมสอบสวนคดีพิเศษ สำนักงานนิติวิทยาศาสตร์ สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์(สพธอ.) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) เป็นต้น เพื่อแลกเปลี่ยนองค์ความรู้ด้านดิจิทัล รวมทั้งเพื่อสร้างมาตรฐานในการดำเนินการเกี่ยวกับการรวบรวมพยานหลักฐานให้ครบถ้วนสมบูรณ์ รวดเร็ว เพียงพอ และรับฟังเป็นพยานหลักฐานในการดำเนินคดีในชั้นศาลได้ เพื่อทดแทนข้อจำกัดของกฎหมายปัจจุบันที่คดีส่วนใหญ่ (นอกจากกรณีที่มีกฎหมายกำหนดไว้เป็นการเฉพาะ) พนักงานอัยการไม่มีอำนาจสอบสวนในชั้นสอบสวน นอกจากนี้ ในส่วนคดีที่มีลักษณะของการกระทำความผิดข้ามชาติ สำนักงานอัยการสูงสุดควรมีแนวทางประสานความร่วมมือกับสำนักงานอัยการและหน่วยงานราชการในต่างประเทศ ทั้งรูปแบบทางการและความร่วมมือที่ไม่เป็นทางการ เพื่อขอความร่วมมือในการรวบรวมพยานหลักฐานทางคอมพิวเตอร์อย่างรวดเร็วภายหลังเกิดเหตุ เพื่อมิให้พยานหลักฐานทางดิจิทัลสูญหายหรือถูกปนเปื้อน เนื่องจากเว็บไซต์ส่วนใหญ่ที่คนร้ายใช้กระทำผิดมักมีถิ่นกำเนิด (สถานที่ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการเว็บไซต์)อยู่ต่างประเทศ รวมทั้งควรมีแนวทางประสานงานกับองค์กรต่างประเทศเพื่อการแลกเปลี่ยนองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์และพยานหลักฐานทางดิจิทัล เพื่อสร้างแผนงานในการรับมืออาชญากรรมรูปแบบใหม่ๆ ที่เริ่มเกิดขึ้นในต่างประเทศด้วย

๒. ข้อเสนอแนะระดับปฏิบัติการ

๒.๑ พัฒนาองค์ความรู้ของบุคลากร โดยสำนักงานอัยการสูงสุดควรมีนโยบายอย่างเร่งด่วนในการฝึกอบรมให้ความรู้ที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ที่มีความซับซ้อนในปัจจุบันให้กับพนักงานอัยการและนิติกรผู้ปฏิบัติงานคดีที่เกี่ยวข้อง ซึ่งรับผิดชอบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ทั้งในกรุงเทพมหานครและในต่างจังหวัด โดยควรจัดให้มีการอบรมให้ความรู้อย่างสม่ำเสมอเมื่อมีกรณีการกระทำผิดใหม่ๆเกิดขึ้น เนื่องจากคดีอาชญากรรมคอมพิวเตอร์จะมีการเปลี่ยนแปลงรูปแบบในการกระทำความผิดอยู่ตลอดเวลา นอกจากนี้ ในการจัดฝึกอบรมความรู้เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามโครงการที่แต่ละสำนักงานภายในสำนักงานอัยการสูงสุดได้รับอนุมัติงบประมาณจากสำนักงานอัยการสูงสุดแล้ว ไม่ควรกำหนดตัวบุคคลที่จะเป็นวิทยากรจำกัดอยู่เพียงพนักงานอัยการเท่านั้น แต่ควรมีองค์ประกอบของวิทยากรที่มาจากพนักงานสอบสวนและเจ้าพนักงานผู้ตรวจพิสูจน์หลักฐานที่มีความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางดิจิทัลด้วย นอกจากนี้ ผู้วิจัยเห็นว่า สำนักงานอัยการสูงสุดควรมีแนวทางประสานงานความร่วมมือด้านการฝึกอบรมความรู้กับหน่วยงานผู้ปฏิบัติงานด้านคดีอาชญากรรมคอมพิวเตอร์อื่น เช่น ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กรมสอบสวนคดีพิเศษ สำนักงานนิติวิทยาศาสตร์ และสำนักงานพิสูจน์หลักฐานตำรวจ เพื่อให้บุคลากรผู้ปฏิบัติงานด้านคดีอาชญากรรมคอมพิวเตอร์และพยานหลักฐานดิจิทัล ของสำนักงานอัยการสูงสุดและหน่วยงานต่างๆดังที่กล่าวมา ได้เข้าร่วมรับการฝึกอบรมร่วมกันเพื่อแบ่งปันข้อมูลประสบการณ์เกี่ยวกับการปฏิบัติงานและการดำเนินคดี เพื่อให้

บุคลากรทั้งหลายเกิดความเข้าใจในการดำเนินคดีอาชญากรรมคอมพิวเตอร์เชิงบูรณาการและสร้างความสัมพันธ์อันดีระหว่างบุคลากรจากหลากหลายหน่วยงาน

๒.๒ พัฒนาเครื่องมือในการปฏิบัติงานของพนักงานอัยการอย่างยั่งยืน โดยสำนักงานอัยการสูงสุดควรเตรียมความพร้อมในการถ่ายทอดเผยแพร่ความรู้ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ให้แก่บุคลากรผู้ปฏิบัติงาน โดยควรจัดตั้งศูนย์รวบรวม วิเคราะห์ และเผยแพร่องค์ความรู้ให้แก่พนักงานอัยการ เพื่อให้พนักงานอัยการสามารถได้รับการถ่ายทอดความรู้ต่างๆ ไปใช้ในการดำเนินคดีได้อย่างทันท่วงทีซึ่งสถาบันพัฒนาข้าราชการฝ่ายอัยการควรสร้างความร่วมมือกับสำนักงานคดีต่างๆที่มีความรับผิดชอบในงานด้านคดีอาชญากรรมคอมพิวเตอร์ เพื่อปรับปรุงคู่มือพนักงานอัยการสำหรับการสอบสวนและดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๔ ให้มีเนื้อหาครบถ้วนและทันสมัยตามรูปแบบการใช้เทคโนโลยีที่เปลี่ยนไปในปัจจุบัน และสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ที่เพิ่งประกาศใช้เมื่อไม่นานมานี้ นอกจากนั้น สถาบันกฎหมายอาญา สำนักงานวิชาการ และสำนักงานพัฒนากฎหมาย ของสำนักงานอัยการสูงสุด ควรประสานงานร่วมมือกันจัดทำแผนการศึกษา วิจัย และรวบรวมองค์ความรู้สำหรับพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์โดยเฉพาะด้วย และเพื่อให้เกิดองค์ความรู้ที่ยั่งยืน สำนักงานอัยการสูงสุดควรจัดให้มีแหล่งข้อมูลศึกษาค้นคว้า เช่น ระบบสืบค้นข้อมูลสำคัญหรือห้องสมุดโดยมีแหล่งความรู้ที่ทันสมัยทั้งกฎหมาย ตำรา บทความคู่มือการปฏิบัติงาน คำพิพากษาของศาลที่น่าสนใจในรูปของสื่อทางอิเล็กทรอนิกส์ เพื่อให้พนักงานอัยการในท้องที่ต่างจังหวัดมีโอกาสและได้รับความสะดวกในการเข้าถึงข้อมูลความรู้เช่นเดียวกันกับพนักงานอัยการในส่วนกลาง เป็นต้น

๓. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

เตรียมความพร้อมด้านข้อมูลสนับสนุนการจัดทำยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด ด้วยการปรับปรุงการบันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดและเพิ่มประสิทธิภาพในการจัดเก็บสถิติอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด ให้มีลักษณะที่เป็นฐานข้อมูลที่สอดคล้องกับฐานข้อมูลสถิติของหน่วยงานในกระบวนการยุติธรรมอื่นด้วย โดยเริ่มต้นจากการเชื่อมโยงกับฐานข้อมูลของพนักงานสอบสวนตลอดถึงผลการพิจารณามีคำสั่งฟ้องหรือไม่ฟ้องของพนักงานอัยการ ไปถึงผลทางคดีท้ายที่สุดตามคำพิพากษาของศาล ในลักษณะเชื่อมโยงให้เห็นถึงประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในแต่ละคดี ตั้งแต่ต้นสายของกระบวนการยุติธรรมไปจนถึงปลายทางในกระบวนการยุติธรรม เพื่อประโยชน์ในการจัดทำรายงานอาชญากรรมระดับชาติตามแนวทางที่ วิทยา สุริยะวงค์ (๒๕๕๒) ได้เสนอแนะไว้ โดยข้อมูลสถิติคดีอาชญากรรมคอมพิวเตอร์ในรูปแบบที่มีความละเอียดดังที่กล่าวมาข้างต้นยังสามารถนำไปใช้ประโยชน์เพื่อกำหนดทิศทางการวางแผนจัดการงบประมาณ และแผนการพัฒนาบุคลากรในองค์กรของสำนักงานอัยการสูงสุดให้เหมาะสมต่อไปด้วย

ผู้วิจัยเชื่อว่าข้อเสนอแนะในการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ภายหลังจากที่รัฐบาลได้ส่งเสริมนโยบายประเทศไทย ๔.๐ ดังที่กล่าวมาในงานวิจัยนี้ สามารถก่อให้เกิดความพร้อมและการพัฒนาประสิทธิภาพการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด ในยุคประเทศไทย ๔.๐ ทำให้สำนักงานอัยการสูงสุดสามารถ

อำนวยความยุติธรรมให้กับผู้มีส่วนได้เสียในคดีรวมทั้งสร้างความมั่นใจให้กับประชาชนซึ่งทำธุรกรรมต่างๆในโลกดิจิทัล เพื่อประโยชน์โดยรวมในการสร้างความมั่นคงปลอดภัยทางเศรษฐกิจและสังคมโดยรวมของชาติต่อไป

บรรณานุกรม

ภาษาไทย

หนังสือ

วีระพงษ์ บุญโญภาส และสุพัตรา แผนวิชิต. อาชญากรรมทางเศรษฐกิจ (Economic Crime). กรุงเทพฯ : นิติธรรม, ๒๕๕๗.

