รายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community) กรณีศึกษา ประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์

โดย กองคดีเทคโนโลยีและสารสนเทศ
กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม

ปี พ.ศ. ๒๕๖๔

คำนิยม

ในปัจจุบันความเจริญก้าวหน้าของเทคโนโลยีคอมพิวเตอร์ที่เข้ามามีบทบาทในชีวิตประจำวันเป็นอย่างมาก แต่ในขณะเดียวกันก็เป็นช่องทางให้ผู้ไม่หวังดีสามารถใช้ในการก่ออาชญากรรมได้ ซึ่งอาชญากรรมทางคอมพิวเตอร์จะมีลักษณะที่ยุ่งยากสลับซับซ้อน ทำให้ยากแก่การระงับยับยั้งความเสียหายได้ทันท่วงที ส่งผลกระทบเป็นวงกว้างต่อระบบเศรษฐกิจ สังคม ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน และมีแนวโน้มที่ผู้กระทำผิดจะนำเทคโนโลยีมาใช้เป็นเครื่องมือในการกระทำผิดเพิ่มมากยิ่งขึ้น

กรมสอบสวนคดีพิเศษ เป็นส่วนราชการสังกัดกระทรวงยุติธรรม ที่มีภารกิจในการป้องกันการปราบปราม การสืบสวนและการสอบสวนคดีพิเศษในความผิดเกี่ยวกับเทคโนโลยีและสารสนเทศ ซึ่งเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติมโดยประกาศ กคพ. (ฉบับที่ ๗) พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะความผิดเกี่ยวกับคอมพิวเตอร์ในรูปแบบต่าง ๆ ซึ่งในการดำเนินการดังกล่าวจำเป็นต้องมีผู้เชี่ยวชาญเฉพาะด้านเป็นผู้ดำเนินการสืบสวนสอบสวนเป็นการเฉพาะ ดังนั้น กรมสอบสวนคดีพิเศษจึงให้ความสำคัญกับการพัฒนาศักยภาพของบุคลากรและหน่วยงาน เพื่อให้การป้องกันปราบปรามการกระทำความผิดดังกล่าวเป็นไปอย่างมีประสิทธิภาพ เกิดผลสัมฤทธิ์สูง ซึ่งการจัดทำรายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community) กรณีศึกษา ประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ ในครั้งนี้จะเป็นส่วนสำคัญที่จะนำความรู้ที่ได้รับมาพัฒนาระบบงานการสืบสวนสอบสวน สามารถกำหนดแนวทางในการรับมือกับอาชญากรรมคอมพิวเตอร์ และบูรณาการการบังคับใช้กฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ของกรมสอบสวนคดีพิเศษกับหน่วยงานต่าง ๆ ไม่ว่าในประเทศหรือต่างประเทศได้ในอนาคต

กรมสอบสวนคดีพิเศษขอแสดงความชื่นชมยินดีแก่คณะทำงานศึกษาวิจัย ตลอดจนถึงผู้ที่มีส่วนเกี่ยวข้องทุก ๆ ท่าน ที่ได้ร่วมกันดำเนินโครงการในครั้งนี้จนประสบผลสำเร็จ และร่วมกันจัดทำรายงานศึกษาวิจัยจนเสร็จสมบูรณ์ ขอให้นำความรู้ที่ได้รับในครั้งนี้มาปรับใช้ให้เกิดประโยชน์สูงสุดเพื่อความสงบสุขเรียบร้อยของสังคมและประเทศชาติต่อไป

พันตำรวจโท กรวัชร์ ปานประภากร
อธิบดีกรมสอบสวนคดีพิเศษ
กรกฎาคม ๒๕๖๔

คำนำ

กองคดีเทคโนโลยีและสารสนเทศ เป็นหน่วยงานบังคับใช้กฎหมายในสังกัดกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม มีภารกิจหน้าที่ในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับการใช้เทคโนโลยีและสารสนเทศเป็นเครื่องมือในการกระทำความผิด มีอำนาจหน้าที่ในการป้องกัน ปราบปราม และสืบสวนสอบสวนดำเนินคดีกับผู้กระทำผิดทางคดีเทคโนโลยีและสารสนเทศ รวมถึงการวิเคราะห์และพิสูจน์ความผิดทางคดีเทคโนโลยีและสารสนเทศ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ ประกอบกับกฎกระทรวง ว่าด้วยการกำหนดความผิดคดีพิเศษเพิ่มเติม ทั้งนี้ ที่ผ่านมาพบว่าผู้ต้องหาหรือผู้กระทำความผิดมักจะใช้ประเทศในกลุ่มอาเซียนเป็นฐานในการกระทำความผิดและเป็นที่หลบซ่อนตัวทำให้ยากแก่การสืบสวน สอบสวน รวมทั้งติดตามจับกุมเพื่อดำเนินคดี ดังนั้นจึงมีความจำเป็นอย่างยิ่งที่ประเทศในกลุ่มประเทศในอาเซียนจะต้องร่วมมือกันในการบังคับใช้กฎหมายด้านต่าง ๆ ได้แก่ การแลกเปลี่ยนเรียนรู้เกี่ยวกับรูปแบบการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ของประเทศในกลุ่มอาเซียน การศึกษาประเด็นข้อกฎหมาย การสร้างเครือข่ายการประสานงาน การเสริมสร้างให้เกิดความสัมพันธ์ที่ดี การสร้างความร่วมมือในการเฝ้าระวังผู้กระทำผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การให้ความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา การแลกเปลี่ยน ข้อมูลข่าวสารของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย รวมทั้ง การฝึกอบรมทางวิชาการ และเทคนิคการสืบสวนสอบสวนต่าง ๆ เพื่อให้ภารกิจการป้องกันปราบปรามคดีอาชญากรรมทางคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของกองคดีเทคโนโลยีและสารสนเทศบรรลุผลสำเร็จอย่างมีประสิทธิภาพ

จากเหตุผลและความจำเป็นดังกล่าวข้างต้น กองคดีเทคโนโลยีและสารสนเทศจึงได้ริเริ่มจัดทำโครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการแนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ตั้งแต่ปีงบประมาณ พ.ศ. ๒๕๕๙ ถึง พ.ศ. ๒๕๖๑ โดยศึกษาดูงานที่ประเทศมาเลเซีย เมื่อปี พ.ศ. ๒๕๕๙ สาธารณรัฐสิงคโปร์ เมื่อปี พ.ศ. ๒๕๖๐ สาธารณรัฐฟิลิปปินส์ เมื่อปี พ.ศ. ๒๕๖๑ และจัดสัมมนาโครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการ แนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม หัวข้อ “การปรับตัวกับ Cyber Warfare ในอนาคต” และ “การเผชิญหน้ากับ Cyber Crime เมื่อวันที่ ๒๗ มิถุนายน ๒๕๖๑ พร้อมรับฟังความคิดเห็นและข้อเสนอแนะ จึงได้รวบรวมข้อมูลและศึกษาค้นคว้าวิเคราะห์เปรียบเทียบเพิ่มเติม ซึ่งข้อมูลการวิเคราะห์จะเป็นประโยชน์ในการพัฒนาบุคลากร เครื่องมือ และกระบวนการสืบสวนสอบสวน รวมถึงการดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมอื่นที่เกี่ยวข้องให้มีประสิทธิภาพมากยิ่งขึ้น

พันตำรวจโท วิชัย สุวรรณประเสริฐ
ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ
ประธานคณะทำงานศึกษาวิจัย
กรกฎาคม ๒๕๖๔

บทคัดย่อ

<u>ชื่อผลงาน</u> : รายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community) กรณีศึกษาประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์

<u>ชื่อเจ้าของผลงาน</u> : กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ

การศึกษาวิจัยในครั้งนี้มีวัตถุประสงค์เพื่อศึกษารูปแบบการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ ทำให้สามารถเห็นภาพรวมอาชญากรรมที่เกิดขึ้นในแต่ละประเทศ เป็นแนวทางการดำเนินคดี (Guidance) พร้อมทั้งนำข้อมูลมาเชื่อมโยงอย่างเป็นทางการและไม่เป็นทางการ รวมถึงพัฒนากระบวนการแลกเปลี่ยนข้อมูลข่าวสาร และประเด็นด้านกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในระดับทวิภาคี และ/หรือพหุภาคี สร้างเครือข่ายให้เกิดความสัมพันธ์ที่ดี และความร่วมมือกับหน่วยงานบังคับใช้กฎหมายของกลุ่มประชาคมอาเซียน อีกทั้งร่วมกันเฝ้าระวัง ป้องกัน และสนับสนุนการดำเนินการตามกฎหมาย เพื่อให้ได้มาซึ่งผู้กระทำผิด ในการนี้คณะทำงานจึงได้จัดทำโครงการแลกเปลี่ยนองค์ความรู้และกำหนดมาตรการแนวทางในการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ ภายใต้การสนับสนุนของสำนักงานปลัดกระทรวงยุติธรรม ครั้งแรกเมื่อปีงบประมาณ พ.ศ. ๒๕๕๙ ร่วมกับหน่วยงานบังคับใช้กฎหมายในประเทศมาเลเซีย กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บอท.) และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ครั้งที่สองเมื่อปีงบประมาณ พ.ศ. ๒๕๖๐ ร่วมกับหน่วยงานบังคับใช้กฎหมายในสาธารณรัฐสิงคโปร์ ครั้งที่สามเมื่อปีงบประมาณ พ.ศ.๒๕๖๑ ร่วมกับหน่วยงานบังคับใช้กฎหมายในสาธารณรัฐฟิลิปปินส์ คณะทำงานจึงได้กำหนดขอบเขตการศึกษาวิจัย โดยเน้นศึกษาข้อกฎหมาย แนวทางการประสานงานด้านการสืบสวนสอบสวนของประเทศไทย เปรียบเทียบกับแต่ละประเทศ ซึ่งแต่ละประเทศก็จะมีลักษณะเฉพาะตัวที่แตกต่างกัน ดังนี้ ประเทศมาเลเซียจะมีผู้กระทำความผิดประเภท Nigerian Fraud แอบแฝงอยู่ในคราบของนักศึกษาไนจีเรีย หรือที่เรียกว่า Romance Scam ที่มีผู้เสียหายในประเทศไทยจำนวนมากและสร้างความเสียหายในแต่ละปีไม่ต่ำกว่าร้อยล้านบาท สาธารณรัฐสิงคโปร์เป็นประเทศที่มีศักยภาพในด้านเทคโนโลยี และเป็นประเทศที่เตรียมพร้อมรับมือภัยอาชญากรรมคอมพิวเตอร์ สาธารณรัฐฟิลิปปินส์ เป็นประเทศที่กำลังเผชิญปัญหาอาชญากรรมคอมพิวเตอร์ ปัญหาการคอร์รัปชัน ช่องว่างทางรายได้ในสังคม การฉ้อโกงทางโทรศัพท์จากแก๊งคอลเซ็นเตอร์ (Telecommunication Fraud) การฉ้อโกงการซื้อขายสินค้าต่าง ๆ ผ่านอินเทอร์เน็ต และปัญหากลุ่มผู้ก่อความไม่สงบทางภาคใต้ของประเทศ ที่มีสภาพปัญหาคล้ายคลึงกับประเทศไทย

ผลจากการศึกษาดูงานในแต่ละหน่วยงานของประเทศทั้ง ๓ ประเทศ พบว่าแต่ละประเทศมีภัยด้านอาชญากรรมทางคอมพิวเตอร์ในรูปแบบที่คล้ายคลึงกัน แต่แนวทางการป้องกันและรับมือแตกต่างกัน ซึ่งอาจจะเกิดจากปัจจัยพื้นฐานในด้านต่าง ๆ เช่น ความพร้อมในด้านสาธารณูปโภค ระบบการสื่อสาร การคมนาคม ความเป็นอยู่ของประชาชน บุคลากรของรัฐ ความพร้อมด้านเทคโนโลยี

ในการนี้คณะทำงานจึงได้นำความรู้ที่ได้รับจากการศึกษาดูงานของทั้ง ๓ ประเทศ มาต่อยอดในการจัดสัมมนา (ในรูปแบบของการปาฐกถาพิเศษและการเสวนา) ในหัวข้อ “การปรับตัวกับ Cyber Warfare ในอนาคต” และการเสวนาในหัวข้อ “การเผชิญหน้ากับ Cyber Crime ในปัจจุบันและปัญหาที่เกิดขึ้นในอาเซียน” พร้อมทั้งนำข้อมูลดังกล่าวมาวิเคราะห์การบูรณาการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์เป็นหัวข้อต่าง ๆ ดังนี้ ๑) แนวโน้มภัยคุกคามทางอาชญากรรมคอมพิวเตอร์ในปัจจุบันและในอนาคต ๒) การวิเคราะห์หน่วยงานและรูปแบบการบริหารจัดการอาชญากรรมคอมพิวเตอร์ (กฎหมาย) ๓) รายละเอียดของความร่วมมือระหว่างประเทศของประเทศมาเลเซีย สาธารณรัฐฟิลิปปินส์ และสาธารณรัฐสิงคโปร์ ๔) กรณีศึกษาและแนวทางแก้ไข ซึ่งได้จัดทำไว้ในรายงานการศึกษาวิจัยฉบับนี้ด้วย

ผลการวิจัยพบว่า การพัฒนาเทคโนโลยีใหม่ ๆ ทำให้ประชาชนต้องตื่นตัวและให้ความสำคัญในความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เพราะภัยคุกคามอาจเกิดขึ้นได้เสมอ เช่น ภัยคุกคามที่เกิดกับระบบ Cloud Crypto Currency สกุลเงินดิจิทัล รวมถึงการทำธุรกรรมทางการเงินผ่านสมาร์ทโฟน สิ่งเหล่านี้เป็นภัยใกล้ตัวที่ไม่อาจคาดคิด ถ้าประชาชนขาดความรู้ความเข้าใจจากการใช้เทคโนโลยี ฉะนั้นแนวทางในการป้องกันอาชญากรรมคอมพิวเตอร์ คณะทำงานเห็นว่าควรให้ความรู้และสร้างความตระหนักรู้แก่ประชาชน หากจะดำเนินการเชิงปราบปรามโดยการสืบสวนสอบสวนเพียงอย่างเดียวคงไม่เท่าทันกับการก้าวกระโดดของเทคโนโลยี ในการนี้หน่วยงานภาครัฐและหน่วยงานภาคเอกชนควรให้ความร่วมมือกันแก้ไขปัญหาที่อาจเกิดขึ้น ดังจะเห็นได้จากแนวทางการกำหนดยุทธศาสตร์ชาติ ๒๐ ปี ที่มีเรื่องการจัดการกับระบบฐานข้อมูลขนาดใหญ่ การนำนวัตกรรม เทคโนโลยีข้อมูลขนาดใหญ่ ระบบการทำงานที่เป็นดิจิทัลเข้ามาประยุกต์ใช้อย่างคุ้มค่าและปฏิบัติงานเทียบได้กับมาตรฐานสากล

ด้วยความก้าวหน้าทางเทคโนโลยี ทำให้ไม่สามารถที่จะป้องกันปัญหาทางเทคโนโลยีได้อย่างครบถ้วนสมบูรณ์ เพราะฉะนั้นแนวคิดที่สำคัญ คือ กรมสอบสวนคดีพิเศษต้องเตรียมบุคลากรและการบริหารจัดการ เพื่อให้เกิดการเรียนรู้และพัฒนาองค์กรให้ทันต่อความเปลี่ยนแปลง และนำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่อ้างอิงจาก NIST ในส่วน Detect และ Respond มาปรับใช้ พร้อมจัดทำ Big Data ข้อมูล Cyber Threat Intelligence ที่จะเป็นการป้องกันปัญหาในเชิงรุก แจ้งเตือนข้อมูลให้ประชาชน หรือองค์กรที่ตกเป็นเป้าหมาย เพื่อเตรียมรับมือหรือหยุดยั้งอาชญากรรมทางคอมพิวเตอร์ได้อย่างทันท่วงที ซึ่งหลักในการดำเนินการนั้น จะต้องคำนึงถึง ๓ ส่วน คือ บุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ดังนั้น คณะทำงานจึงได้จัดทำข้อเสนอแนะในด้านต่าง ๆ ประกอบด้วย ข้อเสนอแนะเชิงนโยบายระดับประเทศ ข้อเสนอแนะเชิงนโยบายระดับองค์กร และข้อเสนอแนะเชิงการนำหลักการบริหารมาประยุกต์ใช้ เมื่อนำหลักการต่าง ๆ มาประยุกต์ใช้ร่วมกันจะทำให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ใช้งานเครื่องมือพิเศษได้อย่างคุ้มค่า และสามารถนำข้อมูลที่ได้มาสนับสนุนหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภาครัฐอื่น ๆ เพื่อเสริมการทำงานร่วมกันให้มีประสิทธิภาพมากยิ่งขึ้น ที่จะเป็นที่พึ่งพิงในการแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ให้แก่ประชาชนและประเทศชาติต่อไป

Abstract

Title: Research on the effectiveness of law enforcement on computer crimes in the ASEAN Economic Community, a case study of Malaysia, the Republic of Singapore and the Republic of the Philippines.