สุนีย์ สกาวรัตน์. การตรวจพิสูจน์หลักฐานดิจิทัลสำหรับผู้ประกอบวิชาชีพกฎหมาย. กรุงเทพฯ : มูลนิธิเพื่ออินเตอร์เน็ตและวัฒนธรรมพลเมือง, ๒๕๕๙.

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

เฉลิมชนม์ แน่นหนา และคณะ. “อาชญากรรมบนสื่อออนไลน์”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๕.

บดิรทร วิยาภรณ์. “การไม่ดำเนินคดีในชั้นพนักงานสอบสวนโดยใช้ดุลพินิจ”. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขากฎหมายอาญา, มหาวิทยาลัยธรรมศาสตร์, ๒๕๕๒.

ปิยฉัตร ผังสุวรรณดำรง. “ความเป็นอิสระขององค์กรอัยการ”. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขากฎหมายอาญา, มหาวิทยาลัยธรรมศาสตร์, ๒๕๕๔.

วิจัย, กอง. “การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์”. เอกสารวิจัย, สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ, ๒๕๕๙.

วิทยา สุริยะวงค์. “ยุทธศาสตร์การต่อสู้ปัญหาอาชญากรรม : ศึกษากรณีการจัดทำรายงานอาชญากรรมระดับชาติ”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๒.

สัมภาษณ์

คงยศ คุณจักร์, รองอัยการจังหวัดสมุทรปราการ. สัมภาษณ์. ๑๒ มีนาคม ๒๕๖๐.

โชติกา ศรีนรเศรษฐ์, อัยการประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๑๐ มีนาคม ๒๕๖๐.

ดวงพร เตชะกำธร, อัยการประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๑๗ มีนาคม ๒๕๖๐.

เบญจพร วัชระวุฒิชัย, อัยการประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๙ มีนาคม ๒๕๖๐.

ปกรณ์ คุณสาระ, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๑๑ มีนาคม ๒๕๖๐.

ปกรณ์ ธรรมโรจน์, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๘ มีนาคม ๒๕๖๐.

วัฒนพงศ์ วงศ์ใหญ่, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๒๒ เมษายน ๒๕๖๐.

สมรัตน์ สุขคะ, อัยการประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๑๗ มีนาคม ๒๕๖๐.

สุดเขต เพิ่มผล, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๒๑ มีนาคม ๒๕๖๐.

สุภกิตต์ โสตถิทัต, อัยการจังหวัดประจำสำนักงานอัยการสูงสุด. สัมภาษณ์. ๒๒ เมษายน ๒๕๖๐.

กฎหมาย

"แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ (พ.ศ. ๒๕๖๐ - ๒๕๖๔)", ราชกิจจานุเบกษา. เล่มที่ ๑๓๓, ๓๐ ธันวาคม ๕๕๙, หน้า ๑–๒๑๕.

"พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. ๒๕๔๖", ราชกิจจานุเบกษา. เล่มที่ ๑๒๐, ๙ ตุลาคม ๒๕๔๖, หน้า ๑–๑๖.

"พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗", ราชกิจจานุเบกษา. เล่มที่ ๑๒๑, ๑๙ มกราคม ๒๕๔๗, หน้า ๑–๑๖.

"พระราชบัญญัติการสอบสวนคดีพิเศษ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑", ราชกิจจานุเบกษา. เล่มที่ ๑๒๕, ๒๐ กุมภาพันธ์ ๒๕๕๑, หน้า ๒๓–๒๗.

"พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. ๒๕๕๖", ราชกิจจานุเบกษา. เล่มที่ ๑๓๐, ๒๖ มิถุนายน ๒๕๕๖, หน้า ๑–๑๑.

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐", ราชกิจจานุเบกษา. เล่มที่ ๑๒๔, ๑๘ มิถุนายน ๒๕๕๐, หน้า ๔–๑๓.

"พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐", ราชกิจจานุเบกษา. เล่มที่ ๑๓๔, ๒๔ มกราคม ๒๕๖๐, หน้า ๒๔–๓๕.

"พระราชบัญญัติองค์กรอัยการและพนักงานอัยการ พ.ศ. ๒๕๕๓", ราชกิจจานุเบกษา. เล่มที่ ๑๒๗, ๗ ธันวาคม ๒๕๕๓, หน้า ๓๘–๕๐.

"ระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการงบประมาณ พ.ศ. ๒๕๕๔", ราชกิจจานุเบกษา. เล่มที่ ๑๒๘, ๒๔ มีนาคม ๒๕๕๔, หน้า ๒๐–๒๕.

เอกสารไม่ตีพิมพ์

เทคโนโลยีสารสนเทศและการสื่อสาร, กระทรวง. "แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม". ๒๕๕๙.

วิชาการป้องกันประเทศ, สถาบัน. "การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม". เอกสารวิชาการ, ศูนย์ศึกษายุทธศาสตร์, สถาบันวิชาการป้องกันประเทศ ๒๕๕๗.

อัยการสูงสุด, สำนักงาน. "คำสั่งกรมอัยการที่ ๑๙/๒๕๓๔ เรื่อง กำหนดอำนาจหน้าที่ของกองคดีเศรษฐกิจและทรัพยากร และความผิดเกี่ยวกับเศรษฐกิจและทรัพยากรแนบท้ายคำสั่งกรมอัยการที่ ๑๙/๒๕๓๔ ลงวันที่ ๑๘ กุมภาพันธ์ ๒๕๓๔". ๒๕๓๔.

อัยการสูงสุด, สำนักงาน. "คู่มือการดำเนินคดีอาญาของพนักงานอัยการ". ๒๕๕๕.

อัยการสูงสุด, สำนักงาน. "คู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์". ๒๕๕๔ ก.

อัยการสูงสุด, สำนักงาน. "ประกาศคณะกรรมการอัยการ เรื่องการแบ่งหน่วยงาน และการกำหนดอำนาจหน้าที่ของหน่วยงานภายในของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๔". ๒๕๕๔ ข.

อัยการสูงสุด, สำนักงาน. “แผนปฏิบัติราชการประจำปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๖๐” . ๒๕๕๙ ก.

อัยการสูงสุด, สำนักงาน. “ระเบียบสำนักงานอัยการสูงสุด ว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ. ๒๕๔๗ (แก้ไขเพิ่มเติม)”. ๒๕๕๑.

อัยการสูงสุด, สำนักงาน. “รายงานประจำปี ๒๕๕๘”. ๒๕๕๙ ค.

ฐานข้อมูลอิเล็กทรอนิกส์

กรรณิกา ภัทรวิศิษฏ์สัณธ์. “Digital Forensics 101 (ตอนที่ 1)”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/papers/general/2013/pa2013ge012.html, ๒๕๖๐.

กองบังคับการปราบปราม. “แนวคิดและทฤษฎีสนับสนุนการสืบสวนสอบสวน”. (ออนไลน์). เข้าถึงได้จาก : http://www.csd.go.th/dimensions_csd/4dimensions-3.pdf, ๒๕๖๐.

ทีมข่าวสืบสวนสอบสวน สำนักข่าวคมชัดลึก. “ยุทธศาสตร์ชาติ กับภัยคุกคามในอีก ๒๐ ปีข้างหน้า”. (ออนไลน์). เข้าถึงได้จาก : http://www.komchadluek.net/news/detail/222584, ๒๕๕๙.

ประยุทธ์ จันทร์โอชา. ปาฐกถาพิเศษเรื่อง “นโยบายการเตรียมความพร้อมบุคคลภาครัฐ เพื่อรองรับการก้าวไปสู่ Digital Thailand”. ณ โรงแรมเซ็นทารา แกรนด์ เซ็นทรัลเวิลด์ กรุงเทพมหานคร, ๒๙ กรกฎาคม ๒๕๕๙. (ออนไลน์). เข้าถึงได้จาก : http://www.thaigov.go.th/index.php/th/government-th1/item/105540-105540.๒๕๕๙.

ปรเมธี วิมลศิริ. บรรยายเรื่อง “ยุทธศาสตร์ชาติ ๒๐ ปี อนาคตประเทศไทยเพื่อความมั่นคง มั่งคั่ง ยั่งยืน” รุ่นที่ ๖. ณ ห้องประชุมสถาบันวิทยาการประกันภัยระดับสูง. (ออนไลน์). เข้าถึงได้จาก : http://plan.vru.ac.th/wp-content/uploads/2016/11/%E0%B9%81%E0%B8%9C%E0%B8%99%E0%B8%8A%E0%B8%B2%E0%B8%95%E0%B8%B4-20-%E0%B8%9B%E0%B8%B5-1.pdf, ๒๕๖๐.

ผู้จัดการ Online. “เตือนภัย! แอปธนาคารปลอมระบาดใน Playstore”. (ออนไลน์). เข้าถึงได้จาก : http://www.manager.co.th/cyberbiz/viewNews.aspx?NewsID=9570000034392, ๒๕๕๗.

ผู้จัดการ Online. “เตือนภัย “Internet Banking” ปล้นวันละแสน!!”. (ออนไลน์). เข้าถึงได้จาก : http://www.manager.co.th/cyberbiz/viewNews.aspx?NewsID=9570000034392, ๒๕๕๖.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “ETDA เสนอกรอบการตรวจพยานหลักฐานดิจิทัล ยกระดับสู่มาตรฐานสากล”. (ออนไลน์). เข้าถึงได้จาก : https://www.etda.or.th/content/etda-recommendation-on-digital-forensics.html, ๒๕๖๐.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “ รายงานผลการสำรวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย ปี 2559”. (ออนไลน์). เข้าถึงได้จาก : https://www.etda.or.th/publishing-detail/value-of-e-commerce-survey-2016.html, ๒๕๖๐.

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “Europol เผยแพร่รายงานวิเคราะห์แนวโน้มอาชญากรรมทางไซเบอร์ประจำปี 2559”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/newsbite/2016-09-29-02.html, ๒๕๖๐.

มั่นพัฒนา, มูลนิธิ. “ความเชื่อมโยงระหว่างยุทธศาสตร์ชาติ – เป้าหมายการพัฒนาที่ยั่งยืน (SDGs) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒”. (ออนไลน์). เข้าถึงได้จาก : http://www.tsdf.or.th/th/article/10267/428-%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B9%80%E0%B8%8A%E0%B8%B7%E0%B9%88%E0%B8%AD%E0%B8%A1%E0%B9%82%E0%B8%A2%E0%B8%87%E0%B8%A3%E0%B8%B0%E0%B8%AB%E0%B8%A7%E0%B9%88%E0%B8%B2%E0%B8%87%E0%B8%A2%E0%B8%B8%E0%B8%97%E0%B8%98%E0%B8%A8%E0%B8%B2%E0%B8%AA%E0%B8%95%E0%B8%A3%E0%B9%8C%E0%B8%8A%E0%B8%B2%E0%B8%95%E0%B8%B4-%E0%B9%80%E0%B8%9B%E0%B9%89%E0%B8%B2%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9E%E0%B8%B1%E0%B8%92, ๒๕๕๙.

ยุติธรรม, กระทรวง. “แผนแม่บทการบริหารงานยุติธรรมแห่งชาติ พ.ศ. ๒๕๕๘-๒๕๖๑”. (ออนไลน์). เข้าถึงได้จาก : http://phitsanulok.moj.go.th/wp-content/pdf/model%20scheme.pdf, ๒๕๕๙.

“ระวังภัย มัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์ รีบอัปเดตทันที”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/alerts/user/2017/al2017us001.html, ๒๕๖๐.

วิศัลย์ ประสงค์สุข และคณะ, “Social Engineering” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/papers/general/2012/pa2012ge017.html, ๒๕๖๐.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต), “รายงานประจำปีไทยเซิร์ต ๒๕๕๘” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/downloads/files/ThaiCERT_Annual_Report_th_2015.pdf, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๔” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2011.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๕” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2012.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๖” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2013.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๗” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2014.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๘” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2015.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “สถิติภัยคุกคามปี ๒๕๕๙” . (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics2016.html, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). “แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ ปี 2557”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/papers/general/2013/pa2013ge013.html, ๒๕๕๙.

สุวิทย์ เมษินทรีย์. “ไขรหัส “ประเทศไทย 4.0” สร้างเศรษฐกิจใหม่ ก้าวข้ามกับดักรายได้ปานกลาง”. (ออนไลน์). เข้าถึงได้จาก : http://www.thairath.co.th/content/613903, ๒๕๕๙.

อนุชาติ คงมาลัย. “คู่มือพนักงานอัยการว่าด้วยการค้นและยึดคอมพิวเตอร์และการได้มาซึ่งพยานหลักฐานทางอิเล็กทรอนิกส์ในการสอบสวนคดีอาญา”. (ออนไลน์). เข้าถึงได้จาก : http://www.ago.go.th/articles/comcrime_061051_1.pdf, ๒๕๕๑.

อัยการสูงสุด, สำนักงาน. “แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒” . (ออนไลน์). เข้าถึงได้จาก : http://www.ps.ago.go.th/ps/images/download/PLAN%202559.pdf, ๒๕๕๙ ข.

“แฮกเกอร์เปิดฉากปฏิบัติการถล่มเว็บไซต์ระบบการบริหารการคลังภาครัฐ”. (ออนไลน์). เข้าถึงได้จาก : https://www.it24hrs.com/2016/hacker-attack-egp-e-bidding-website/, ๒๕๕๙.

“แฮกเกอร์ลุยแฮกข้อมูลกองทัพพร้อมประกาศเผยข้อมูลงบประมาณกองทัพบก คืนนี้”. (ออนไลน์). เข้าถึงได้จาก : https://www.it24hrs.com/2016/cyber-attack-anti-single-gateway-vs-military/, ๒๕๕๙.

“แฮกเว็บประท้วง พ.ร.บ.คอมพ์ สัญญาเตือนติดอาวุธไอทีภาครัฐ”. (ออนไลน์). เข้าถึงได้จาก : http://m.prachachat.net/news_detail.php?newsid=1482307206, ๒๕๕๙.

“Anonymous แฮกเว็บศาลไทยล่ม 296 เว็บไซต์ ค้านคดีเกาะเต่า”. (ออนไลน์). เข้าถึงได้จาก : https://hilight.kapook.com/view/131583, ๒๕๕๙.

“๔ เว็บรัฐบาล ล่ม ไม่ทราบสาเหตุ คาดถูกแฮก”. (ออนไลน์). เข้าถึงได้จาก : https://www.matichon.co.th/nws/399580, ๒๕๕๙.

Attorney General, Department. “National Plan to Combat Cybercrime”. (Online). Available : http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf, 2016.

Cyber Security, Agency. “Singapore’s Cybersecurity Strategy”. (Online). Available : https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf?la=en, 2016.

Homeland Security. “National Cybercrime Incident Response Plan Now Available For Public Comment”. (Online). Available : https://www.dhs.gov/blog/2016/09/30/national-cyber-incident-response-plan-now-available-public-comment, 2016.

PWC. “Economic Crime in Thailand”. (Online). Available : http://www.pwc.com/th/en/publications/economic-crime-in-thailand.html, 2016.

Veedvil. “Digital in Thailand”. (Online). Available : http://www.veedvil.com/news/digital-in-thailand-2016/, 2016.

ภาษาต่างประเทศ

Yong, John. “Cybersecurity Trends and Issues : A Singapore Perspective”. (Paper Presented at Workshop on “Cybersecurity : Emerging Issues, Trends, Technologies and Threats in 2015 and Beyond”). 2015.

ภาคผนวก

ผนวก ก

แผนปฏิบัติการสำนักงานอัยการสูงสุด ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ โครงการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒

(เฉพาะยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา)

แผนปฏิบัติการ
สำนักงานอัยการสูงสุด
ประจำปีงบประมาณ พ.ศ. ๒๕๖๐

โครงการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี
สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ - ๒๕๖๒

ด่วนที่สุด **บันทึกข้อความ**

ส่วนราชการ สำนักงานอัยการสูงสุด สำนักงานนโยบาย ยุทธศาสตร์ และงบประมาณ สนฝย. โทร. ๐ ๒๑๔๒ ๑๔๗๙
ที่ อส ๐๐๐๖(นย)/ว๓๖๖ **วันที่** ๗ ตุลาคม ๒๕๕๙
เรื่อง แผนปฏิบัติการสำนักงานอัยการสูงสุด ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ (Action Plan) โครงการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒

เรียน รองอัยการสูงสุด ผู้ตรวจการอัยการ อธิบดีอัยการ อธิบดีอัยการภาค อัยการพิเศษฝ่าย เลขานุการอัยการสูงสุด อัยการจังหวัด ผู้อำนวยการสำนักงานกิจการและโครงการในพระดำริ พระเจ้าหลานเธอพระองค์เจ้าพัชรกิติยาภา ผู้อำนวยการสำนักงานบริหารกิจการสำนักงานอัยการสูงสุด ผู้อำนวยการสำนักงานพัฒนาระบบบริหาร และผู้อำนวยการสำนักงานตรวจสอบภายใน