Owner: Bureau of Technology and Cyber Crime, Department of Special Investigation.

The purpose of this research is to study the inquiry of cybercrime of Malaysia, Singapore and The Philippines respectively which is to see an overview of crimes occurring in each country. It is to be a litigation guidelines and linked information both formal and informal way including the exchange of the intelligence and legal issues for prevention and suppression cybercrime in bilateral and/or multilateral. To build a good relation and cooperation with the law enforcement agencies in ASEAN countries in order to prevent and support in legal actions.

In this regard, the working group has prepared a project of knowledge and guideline exchange program for law enforcements in ASEAN Economic Community (AEC), under the support of the office of the Permanent Secretary, Ministry of Justice. The first time cooperated in the fiscal year 2016 with Malaysian Law enforcements, Thailand Technology Crime Suppression Division (TCSD) and Ministry of Digital Economic and Society. The second time in the fiscal year 2017, cooperated with law enforcements in Singapore. The third time in the fiscal year 2018, cooperated with law enforcements in The Philippines.

The working group defines the research scopes focusing on an underlining law and coordination process compared with each country which has a differentiation. In Malaysia, the perpetrators of Nigerian Fraud are hidden in the form of Nigerian students known as Romance Scam, those victims are mostly living in Thailand and damages are more a hundred million baht in each year. The Republic of Singapore is a highly potential technology country and is anticipating cybercrimes. The Philippines is currently received floods of Cybercrime Threats, Corruptions, Income gap, Telecommunication Fraud, Online Shopping Scam and Insurgents in the south of country.

The result of study visits in each department indicated that all three countries receiving similar cyber threats but using different Prevention Guidelines which caused by various fundamental factors such as readiness of Public Utilities, Communication System, Transportation, People well-being, Government Official and Technology. The working group then creates a seminar on the topic “Future Adaptation to Cyber Warfare” and a debate on the topic “Facing modern Cyber Crime and Problems in ASEAN”. Using such data to analyze for integration of law enforcement on cybercrimes are covered in the following lists;

1) Modern and Future in Cybercrime trends.

2) Organizational Analysis and Computer Crime Law Management Model.

3) Cooperation details between Malaysia, Singapore and Philippines and;

4) Case studies and Solutions.

The result of research indicates that people are being more aware of Cyber threats, as new technologies developed, because threats can always arise, for example, threat to digital currency and threat to mobile transaction which are unforeseen imminent dangers if people lack of understanding in technologies. The working group sees that people should be educated an awareness along with repression through investigation would be more effective. In doing this, government agencies and private sectors should cooperate in solving problems that may arise according to 20-years National Strategy including dealing with big data and applying digital working systems cost-effectively comparable to international standards.

In conclusion, with technological advancement, prevention of cyber threats is difficult. Department of Special Investigation needs to prepare its personnel and management to keep up with changes referencing and applying NIST’s Code of Conduct and Standards on Cybersecurity in part Detect and Respond. And prepare Big Data, Cyber Threat Intelligence data that will proactively prevent problems, notify the public or the targeted organization to prepare to deal with or stop computer crimes in a timely manner, that action must take these 3 parts into account 1) People 2) Process 3) Technology. Therefore; the working group prepares the recommendations in various fields comprised of National Policy Recommendations, Corporate Policy Recommendations and Recommendations for the Implementation of Management Principles. It could be more effective when the principles are applied together with effectively use of special tools and exchange these information with other government agencies for efficient collaboration on solving computer crimes for people and nation in the future.

สารบัญ

สารบัญ (ต่อ)

บทที่ ๑
บทนำ

๑.๑ ความเป็นมาและความสำคัญของปัญหา

ประชาคมอาเซียน (ASEAN Community) ประกอบด้วยสมาชิกในเอเชียตะวันออกเฉียงใต้ รวม ๑๐ ประเทศ ได้แก่ ประเทศไทย มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ สิงคโปร์ บรูไน เวียดนาม ลาว พม่า และกัมพูชา ทั้งนี้ จากผลการหารือในที่ประชุมสุดยอดอาเซียนในช่วงที่ผ่านมา ทุกประเทศต่างเห็นพ้องกันในการดำเนินการต่าง ๆ ภายใต้กรอบความร่วมมือประชาคมอาเซียนทั้ง ๓ เสาหลัก ซึ่งรวมถึงการเร่งรัดการพัฒนาความร่วมมือเพื่อให้มีการเคลื่อนย้ายสินค้า บริการ การลงทุน แรงงานฝีมือ และเงินทุนได้อย่างเสรี โดยเปิดให้มีการลงทุนจากประเทศสมาชิกได้สูงถึงร้อยละ ๗๐ ซึ่งจะเห็นได้ว่าในช่วงไม่กี่ปีที่ผ่านมานี้ การประกอบธุรกิจทุกประเทศในอาเซียนนั้น มีแนวโน้มที่จะนำเทคโนโลยีสารสนเทศและระบบอินเทอร์เน็ตมาใช้ในการสนับสนุนและบริหารจัดการธุรกิจกันอย่างกว้างขวางและแพร่หลายมากขึ้นเรื่อย ๆ โดยเฉพาะในส่วนของประเทศไทยนั้น รัฐบาลมีนโยบายสำคัญในการนำเทคโนโลยีสารสนเทศหรืออินเทอร์เน็ตมาใช้ในการขับเคลื่อนเศรษฐกิจ (Digital Economy) ซึ่งล่าสุดได้มีการปรับเปลี่ยนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เมื่อวันที่ ๑๖ กันยายน ๒๕๕๙ เพื่อทำหน้าที่พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั้งประเทศ และเพื่อขับเคลื่อนเศรษฐกิจและสร้างสังคมคุณภาพด้วยเทคโนโลยีดิจิทัล

แม้ว่าการดำเนินการดังกล่าวข้างต้นจะเป็นประโยชน์และเอื้อต่อการขยายตัวทางเศรษฐกิจตลอดจนช่วยให้การติดต่อสื่อสารของประชาชนทั้งในประเทศและระหว่างประเทศนั้นเป็นไปโดยสะดวกรวดเร็วและมีค่าใช้จ่ายที่ถูกลง แต่ในขณะเดียวกัน การดำเนินการดังกล่าวก็ส่งผลให้อาชญากรสามารถใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือและช่องทางในการประกอบอาชญากรรมในรูปแบบใหม่ ๆ ได้ด้วยเช่นกัน ซึ่งรูปแบบการกระทำความผิดทางด้านอาชญากรรมคอมพิวเตอร์นั้น สามารถที่จะเกิดขึ้นหรือควบคุมจากสถานที่แห่งใดในโลกก็ได้ และการกระทำความผิดดังกล่าวมักพบว่า มีสถานที่ในการกระทำผิดในระบบคอมพิวเตอร์มากกว่าหนึ่งประเทศและใช้ระยะเวลาในการก่ออาชญากรรมที่รวดเร็ว โดยมีการควบคุมระยะไกลจากเครื่องคอมพิวเตอร์ มีการใช้เทคโนโลยีหรือโปรแกรมที่มีความซับซ้อนเพื่อปิดบังอำพรางตัวตนของผู้กระทำความผิด ข้อมูลสำคัญหลายอย่างที่ต้องใช้ประกอบการสืบสวนสอบสวนและเพื่อใช้เป็นพยานหลักฐานมักจะถูกจัดเก็บอยู่ในต่างประเทศ หรือระบบคลาวด์ และรูปแบบขององค์กรอาชญากรรมมีการพัฒนาด้วยเทคโนโลยีชั้นสูงซึ่งเกินกว่าประเทศหนึ่งประเทศใดจะสามารถตรวจจับ ควบคุม กำกับ หรือป้องกันปราบปรามได้แต่เพียงลำพัง จึงจำเป็นต้องอาศัยเครือข่ายความร่วมมือระหว่างประเทศ เพื่อประโยชน์ทั้งทางด้านการสืบสวนสอบสวนและดำเนินคดีให้มีประสิทธิภาพ

กองคดีเทคโนโลยีและสารสนเทศ เป็นหน่วยงานบังคับใช้กฎหมายในสังกัดกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม มีภารกิจหน้าที่ในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับการใช้เทคโนโลยีและสารสนเทศเป็นเครื่องมือในการกระทำความผิด ตามที่กำหนดไว้ในกฎกระทรวงแบ่งส่วนราชการกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ. ๒๕๖๐ ข้อ ๓ (๑๑) คือ มีอำนาจหน้าที่ในการ

ป้องกัน ปราบปราม และสืบสวนสอบสวนดำเนินคดีกับผู้กระทำผิดทางคดีเทคโนโลยีและสารสนเทศ รวมถึงการวิเคราะห์และพิสูจน์ความผิดทางคดีเทคโนโลยีและสารสนเทศ ตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. ๒๕๔๗ ประกอบกับกฎกระทรวง ว่าด้วยการกำหนดความผิดคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ (ฉบับที่ ๒) พ.ศ. ๒๕๕๕ ข้อ (๖) คือ คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทั้งนี้ ที่ผ่านมาพบว่าผู้ต้องหาหรือผู้กระทำความผิดมักจะใช้ประเทศในกลุ่มอาเซียนเป็นฐานในการกระทำความผิดและเป็นที่หลบซ่อนตัวทำให้ยากแก่การติดตามจับกุมเพื่อดำเนินคดี ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่ประเทศในกลุ่มประเทศในอาเซียนจะต้องร่วมมือกันในการบังคับใช้กฎหมายด้านต่าง ๆ ได้แก่ การให้ความรู้เกี่ยวกับรูปแบบการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ของประเทศในกลุ่มอาเซียน ประเด็นข้อกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ การสร้างเครือข่ายการประสานงาน การเสริมสร้างให้เกิดความสัมพันธ์ที่ดี การสร้างความร่วมมือในการเฝ้าระวังผู้กระทำผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ การให้ความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญา การแลกเปลี่ยนข้อมูลข่าวสารของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย รวมทั้ง การฝึกอบรมทางวิชาการและเทคนิคการสืบสวนสอบสวนต่าง ๆ เพื่อให้ภารกิจการป้องกันปราบปรามคดีอาชญากรรมทางคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของกองคดีเทคโนโลยีและสารสนเทศบรรลุผลสำเร็จอย่างมีประสิทธิภาพ

จากเหตุผลและความจำเป็นดังกล่าวข้างต้น กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ จึงได้ริเริ่มจัดทำโครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการแนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ภายใต้การสนับสนุนของสำนักงานปลัดกระทรวงยุติธรรม ครั้งแรกเมื่อปีงบประมาณ พ.ศ. ๒๕๕๙ โดยใช้ชื่อโครงการว่า “โครงการสัมมนาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเสริมสร้างแนวร่วมและความร่วมมือของประชาคมอาเซียน” ซึ่งประกอบไปด้วย ๒ กิจกรรม คือ กิจกรรมที่ ๑ : การสร้างเครือข่ายกับหน่วยงานบังคับใช้กฎหมายในประเทศมาเลเซีย ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย เมื่อระหว่างวันที่ ๑๗ - ๑๘ มีนาคม ๒๕๕๙ และกิจกรรมที่ ๒ : การสัมมนากับกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สังกัดสำนักงานตำรวจแห่งชาติ และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ณ กรมสอบสวนคดีพิเศษ เมื่อวันที่ ๒๙ มีนาคม ๒๕๕๙ โดยผลที่ได้จากการดำเนินโครงการดังกล่าว คือ ก่อให้เกิดความร่วมมือที่เป็นรูปธรรมมากขึ้น ตลอดจนเพิ่มช่องทางในการได้มาซึ่งข้อมูลข่าวสารทั้งจากในประเทศและต่างประเทศ ซึ่งเป็นประโยชน์โดยตรงต่อการสืบสวนสอบสวนและดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมอื่นที่เกี่ยวข้อง สำหรับในปีที่สองของการดำเนินโครงการหรือปีงบประมาณ พ.ศ. ๒๕๖๐ นั้น สำนักคดีเทคโนโลยีและสารสนเทศได้รับความเห็นชอบให้ดำเนิน “โครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการ แนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ณ สาธารณรัฐสิงคโปร์ เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม” ซึ่งสาธารณรัฐสิงคโปร์เป็นประเทศที่ได้รับการยอมรับจากนานาชาติว่าเป็นประเทศที่มีความก้าวหน้าในการบริหารจัดการการสืบสวนสอบสวน และการตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ในคดีอาชญากรรมทางคอมพิวเตอร์ นอกจากนี้ สาธารณรัฐสิงคโปร์ยังเป็นที่ตั้งของหน่วยงาน Interpol Global Complex for Innovation (IGCI)

ซึ่งเป็นส่วนงานหนึ่งขององค์การตำรวจสากล ที่ได้เปิดทำการอย่างเป็นทางการแล้วเมื่อเดือนเมษายน พ.ศ. ๒๕๕๘ ที่ผ่านมา โดยมีภารกิจหน้าที่เกี่ยวกับการวิจัยและพัฒนาอุปกรณ์และเครื่องมือต่าง ๆ ที่ใช้ในการระบุอาชญากรรมและตัวตนของผู้กระทำความผิด สนับสนุนงานด้านการตรวจพิสูจน์ทางคอมพิวเตอร์ ตลอดจนการฝึกอบรมเกี่ยวกับนวัตกรรมและเทคโนโลยีใหม่ ๆ ที่ช่วยในการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ ซึ่งประโยชน์หลักที่จะได้รับจากการดำเนินโครงการดังกล่าว คือ การพัฒนาขีดความสามารถและศักยภาพในการสืบสวนสอบสวนของเจ้าหน้าที่บังคับใช้กฎหมาย การขยายความร่วมมือในการฝึกอบรมเจ้าหน้าที่ด้านการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์และการตรวจพิสูจน์ทางคอมพิวเตอร์ และการขยายเครือข่ายความร่วมมือในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในกลุ่มประเทศอาเซียน