ด้วยอัยการสูงสุดได้เห็นชอบแผนปฏิบัติการสำนักงานอัยการสูงสุด ประจำปีงบประมาณ พ.ศ. ๒๕๖๐ (Action Plan) โครงการตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ – ๒๕๖๒ เพื่อใช้เป็นกรอบในการปฏิบัติงานของหน่วยงานที่เกี่ยวข้อง และเพื่อให้ผู้บริหารใช้ประกอบการพิจารณาอนุมัติโครงการ/กิจกรรม และงบประมาณ รวมทั้งการติดตามผลการดำเนินโครงการ/กิจกรรมของหน่วยงานที่อยู่ในความรับผิดชอบดูแล โดยมีโครงการที่ได้รับจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๐ รวมทั้งสิ้น จำนวน ๑๖ โครงการ เป็นเงิน ๑๒,๐๐๐,๐๐๐ บาท

สำนักงานอัยการสูงสุด ขอให้หน่วยงานที่รับผิดชอบโครงการ/กิจกรรมตามแผนปฏิบัติการดังกล่าว ดำเนินโครงการ/กิจกรรมให้แล้วเสร็จตามแผนที่กำหนด และถือปฏิบัติตามมาตรการเพิ่มประสิทธิภาพการใช้จ่ายงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. ๒๕๖๐ ของสำนักงบประมาณ กรณีค่าใช้จ่ายในการฝึกอบรม ประชุม สัมมนา ให้คำนึงถึงประโยชน์ที่ทางราชการจะได้รับและระยะเวลาที่เหมาะสมเป็นสำคัญฯ สามารถเบิกจ่ายงบประมาณได้ในไตรมาสที่ ๑ ให้มากที่สุดหรือไม่น้อยกว่าร้อยละ ๕๐ ของวงเงินงบประมาณที่ได้รับจัดสรร ตามนัยหนังสือ สำนักงานอัยการสูงสุด ด่วนที่สุด ที่ อส ๐๐๐๖(งป)/ว ๓๑๑ ลงวันที่ ๘ กันยายน ๒๕๕๙ โดยก่อนดำเนินการให้เสนอขออนุมัติโครงการ/กิจกรรมผ่านผู้บังคับบัญชาตามสายงาน และเมื่ออัยการสูงสุดได้อนุมัติแล้วให้ส่งสำเนาเรื่องการอนุมัติพร้อมปฏิทินการดำเนินงาน จำนวน ๑ ชุด ให้สำนักงานอัยการพิเศษฝ่ายนโยบายและยุทธศาสตร์ เพื่อใช้ประกอบการติดตามและประเมินผลการดำเนินงาน สำหรับโครงการ/กิจกรรมที่เป็นการจัดประชุม ฝึกอบรมหรือสัมมนา ให้ประสานงานไปยังสถาบันพัฒนาข้าราชการฝ่ายอัยการเพื่อจัดตารางเวลาดำเนินงาน ทั้งนี้ เพื่อหลีกเลี่ยงการจัดกลุ่มเป้าหมายและระยะเวลาที่ซ้ำซ้อนกัน รายละเอียดปรากฏตามแผนปฏิบัติการฯ แนบท้าย

จึงเรียนมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

(นายนิตสิต ระเบียบธรรม)
รองอัยการสูงสุด ปฏิบัติราชการแทน
อัยการสูงสุด

ส่วนที่ ๑
แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด
พ.ศ. ๒๕๕๙ – ๒๕๖๒ (โดยย่อ)

๑. วิสัยทัศน์ (Vision)

องค์กรอัยการมีความเป็นเลิศในการยุติธรรม และเป็นที่เชื่อมั่นของประชาชน

๒. พันธกิจ (Missions)

(๑) อำนวยความยุติธรรมทางอาญาและบังคับใช้กฎหมายตามหลักนิติธรรม

(๒) รักษาผลประโยชน์ของรัฐและประชาชน

(๓) พัฒนางานด้านสิทธิมนุษยชน คุ้มครองสิทธิและเสรีภาพของประชาชนทั้งในและนอกประเทศตามหลักมาตรฐานสากล

(๔) พัฒนาเครือข่ายความร่วมมือทางกฎหมายกับองค์กรหรือหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

(๕) พัฒนาองค์กรสู่ความเป็นเลิศ

๓. ปรัชญาการดำเนินงาน

ยึดมั่นจงรักภักดีต่อพระมหากษัตริย์ และจะปฏิบัติหน้าที่ด้วยความซื่อสัตย์สุจริตและเที่ยงธรรม โดยปราศจากอคติทั้งปวง เพื่อให้เกิดความยุติธรรมแก่ประชาชน และความสงบสุขแห่งราชอาณาจักร ทั้งจะรักษาไว้และปฏิบัติตามซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทยและกฎหมายทุกประการ"

๔. ค่านิยมร่วม (Shared value)

"JUSTICE"

J = Judgment การใช้ดุลยพินิจอย่างรอบคอบ

U = Unity ความเป็นอันหนึ่งอันเดียวกันภายในองค์กร

S = Service mind ความมีจิตใจให้บริการ

T = Transparency ความโปร่งใสและตรวจสอบได้

I = Integrity ความซื่อสัตย์เชื่อถือได้

C = Contribution อุทิศตนต่อองค์กรและสังคม

E = Equality การปฏิบัติต่อประชาชนอย่างเท่าเทียมกัน

๔. เป้าประสงค์

(๑) สามารถอำนวยความยุติธรรมทางอาญาตามหลักนิติธรรม

(๒) สามารถรักษาผลประโยชน์ของรัฐและประชาชน

(๓) สามารถรักษาและคุ้มครองสิทธิมนุษยชนและเสรีภาพของประชาชนตามหลักมาตรฐานสากล

(๔) สามารถพัฒนาเครือข่ายความร่วมมือทางกฎหมายกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

๕. ประเด็นยุทธศาสตร์ กลยุทธ์ วัตถุประสงค์ และตัวชี้วัดที่สำคัญ

แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี ของสำนักงานอัยการสูงสุด พ.ศ. ๒๕๕๙ - ๒๕๖๒ ประกอบด้วย ๖ ประเด็นยุทธศาสตร์ และกลยุทธ์ ๑๘ กลยุทธ์ โดยแต่ละกลยุทธ์จะมีวัตถุประสงค์และตัวชี้วัดการดำเนินงานดังต่อไปนี้

ประเด็นยุทธศาสตร์	วัตถุประสงค์	ตัวชี้วัด
ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา		
กลยุทธ์ที่ ๑.๑ สร้างมาตรฐานและศักยภาพในการอำนวยความยุติธรรม	๑. เพื่อเพิ่มประสิทธิภาพในการดำเนินคดีอาญาของพนักงานอัยการและการให้บริการประชาชน	๑. ร้อยละขององค์ความรู้ที่ได้ มีมาตรฐานการจัดการความรู้ตามที่สำนักงานอัยการสูงสุดกำหนด ๒. ร้อยละของผู้เข้าร่วมโครงการผ่านเกณฑ์การทดสอบความรู้
กลยุทธ์ที่ ๑.๒ พัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน	๑. เพื่อเพิ่มขีดความสามารถของพนักงานอัยการในด้านการสอบสวนคดีอาญา	๑. ร้อยละขององค์ความรู้ที่ได้ มีมาตรฐานการจัดการความรู้ตามที่สำนักงานอัยการสูงสุดกำหนด ๒. ร้อยละของผู้เข้าร่วมโครงการผ่านเกณฑ์การทดสอบความรู้
กลยุทธ์ที่ ๑.๓ พัฒนาบทบาทหน้าที่ ของพนักงานอัยการในกระบวนการยุติธรรมทางเลือก	๑. เพื่อลดปริมาณคดีอาญาขึ้นสู่ศาลด้วยกระบวนการยุติธรรมทางเลือก	๑. ร้อยละของคดีที่เข้าเกณฑ์สามารถใช้กระบวนการยุติธรรมทางเลือกและพนักงานอัยการได้ใช้กระบวนการดังกล่าว เป็นเหตุให้คดียุติไม่ขึ้นสู่การพิจารณาของศาล
กลยุทธ์ที่ ๑.๔ เพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญา	๑. เพื่อเพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในทางอาญา	๑. ระดับความสำเร็จของการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา

ส่วนที่ ๒

แผนปฏิบัติราชการสำนักงานอัยการสูงสุดประจำปี พ.ศ. ๒๕๖๐

(โครงการตามกรอบคำของบประมาณ)

ยุทธศาสตร์ที่ ๑ การอำนวยความยุติธรรมทางอาญา

กลยุทธ์ที่ ๑.๑ สร้างมาตรฐานและศักยภาพในการอำนวยความยุติธรรม

๑. โครงการพัฒนาระบบฐานข้อมูลสำนักงานการสอบสวน (โครงการใหม่)

๒. โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญา

๓. โครงการพัฒนาศักยภาพพนักงานอัยการและบุคลากรของหน่วยงานที่เกี่ยวข้องกับคดีค้ามนุษย์ (โครงการใหม่ ของบประมาณตามแผนบูรณาการของรัฐบาล)

๔. โครงการฝึกอบรมหลักสูตรพื้นฐานการดำเนินคดีค้ามนุษย์ (โครงการใหม่ ของบประมาณตามแผนบูรณาการของรัฐบาล)