สำหรับโครงการต่อเนื่องในปีที่สามเมื่อปีงบประมาณ พ.ศ.๒๕๖๑ นั้น กองคดีเทคโนโลยีและสารสนเทศพิจารณาแล้ว เห็นควรดำเนินโครงการต่อเนื่องจากปีงบประมาณ พ.ศ. ๒๕๖๐ คือ “โครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการแนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community หรือ AEC ในการป้องกันและปราบปรามการละเมิดทรัพย์สินทางปัญญาและอาชญากรรมทางคอมพิวเตอร์ ณ สาธารณรัฐฟิลิปปินส์ เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม” ซึ่งคาดว่าจะเดินทางไปดูงานและประชุมหารือหน่วยงานที่เกี่ยวข้องทางด้านการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ รวมถึงหน่วยงานที่มีหน้าที่กำกับดูแลผู้ให้บริการในการติดต่อสื่อสาร ที่อยู่ในสังกัดกระทรวงยุติธรรม (Department of Justice) สำนักงานตำรวจแห่งชาติฟิลิปปินส์ (Philippine National Police: PNP) และกระทรวงเทคโนโลยีการติดต่อสื่อสารและข้อมูลสารสนเทศ (Department of Information and Communications Technology) โดย ๔ หน่วยงานหลักที่จะเดินทางไปประชุมหารือ ประกอบด้วย

๑.๑.๑ หน่วยงาน National Bureau of Investigation (NBI) สังกัดกระทรวงยุติธรรม ซึ่งเป็นหน่วยงานสำคัญทางด้านการสืบสวนสอบสวนที่ก่อตั้งขึ้นอย่างเป็นทางการเมื่อปี ค.ศ. ๑๙๔๗ (พ.ศ. ๒๔๙๐) โดยมีภารกิจหลัก คือ การสืบสวนสอบสวนคดีอาชญากรรมต่าง ๆ โดยเฉพาะอย่างยิ่งคดีที่อยู่ในความสนใจของรัฐบาล รวมถึงให้ความช่วยเหลือหน่วยงานอื่น ๆ ในการสืบสวนสอบสวนตามการร้องขอ โดยเป็นหน่วยงานกลางระดับชาติในการประสานข้อมูลอาชญากรรมเพื่อประโยชน์ในการดำเนินคดีสำคัญที่มีความซับซ้อน ก่อความเสียหายรุนแรง

๑.๑.๒ ส่วนแผนงาน (Programme) Office of Cybercrime (OOC) สังกัดกระทรวงยุติธรรม ซึ่งจัดตั้งขึ้นตามกฎหมายสาธารณรัฐ ฉบับที่ ๑๐๑๗๕ หรือพระราชบัญญัติป้องกันอาชญากรรมทางคอมพิวเตอร์ ค.ศ. ๒๐๑๒ (The Cybercrime Prevention Act of ๒๐๑๒) โดยมีภารกิจหลัก คือ เป็นผู้ประสานงานกลาง (Central Authority) ในกรอบความร่วมมือระหว่างประเทศในเรื่องทางอาญาและการส่งผู้ร้ายข้ามแดนในคดีอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมอื่น ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ให้คำปรึกษาทางกฎหมายและเทคนิค การจัดทำและสงวนรักษาข้อมูล การเก็บรวบรวมพยานหลักฐาน ออกคู่มือ/แนวทางปฏิบัติที่เกี่ยวข้องกับการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ การกู้คืนพยานหลักฐานทางอิเล็กทรอนิกส์ และการวิเคราะห์ข้อมูลการตรวจพิสูจน์ตามแนวทางปฏิบัติที่เป็นมาตรฐานสากล

๑.๑.๓ หน่วยงาน Anti - Cybercrime Group (ACG) สังกัดสำนักงานตำรวจแห่งชาติฟิลิปปินส์ ซึ่งจัดตั้งขึ้นอย่างเป็นทางการเมื่อเดือนมีนาคม พ.ศ. ๒๕๕๖ โดยมีภารกิจหลัก คือ สืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศและการติดต่อสื่อสาร จัดทำและดูแลระบบฐานข้อมูลการข่าวเกี่ยวกับ blogs ใต้ดิน ห้อง chat และอื่น ๆ ที่ถูกใช้โดยองค์กรอาชญากรรมต่าง ๆ จัดการฝึกอบรมและสัมมนาด้านปฏิบัติการต่อต้านอาชญากรรมทางคอมพิวเตอร์ รวมถึงจัดกิจกรรมการรณรงค์ต่อต้านอาชญากรรมทางคอมพิวเตอร์

๑.๑.๔ ศูนย์การประสานงานและสืบสวนอาชญากรรมทางคอมพิวเตอร์ (Cybercrime Investigation and Coordinating Center: CICC) กระทรวงเทคโนโลยีการติดต่อสื่อสารและข้อมูลสารสนเทศ ซึ่งเป็นศูนย์ฯ ที่จัดตั้งขึ้นตามพระราชบัญญัติป้องกันอาชญากรรมทางคอมพิวเตอร์ ค.ศ. ๒๐๑๒ (Cybercrime Prevention Act of ๒๐๑๒) โดยมีภารกิจหลัก คือ จัดทำแผนความมั่นคงปลอดภัยทางคอมพิวเตอร์แห่งชาติ และให้ความช่วยเหลือในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ผ่านทางทีมตอบสนองเรื่องฉุกเฉินทางคอมพิวเตอร์ (Computer Emergency Response Team: CERT) ให้ความร่วมมือระหว่างประเทศทางด้านการข่าว การสืบสวน และการฝึกอบรม ที่เกี่ยวข้องกับการป้องกันปราบปราม และดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ รวมถึงประสานให้การสนับสนุน และมีส่วนร่วมกับภาคธุรกิจ หน่วยงานรัฐบาลท้องถิ่น และองค์กรภาคเอกชน ในการดำเนินแผนงานการป้องกันอาชญากรรมทางคอมพิวเตอร์ ตลอดจนให้ข้อเสนอแนะในการออกกฎหมาย มาตรการ และนโยบายต่าง ๆ ตามความเหมาะสม

๑.๒ วัตถุประสงค์ของงานวิจัย

๑.๒.๑ เพื่อศึกษารูปแบบการสืบสวนสอบสวนอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ ทำให้สามารถเห็นภาพรวมอาชญากรรมที่เกิดขึ้นในแต่ละประเทศ เป็นแนวทางการดำเนินคดี (Guidance) และการนำข้อมูลมาเชื่อมโยงอย่างเป็นทางการ และอย่างไม่เป็นทางการ

๑.๒.๒ เพื่อพัฒนาการแลกเปลี่ยนข้อมูลข่าวสาร และประเด็นด้านกฎหมายระหว่างกันในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในระดับทวิภาคี และ/หรือพหุภาคี สร้างเครือข่ายในการประสานการดำเนินงานการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ และเสริมสร้างให้เกิดความสัมพันธ์ที่ดีและความร่วมมือกับหน่วยงานบังคับใช้กฎหมายของกลุ่มประชาคมอาเซียน

๑.๒.๓ เพื่อร่วมกันเฝ้าระวัง ป้องกัน และสนับสนุนการดำเนินการตามกฎหมาย เพื่อให้ได้มาซึ่งผู้กระทำผิด

๑.๓ ขอบเขตการศึกษาวิจัย

คณะทำงานได้ศึกษาวิจัย ด้านการบูรณาการการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน โดยเน้นการศึกษาข้อกฎหมาย แนวทางการประสานงานด้านการสืบสวนสอบสวนด้านอาชญากรรมคอมพิวเตอร์ทั้งแบบทางการ และไม่เป็นทางการของประเทศไทย

เปรียบเทียบกับประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ เพื่อนำไปสู่การเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน

ประเทศที่มีศักยภาพในด้านเทคโนโลยีในแถบอาเซียน ได้แก่ สาธารณรัฐสิงคโปร์ และเป็นประเทศที่เตรียมพร้อมกับภัยอาชญากรรมคอมพิวเตอร์ จึงเป็นเหตุผลหนึ่งที่ทางคณะทำงานวิจัยได้วิจัยและศึกษาดูงาน พร้อมทั้งสร้างแนวทางการบูรณาการการสืบสวนสอบสวนคดีอาชญากรรมคอมพิวเตอร์ร่วมกับหน่วยงานบังคับใช้กฎหมายในประเทศไทย

ประเทศมาเลเซีย เป็นประเทศที่มีผู้กระทำความผิดอาชญากรรมคอมพิวเตอร์ประเภท Nigerian Fraud แอบแฝงอยู่ในคราบของนักศึกษาไนจีเรียที่มาศึกษาในประเทศมาเลเซีย หรือที่เรียกว่า Romance Scam การกระทำความผิดในลักษณะนี้มีผู้เสียหายในประเทศไทยเป็นจำนวนมาก และสร้างความเสียหายต่อรายเป็นจำนวนหลักแสนถึงหลักล้านบาทในแต่ละปีความเสียหายไม่ต่ำกว่าร้อยล้านบาท ด้วยเหตุดังกล่าวทำให้ทางคณะทำงานวิจัยต้องเดินทางไปศึกษาและสร้างความสัมพันธ์ระหว่างหน่วยงานเพื่อเกิดการบูรณาการร่วมกัน เพื่อให้การสืบสวนสอบสวนคดีด้านอาชญากรรมคอมพิวเตอร์ประสบผลสำเร็จในเชิงป้องกันและปราบปรามการกระทำความผิด

สาธารณรัฐฟิลิปปินส์กำลังเผชิญปัญหาอาชญากรรมทั่วไป อาชญากรรมคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ปัญหาการคอร์รัปชันประชาชน ช่องว่างทางฐานะรายได้ของคนในสังคม และปัญหากลุ่มผู้ก่อความไม่สงบในพื้นที่ทางภาคใต้ของประเทศซึ่งสภาพปัญหาคล้ายกันกับประเทศไทย การนำเข้ารถหรูผิดกฎหมาย และการกระทำผิดในตลาดหลักทรัพย์สำหรับปัญหาอาชญากรรมคอมพิวเตอร์ ได้แก่ การฉ้อโกงทางโทรศัพท์จากแก๊งคอลเซ็นเตอร์ (Telecommunication Fraud) การฉ้อโกงการซื้อขายทางอินเทอร์เน็ต

๑.๔ สมมติฐานของงานวิจัย

การบูรณาการการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน

๑.๔.๑ ศึกษาข้อมูล ข้อกฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ของกลุ่มประเทศอาเซียนในด้านการสืบสวนและสอบสวนของหน่วยงานบังคับใช้กฎหมาย

๑.๔.๒ สร้างความร่วมมือระหว่างประเทศจะเป็นการเพิ่มประสิทธิภาพในการป้องกันอาชญากรรมคอมพิวเตอร์

๑.๔.๓ การเรียนรู้และแลกเปลี่ยนข้อมูลระหว่างประเทศในกลุ่มอาเซียนจะนำไปสู่การเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์

๑.๕ วิธีการศึกษาวิจัย

ศึกษาวิจัยโดยการศึกษาในข้อกฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ เพื่อเป็นแนวทางในการเพิ่มประสิทธิภาพ การบูรณาการด้านการสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์กับหน่วยงานบังคับใช้กฎหมายของประเทศไทย

๑.๖ ผลที่คาดว่าจะได้รับ

๑.๖.๑ ได้ความรู้เรื่องรูปแบบอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ เห็นภาพรวมอาชญากรรมที่เกิดขึ้นในแต่ละประเทศ เป็นแนวทางการดำเนินคดี (Guidance) และการนำข้อมูลมาเชื่อมโยงอย่างเป็นทางการ และอย่างไม่เป็นทางการ

๑.๖.๒ ได้รับข้อมูลข่าวสาร และประเด็นด้านกฎหมายระหว่างกันในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์ รวมถึงได้สร้างเครือข่ายในการประสานการดำเนินงานการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ เสริมสร้างให้เกิดความสัมพันธ์ที่ดีและความร่วมมือกับหน่วยงานบังคับใช้กฎหมายของกลุ่มประชาคมอาเซียน

๑.๖.๓ ได้ทราบรูปแบบอาชญากรรมคอมพิวเตอร์เพื่อเป็นแนวทางในการป้องกันและสนับสนุนการดำเนินการตามกฎหมายของแต่ละประเทศ เพื่อให้ได้มาซึ่งผู้กระทำผิด

บทที่ ๒
ข้อมูลทั่วไปของสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้

๒.๑ ที่มาและความหมายของประชาคมอาเซียน

สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of South East Asian Nations หรือ ASEAN) หรืออาเซียน ก่อตั้งเมื่อวันที่ ๘ สิงหาคม ๒๕๑๐ หลังการลงนามในปฏิญญากรุงเทพฯ (Bangkok Declaration) โดยรัฐมนตรีจาก ๕ ประเทศ โดยการจัดตั้งในครั้งแรกมีจุดประสงค์เพื่อส่งเสริมและร่วมมือในเรื่องสันติภาพ ความมั่นคง เศรษฐกิจ องค์ความรู้ สังคมวัฒนธรรม บนพื้นฐานความเท่าเทียมกันและผลประโยชน์ร่วมกันของประเทศสมาชิก

๒.๑.๑ สภาพทั่วไปของอาชญากรรมทางคอมพิวเตอร์ในอาเซียน

ความมั่นคงไซเบอร์ (Cybersecurity) หมายถึง การใช้ประโยชน์จากเทคโนโลยีเพื่อปกป้องระบบเครือข่ายคอมพิวเตอร์ รวมถึงข้อมูลในโลกออนไลน์จากการถูกโจมตี โจรกรรม หรือการเข้าถึงโดยไม่ได้รับอนุญาต[๑]

ในโลกยุคปัจจุบันที่เทคโนโลยีสารสนเทศได้กลายเป็นองค์ประกอบสำคัญของวิถีชีวิตแทบทุกด้านของมนุษย์ โลกไซเบอร์ได้กลายเป็นดาบสองคม เพราะนอกจากจะมีประโยชน์ต่อการเจริญเติบโตทางเศรษฐกิจและยกระดับคุณภาพชีวิตของประชาชน ยังกลายเป็นพื้นที่สุ่มเสี่ยงต่อการถูกคุกคาม อันทำให้รัฐต่าง ๆ ต้องหันกลับมาทบทวนถึงความจำเป็นในการรับมือกับภัยคุกคามความมั่นคงที่ติดตามมาพร้อมกับความเจริญก้าวหน้าทางเทคโนโลยี

สำหรับอาเซียน ความมั่นคงไซเบอร์เป็นส่วนหนึ่งของความร่วมมือภายใต้เสาหลักประชาคมการเมือง ความมั่นคง โดยกลไกหลักที่เป็นเวทีหารือและทบทวนความร่วมมือด้านความมั่นคงไซเบอร์ คือ การประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) และการประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC) ถึงแม้ว่าความร่วมมือในช่วงต้นจะเน้นไปที่การต่อต้านยาเสพติดเป็นสำคัญ แต่ในการประชุม AMMTC ครั้งที่ ๓ เมื่อเดือนตุลาคม ๒๕๔๔ ณ สาธารณรัฐสิงคโปร์ ที่ประชุมได้ตกลงที่จะผนวกความร่วมมือด้านความมั่นคงไซเบอร์ให้เป็นส่วนหนึ่งในแผนงาน เพื่อจัดทำแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ (ASEAN Plan of Action to Combat Transnational Crime) เป็นครั้งแรก สะท้อนถึงการตระหนักว่าอาชญากรรมข้ามชาติมิได้จำอยู่เพียงอาชญากรรมที่พบเห็นได้เฉพาะหน้า เช่น การก่อการร้าย การค้ามนุษย์หรือการค้าอาวุธสงครามเท่านั้น แผนปฏิบัติการดังกล่าวได้รับการรับรองโดยที่ประชุม SOMTC ครั้งที่ ๒ ที่ประเทศมาเลเซียในอีกหนึ่งปีให้หลัง ในหัวข้อว่าด้วยความมั่นคงไซเบอร์ แผนปฏิบัติการฉบับนี้ได้จำแนกความร่วมมือของประเทศสมาชิกออกเป็น ๕ ประเภท ได้แก่ ความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ความร่วมมือด้านข้อกฎหมาย ความร่วมมือด้านการบังคับใช้กฎหมาย ความร่วมมือด้านการฝึกอบรม

---

[๑]กองบรรณาธิการจุลสาร “จับตาอาเซียน”. (๒๕๕๙). *อาเซียนกับความร่วมมือด้านความมั่นคงไซเบอร์.* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: https://aseanwatch.org/๒๐๑๖/๐๖/๓๐/current-issue-๐๒๕๙

และการพัฒนาขีดความสามารถ และความร่วมมือนอกภูมิภาค ในเวลาต่อมาความร่วมมือด้านความมั่นคงไซเบอร์ของอาเซียนได้ขยายสู่การรับรองกรอบการทำงานร่วมในการพัฒนาขีดความสามารถเพื่อต่อต้านอาชญากรรมไซเบอร์ โดยมีเป้าหมายเพื่อสนับสนุนการต่อสู้กับอาชญากรรมไซเบอร์รูปแบบต่าง ๆ ในระดับโลก รวมถึงการคณะทำงานด้านอาชญากรรมไซเบอร์ขึ้นตามมติของที่ประชุม SOMTC ครั้งที่ ๑๓ ณ กรุงเวียงจันทน์ สปป.ลาว เมื่อปี ๒๕๕๖ คณะทำงานดังกล่าวมีบทบาทสำคัญอย่างยิ่งในการหาข้อสรุปให้กับโร้ดแมปว่าด้วยการต่อต้านอาชญากรรมไซเบอร์ในอาเซียน (ASEAN roadmap on combating cybercrime) ซึ่งมีเป้าหมายเพื่อส่งเสริมความร่วมมือระดับภูมิภาคในการรับมือภัยคุกคามไซเบอร์ตามแนวทางทั้ง ๕ ประการ ของแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ

ความร่วมมือด้านความมั่นคงไซเบอร์ยังปรากฏอยู่ในการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชียและแปซิฟิก (ASEAN Regional Forum: ARF) โดยที่ประชุมได้ออกแถลงการณ์หลายฉบับ เพื่อเน้นย้ำถึงความสำคัญของการออกแบบกรอบความร่วมมือด้านความมั่นคงไซเบอร์ระหว่างประเทศสมาชิก นอกจากนี้ ในปี ๒๕๕๕ ที่ประชุม ARF ยังได้ออกแถลงการณ์ที่ระบุอย่างชัดเจนถึงเป้าหมายภายในของอาเซียนในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ อันรวมถึงการสร้างมาตรการส่งเสริมความไว้เนื้อเชื่อใจระหว่างกันอย่างเป็นรูปธรรม

ความจริงจังของภัยคุกคามทางไซเบอร์ในช่วงหลายปีที่ผ่านมา กอปรกับการตระหนักรู้ในความเชื่อมโยงระหว่างความมั่นคงไซเบอร์กับความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้ที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and IT Ministers Meeting: TELMIN) ครั้งที่ ๑๔ เมื่อเดือนมกราคม ๒๕๕๘ ได้บรรจุประเด็นความมั่นคงไซเบอร์ลงในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของอาเซียน ฉบับที่ ๒ ระหว่าง ปี ๒๕๕๙ - ๒๕๖๓ (ASEAN ICT Masterplan ๒๐๒๐)

แผนแม่บทดังกล่าวได้กำหนดกลยุทธ์หลัก (Strategic Thrusts) เพิ่มเติมจากแผนแม่บทฉบับเดิม ๓ ประการ โดยหนึ่งในนั้น คือ กลยุทธ์ด้านความปลอดภัยและหลักประกันด้านข้อมูลข่าวสาร ซึ่งประกอบด้วยการพัฒนาหลักการด้านความปลอดภัยของข้อมูลระดับภูมิภาค และส่งเสริมความเข้มแข็งและประสิทธิภาพของความร่วมมือเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินด้านไซเบอร์อย่างทันท่วงที โดยมีเป้าหมายเพื่อเสริมสร้างความเชื่อมั่นให้กับเศรษฐกิจดิจิทัลของอาเซียนและปรับปรุงความร่วมมือในการรับมือกับสถานการณ์ฉุกเฉินด้านไซเบอร์ของภูมิภาคให้มีประสิทธิภาพยิ่งขึ้น

นอกจากความร่วมมือภายในภูมิภาค อาเซียนยังขยายความร่วมมือด้านความมั่นคงไซเบอร์กับประเทศคู่เจรจา เช่น ญี่ปุ่น ทั้งสองประเทศได้ร่วมกันออกแถลงการณ์ร่วมเพื่อส่งเสริมความร่วมมือด้านการต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ พร้อมทั้งยืนยันว่าจะส่งเสริมความมั่นคงปลอดภัยของการใช้เทคโนโลยีสารสนเทศและการสื่อสาร และต่อต้านอาชญากรรมไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งยังร่วมกันจัดการประชุมหารืออาเซียน - ญี่ปุ่น ว่าด้วยอาชญากรรมไซเบอร์ (ASEAN - Japan Cybercrime Dialogue) เพื่อเป็นเวทีหารือกรอบความร่วมมือและส่งเสริมศักยภาพการรับมือกับภัยคุกคามไซเบอร์ระหว่างกัน

ปัจจุบันสถานการณ์ด้านความมั่นคงไซเบอร์ของชาติอาเซียนที่ค่อนข้างล่อแหลม ส่งผลใช้ความมั่นคงไซเบอร์กลายเป็นวาระเชิงนโยบายที่สำคัญของหลายประเทศ อาทิ มาเลเซีย

ซึ่งได้รับการจัดอันดับให้มีความเสี่ยงการก่ออาชญากรรมทางอินเทอร์เน็ตสูงเป็นอันดับ ๖ ของโลก ได้เริ่มบังคับใช้มาตรการต่าง ๆ ตามนโยบายความมั่นคงไซเบอร์แห่งชาติ (National Cyber Security Policy) อย่างจริงจังตั้งแต่ พ.ศ. ๒๕๔๙ ก่อนหน้านี้ รัฐบาลมาเลเซียได้ตั้ง “คณะกรรมการด้านการสื่อสารและมัลติมีเดียแห่งมาเลเซีย” (The Malaysian Communications and Multimedia Commission: MCMC) เพื่อสอดส่องการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ภายใต้กฎหมายการสื่อสารและมัลติมีเดีย พ.ศ. ๒๕๔๑ รวมถึงมีการแก้ไขพระราชบัญญัติว่าด้วยการยุยงปลุกปั่น เพื่อควบคุมสื่อออนไลน์ให้เข้มงวดยิ่งขึ้นโดยให้อำนาจเจ้าหน้าที่รัฐในการปิดกันการเข้าถึงเว็บไซต์ที่มีเนื้อหายุยงปลุกปั่นเป็นภัยต่อความมั่นคงของชาติ พร้อมเพิ่มโทษผู้กระทำผิดเป็น ๓ - ๗ ปี

ขณะที่สิงคโปร์ ซึ่งมุ่งมั่นพัฒนาประเทศตามโครงการ “ชาติอัจฉริยะ” (Smart Nation Programme) โดยมีเป้าหมายหลักเพื่อใช้เทคโนโลยียกระดับคุณภาพชีวิตของประชาชนและส่งเสริมผลิตภาพของประเทศ ได้ลงนามในบันทึกความเข้าใจเพื่อส่งเสริมความมั่นคงไซเบอร์กับอังกฤษ พร้อมทั้งร่วมมือกับบริษัทไมโครซอฟท์เพื่อจัดตั้งศูนย์อาชญากรรมไซเบอร์แห่งแรกของอาเซียนเมื่อปี ๒๕๕๘

ด้านฟิลิปปินส์ได้ออกกฎหมายป้องปรามอาชญากรรมไซเบอร์ (Cybercrime Prevention Act) เมื่อปี ๒๕๕๗ โดยมีจุดประสงค์เพื่อป้องกันการโจรกรรมหรือล้วงข้อมูลทางอินเทอร์เน็ต รวมถึงป้องกันไม่ให้มีการเผยแพร่ภาพอนาจารของเด็กและเยาวชน แม้หลายฝ่ายมองว่ากฎหมายฉบับดังกล่าวมีเนื้อหาลดทอนเสรีภาพในการแสดงความคิดเห็น เนื่องจากรัฐบาลสามารถสั่งปิดเว็บไซต์และสอดส่องกิจกรรมออนไลน์ของประชาชนได้โดยไม่ต้องขอหมายอนุญาตจากตุลาการก่อน

ถึงแม้ชาติอาเซียนจะตระหนักถึงปัญหาความมั่นคงไซเบอร์มากขึ้นในช่วงหลัง แต่น่าสังเกตว่าการรับมือกับภัยคุกคามไซเบอร์ในระดับประเทศยังเน้นหนักไปที่การปราบปรามผู้กระทำผิดที่ส่งผลต่อสถานะของรัฐบาลเป็นสำคัญ ดังเห็นได้จากการบังคับกฎหมายของประเทศต่าง ๆ ที่มุ่งเป้าเพื่อการปิดกั้นการแสดงความคิดเห็นและวิพากษ์วิจารณ์รัฐบาล ทำให้ประเด็นความขัดแย้งระหว่างการบังคับใช้กฎหมายด้านความมั่นคงกับสิทธิเสรีภาพของประชาชนได้รับการหยิบยกขึ้นมาถกเถียงอยู่เสมอ และบดบังประเด็นเกี่ยวกับความมั่นคงไซเบอร์ในลักษณะอื่น ๆ ซึ่งยังคงไม่ค่อยคืบหน้ามากนัก ปัญหาหลักเกิดจากการที่ชาติอาเซียนหลายประเทศยังคงขาดแคลนบุคลากรที่มีความรู้ความสามารถเกี่ยวกับเทคโนโลยีสารสนเทศและมีความเข้าใจเกี่ยวกับธรรมชาติของภัยคุกคามความมั่นคงไซเบอร์จริง ๆ แม้สมาชิกบางประเทศ เช่น สิงคโปร์ และมาเลเซีย จะมีความเข้มแข็งด้านความมั่นคงไซเบอร์เป็นลำดับต้น ๆ ของโลก แต่ประเทศอื่นๆ โดยเฉพาะกลุ่มประเทศ CLMV ยังคงมีมาตรฐานด้านความมั่นคงไซเบอร์ที่ต่างกันอยู่มาก สิ่งนี้ส่งผลให้หลายประเทศยังขาดนโยบายด้านความมั่นคงไซเบอร์ที่มีประสิทธิภาพ ประเมินว่าในปี ๒๕๕๗ ชาติสมาชิกอาเซียนจำต้องสูญเสียเงินรวมกันกว่า ๗.๒ พันล้านดอลลาร์สหรัฐฯ (ประมาณ ๒.๕ แสนล้านบาท) ในการสอดส่องและติดตามผู้กระทำความผิดเกี่ยวกับคอมพิวเตอร์และอาชญากรรมไซเบอร์

นอกจากนี้ หลายประเทศยังคงเปราะบางต่อการโจมตีทางไซเบอร์ ทั้งการเข้าถึงโดยไม่ได้รับอนุญาตการรบกวนการทำงานของคอมพิวเตอร์ การใช้คอมพิวเตอร์เพื่อการหลอกลวงและทำลายข้อมูล รวมถึงการสอดแนมข้อมูลทางการเมืองและการทหารโดยหน่วยงานที่คาดว่าได้รับการสนับสนุนจากชาติมหาอำนาจบางประเทศ

ข้อจำกัดและความท้าทายเหล่านี้อาจเริ่มแก้ไขได้ด้วยการร่วมแลกเปลี่ยนข้อมูล ความรู้ และเทคโนโลยีที่จำเป็น ทั้งภายในภูมิภาคและร่วมกับประเทศคู่เจรจานอกภูมิภาค การวางกรอบความร่วมมือระดับภูมิภาคร่วมกันอย่างจริงจัง การพัฒนาบุคลากรด้านความมั่นคงไซเบอร์ตั้งแต่วัยเยาว์ การสนับสนุนการเคลื่อนย้ายโดยเสรีของบุคลากรด้านเทคโนโลยีสารสนเทศและผู้ที่มีความรู้ความสามารถด้านความมั่นคงไซเบอร์ รวมถึงอาจสนับสนุนการฝึกอบรมด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและความมั่นคงไซเบอร์ให้กับนักเรียนนักศึกษาและประชาชนทั่วไป

ปัจจุบันประเทศในแถบเอเชียแปซิฟิกกำลังเผชิญภัยคุกคามจากอาชญากรรมในโลกไซเบอร์ ที่กำลังสั่นคลอนเสถียรภาพทางเศรษฐกิจของหลายประเทศในภูมิภาคนี้ ขณะที่บรรดาผู้นำภาคธุรกิจและเจ้าหน้าที่รัฐบาลในเอเชีย ต่างต้องการให้มีการปรับปรุงนโยบายเพื่อให้สามารถรับมือการเปลี่ยนแปลงที่รวดเร็วของการโจมตีทางไซเบอร์ สิงคโปร์ถือเป็นหนึ่งในประเทศผู้นำของอาเซียนในด้านการป้องกันภัยคุกคามจากการโจมตีหรือลอบเจาะล้วงข้อมูลทางไซเบอร์ โดยเมื่อเดือนตุลาคมปีที่แล้ว สิงคโปร์ได้เป็นเจ้าภาพการประชุมระดับรัฐมนตรีของอาเซียน ที่มีวาระสำคัญเรื่องการพัฒนาศักยภาพของอาเซียนในการรับมืออาชญากรรมทางอินเทอร์เน็ต ขณะเดียวกัน คณะกรรมการพัฒนาเศรษฐกิจของสิงคโปร์ หรือ EDB ได้จับมือกับบริษัทเทคโนโลยี Honeywell ของสหรัฐฯ เพื่อจัดตั้งศูนย์ความปลอดภัยทางไซเบอร์แห่งใหม่ประจำภาคพื้นเอเชียแปซิฟิก ซึ่งจะมีทั้งห้องปฏิบัติการและการฝึกอบรมพิเศษในด้านความปลอดภัยทางไซเบอร์ในเดือนมิถุนายน สิงคโปร์และออสเตรเลียได้ลงนามในข้อตกลงความร่วมมือป้องกันอาชญากรรมทางไซเบอร์ โดยออสเตรเลียตกลงจะร่วมมือกับจีนและไทยในด้านนี้ด้วย[๒]