๕. โครงการเพิ่มประสิทธิภาพการดำเนินคดียาเสพติด (ขอเพิ่มเติมไม่ทัน)

๖. โครงการเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาชญากรรมทางเทคโนโลยี

๗. โครงการเพิ่มประสิทธิภาพการดำเนินคดีปราบปรามการทุจริต กิจกรรมเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญาเกี่ยวกับการทุจริตคอร์รัปชั่น (โครงการใหม่)

กลยุทธ์ที่ ๑.๒ พัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน

๑. โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน

กลยุทธ์ที่ ๑.๓ พัฒนาบทบาทหน้าที่ของพนักงานอัยการในกระบวนการยุติธรรมทางเลือก

(ไม่มีโครงการที่เสนอของบประมาณ)

กลยุทธ์ที่ ๑.๔ เพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญา

๑. โครงการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา

ลำดับ	โครงการ/กิจกรรม	ตัวชี้วัด	ค่าเป้าหมาย	งบประมาณ (บาท)	ระยะเวลาดำเนินงาน	หน่วยงานรับผิดชอบ
๔.	**โครงการเพิ่มประสิทธิภาพการดำเนินคดีปราบปรามการทุจริต**					
	กิจกรรมเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญาเกี่ยวกับการทุจริตคอร์รัปชั่น	๑. จำนวนองค์ความรู้ที่ได้มีมาตรฐานการจัดการความรู้ตามที่สำนักงานอัยการสูงสุดกำหนด ๒. ร้อยละของผู้เข้าร่วมโครงการที่ผ่านเกณฑ์การทดสอบความรู้	๑ ๘๐	๑,๒๐๐,๐๐๐	๑ ต.ค. ๕๙ ถึง ๓๐ ก.ย. ๖๐	สคปท.

กลยุทธ์ที่ ๑.๒ พัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน

วัตถุประสงค์ : เพื่อเพิ่มขีดความสามารถของพนักงานอัยการในด้านการสอบสวนคดีอาญา

ตัวชี้วัด ๑. ร้อยละขององค์ความรู้ที่ได้มีมาตรฐานการจัดการความรู้ตามที่สำนักงานอัยการสูงสุดกำหนด

๒. ร้อยละของผู้เข้าร่วมโครงการผ่านเกณฑ์การทดสอบความรู้

ลำดับ	โครงการ/กิจกรรม	ตัวชี้วัด	ค่าเป้าหมาย	งบประมาณ (บาท)	ระยะเวลาดำเนินงาน	หน่วยงานรับผิดชอบ
๕.	**โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน**	๑. จำนวนองค์ความรู้ที่ได้มีมาตรฐานการจัดการความรู้ตามที่สำนักงานอัยการสูงสุดกำหนด ๒. ร้อยละของผู้เข้าร่วมโครงการที่ผ่านเกณฑ์การทดสอบความรู้	๑ ๘๐	๗๕๐,๐๐๐	๑ ต.ค. ๕๙ ถึง ๓๐ ก.ย. ๖๐	สกส.

กลยุทธ์ที่ ๑.๔ เพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศทางอาญา

วัตถุประสงค์ : เพื่อเพิ่มประสิทธิภาพการดำเนินการเกี่ยวกับความร่วมมือระหว่างประเทศในทางอาญา

ตัวชี้วัด : ระดับความสำเร็จของการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา

ลำดับ	โครงการ/กิจกรรม	ตัวชี้วัด	ค่าเป้าหมาย	งบประมาณ (บาท)	ระยะเวลาดำเนินงาน	หน่วยงานรับผิดชอบ
๖.	โครงการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา	๑. รายงานสรุปผลการดำเนินงานหรือข้อเสนอแนะการปฏิบัติงานที่เป็นรูปธรรม ๒. จำนวนกระบวนงานมาตรฐาน/คู่มือการปฏิบัติงาน	๑ ๑	๒๐๐,๐๐๐	๑ ต.ค. ๕๙ ถึง ๓๐ ก.ย. ๖๐	สตป.

สรุป

โครงการ/กิจกรรมที่ได้รับการจัดสรรงบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2560

ตามแผนยุทธศาสตร์และแผนปฏิบัติราชการ 4 ปี สำนักงานอัยการสูงสุด พ.ศ. 2559 – 2562

ลำดับ	ผลผลิต/กิจกรรม/รายการ	งบประมาณ (บาท)	หน่วยงานรับผิดชอบ
แผนงานพื้นฐานด้านการปรับสมดุลและพัฒนาระบบบริหารจัดการภาครัฐ			
แผนงานรอง : การจัดการของรัฐสภา ศาล และหน่วยงานอิสระของรัฐ			
ผลผลิต : การอำนวยการยุติธรรม รักษาผลประโยชน์ของรัฐ และคุ้มครองสิทธิของประชาชน		12,000,000	
กิจกรรม : งานอำนวยความยุติธรรมทางอาญา		4,000,000	
ค่าใช้จ่ายดำเนินงาน		4,000,000	
1	โครงการพัฒนาบทบาทหน้าที่ของพนักงานอัยการด้านการสอบสวน	750,000	สกส.
2	โครงการเพิ่มประสิทธิภาพการให้บริการประชาชนด้วยระบบมาตรฐานงานธุรการ	900,000	สนย.
3	โครงการเพิ่มประสิทธิภาพการบริหารจัดการสำนักงานอัยการสูงสุดเพื่อรองรับการเปลี่ยนแปลง	750,000	สนย.
4	โครงการการเสริมสร้างศักยภาพพนักงานอัยการในการประสานความร่วมมือด้านอาชญากรรมข้ามชาติและความร่วมมือระหว่างประเทศในเรื่องทางอาญา	200,000	สตป.
5	โครงการพัฒนาศักยภาพและการเพิ่มประสิทธิภาพในการดำเนินงานห้องสมุดสำนักงานอัยการสูงสุดเพื่อรองรับการเปลี่ยนแปลง	200,000	สวก.
6	โครงการเพิ่มประสิทธิภาพการดำเนินคดีปราบปรามการทุจริต กิจกรรมเพิ่มศักยภาพของพนักงานอัยการในการดำเนินคดีอาญาเกี่ยวกับการทุจริตคอร์รัปชั่น	1,200,000	สคปท.

ผนวก ข

แบบสอบถามการสัมภาษณ์เชิงลึก (In-depth Interview)

เรื่อง แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย ๔.๐

คำชี้แจง

๑. แบบสอบถามนี้เป็นแบบสอบถาม**ผู้ทรงคุณวุฒิด้านงานคดีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์** มีวัตถุประสงค์เพื่อนำคำตอบที่ได้ไปใช้ประโยชน์ในการทำวิจัยทางวิชาการ ของ นายธีระวัฒน์ พุฒิบูรณวัฒน์ ตำแหน่งอัยการผู้เชี่ยวชาญ สำนักงานอัยการพิเศษฝ่ายนโยบายและยุทธศาสตร์ สำนักงานอัยการสูงสุด ผู้วิจัย ซึ่งเป็นส่วนหนึ่งของหลักสูตรการป้องกันราชอาณาจักร (วปอ.)

๒. ในแบบสอบถามนี้

“คดีอาชญากรรมคอมพิวเตอร์” หมายถึง (๑) คดีอาญาที่กระทำผิดต่อระบบคอมพิวเตอร์ เช่น การเข้าถึงและการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ หรือการขัดขวางการเข้าสู่ระบบคอมพิวเตอร์โดยปกติของผู้อื่น และ (๒) คดีอาญาซึ่งมีการใช้คอมพิวเตอร์ในการกระทำความผิด เช่น การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลเท็จเพื่อการฉ้อโกงทรัพย์ การใช้ระบบคอมพิวเตอร์ในการเล่นพนันออนไลน์ การนำเข้าข้อมูลคอมพิวเตอร์ในการกระทำผิดละเมิดลิขสิทธิ์ และการนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นการเผยแพร่ภาพข้อมูลที่มีลักษณะลามกอนาจาร เป็นต้น

“ประเทศไทย ๔.๐” หมายถึง นโยบาย “ประเทศไทย ๔.๐” หรือ “ไทยแลนด์ ๔.๐” ซึ่งเป็นกลไกขับเคลื่อนการปฏิรูปเศรษฐกิจและความมั่นคงในศตวรรษที่ ๒๑ ไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม (Value-Based Economy) โดยการเติมเต็มด้วยวิทยาการ ความคิดสร้างสรรค์ นวัตกรรม วิทยาศาสตร์ เทคโนโลยี และการวิจัยและการพัฒนา โดยมีกลุ่มดิจิทัลเทคโนโลยีอินเตอร์เน็ตที่เชื่อมต่อและบังคับอุปกรณ์ต่างๆ เป็นหนึ่งในกลุ่มเทคโนโลยีและอุตสาหกรรมเป้าหมาย ส่งเสริมการใช้เทคโนโลยีด้านดิจิทัลและคอมพิวเตอร์ในการพัฒนาเศรษฐกิจและสังคมทั้งภาครัฐและเอกชน ซึ่งแนวนโยบายนี้ได้ถูกผนวกรวมอยู่ในยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐-๒๕๗๙) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ. ๒๕๖๐-๒๕๖๔)

ในแบบสอบถามนี้ มุ่งเน้นความหมายของประเทศไทย ๔.๐ ในส่วนของการพัฒนาและส่งเสริมการใช้ระบบคอมพิวเตอร์ อินเตอร์เน็ต และระบบสื่อสารดิจิทัล ในการทำธุรกิจของภาคเอกชน เช่น การทำธุรกรรมด้านการค้าและบริการทางอิเล็กทรอนิกส์ (e-commerce) ธุรกรรมการชำระราคา (e-payment) และธุรกรรมการเงินทางอิเล็กทรอนิกส์ (e-banking) รวมถึงการใช้งานระบบคอมพิวเตอร์ในสื่อสังคมออนไลน์ (social media)

๓. แบบสอบถามชุดนี้ แบ่งออกเป็น ๒ ตอน คือ

ตอนที่ ๑ ข้อมูลทั่วไป

ตอนที่ ๒ ความคิดเห็นเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์

ขอความกรุณาโปรดตอบแบบสอบถาม และขอขอบพระคุณล่วงหน้าในความร่วมมือตอบแบบสอบถามของท่าน

ตอนที่ ๑ ข้อมูลทั่วไป

๑.ชื่อผู้ตอบแบบสอบถาม.....