Tobias Freakin ผู้แทนด้านอาชญากรรมไซเบอร์ของออสเตรเลียได้เจรจากับเจ้าหน้าที่ไทยเมื่อเร็ว ๆ นี้ โดยได้กล่าวว่าความร่วมมือระหว่างประเทศต่าง ๆ ในเอเชีย คือ สิ่งสำคัญในการรับมือกับเครือข่ายอาชญากรรมไซเบอร์กำลังขยายตัวอย่างรวดเร็วในเอเชีย คุณ Freakin ระบุว่าเวลานี้อาชญากรและคนร้ายสามารถประยุกต์ใช้ข้อมูลทางอินเทอร์เน็ตได้รวดเร็วกว่ารัฐบาล ดังนั้นหากประเทศต่าง ๆ พากันนิ่งเฉยและยังขาดความร่วมมือ ในที่สุดก็จะถูกกลุ่มอาชญากรไซเบอร์เหล่านี้แซงหน้าไปไกล

รายงานของสำนักงานควบคุมยาเสพติดและอาชญากรรมของสหประชาชาติ หรือ UNODC เตือนว่า อาชญากรรมทางไซเบอร์กำลังเติบโตอย่างรวดเร็วในเอเชีย และได้กลายไปเป็นเครือข่ายอาชญากรรมข้ามชาติขนาดใหญ่ในปัจจุบัน ซึ่งรวมถึง การลอบขโมยข้อมูลส่วนบุคคล การโจมตีด้วยไวรัสหรืออีเมลล่อลวง ตลอดจนการฉ้อโกงต่าง ๆ ผ่านทางเว็บไซต์ สื่อสังคมออนไลน์หรือแอพในโทรศัพท์มือถือ

เหตุการณ์การโจมตีทางไซเบอร์ครั้งใหญ่หลายต่อหลายครั้งในช่วงหลัง ๆ ได้ทำให้หลายประเทศในเอเชีย หันมาใส่ใจกับปัญหาอาชญากรรมทางไซเบอร์มากขึ้น รวมทั้งกรณีล่าสุดเมื่อเดือนพฤษภาคม ที่มีการปล่อยมัลแวร์เรียกค่าไถ่ Wanna Cry ออกมาโจมตีเครือข่ายคอมพิวเตอร์ขององค์กรต่าง ๆ มากกว่า ๒๐๐,๐๐๐ เครื่อง ใน ๑๕๐ ประเทศทั่วโลกรวมทั้งประเทศไทย

---

[๒]ทรงพจน์ สุภาผล. (๒๕๖๐). *'อาชญากรรมไซเบอร์ส' ภัยคุกคามใหม่ของประเทศในแถบเอเชียแปซิฟิก.* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔ จาก: https://www.voathai.com/a/asia-cybercrime/๓๙๐๐๘๖๑.html

บริษัทตรวจสอบภัยคุกคามทางไซเบอร์ Trend Micro รายงานว่า การโจมตีทางไซเบอร์ได้ทำให้เกิดความสูญเสียทางเศรษฐกิจในเอเชียเป็นมูลค่าหลายล้านดอลลาร์ ส่วนที่ฟิลิปปินส์นักวิเคราะห์ด้านความปลอดภัยกล่าวว่าภาคธุรกิจต่าง ๆ จำเป็นต้องเพิ่มมาตรการในการรักษาความปลอดภัยทางอินเทอร์เน็ตมากขึ้น ขณะที่รายงานสำรวจด้านความมั่นคงปลอดภัยของบริษัทที่ปรึกษา Price Waterhouse Coopers (PwC) เรียกร้องให้มีการเพิ่มความร่วมมือระหว่างประเทศ เพื่อรับมือกับเครือข่ายอาชญากรรมดังกล่าว ซึ่งกำลังแพร่กระจายไปทั่วโลกพร้อมกับอุปกรณ์สมัยใหม่ เช่น โทรศัพท์มือถือ คอมพิวเตอร์ และแท็บเล็ต รวมทั้งเทคโนโลยีที่เรียกว่า Internet of Things หรืออุปกรณ์ต่าง ๆ รอบตัวเราที่สามารถเชื่อมกับอินเทอร์เน็ตได้เช่นกัน

๒.๑.๒ ความร่วมมือทางกฎหมายระหว่างประชาคมอาเซียน

การประชุมใหญ่สมัชชารัฐสภาอาเซียนครั้งที่ ๔๐ ที่เพิ่งปิดฉากลง เมื่อวันที่ ๓๐ สิงหาคม ๒๕๖๒ ได้มีการประชุมกลุ่มย่อย ภายใต้หัวข้อ “หุ้นส่วนความร่วมมือด้านแนวปฏิบัติที่ดีด้านกฎระเบียบ” ระหว่างประเทศสมาชิกอาเซียนโดยมีผู้สังเกตการณ์จาก ๕ ประเทศ ประกอบด้วย จีน เกาหลีใต้ แคนาดา รัสเซีย และออสเตรเลีย ซึ่งประเด็นดังกล่าวจะส่งผลต่อความสามารถในการแข่งขันและความเข้มแข็งของอาเซียน โดยสอดคล้องกับแผนแม่บทว่าด้วยความเชื่อมโยงระหว่างกันในอาเซียนและแผนงานประชาคมอาเซียน ปี ๒๕๖๘ ซึ่งประเทศไทยคาดหวังว่าประเทศสมาชิกจะสนับสนุนให้มีความร่วมมือด้านกฎหมายและกฎระเบียบระหว่างกัน และระหว่างประเทศสมาชิกอาเซียนกับจีน อันจะเป็นโอกาสที่จะได้เรียนรู้และแบ่งปันประสบการณ์ ในด้านแนวทางการปฏิบัติตามกฎหมายภายในประเทศและภายในภูมิภาค ให้มีความก้าวหน้า ลดขั้นตอนความยุ่งยาก ลดความซ้ำซ้อน และลดภาระเรื่องของกฎระเบียบในอนาคต อันจะส่งผลดีต่อภาพรวมของประชาคมอาเซียน[๓]

๒.๒ แนวคิดการเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย

ปัจจุบันโครงสร้างของหน่วยงานบังคับใช้กฎหมาย ระบบกฎหมายภายในและกรอบความร่วมมือระหว่างประเทศของภูมิภาคอาเซียนที่มีอยู่ในปัจจุบันไม่เพียงพอที่จะจัดการกับปัญหาอาชญากรรมข้ามชาติ โดยเฉพาะอย่างยิ่งในช่วงเปลี่ยนผ่านไปสู่ประชาคมเศรษฐกิจอาเซียนเมื่อปี พ.ศ. ๒๕๕๘ ดังนั้นกระบวนการยุติธรรมทางอาญาจึงจำเป็นต้องถูกปรับเปลี่ยนให้เหมาะสมเพื่อให้สามารถจัดการกับอาชญากรรมข้ามชาติรูปแบบใหม่ ๆ ได้อย่างมีประสิทธิภาพ โดยรัฐอาเซียนควรกำหนดยุทธศาสตร์ว่าด้วยความร่วมมือระหว่างประเทศด้านกระบวนการยุติธรรมทางอาญา เพื่อลดข้อจำกัดด้านกฎหมายภายในของแต่ละประเทศ และเสริมสร้างความร่วมมือในการป้องกันอาชญากรรมข้ามชาติระหว่างหน่วยงานบังคับใช้กฎหมายของอาเซียนให้มากขึ้น ฉะนั้นการทำให้เกิดพันธกรณีทางกฎหมายร่วมกันที่รัฐผู้ร่วมลงนามรับรองจะต้องนำไปปฏิบัติอย่างจริงจังในลักษณะกฎหมายระหว่างประเทศแบบต่าง ๆ เช่น สนธิสัญญา อนุสัญญา พิธีสาร และความตกลงระหว่างประเทศรูปแบบอื่น ๆ[๔]

---

[๓] กรุงเทพธุรกิจ. (๒๕๖๒). *อาเซียน๑๐+๕ ถกกฎระเบียบเพิ่มขีดแข่งขันการค้า*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: www.bangkokbiznews.com/news/detail/๘๔๕๕๖๓

[๔] ชิตพล กาญจนกิจ. (๒๕๕๙). *ความร่วมมือระหว่างประเทศว่าด้วยกระบวนการยุติธรรมทางอาญาอาเซียน: ข้อเสนอเชิงยุทธศาสตร์เพื่อการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียน*, หน้า ๕

๒.๓ ข้อมูลและสภาพทั่วไปเกี่ยวกับอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้องของประเทศมาเลเซีย

๒.๓.๑ ด้านสังคมการเมือง ความมั่นคง และด้านเศรษฐกิจ

มาเลเซียเป็นหนึ่งในสมาชิกสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ หรืออาเซียน (ASEAN) ที่มีเศรษฐกิจสดใสที่สุด มาเลเซียมีความอุดมสมบูรณ์ของทรัพยากรธรรมชาติ และหลากหลายไปด้วยประชากร ๔ เชื้อชาติและศาสนา มาเลเซียตั้งอยู่บริเวณตอนใต้ของคาบสมุทรไทยและทางเหนือของอินโดนีเซีย มาเลเซียแบ่งออกเป็น ๒ ภูมิภาค มาเลเซียตะวันตก ประกอบด้วยรัฐบนคาบสมุทรมลายูซึ่งเชื่อมกับสิงคโปร์ด้วยทางหลวง และมาเลเซียตะวันตกประกอบด้วยรัฐซาบาห์และซาราวักบนเกาะบอร์เนียว แยกออกจากกันโดยทะเลจีนใต้ ชายแดนติดกับบรูไน และเกาะกาลิมันตันของอินโดนีเซีย ขนาดพื้นที่ของมาเลเซียใหญ่กว่ารัฐนิวเม็กซิโกเล็กน้อย พื้นที่ส่วนใหญ่เป็นเทือกเขาปกคลุมหนาแน่นไปด้วยป่าเขตร้อนล้อมรอบด้วยที่ราบชายฝั่ง มาเลเซียมีประชากรประมาณ ๒๖ ล้านคน มาเลเซียตะวันออกมีประชากรหนาแน่นน้อยกว่าฝั่งตะวันตก ที่ตั้งทางยุทธศาสตร์ของมาเลเซียอยู่บริเวณช่องแคบมะละกา และตอนใต้ของทะเลจีนใต้ เป็นทางแยกของการค้าตะวันตกและตะวันออก

๒.๓.๑.๑ ระบบการเมืองการปกครอง

มาเลเซียเป็นรัฐสภาประชาธิปไตยแห่งชาติแบบอังกฤษ โดยมีกษัตริย์ภายใต้รัฐธรรมนูญ ซึ่งประกาศตามรัฐธรรมนูญฉบับ ค.ศ. ๑๙๕๗ ประมุขของประเทศคือ ยังดี เปอร์ตวน อากง (กษัตริย์) ซึ่งจะได้รับเลือกมาดำรงตำแหน่งคราวละ ๕ ปี โดยเลือกมาจากทายาทบรรพบุรุษสุลต่านทั้ง ๙ จากรัฐต่าง ๆ ในคาบสมุทรมลายูเท่านั้นหัวหน้ารัฐบาลหรือนายกรัฐมนตรี ผู้ที่ได้รับเลือกมาจากสมาชิกสภาผู้แทนราษฎร และต้องได้รับการสนับสนุนจากเสียงส่วนใหญ่ของสมาชิกในสภา มาเลเซียใช้ระบบ ๒ สภา Dewan Rakyat (สภาของประชาชน) เป็นสภาล่าง (หรือสภาผู้แทนราษฎร) ประกอบด้วยผู้แทนทั้งหมด ๒๒๒ ที่นั่ง มาจาการเลือกตั้งเดี่ยว ดำรงตำแหน่งวาระละ ๕ ปี ส่วน Dewan Negara (สภาแห่งชาติ) เป็นสภาสูง หรือวุฒิสภา มีสมาชิก ๗๐ คน ดำรงตำแหน่งวาระละ ๓ ปี จำนวน ๓๐ ที่นั่งมาจากการเลือกตั้งจากสภาของทั้ง ๑๔ รัฐ และเขตสหพันธรัฐ (FTs, Federal Territories) ทั้ง ๓ เขต และอีก ๔๐ ที่นั่งมาจากการแต่งตั้งของกษัตริย์ อำนาจสภานิติบัญญัติเป็นการแบ่งสรรระหว่างกฎหมายรัฐบาลกลางและกฎหมายของรัฐ รัฐบาลกลางจะรับผิดชอบในความสัมพันธ์ภายนอก การป้องกันประเทศ ความปลอดภัยในประเทศ สิทธิการเป็นพลเมืองของชาติ การคลัง การพาณิชย์ และอุตสาหกรรม การสื่อสารและการขนส่ง แต่ละรัฐจะมีสภาเป็นของตัวเองควบคุมโดยหัวหน้าคณะรัฐมนตรี ในรัฐที่มีผู้ปกครองเป็นทายาทบรรพบุรุษ หัวหน้าคณะรัฐมนตรีจะต้องเป็นชาวมุสลิมมลายู ทั้งนี้ขึ้นอยู่กับดุลพินิจของผู้ปกครองรัฐ ส่วนรัฐบาลรัฐต่าง ๆ จะรับผิดชอบด้านการพัฒนาโครงสร้างพื้นฐาน ที่ดิน การแสวงหาผลประโยชน์จากทรัพยยากรธรรมชาติยกเว้นป่าไม้ ผู้มีสิทธิในการเลือกตั้ง คือ ประชาชนทุกคนที่มีอายุครบ ๒๑ ปีบริบูรณ์

มาเลเซียแบ่งเขตการปกครองออกเป็น ๑๓ รัฐ (๑๑ รัฐอยู่บนคาบสมุทร ส่วนอีก ๒ รัฐอยู่บนเกาะบอร์เนียว) และสหพันธรัฐ ๓ เขต (FTs, Federal Territories) ได้แก่ กัวลาลัมเปอร์ ลาบวน และปุตราจายา และรัฐต่าง ๆ ได้แก่ ยะโฮร์ เกดะห์ กลันตัน มะละกา เนกรีเซมบีลัน ปะหัง เประ ปะลิส ปีนัง ซาบาห์ ซาลาวัก และตรังกานู แต่ละรัฐแบ่งออกเป็น Daerah (อำเภอ) และ Mukim