๒.ตำแหน่งและสำนักงานที่ทำงานปัจจุบัน.....

๓.ลักษณะงาน ☐ ผู้บริหาร (ในแต่ละสำนักงานที่ทำงานอยู่) ☐ ผู้ปฏิบัติงาน

๔.ลักษณะหน้าที่และความรับผิดชอบในปัจจุบัน (รวมถึงลักษณะงานที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์)

.....

.....

๕.ระยะเวลาการปฏิบัติงานอัยการ รวม ..... ปี แบ่งเป็น

☐ ด้านงานคดีอาญา ..... ปี

☐ ด้านงานคดีอื่นๆ ..... ปี

๖.ท่านเคยมีประสบการณ์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ (การสั่งคดี, การว่าความ, การร่วมสอบสวน) หรือไม่

☐ เคย ☐ ไม่เคย

ตอนที่ ๒ ความคิดเห็นเกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์

๗.ท่านเห็นว่า นโยบายประเทศไทย ๔.๐ จะมีผลกระทบต่อจำนวนปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดหรือไม่ อย่างไร

.....

.....

.....

๘.ท่านเห็นว่า ลักษณะการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความแตกต่างจากการดำเนินคดีอาญาทั่วไป หรือไม่ อย่างไร (การรวบรวมพยานหลักฐาน, การพิสูจน์การกระทำความผิดของผู้ต้องหา/จำเลย, การรับฟังพยานหลักฐานดิจิทัล, ความซับซ้อนยุ่งยากทางคดี)

.....

.....

.....

๙.โปรดยกตัวอย่างคดีอาชญากรรมคอมพิวเตอร์ที่น่าสนใจหรือมีความยุ่งยากที่อยู่ระหว่างการดำเนินการหรือเคยดำเนินการโดยท่าน (ข้อเท็จจริงโดยย่อ พยานหลักฐานที่เกี่ยวข้อง ความเห็นและคำสั่งโดยย่อ ลักษณะปัญหา/อุปสรรคที่พบ แนวทางการแก้ไขปัญหา ฯลฯ ทั้งนี้ไม่จำต้องเปิดเผยชื่อที่แท้จริงของบุคคลที่เกี่ยวข้อง)

.....

.....

.....

.

๑๐.ในการปฏิบัติงานด้านคดีอาชญากรรมคอมพิวเตอร์ตามภาระงานในหน้าที่ของท่าน สำนักงานอัยการสูงสุดได้กำหนดระเบียบ ประกาศ คำสั่ง หนังสือเวียน คู่มือ หรือแนวทางปฏิบัติด้านการดำเนินคดีอาชญากรรมคอมพิวเตอร์ไว้หรือไม่ อย่างไร (โปรดระบุเท่าที่ทราบ)

.....

.....

.....

๑๑.ท่านเห็นว่าการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ (การสั่งคดี, การว่าความ, การร่วมสอบสวน) มีปัญหาและอุปสรรคตั้งแต่ชั้นรับสำนวนการสอบสวนถึงชั้นพิจารณาคดี อย่างไรบ้าง (เช่น ความสมบูรณ์ของสำนวนการสอบสวน, การประสานงานและความร่วมมือของหน่วยงานที่เกี่ยวข้อง, องค์ความรู้ที่เกี่ยวข้อง, การนำเสนอพยานหลักฐาน)

.....

.....

.....

๑๒.ท่านเห็นว่า โครงสร้างความรับผิดชอบงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานคดีภายในสำนักงานอัยการสูงสุด ปัญหาความซ้ำซ้อน หรือไม่ อย่างไร (โปรดระบุแนวทางการแก้ไขปัญหาด้วย)

.....

.....

.....

๑๓.ท่านเห็นว่า สถิติเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ มีความเกี่ยวข้องหรือมีความสำคัญในการกำหนดแนวนโยบายผู้บริหาร แผนยุทธศาสตร์ และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด หรือไม่ อย่างไร

.....

.....

.....

๑๔.ท่านเห็นว่า แผนยุทธศาสตร์และแผนปฏิบัติราชการ ๔ ปี สำนักงานอัยการสูงสุด พ.ศ.๒๕๕๙-๒๕๖๒ และแผนปฏิบัติการสำนักงานอัยการสูงสุดประจำปี (Action Plan) มีความเกี่ยวข้องกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของผู้ปฏิบัติงาน หรือไม่อย่างไร (เช่น มีการกำหนดแนวทางการดำเนินคดีอาชญากรรมคอมพิวเตอร์สำหรับผู้ปฏิบัติงานหรือไม่ อย่างไร)

.....

.....

.....

๑๕.ท่านเห็นว่า ภายหลังจากที่รัฐบาลดำเนินนโยบายประเทศไทย ๔.๐ แล้ว สำนักงานอัยการสูงสุดควรมีแนวนโยบายการบริหาร หรือแผนยุทธศาสตร์องค์กรเพื่อเตรียมความพร้อมสำหรับพนักงานอัยการซึ่งรับผิดชอบในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ หรือไม่ อย่างไร

.....

.....

.....

๑๖.ท่านเห็นว่า สำนักงานอัยการสูงสุดควรมีแนวทางปรับปรุงยุทธศาสตร์ในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดเพื่อรองรับปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ภายหลังรัฐบาลดำเนินนโยบายประเทศไทย ๔.๐ โดยปรับปรุงหรือจัดให้มีสิ่งใดเพื่อประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์

(เช่น การฝึกอบรมความรู้, การจัดการแหล่งข้อมูลศึกษาค้นคว้า เช่นระบบสืบค้นข้อมูลสำคัญหรือห้องสมุด, การเตรียมความพร้อมด้านอุปกรณ์และเครื่องมือในการปฏิบัติงาน, การจัดทำหรือปรับปรุงคู่มือหรือแนวปฏิบัติในการดำเนินคดีอาชญากรรมคอมพิวเตอร์, การประสานความร่วมมือของหน่วยงานภายในและภายนอก ฯลฯ โปรดระบุรูปแบบและรายละเอียด)

.....

.....

.....

๑๗.ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

ลงชื่อ ..... ผู้ตอบแบบสอบถาม

ประวัติย่อผู้วิจัย

ชื่อ นายธีระวัฒน์ พุฒิบูรณวัฒน์

วัน เดือน ปี เกิด ๒๓ มกราคม ๒๕๐๖

การศึกษา นิติศาสตร์บัณฑิต มหาวิทยาลัยรามคำแหง
เนติบัณฑิตไทย สำนักอบรมศึกษากฎหมาย แห่งเนติบัณฑิตยสภา

ประวัติการทำงาน อัยการจังหวัดชัยภูมิ
อัยการจังหวัดพัทยา

ตำแหน่งปัจจุบัน อัยการผู้เชี่ยวชาญพิเศษ

สรุปย่อ

ลักษณะวิชา ยุทธศาสตร์

เรื่อง แนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาเพื่อตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย 4.0