(ตำบล) การบริหารอำเภอทำโดยเจ้าหน้าที่อำเภอ ซึ่งได้รับการแต่งตั้งมาจากรัฐบาลของรัฐนั้น ๆ สุลต่าน (หรือราชาในกรณีของรัฐปะลิส และยังดี เปอร์ตวน เบอซาร์ในกรณีของรัฐเนกรีเซมบีลัน) และผู้ว่าราชการในกรณีของรัฐมะละกา รัฐปีนัง รัฐซาบาห์ และรัฐซาราวัก ซึ่งได้ใช้อำนาจเหมือนกษัตริย์อย่างเต็มที่

พรรคการเมืองต่าง ๆ มีพื้นฐานมาจากเชื้อชาติ และถึงแม้ว่ามีพรรคการเมืองลงทะเบียนถึง ๓๐ พรรค แต่มีเพียงรัฐบาลพรรคพันธมิตรกลุ่มเดียวที่ครองประเทศนับตั้งแต่ได้รับอิสระภาพ พันธมิตรดังกล่าวเรียกว่า Barison National (แนวหน้าแห่งชาติ) ได้แก่ พรรคองค์การมลายูสามัคคีแห่งชาติ หรือ UMNO (United malay National Organization) ซึ่งเป็นตัวแทนเชื้อชาติมลายู พรรคสมาคมมาเลเซีย จีน หรือ MCA (Malasian Chinese Association) เป็นพรรคตัวแทนเชื้อชาติจีน และพรรคคองเกรสมาเลเซียอินเดีย หรือ MIC (Malaysian Indian congress) เป็นพรรคตัวแทนเชื้อชาติอินเดีย และพรรคเล็ก ๆ ส่วนใหญ่มาจากรัฐซาบาห์ และรัฐซาราวัก ซึ่งเป็นพรรคตัวแทนชนพื้นเมือง พรรคฝ่ายค้านหลัก ได้แก่ พรรคประชาธิปไตย หรือ DAP (Democratic Action Party) ซึ่งส่วนใหญ่มีเชื้อสายจีน พรรคอิสลามมาเลเซีย หรือ PAS (Pan - malaysian Islamic party) ซึ่งมีเชื้อสายมุสลิมมลายู และพรรคความยุติธรรมประชาชน (People's Justice Party) หรือ PKR (Parti Keadilan Rakyat) ซึ่งมีหลายหลากหลายเชื้อชาติ ทั้ง ๓ พรรคการเมืองนี้รวมตัวกันเป็นพรรคพันธมิตรอิสระ เรียกว่า Pakatan Rakyat (พันธมิตรประชาชน) ในการเลือกตั้ง ค.ศ. ๒๐๐๘ และเรียกคะแนนเสียงได้มากพอสมควร การประท้วงของชาวเชื้อชาติอินเดียเรียกร้องการปฏิบัติอย่างยุติธรรม ก่อให้เกิดเหตุการณ์ที่เป็นสาเหตุแห่งการสูญเสียความสมดุลต่อความสัมพันธ์ของแต่ละเชื้อชาติ รัฐบาลใหม่นำโดยนายกรัฐมนตรี นาจิบ ตัน ราซัค ร่วมการต่อสู้ครั้งนี้ด้วยเพื่อเพิ่มคะแนนเสียงของพรรคในฐานะพรรคร่วมฝ่ายค้าน ซึ่งให้ความสำคัญกับเศรษฐกิจและความสัมพันธ์ด้านเชื้อชาติ

มาเลเซียเป็นสมาชิกผู้ร่วมก่อตั้งอาเซียน และเป็นแรงสนับสนุนสำคัญในด้านความร่วมมือระดับภูมิภาค มาเลเซียเป็นสมาชิกองค์การสหประชาชาติ หรือ UN (United Nations) และได้เข้าร่วมปฏิบัติภารกิจเพื่อรักษาสันติภาพ หลายอย่าง เช่น การเคลื่อนไหวกำลังพลพร้อมอาวุธในเลบานอน ติมอร์ตะวันออก ฟิลิปปินส์ อินโดนีเซีย ปากีสถาน เซียร์ราลิโอน และโคโซโว มาเลเซีย ยังเป็นสมาชิกของเครื่องจักรภพ (Commonwealth) องค์กรความร่วมมือทางเศรษฐกิจเอเชีย - แปซิฟิก หรือ APEC (Asia - Pacific Economic Cooperation) องค์การความร่วมมืออิสลาม หรือ OIC (Organization of Islamic Cooperation) กลุ่มประเทศไม่ฝักใฝ่ฝ่ายใด หรือ NAM (Non - Aligned Movement) กลุ่มประเทศกำลังพัฒนา ๘ ประเทศ (the Developing ๘ Countries) มาเลเซียเป็นสมาชิกองค์การค้าระหว่างประเทศ หรือ WTO (World Trade Organization) ใน ค.ศ. ๑๙๙๕

๒.๓.๑.๒ ระบบเศรษฐกิจ

มาเลเซียเป็นหนึ่งในกลุ่มที่มีเศรษฐกิจที่รุ่งเรือง และได้ประกาศเป็นประเทศที่มีรายได้ปานกลาง มีเศรษฐกิจแบบตลาดเสรีและผนวกเข้ากับเศรษฐกิจโลก มาเลเซียได้รับประโยชน์จากการได้เปรียบด้านที่ตั้ง ซึ่งอยู่ใกล้ช่องแคบมะละกา เส้นทางเดินเรือสายสำคัญสายหนึ่งของโลก ซึ่งเชื่อมเส้นทางการค้าระหว่างตะวันออกกับตะวันตก มาเลเซียเคยมีพื้นฐานเศรษฐกิจมาจากเกษตรกรรมและเหมืองแร่ใน ค.ศ. ๑๙๗๐ และได้เปลี่ยนแปลงเป็นชาติอุตสาหกรรมเทคโนโลยีชั้นสูง มาเลเซียมีการพัฒนาโครงสร้างอยู่ในขั้นดีและมีทรัพยากรธรรมชาติมากมาย พื้นที่กว่า ๕๙% ของมาเลเซียเลยเป็นป่าไม้

ผลิตผลหลัก ได้แก่ ดีบุก น้ำมันปาล์ม ยางพารา ปิโตเลียม ทองแดง แร่เหล็ก ก๊าซธรรมชาติ และแร่อะลูมิเนียม การบริการคิดเป็น ๔๘% ของ GDP อุตสาหกรรมคิดเป็น ๔๒% และเกษตรกรรมคิดเป็น ๑๐% อุตสาหกรรมภาคการผลิต ได้แก่ ผลิตภัณฑ์อิเล็กทรอนิกส์ ฮาร์ดไดรฟ์ และยานยนต์ อุตสาหกรรมภาคการบริการมีความสำคัญเพิ่มมากขึ้น รวมถึงการเติบโตของธุรกิจอสังหาริมทรัพย์ การขนส่งพลังงาน การสื่อสารโทรคมนาคม การจำหน่ายเพื่อการค้า การโรงแรมและการท่องเที่ยว การบริการทางการเงิน บริการด้านข้อมูลและคอมพิวเตอร์ และบริการด้านสุขภาพ

มาเลเซียมีความหลากหลายทางเศรษฐกิจ เศรษฐกิจเติบโต ๖ - ๘% และ GDP ราว ๓๘๑ พันล้านดอลลาร์สหรัฐฯ ใน ค.ศ. ๒๐๐๙ จนกระทั่งต่อมาเศรษฐกิจได้ทรุดตัวลงในช่วงวิกฤติการณ์ทางการเงินในเอเชีย เมื่อรัฐบาลกำหนดอัตราแลกเปลี่ยนริงกิตต่อดอลลาร์สหรัฐฯ เพื่อรับมือเศรษฐกิจที่ทรุดตัวลง เงินสกุลริงกิตของมาเลเซียเปลี่ยนแปลงมาเป็นแบบลอยตัวตั้งแต่ ค.ศ. ๒๐๐๖ มาเลเซียได้ทรุดตัวลงอย่างหนักอีกครั้ง เมื่อเศรษฐกิจโลกอยู่ในภาวะซบเซาในช่วง ค.ศ. ๒๐๐๘ - ๒๐๐๙ แต่ก็ค่อย ๆ เริ่มฟื้นตัวขึ้นอย่างช้า ๆ ต่อมารัฐบาลเพิ่มมาตราการกระตุ้นเศรษฐกิจเพื่อการเติบโตแบบก้าวกระโดด อัตราเงินเฟ้อ อัตราการว่างงาน และปัญหาความยากจนอยู่ในระดับต่ำ รัฐบาลจัดการปฏิรูปการเงินและการธนาคาร ธนาคารในประเทศรวมตัวกันและค่อย ๆ เข้าสู่การเปิดเสรี เพิ่มสิ่งดึงดูดการลงทุนจากต่างประเทศ โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีชั้นสูง เช่น จัดตั้งโครงการทางด่วนมัลติมีเดีย หรือ MSC (Multimedia Super Corridor)

การส่งออกยังเป็นการขับเคลื่อนทางเศรษฐกิจ ซึ่งมีมูลค่าถึง ๑๕๖ พันล้านดอลลาร์สหรัฐฯ ใน ค.ศ. ๒๐๐๙ การส่งออกน้ำมันและก๊าซคิดเป็น ๔๐% ของรายได้รวมของรัฐบาล นอกจากนี้ยังมีสินค้าส่งออกหลักอื่น ๆ ได้แก่ อุปกรณ์อิเล็กทรอนิกส์ สารกึ่งตัวนำ ไม้และผลิตภัณฑ์จากไม้ น้ำมันปาล์ม ยางพารา สิ่งทอและเคมีภัณฑ์ รัฐบาลปัจจุบันดำเนินงาน เพื่อเลื่อนระดับเศรษฐกิจเพิ่มมูลค่าห่วงโซ่การผลิตเพื่อลดการพึ่งพาการส่งออก ซึ่งส่วนนี้เป็นการช่วยสนับสนุนการลงทุนในด้านเทคโนโลยีชีวภาพ เภสัชกรรม การผลิตชิ้นส่วนยานยนต์ การท่องเที่ยว การวิจัยและพัฒนา การพัฒนากำลังคน และการจัดการสิ่งแวดล้อม มาเลเซียมีเขตอุตสาหกรรมเสรี หรือ FIZ (Free Industrial Zone) ๑๓ เขต และเขตการค้าเสรี หรือ FCZ (Free Commercial Zone) ๑๒ เขต ซึ่งวัตถุดิบ ผลิตภัณฑ์ และอุปกรณ์ จะนำเข้ามาโดยใช้กฎระเบียบการนำเข้าต่าง ๆ ในขั้นต่ำที่สุด

ลักษณะเด่นของเศรษฐกิจมาเลเซีย คือ นโยบายเศรษฐกิจใหม่ หรือ NEP (New Economic Policy) ที่ออกมาใน ค.ศ. ๑๙๗๑ เพื่อลดความแตกต่างทางสังคมและเศรษฐกิจระหว่างชาวมลายู ซึ่งเป็นประชากรส่วนใหญ่และชนกลุ่มน้อยชาวจีนโดยหลัก ๆ แล้วเป็นระบบยืนยันสิทธิประโยชน์ โดยมีเป้าหมายเพื่อถ่ายโอน ๓๐% ของความร่ำรวยของประเทศไปสู่ชาวมลายู Bumiputera (พื้นเมือง) นโยบายนี้นำมาใช้ โดยใช้โครงการที่ให้สิทธิประโยชน์แก่ชาวมลายู ผ่านสิทธิพิเศษในการ เป็นเจ้าของที่ดินและอสังหาริมทรัพย์ ธุรกิจ งานข้าราชการพลเรือน การศึกษา การเมือง ศาสนา และภาษา ต่อมาใน ค.ศ. ๑๙๙๑ นโยบายนี้ได้ถูกเปลี่ยนชื่อเป็น แผนนโยบายการพัฒนาแห่งชาติ หรือ NDP (National Development Policy) มีการเปลี่ยนแปลงบ้างแต่ยังคงยึดเป้าหมายเดิม แม้ว่าความไม่สมดุลด้านรายได้จะลดลงแล้วก็ตาม แต่นับว่ายังไม่บรรลุวัตถุประสงค์หลัก มีการถกเถียงในเรื่องนี้ตามมาหลายครั้งและหลายฝ่ายเห็นว่านโยบายนี้ทำให้เกิดความร่ำรวยในกลุ่มมุสลิมชั้นสูงเพียงกลุ่มเล็ก ๆ เท่านั้น ราวกับว่านโยบายนี้จะลดชนชาวจีนและชาวอินเดียซึ่งมีน้อยกว่ากลายเป็น

พลเมืองชั้นที่ ๒ ในเดือนเมษายน ค.ศ. ๒๐๐๙ รัฐบาลจึงยกเลิกข้อกำหนดด้านสิทธิประโยชน์บางประการของชาวมลายู

โดยรวมแล้วรัฐบาลมาเลเซียได้ปรับปรุงบรรยากาศที่อำนวยต่อการลงทุน โดยอนุญาตให้เป็นเจ้าของกรรมสิทธิ์ได้ ๑๐๐% ในอุตสาหกรรมการผลิต เปิดเสรีภาคการเงิน และยกเลิกการควบคุมเงินทุนในการลงทุนต่างประเทศ โครงการในด้านโครงสร้างพื้นฐานหลายโครงการที่ใช้งบประมาณของรับได้เริ่มต้นขึ้น กำลังซื้อของมาเลเซียยังคงอยู่ในลำดับสูงสุดของอาเซียน

๒.๓.๑.๓ ระบบกฎหมาย

มาเลเซียมีระบบตุลาการแบบรวม ศาลทุกแห่งรับอำนาจการพิจารณาคดีทั้งจากกฎหมายรัฐบาลกลางและของรัฐ ระบบกฎหมายของมาเลเซียมีพื้นฐานมาจากกฎหมายจารีตประเพณีของอังกฤษ ตามที่บัญญัติไว้ในรัฐธรรมนูญ ซึ่งถูกกำหนดระหว่างที่เป็นอาณานิคมของอังกฤษ และได้รับอิทธิพลมาจากระบบกฎหมายของอินเดียในกระบวนพิจารณาความคดีอาญา และรัฐบัญญัติว่าด้วยเรื่องสัญญารวมถึงระบบกฎหมายออสเตรเรียในด้านกฎหมายที่ดิน สาขาอำนาจตุลาการมาเลเซียมีศาลสหพันธรัฐเป็นศาลสูงสุด ศาลอุทธรณ์ ศาลสูงของคาบสมุทรมลายู ซาบาร์ และซาราวัก ศาลสหพันธรัฐนำโดยกษัตริย์ที่มีอำนาจศาลพิเศษในด้านข้อพิพาทระหว่างรัฐกับรัฐ หรือระหว่างรัฐบาลรัฐกับรัฐบาลกลาง ศาลสหพันธรัฐ ประกอบด้วย ประธานศาลสูงสุด ผู้พิพากษาหัวหน้าศาล ๒ คน จากศาลสูง และผู้พิพากษาอื่น ๆ อีก ๗ คน ศาลสูงมีอำนาจตุลาการ ในการพิจารณาคดีอาญาร้ายแรงและคดีแพ่งเป็นส่วนใหญ่ ศาลเซสชั่น (Session Court) จะพิจารณาคดีเกี่ยวกับข้อพิพาทระหว่างผู้ให้เช่ากับผู้เช่า และอุบัติเหตุรถยนต์ ศาลแขวงพิจารณาคดีอาญาที่ตัดสินโทษสูงสุดไม่เกิด ๑๒ เดือน ศาลอุทรณ์ มีอำนาจเหนือการตัดสินของศาลสูงและศาลเซสชั่น ศาลพิเศษมาเลเซียเกิดขึ้นเมื่อ ค.ศ. ๑๙๙๓ เพื่อจัดการกับการกระทำผิดกฎหมายของผู้นำประเทศ (เช่น ผู้นำของรัฐย่อยต่าง ๆ ในสหพันธรัฐมาเลเซีย) รวมทั้งกษัตริย์ ศาลพิเศษพิจารณาคดีแพ่งต่าง ๆ จากผู้นำรัฐหรือผู้ที่ยื่นฟ้องผู้นำรัฐมีประธานศาลสูงสุดเป็นผู้นำ และมีผู้ช่วยเป็นผู้พิพากษาจากศาลสูง ๒ คน และบุคคลอื่นอีก ๒ คน ที่ได้รับการแต่งตั้งจากที่ประชุมผู้นำ (Conference of Rulers) ผู้ที่มีตำแหน่งหรือเคยดำรงตำแหน่งเป็นผู้พิพากษา

มาเลเซียเป็นสมาชิกองค์การทรัพย์สินทางปัญญาโลก หรือ WIPO (World Intellectual Property Organization) แต่ก็มีปัญหาเรื่องการละเมิดลิขสิทธิ์ มาเลเซียมีกฎหมายการเซ็นเซอร์บางอย่างที่เคร่งครัดที่สุดในโลก รัฐพยายามควบคุมสื่ออย่างมาก โดยระบุว่าเป็นความมั่นคงของชาติและปัญหาด้านเชื้อชาติ การค้ายาเสพติด และพกอาวุธ จะได้รับโทษขั้นรุนแรงอาจถึงขั้นประหารชีวิต มาเลเซียยังไม่ยอมรับอำนาจบังคับจากศาลยุติธรรมระหว่างประเทศ หรือศาลโลก (ICJ: International Court of Justice) มาเลเซียเป็นสมาชิกที่มีประสิทธิภาพขององค์การค้าโลก หรือ WTO และเขตการค้าเสรีอาเซียน หรือ AFTA มาเลเซียได้ลงนามข้อตกลงพันธมิตรการค้ากับญี่ปุ่น (FAT: Federal Trade Agreements) ปากีสถานและนิวซีแลนด์ มาเลเซียเข้าร่วมการค้ากับ ๕ ภูมิภาค ในเขตการค้าเสรีอาเซียน หรือ AFTA และเจรจาต่อรองเรื่องการค้าเสรีโดยตรงกับประเทศอินเดีย ชิลี ออสเตรเรีย และเขตการค้าเสรีอาเซียน – ยุโรป (ASEAN-EU FTA) และมาเลเซียยังเป็นสมาชิกองค์กรความร่วมมือทางเศรษฐกิจเอเชีย - แปซิฟิก หรือ APEC อีกด้วย

๒.๓.๒ ด้านอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

กฎหมายมาเลเซีย

พ.ร.บ. ๕๖๓

อาชญากรรมคอมพิวเตอร์ พ.ศ. ๒๕๔๐

ส่วนที่ ๑

เบื้องต้น

๑. ชื่อย่อ/การริเริ่มใช้

๒. การตีความ

ส่วนที่ ๒

ความผิด

๓. การเข้าถึงเนื้อหาโดยไม่ได้รับอนุญาต

๔. การเข้าถึงโดยไม่ได้รับอนุญาตโดยมีเจตนาที่จะกระทำหรืออำนวยความสะดวกในการกระทำความผิดเพิ่มเติม

๕. การดัดแปลงเนื้อหาของคอมพิวเตอร์ใด ๆ โดยไม่ได้รับอนุญาต

๖. การสื่อสารที่ไม่ถูกต้อง

๗. การยกเลิกและพยายามลงโทษเป็นความผิด

๘. ข้อสันนิษฐาน

ส่วนที่ ๓

บทบัญญัติและข้อกำหนดทั่วไป

๙. ขอบเขตการกระทำความผิดภายใต้พระราชบัญญัตินี้

๑๐. อำนาจในการค้นหายึดและจับกุม

๑๑. ขัดขวางการค้นหา

๑๒. การฟ้องร้อง

กฎหมายของประเทศมาเลเซีย

พ.ร.บ. ๕๖๓

พระราชบัญญัติอาชญากรรมคอมพิวเตอร์ พ.ศ. ๒๕๔๐

พระราชบัญญัติเพื่อจัดให้มีการกระทำความผิดเกี่ยวกับการใช้คอมพิวเตอร์ในทางที่ผิดไม่ว่าจะเป็นการออกโดย Seri aduka Baginda Yang di-Pertuan Agong โดยคำแนะนำและความยินยอมของ Dewan Negara และ Dewan Rakyat ในการชุมนุมในรัฐสภาและโดยอำนาจดังต่อไปนี้ :

ส่วนที่ ๑
เบื้องต้น
ชื่อย่อและการเริ่มใช้

มาตรา ๑

(๑) พระราชบัญญัตินี้อาจอ้างถึงเป็นพระราชบัญญัติอาชญากรรมคอมพิวเตอร์ พ.ศ. ๒๕๔๐

(๒) พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันที่นายกรัฐมนตรีประกาศโดยประกาศในราชกิจจานุเบกษา

การตีความ

มาตรา ๒

(๑) ในพระราชบัญญัตินี้เว้นแต่บริบทจะกำหนดไว้เป็นอย่างอื่น -

"คอมพิวเตอร์" หมายถึง อุปกรณ์ประมวลผลอิเล็กทรอนิกส์ แม่เหล็ก ออปติคอล เคมีไฟฟ้า หรือข้อมูลอื่น ๆ หรือกลุ่มของอุปกรณ์ที่เชื่อมต่อหรือที่เกี่ยวข้องดังกล่าว แสดงฟังก์ชันตรรกะการคำนวณ การจัดเก็บ และการแสดงผล และรวมถึงสถานที่จัดเก็บข้อมูลใด ๆ ทำงานร่วมกับอุปกรณ์หรือกลุ่มของอุปกรณ์เชื่อมต่อหรืออุปกรณ์ที่เกี่ยวข้องดังกล่าว แต่ไม่รวมเครื่องพิมพ์ดีดหรือเครื่องพิมพ์ดีดอัตโนมัติหรือเครื่องคิดเลขแบบพกพา มือถือ หรืออุปกรณ์อื่น ๆ ที่คล้ายกันซึ่งไม่สามารถตั้งโปรแกรมได้หรือการสื่อสาร

"เครือข่ายคอมพิวเตอร์" หมายถึง การเชื่อมต่อโครงข่ายสายสัญญาณ และวงจรสื่อสารกับคอมพิวเตอร์หรือคอมเพล็กซ์ ซึ่งประกอบด้วย คอมพิวเตอร์ที่เชื่อมต่อกันตั้งแต่สองเครื่องขึ้นไป

"เอาต์พุตคอมพิวเตอร์" หรือ "เอาต์พุต" หมายถึง คำสั่งหรือการเป็นตัวแทนไม่ว่าจะเป็นในรูปแบบที่เป็นลายลักษณ์อักษร พิมพ์ภาพฟิล์มกราฟิกอะคูสติก หรือรูปแบบอื่น ๆ –

(a) ผลิตโดยคอมพิวเตอร์

(b) แสดงบนหน้าจอคอมพิวเตอร์ หรือ

(c) แปลอย่างถูกต้องจากคำแถลงหรือการเป็นตัวแทนที่ผลิตขึ้นดังนั้น

"ข้อมูล" หมายถึง การนำเสนอข้อมูลหรือแนวคิดที่จัดทำหรือจัดทำในรูปแบบที่เหมาะสมสำหรับใช้ในคอมพิวเตอร์

"ฟังก์ชั่น" รวมถึง ตรรกะการควบคุมการคำนวณ การลบ การจัดเก็บ และการค้นคืน และการสื่อสารหรือการสื่อสารโทรคมนาคมไปยังจากหรือภายในคอมพิวเตอร์

"สถานที่" รวมถึง ที่ดินอาคารสิ่งปลูกสร้างที่เคลื่อนย้ายได้ และพาหนะใด ๆ ทางบก ทางน้ำและทางอากาศ

"โปรแกรม" หมายถึง ข้อมูลที่แสดงคำสั่งหรือข้อความที่เมื่อใช้งานในคอมพิวเตอร์จะทำให้คอมพิวเตอร์ทำงานได้

(๒) เพื่อความมุ่งประสงค์ของพระราชบัญญัตินี้ บุคคลจะได้รับสิทธิ์ในการเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ ถ้าหากคอมพิวเตอร์ทำให้การทำงานใด ๆ เกิดขึ้น

(a) เปลี่ยนแปลงหรือลบโปรแกรมหรือข้อมูล

(b) คัดลอกหรือย้ายไปยังสื่อบันทึกข้อมูลอื่นนอกเหนือจากที่จัดเก็บ หรือไปยังตำแหน่งอื่นในสื่อบันทึกข้อมูลที่จัดเก็บอยู่

(c) ใช้งาน หรือ

(d) ทำให้คอมพิวเตอร์ถูกส่งออกจากคอมพิวเตอร์ที่แสดงว่ามีการแสดงผล หรือในลักษณะอื่นใด และการอ้างอิงถึงการเข้าถึงโปรแกรมหรือข้อมูล และเพื่อเจตนาในการรักษาความปลอดภัยการเข้าถึงดังกล่าวจะถูกตีความตามนั้น

(๓) สำหรับจุดประสงค์ของย่อหน้า (๒) (C) บุคคลใช้โปรแกรมหากฟังก์ชันที่ทำให้คอมพิวเตอร์ทำงาน

(a) ทำให้โปรแกรมทำงาน หรือ

(b) เป็นฟังก์ชันของโปรแกรม

(๔) สำหรับวัตถุประสงค์ของวรรค (๒) (d) รูปแบบที่โปรแกรมหรือข้อมูลใด ๆ ถูกส่งออกและโดยเฉพาะอย่างยิ่งมันแสดงถึงรูปแบบที่ในกรณีของโปรแกรมมันสามารถที่จะเป็น ดำเนินการหรือในกรณีของข้อมูลคอมพิวเตอร์นั้น มีความสามารถในการประมวลผลที่ไม่เป็นสาระสำคัญ

(๕) เพื่อวัตถุประสงค์ของพระราชบัญญัตินี้การเข้าถึงข้อมูลหรือโปรแกรมใด ๆ ที่จัดขึ้นในคอมพิวเตอร์ไม่ได้รับอนุญาตหากบุคคลใด ๆ

(a) เขาไม่มีสิทธิ์ควบคุมการเข้าถึงโปรแกรมหรือข้อมูลที่เป็นปัญหา และ

(b) เขาไม่ได้รับความยินยอมหรือเกินกว่าสิทธิ์หรือความยินยอมใด ๆ ในการเข้าถึงโดยบุคคลที่มีปัญหากับโปรแกรมหรือข้อมูลจากบุคคลใด ๆ ที่ได้รับสิทธิดังกล่าว

(๖) การอ้างอิงในพระราชบัญญัตินี้ไปยังโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์รวมถึงการอ้างอิงถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในสื่อบันทึกข้อมูลแบบถอดได้ใด ๆ ซึ่งเป็นเวลาที่อยู่ในคอมพิวเตอร์

(๗) เพื่อความมุ่งประสงค์ของพระราชบัญญัตินี้การแก้ไขเนื้อหาของคอมพิวเตอร์ใด ๆ จะเกิดขึ้นถ้าโดยการทำงานของคอมพิวเตอร์ใด ๆ ที่เกี่ยวข้องหรือคอมพิวเตอร์อื่น ๆ

(a) โปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ที่เกี่ยวข้อง หรือลบ;

(b) โปรแกรมหรือข้อมูลใด ๆ ที่มีการแนะนำหรือเพิ่มเนื้อหาของมัน; หรือ

(c) เหตุการณ์ใด ๆ เกิดขึ้นซึ่งทำให้การทำงานปกติของคอมพิวเตอร์ใด ๆ

(๘) การดัดแปลงใด ๆ ที่อ้างถึงในส่วนย่อย (๗) ไม่ได้รับอนุญาตหาก

(a) บุคคลที่มีการกระทำทำให้ไม่มีสิทธิ์ในการพิจารณาว่าควรทำการแก้ไขหรือไม่ และ

(b) เขาไม่ได้ยินยอมให้มีการแก้ไขจากบุคคลใด ๆ ที่มีสิทธิเช่นนั้น

(๙) การอ้างอิงในพระราชบัญญัตินี้ไปยังโปรแกรมรวมถึงการอ้างอิงถึงส่วนหนึ่งของโปรแกรม

(๑๐) การอ้างอิงในพระราชบัญญัตินี้ไปยังคอมพิวเตอร์รวมถึงการอ้างอิงไปยังเครือข่ายคอมพิวเตอร์

ส่วนที่ ๒
ความผิด
การเข้าถึงสื่อคอมพิวเตอร์โดยไม่ได้รับอนุญาต

มาตรา ๓

(๑) บุคคลต้องมีความผิดถ้า –

(a) เขาทำให้คอมพิวเตอร์ทำงานใด ๆ โดยมีเจตนาเพื่อความปลอดภัยในการเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ใด ๆ;

(b) เขามีเจตนาเข้าถึงโดยที่ไม่มีอำนาจ และ

(c) เขารู้อยู่ว่าทำให้คอมพิวเตอร์ปฏิบัติหน้าที่ที่เป็นจริง

(๒) บุคคลจะต้องมีเจตนากระทำความผิดตามมาตรานี้ไม่จำเป็นต้องถูกนำไปที่ –

(a) โปรแกรมหรือข้อมูลใด ๆ โดยเฉพาะ

(b) โปรแกรมหรือข้อมูลใด ๆ หรือ

(c) โปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ได้

(๓) ผู้กระทำความผิดตามความในมาตรานี้ต้องระวางโทษปรับไม่เกินห้าหมื่นริงกิตหรือจำคุกไม่เกินห้าปีหรือทั้งจำทั้งปรับ

การเข้าถึงที่ไม่ได้รับอนุญาตโดยมีเจตนาที่จะกระทำหรืออำนวยความสะดวกในการกระทำความผิดเพิ่มเติม

มาตรา ๔

(๑) บุคคลนั้นมีความผิดตามมาตรานี้ถ้าเขาได้กระทำความผิดตามที่อ้างถึงในส่วนที่ ๓ โดยเจตนา -

(a) กระทำความผิดที่เกี่ยวข้องกับการฉ้อโกงหรือความไม่ซื่อสัตย์ซึ่งเป็นสาเหตุหรือการบาดเจ็บตามที่กำหนดไว้ในประมวลกฎหมายอาญา [พระราชบัญญัติ ๕๗๔] หรือ

(b) เพื่ออำนวยความสะดวกในการกระทำความผิดดังกล่าวไม่ว่าจะด้วยตนเองหรือโดยบุคคลอื่นใด