ผู้วิจัย นายธีระวัฒน์ พุฒิบูรณวัฒน์ หลักสูตร วปอ. รุ่นที่ 59

ตำแหน่ง อัยการผู้เชี่ยวชาญพิเศษ สำนักงานอัยการสูงสุด

ความเป็นมาและความสำคัญของปัญหา

การกำหนดยุทธศาสตร์และแผนปฏิบัติราชการของหน่วยงานภาครัฐจำเป็นต้องสอดคล้องกับแผนยุทธศาสตร์ชาติซึ่งเป็นกรอบภาพรวมของการจัดทำนโยบายและการจัดสรรงบประมาณของรัฐบาล รวมไปถึงต้องสอดคล้องกับแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติด้วย เพื่อให้การปฏิบัติราชการของหน่วยราชการต่างๆเป็นไปในทิศทางเดียวกันและสอดคล้องกัน ทั้งนี้ เมื่อประมาณกลางปีพ.ศ. 2559 พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) ได้กล่าวมอบนโยบายเกี่ยวกับการนำพาประเทศไทยก้าวสู่โมเดล “ประเทศไทย 4.0” หรือ “ไทยแลนด์ 4.0” อันเป็นกลไกขับเคลื่อนการปฏิรูปเศรษฐกิจและความมั่นคงในศตวรรษที่ 21 ไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม โดยมีกลุ่มดิจิทัล และเทคโนโลยีอินเทอร์เน็ต เป็นหนึ่งในกลุ่มเทคโนโลยีเป้าหมาย แนวนโยบายนี้ได้ถูกผนวกรวมอยู่ในยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ. 2560 – 2579) และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 (พ.ศ. 2560 – 2564) ในส่วนของสำนักงานอัยการสูงสุดซึ่งเป็นหน่วยงานสำคัญในกระบวนการยุติธรรมทางอาญา ได้ประกาศใช้ยุทธศาสตร์และแผนปฏิบัติราชการ 4 ปี (พ.ศ. 2559 – 2562) อันเป็นแผนแม่บทยุทธศาสตร์เฉพาะขององค์กรอัยการ โดยในส่วนของแผนงานด้านการอำนวยความยุติธรรมทางอาญา แม้ว่าสำนักงานอัยการสูงสุดได้กำหนดกลยุทธ์เพื่อเพิ่มประสิทธิภาพในการดำเนินคดีอาญาของพนักงานอัยการไว้แล้วก็ตาม แต่ยุทธศาสตร์สำนักงานอัยการสูงสุดฉบับดังกล่าวมีการจัดทำและประกาศใช้ก่อนที่ยุทธศาสตร์ชาติระยะ 20 ปี และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 ซึ่งผนวกรวมแนวนโยบายประเทศไทย 4.0 ไว้ จะบังคับใช้ เนื่องจากสภาพเศรษฐกิจและสังคมของโลกในยุคปัจจุบันได้เปลี่ยนแปลงไปจากอดีตอย่างมาก จนมีคำพูดว่า “The whole world has gone digital” หรือ “โลกทั้งใบได้เปลี่ยนเป็นดิจิทัลแล้ว” เห็นได้จากอัตราการเติบโตในแต่ละปีของจำนวนผู้ใช้งานอินเทอร์เน็ตผ่านอุปกรณ์สื่อสารและโทรศัพท์สมาร์ทโฟน นอกจากนี้ รูปแบบการประกอบธุรกิจทางการค้าแบบดั้งเดิมถูกแทนที่โดยธุรกรรมทางอิเล็กทรอนิกส์ซึ่งได้รับความนิยมจากผู้บริโภคเพิ่มมากขึ้นทุกปีโดยผู้ซื้อและผู้ขายไม่จำต้องพบหน้ากันและไม่ต้องส่งมอบเงินสดในการชำระค่าราคาสินค้า อันเป็นการประหยัดทั้งเวลาและค่าใช้จ่าย ทั้งสองฝ่ายสามารถจัดการทางการเงินผ่านระบบธนาคารทางอินเทอร์เน็ต (I-Banking) หรือระบบธนาคารทางโทรศัพท์เคลื่อนที่ (Mobile Banking) แต่ทว่า ธุรกรรมต่างๆ ดังกล่าวก็อาจตกเป็นเป้าหมายของกลุ่มมิจฉาชีพได้โดยง่าย ซึ่งความเสียหายของอาชญากรรมเกี่ยวกับคอมพิวเตอร์มักเกิดเป็นความเสียหายในวงกว้างและมีมูลค่าความเสียหายจำนวนสูงมาก เมื่อมีการกระทำความผิดอาญา

เกี่ยวกับคอมพิวเตอร์เกิดขึ้น บุคลากรในหน่วยงานด้านการยุติธรรมที่มีอำนาจหน้าที่พิจารณามีคำสั่งฟ้องหรือไม่ฟ้องผู้ต้องหาในคดีอาญาและดำเนินคดีอาญาชั้นพิจารณาในศาล คือ พนักงานอัยการ แต่ทว่าลักษณะของการดำเนินคดีอาชญากรรมคอมพิวเตอร์มีความพิเศษแตกต่างไปจากการดำเนินคดีอาญาทั่วไปบางประการ อาทิเช่น รูปแบบการรวบรวมพยานหลักฐาน การพิจารณาพยานหลักฐาน และการนำสืบคดีในชั้นศาล พนักงานอัยการผู้ดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์จึงจำเป็นต้องมีองค์ความรู้ด้านระบบคอมพิวเตอร์และองค์ความรู้ด้านพยานหลักฐานทางดิจิทัลอย่างเหมาะสม ปริมาณงานด้านคดีอาชญากรรมคอมพิวเตอร์ภายหลังการดำเนินการภายใต้นโยบายประเทศไทย 4.0 ที่ภาครัฐส่งเสริมให้มีการใช้อุปกรณ์ดิจิทัลและระบบคอมพิวเตอร์ในการพัฒนาเศรษฐกิจและสังคมย่อมมีแนวโน้มสูงขึ้น หากสำนักงานอัยการสูงสุดซึ่งมีบทบาทหน้าที่ด้านงานคดีอาชญากรรมคอมพิวเตอร์ยังไม่มีแผนงานที่ชัดเจนเพื่อเตรียมความพร้อมในด้านต่างๆเพื่อการตอบโต้อาชญากรรมคอมพิวเตอร์ย่อมส่งผลทำให้เกิดปัญหาในประสิทธิภาพในการอำนวยความยุติธรรมทางอาญาในคดีอาชญากรรมคอมพิวเตอร์ และส่งผลกระทบในภาพรวมถึงความมั่นคงทางเศรษฐกิจและสังคมของชาติดังได้

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวโน้มปริมาณงานและพัฒนาการความซับซ้อนของคดีอาชญากรรมคอมพิวเตอร์ และสภาพปัญหาและอุปสรรคของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย 4.0
2. เพื่อเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดและแนวทางการกำหนดแผนงานด้านการอำนวยความยุติธรรมของหน่วยงานภายในสำนักงานอัยการสูงสุดที่มีความรับผิดชอบงานด้านคดีอาชญากรรมคอมพิวเตอร์ ตามยุทธศาสตร์และแผนปฏิบัติราชการ 4 ปี สำนักงานอัยการสูงสุด พ.ศ. 2559 – 2562 เพื่อให้สอดคล้อง เพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในชั้นพนักงานอัยการ ภายหลังการดำเนินการขับเคลื่อนเศรษฐกิจตามนโยบายประเทศไทย 4.0

ขอบเขตของการวิจัย

1. ด้านเนื้อหา ศึกษาผลกระทบด้านคดีอาชญากรรมทางเศรษฐกิจที่มีการใช้คอมพิวเตอร์ในการกระทำความผิด และคดีที่มีการกระทำความผิดต่อระบบคอมพิวเตอร์ ภายหลังการดำเนินนโยบายประเทศไทย 4.0 โดยเสนอแนะแนวทางการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเฉพาะงานด้านการอำนวยความยุติธรรม
2. ด้านประชากร ศึกษาแนวคิดของผู้ทรงคุณวุฒิผ่านการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านการคดีอาชญากรรมคอมพิวเตอร์ รวม 10 คน
3. ด้านพื้นที่ ศึกษาแนวทางการกำหนดยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของต่างประเทศ ได้แก่ สหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์
4. ด้านเวลา ศึกษาสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ย้อนหลังไม่เกิน 5 ปี

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ เป็นการศึกษาบทบัญญัติกฎหมาย ระเบียบ คำสั่ง คู่มือแนวทางปฏิบัติของหน่วยงาน รวมถึงเอกสารทางวิชาการและงานวิจัยต่างๆ ที่มีเนื้อหาเกี่ยวกับนโยบายประเทศไทย 4.0 ตามยุทธศาสตร์ชาติ 20 ปี และแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 การพัฒนาเศรษฐกิจและสังคมดิจิทัลของไทย สถิติเกี่ยวกับการใช้งานระบบคอมพิวเตอร์และสถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ แนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มประเทศผู้นำด้านเทคโนโลยีดิจิทัล อำนาจหน้าที่ตามกฎหมายของพนักงานอัยการในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ และแนวคิดด้านการอำนวยความยุติธรรมในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ตามยุทธศาสตร์สำนักงานอัยการสูงสุด

1.2 ข้อมูลปฐมภูมิ จากการสัมภาษณ์ข้อมูลเชิงลึกกลุ่มตัวอย่างพนักงานอัยการในหลากหลายสำนักงานคดีของสำนักงานอัยการสูงสุด

2. การวิเคราะห์ข้อมูล โดยการนำเอาข้อมูลรวมสถิติที่รวบรวมได้ในข้อ 1.1 ในห้วงเวลาย้อนหลังไม่เกิน 5 ปี มาวิเคราะห์แนวโน้มสภาพปัญหาอาชญากรรมคอมพิวเตอร์ภายหลังการขับเคลื่อนนโยบายประเทศไทย 4.0 จากนั้นวิเคราะห์แนวคิดในการกำหนดยุทธศาสตร์สำนักงานอัยการสูงสุดในการตอบโต้อาชญากรรมคอมพิวเตอร์ เปรียบเทียบกับแนวคิดแผนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศต้นแบบด้านการตอบโต้ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ ได้แก่ สหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ พิจารณาร่วมกับข้อมูลผลการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิด้านคดีอาชญากรรมคอมพิวเตอร์โดยใช้วิธีการประสมประสานข้อมูลเข้าด้วยกัน แล้วนำข้อมูลที่ได้จากการวิเคราะห์ดังที่ได้กล่าวมาทั้งหมดมาใช้วิเคราะห์สภาพปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ของพนักงานอัยการ และเสนอแนะแนวทางในการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดด้านการอำนวยความยุติธรรมทางอาญาให้เหมาะสมและมีประสิทธิภาพในการตอบโต้อาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย 4.0

ผลการวิจัย

ผลการวิจัยพบว่า สถิติภัยคุกคามทางไซเบอร์ที่มีการรายงานผ่านศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) และการสัมภาษณ์เชิงลึกพนักงานอัยการผู้ทรงคุณวุฒิ สะท้อนปริมาณงานคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดว่ามีแนวโน้มเพิ่มมากขึ้นและมีรูปแบบการกระทำผิดซับซ้อนมากขึ้นกว่าในอดีต อย่างไรก็ดีระหว่างการวิจัยพบปัญหาการจัดเก็บสถิติคดีอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุดซึ่งใช้การบันทึกสารบบคดีที่อาจไม่สะท้อนสถิติคดีอาชญากรรมคอมพิวเตอร์โดยตรง กล่าวคือ การบันทึกสถิติคดีแต่ละสำนวนคดียังคงยึดฐานความผิดซึ่งมีอัตราโทษตามกฎหมายที่สูงกว่าเป็นหลัก อีกทั้งการจัดเก็บสถิติมิได้มีการบูรณาการร่วมกับฐานข้อมูลสถิติหน่วยงานในกระบวนการยุติธรรมอื่น จึงอาจทำให้การใช้ประโยชน์สถิติจำกัดอยู่เพียงภายในงานของสำนักงานอัยการสูงสุด อีกทั้ง ข้อมูลสถิติอาจไม่เพียง

พอที่จะใช้สนับสนุนในการขอจัดสรรงบประมาณเพิ่มเติมสำหรับการพัฒนาองค์ความรู้ด้านดิจิทัลให้กับพนักงานอัยการ ในด้านโครงสร้างการดำเนินคดีอาชญากรรมคอมพิวเตอร์ภายใต้ยุทธศาสตร์สำนักงานอัยการสูงสุดปัจจุบัน พบว่า ไม่มีสำนักงานคดีใดเป็นผู้รับผิดชอบเป็นการเฉพาะเนื่องจากการก่ออาชญากรรมคอมพิวเตอร์มักมีความผิดทางอาญาอื่นรวมอยู่ด้วย อาทิเช่น ความผิดอาชญากรรมทางเศรษฐกิจ ความผิดเกี่ยวกับทรัพย์สินทางปัญญา หรือความผิดทางอาญาตามประมวลกฎหมายอาญา เป็นต้น ทำให้อำนาจการดำเนินคดีบางกรณียังคงมีความซ้ำซ้อนระหว่างสำนักงานคดีในส่วนกลางของสำนักงานอัยการสูงสุด ในด้านการอบรมให้ความรู้ด้านพยานหลักฐานทางดิจิทัลแก่พนักงานอัยการ พบว่า โครงการภายใต้แผนยุทธศาสตร์สำนักงานอัยการสูงสุดมีลักษณะอยู่ภายใต้การดำเนินงานพัฒนาศักยภาพของพนักงานอัยการในแต่ละสำนักงานคดี ซึ่งแต่ละแห่งจำเป็นต้องจัดอบรมความรู้ให้กับพนักงานอัยการในงานคดีอย่างอื่นซึ่งมีความจำเป็นเช่นเดียวกัน ประกอบกับปัจจุบันยังไม่มีการปรับปรุงคู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์ที่มีการจัดทำตั้งแต่ปี 2554 ทำให้การขาดองค์ความรู้ด้านพยานหลักฐานดิจิทัลอย่างเหมาะสมถือได้ว่าเป็นปัญหาและอุปสรรคประการสำคัญในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ นอกจากนี้เมื่อเปรียบเทียบแนวทางในการตอบโต้ภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ของสหรัฐอเมริกา เครือรัฐออสเตรเลีย และสาธารณรัฐสิงคโปร์ พบว่า เว้นแต่กรณีที่มีกฎหมายกำหนดเป็นการเฉพาะในคดีอาญาทั่วไป พนักงานสอบสวนจะเป็นผู้มีอำนาจสอบสวน แตกต่างจากพนักงานอัยการในกลุ่มประเทศต้นแบบที่มีบทบาทและอำนาจในการเข้าร่วมสอบสวนหรือให้คำแนะนำอย่างใกล้ชิดแก่พนักงานสอบสวนได้ ซึ่งแม้ว่าพนักงานอัยการไทยจะมีอำนาจสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติมภายหลังที่พนักงานสอบสวนทำการสอบสวนเสร็จสิ้น แต่จากการขาดการประสานงานอย่างบูรณาการระหว่างหน่วยงานในกระบวนการยุติธรรมทางอาญาและความเชี่ยวชาญในการรวบรวมพยานหลักฐานทางดิจิทัลย่อมส่งผลให้การดำเนินการล่าช้าและอาจส่งผลให้พยานหลักฐานทางดิจิทัลสูญหายหรือเสียหายได้

ข้อเสนอแนะ

ผู้วิจัยเห็นว่า ในการปรับปรุงยุทธศาสตร์สำนักงานอัยการสูงสุดเพื่อให้สอดคล้องเพียงพอ และมีประสิทธิภาพในการดำเนินคดีอาชญากรรมคอมพิวเตอร์ในยุคประเทศไทย 4.0 สำนักงานอัยการสูงสุดควรมีการดำเนินการ ดังต่อไปนี้

1. ข้อเสนอแนะระดับนโยบาย ควรแก้ไขปัญหาด้านโครงสร้างหน่วยงานผู้รับผิดชอบคดีอาชญากรรมคอมพิวเตอร์ให้ชัดเจนขึ้นโดยรับฟังความคิดเห็นและข้อเสนอแนะจากทุกสำนักงานที่เกี่ยวข้องประกอบด้วย พร้อมทั้งสร้างแนวทางประสานความร่วมมือในการดำเนินคดีอาชญากรรมคอมพิวเตอร์กับหน่วยงานอื่นทั้งรูปแบบทางการและความร่วมมือที่ไม่เป็นทางการ รวมถึงแนวทางประสานงานกับองค์กรต่างประเทศเพื่อการแลกเปลี่ยนองค์ความรู้ด้านอาชญากรรมคอมพิวเตอร์และพยานหลักฐานทางดิจิทัลในการรับมืออาชญากรรมรูปแบบใหม่ๆ ที่เริ่มเกิดขึ้นในปัจจุบัน

2. ข้อเสนอแนะระดับปฏิบัติการ ควรเร่งจัดฝึกอบรมให้ความรู้ที่เกี่ยวกับการดำเนินคดีอาชญากรรมคอมพิวเตอร์ที่มีความซับซ้อนในปัจจุบันให้กับพนักงานอัยการ โดยควรมีองค์ประกอบของวิทยากรและผู้ฝึกอบรมที่มาจากพนักงานสอบสวนและเจ้าพนักงานผู้ตรวจพิสูจน์หลักฐานที่มี

ความรู้ความเข้าใจเกี่ยวกับพยานหลักฐานทางดิจิทัลด้วย เพื่อแบ่งปันข้อมูลประสบการณ์เกี่ยวกับการปฏิบัติงานและการดำเนินคดีเชิงบูรณาการ ควบคู่ไปกับการสร้างเครื่องมือในการปฏิบัติงานของพนักงานอัยการอย่างยั่งยืน เช่น ปรับปรุงคู่มือการดำเนินคดีอาชญากรรมคอมพิวเตอร์และจัดตั้งศูนย์รวบรวม วิเคราะห์ และเผยแพร่องค์ความรู้ให้แก่พนักงานอัยการ

3. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป ควรปรับปรุงการบันทึกรายการคดีในระบบสารบบคดีของสำนักงานอัยการสูงสุดและเพิ่มประสิทธิภาพในการจัดเก็บสถิติอาชญากรรมคอมพิวเตอร์ของสำนักงานอัยการสูงสุด ให้มีลักษณะที่เป็นฐานข้อมูลที่สอดคล้องกับฐานข้อมูลสถิติของหน่วยงานในกระบวนการยุติธรรมอื่นด้วยตั้งแต่ต้นสายของกระบวนการยุติธรรมไปจนถึงปลายทางในกระบวนการยุติธรรม เพื่อประโยชน์ในการจัดทำรายงานอาชญากรรมระดับชาติตามแนวทางที่ วิทยา สุริยะวงค์ (2552) ได้เสนอแนะไว้ และเพื่อเป็นข้อมูลสนับสนุนการขอรับจัดสรรงบประมาณประจำปีต่อไป