(๒) เพื่อความมุ่งประสงค์ของส่วนนี้มันเป็นสาระสำคัญไม่ว่าจะเป็นการกระทำความผิดซึ่งส่วนนี้มีผลในเวลาเดียวกันเมื่อการเข้าถึงที่ไม่ได้รับอนุญาตมีความปลอดภัยหรือในโอกาสใด ๆ ในอนาคต

(๓) ผู้กระทำความผิดตามมาตรานี้ต้องระวางโทษปรับไม่เกินหนึ่งแสนห้าหมื่นริงกิตหรือจำคุกไม่เกินสิบปีหรือทั้งจำทั้งปรับ

การดัดแปลงเนื้อหาของคอมพิวเตอร์ใด ๆ โดยไม่ได้รับอนุญาต

มาตรา ๕

(๑) บุคคลนั้นมีความผิดถ้าเขากระทำการใด ๆ ที่เขารู้ว่าจะทำให้เกิดการดัดแปลงเนื้อหาของคอมพิวเตอร์เครื่องใด ๆ โดยไม่ได้รับอนุญาต

(๒) เพื่อความมุ่งประสงค์ของส่วนนี้มันไม่มีสาระสำคัญที่การกระทำที่เป็นปัญหาไม่ได้มุ่งไปที่ -

(a) โปรแกรมหรือข้อมูลใด ๆ โดยเฉพาะ

(b) โปรแกรมหรือข้อมูลใด ๆ หรือ

(c) โปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ได้

(๓) เพื่อความมุ่งประสงค์ของส่วนนี้มันเป็นสาระสำคัญไม่ว่าจะมีการดัดแปลงที่ไม่ได้รับอนุญาตหรือมีวัตถุประสงค์ เพื่อถาวรหรือเพียงชั่วคราว

(๔) ผู้กระทำความผิดตามมาตรานี้ต้องระวางโทษปรับไม่เกินหนึ่งแสนริงกิตหรือจำคุกไม่เกินเจ็ดปี หรือทั้งสองจำทั้งปรับ หรือต้องระวางโทษปรับไม่เกินหนึ่งแสนห้าหมื่นริงกิตหรือต้องระวางโทษจำคุกไม่เกินสิบปีหรือทั้งจำทั้งปรับ หากการกระทำนั้นมีเจตนาทำให้เกิดการบาดเจ็บตามที่กำหนดไว้ในประมวลกฎหมายอาญา

การสื่อสารที่ผิดพลาด

มาตรา ๖

(๑) ผู้กระทำความผิดจะต้องมีความผิดถ้าเขาสื่อสารหมายเลขรหัส รหัสผ่านหรือวิธีการอื่น ๆ ของคอมพิวเตอร์โดยตรงหรือโดยอ้อมให้กับบุคคลอื่นที่ไม่ใช่บุคคลที่ได้รับอนุญาตให้ทำการสื่อสาร

(๒) ผู้กระทำความผิดตามความในมาตรานี้ต้องระวางโทษปรับไม่เกินสองหมื่นห้าพันริงกิตหรือจำคุกไม่เกินสามปี หรือ ทั้งสองกรณี

การช่วยเหลือและพยายามลงโทษเป็นความผิด

มาตรา ๗

(๑) บุคคลที่สนับสนุนคณะกรรมการหรือผู้ที่พยายามกระทำความผิดตามพระราชบัญญัตินี้มีความผิดในความผิดนั้นและจะต้องมีความเชื่อมั่นต่อการลงโทษที่กำหนดไว้สำหรับความผิด

(๒) บุคคลที่กระทำการใด ๆ ที่ได้เตรียมการหรือดำเนินการต่อไปของการกระทำความผิดใด ๆ ภายใต้พระราชบัญญัตินี้จะต้องมีความผิดในการกระทำความผิดนั้น และจะต้องรับผิดชอบต่อการลงโทษที่กำหนดไว้สำหรับความผิด: โดยมีเงื่อนไขว่าการจำคุกใด ๆ ที่กำหนดจะต้องไม่เกินครึ่งหนึ่งของระยะเวลาสูงสุดที่กำหนดไว้สำหรับความผิด

ข้อสันนิษฐาน

มาตรา ๘ บุคคลที่อยู่ในความดูแลของเขาหรือควบคุมโปรแกรมใด ๆ ข้อมูลหรือข้อมูลอื่น ๆ ที่เก็บไว้ในคอมพิวเตอร์หรือเรียกคืนจากคอมพิวเตอร์ใด ๆ ที่เขาไม่ได้รับอนุญาตให้มีในการดูแลหรือควบคุมของเขาจะถือว่าได้รับการเข้าถึงโปรแกรมดังกล่าวโดยไม่ได้รับอนุญาต ข้อมูลหรือข้อมูลเว้นแต่จะมีการพิสูจน์ตรงกันข้าม

ส่วนที่๓

บทบัญญัติและขอบเขตทั่วไปของความผิดตามขอบเขตของความผิดตามพระราชบัญญัตินี้

มาตรา ๙

(๑) บทบัญญัติของพระราชบัญญัตินี้จะเกี่ยวข้องกับบุคคลใด ๆ ไม่ว่าสัญชาติหรือสัญชาติของเขาจะมีผลกระทบภายนอกเช่นเดียวกับในมาเลเซีย และในกรณีที่มีการกระทำความผิดตามพระราชบัญญัตินี้โดยบุคคลใดในสถานที่ใดนอกประเทศมาเลเซียเขาอาจได้รับการจัดการในส่วนที่เกี่ยวกับความผิดดังกล่าวราวกับว่าได้กระทำในสถานที่ใด ๆ ในมาเลเซีย

(๒) เพื่อความมุ่งประสงค์ของส่วนย่อย (๑) พระราชบัญญัตินี้จะใช้บังคับถ้าหากมีความผิดคอมพิวเตอร์ คอมพิวเตอร์โปรแกรมหรือข้อมูลอยู่ในมาเลเซียหรือสามารถเชื่อมต่อหรือส่งไปยังหรือใช้โดยหรือกับคอมพิวเตอร์ในมาเลเซียในเวลาวัสดุ

(๓) การดำเนินการใด ๆ กับบุคคลใด ๆ ในส่วนนี้ซึ่งจะเป็นบาร์ในการดำเนินคดีต่อบุคคลดังกล่าวในความผิดเดียวกัน หากความผิดดังกล่าวได้กระทำในประเทศมาเลเซียจะเป็นบาร์ที่จะดำเนินคดีต่อเขาภายใต้กฎหมายเป็นลายลักษณ์อักษรของบุคคลในความผิดเดียวกันนอกประเทศมาเลเซีย

อำนาจในการค้นหา ยึดและการจับกุม

มาตรา ๑๐

(๑) เมื่อใดก็ตามที่ปรากฏแก่ผู้พิพากษาตามข้อมูลและหลังจากการไต่สวนตามที่เขาคิดว่าจำเป็นต้องมีเหตุอันควรเชื่อได้ว่าในสถานที่ใดก็ตามมีหลักฐานของการกระทำความผิด การกระทำเขาอาจโดยหมายจับไปยังเจ้าหน้าที่ตำรวจคนใดหรือสูงกว่าตำแหน่งของผู้ตรวจการให้อำนาจเจ้าหน้าที่เข้ามาในสถานที่โดยการบังคับถ้าจำเป็นและมีการค้นหายึดและกักตัวพยานหลักฐานดังกล่าว และเขาจะมีสิทธิ์

(a) มีการเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ได้หรือมีการเข้าถึงตรวจสอบคอมพิวเตอร์ และอุปกรณ์หรือวัสดุที่เกี่ยวข้อง ซึ่งเขามีเหตุอันควรสงสัยว่ามีหรือถูกใช้ในการเชื่อมต่อกับความผิดตามพระราชบัญญัตินี้

(b) ต้องการ

(i) เจ้าหน้าที่มีเหตุอันควรสงสัยว่ามีการใช้คอมพิวเตอร์หรือถูกใช้งานหรือโดยใครหรือในนามของตำรวจ

(ii) บุคคลใดที่รับผิดชอบหรือเกี่ยวข้องกับการทำงานของคอมพิวเตอร์อุปกรณ์หรือวัสดุเพื่อให้ความช่วยเหลือตามสมควรแก่เขาตามที่เขาอาจต้องการ สำหรับวัตถุประสงค์ของวรรค (ก); และ

(c) ต้องการข้อมูลใด ๆ ที่มีอยู่ในคอมพิวเตอร์และสามารถเข้าถึงได้จากสถานที่เพื่อผลิตในรูปแบบที่สามารถนำออกไป และที่สามารถมองเห็นได้และชัดเจน

(๒) เมื่อใดก็ตามที่ปรากฏต่อเจ้าหน้าที่ตำรวจระดับสูงกว่าผู้ตรวจสอบของตนว่ามีเหตุอันควรเชื่อได้ว่าในสถานที่ใดมีการปกปิดหรือวางหลักฐานการกระทำความผิดตามพระราชบัญญัตินี้และเจ้าหน้าที่ตำรวจมีเหตุผลอันสมควร สำหรับความเชื่อที่ว่าด้วยเหตุผลของความล่าช้าในการได้รับหมายเรียกวัตถุของการค้นหานั้นน่าจะทำให้เขาผิดหวังเขาอาจใช้และในแง่ของอำนาจทั้งหมดที่กล่าวถึงในส่วนย่อย (๑) เต็มและเพียงพอราวกับว่าเขามีอำนาจที่จะทำเช่นนั้นโดยออกหมายจับภายใต้หมวดย่อย

(๓) เจ้าหน้าที่ตำรวจใด ๆ อาจจับกุมโดยไม่มีหมายจับบุคคลใด ๆ ที่เขาเชื่ออย่างสมเหตุสมผลว่าได้กระทำหรือกระทำความผิดตามพระราชบัญญัตินี้และการกระทำผิดต่อพระราชบัญญัตินี้ทุกครั้งจะถือว่าเป็นการกระทำความผิดตามวัตถุประสงค์ของกฎหมายสำหรับ เวลาที่ใช้บังคับกับกระบวนการทางอาญา

การขัดขวางการค้นหา

มาตรา ๑๑

(๑) บุคคลนั้นมีความผิดถ้าเขา

(ก) ข่มขืนขัดขวางกีดขวางหรือมีผลต่อการเข้าสถานที่ใด ๆ ภายใต้พระราชบัญญัตินี้หรือในการปฏิบัติหน้าที่ใด ๆ ตามพระราชบัญญัตินี้ หรือความล่าช้าของเจ้าหน้าที่ตำรวจหรืออำนาจที่ได้รับ

(ข) ไม่ปฏิบัติตามข้อเรียกร้องทางกฎหมายใด ๆ ของเจ้าหน้าที่ตำรวจที่ปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

(๒) ผู้กระทำความผิดตามความในมาตรานี้ต้องระวางโทษปรับไม่เกินสองหมื่นห้าพันริงกิต หรือต้องระวางโทษจำคุกไม่เกินสามปี หรือทั้งจำทั้งปรับ

การฟ้องร้อง

มาตรา ๑๒

การฟ้องคดีตามพระราชบัญญัตินี้จะไม่กระทำขึ้นเว้นแต่จะได้รับความยินยอมจากพนักงานอัยการเป็นลายลักษณ์อักษร

๒.๔ ข้อมูลและสภาพทั่วไปเกี่ยวกับอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้องของสาธารณรัฐสิงคโปร์

๒.๔.๑ ด้านสังคมการเมือง ความมั่นคง และด้านเศรษฐกิจ

๒.๔.๑.๑ ระบบการเมืองการปกครอง

สิงคโปร์เป็นประเทศที่มีเสถียรภาพทางการเมืองมากที่สุดในอาเซียน และรัฐบาลปัจจุบันได้เข้าดำรงตำแหน่งตั้งแต่ได้รับเลือก เมื่อสิงคโปร์ได้ปกครองตนเองใน ค.ศ. ๑๙๕๙ ช่วงรวมตัวเข้ากับมาเลเซีย และเมื่อได้รับเอกราชเต็มตัวใน ค.ศ. ๑๙๖๕ สิงคโปร์เป็นสาธารณรัฐและประชาธิปไตยแบบสภา โดยเลือกประธานาธิบดีในฐานะประมุขของประเทศ ซึ่งดำรงตำแหน่งวาระละ ๖ ปี หัวหน้ารัฐบาล คือ นายกรัฐมนตรี ผู้ที่เป็นหัวหน้าพรรคซึ่งได้ที่นั่งสูงสุดในสภาสามารถดำรงตำแหน่งได้หลายวาระ รัฐมนตรีผู้บริหารจะได้รับเลือกจากผู้นำ แต่ต้องมาจากสมาชิกที่ได้รับเลือกเท่านั้น สิงคโปร์ใช้ระบบสภาเดียวมีสมาชิก ๙๔ ที่นั่ง ซึ่ง ๙ ที่นั่ง จะถูกระบุชื่อเป็นตัวแทนฝ่ายค้าน เนื่องจากมีการออกบทบัญญัติไว้ใน ค.ศ. ๑๙๘๔ เพราะสิงคโปร์ไม่มีฝ่ายค้านที่แท้จริง ตั้งแต่ที่ได้เป็นอิสระ ที่นั่งฝ่ายค้านไม่ได้มาจากการเลือกตั้ง แต่ถูกเสนอให้ผู้สมัครที่ได้รับคะแนนสูงสุดหรือมากกว่า ๑๕% จากการเลือกตั้ง ซึ่งได้รับการแต่งตั้งโดยประธานาธิบดีในตำแหน่งสมาชิกรับสภาที่ได้แต่งตั้ง หรือ NMP (Nominated Member of Parliament) และได้รับเลือกจากคณะกรรมการพิเศษที่แต่งตั้งโดยรัฐบาลพวกเขาได้รับสิทธิประโยชน์ต่าง ๆ เช่นเดียวกับสมาชิกทั่วไปของรัฐสภาแต่ไม่มีสิทธิ์ออกเสียงในด้านรัฐธรรมนูญที่เกี่ยวข้องกับงบประมาณไม่มีสิทธิ์ไม่ไว้วางใจรัฐบาล หรือขับไล่ประธานาธิบดีออกจากตำแหน่ง จะมีการเลือกตั้งสมาชิกรัฐสภาทุก ๆ ๕ ปี แต่ฝ่ายค้าน (NMP) ดำรงตำแหน่งวาระละ ๒ ปีครึ่ง การเลือกตั้งในสิงคโปร์เป็นมาตรการบังคับ สำหรับทุกคนที่มีอายุมากกว่า ๒๑ ปีขึ้นไป ตุลาการสิงคโปร์ ประกอบด้วยศาลสูงสุดและศาลอุทธรณ์ รวมถึงศาลท้องถิ่นและศาลแขวง หัวหน้าผู้พิพากษา ผู้พิพากษาอาวุโส ๑๒ คน

จะได้รับการแต่งตั้งจากประธานาธิบดี และจากการแนะนำของรัฐบาล แม้ว่าสิงคโปร์จะมีพรรคการเมืองหลายพรรค แต่พรรคกิจประชาชน (PAP) จะได้ตั้งรัฐบาลเสมอ ได้ถูกกล่าวหาว่าป้องกันการเกิดฝ่ายค้านที่ปฏิบัติงานได้ การทำให้ฝ่ายค้านไม่มีความสำคัญนั้นได้บรรลุผล มาจากมาตรการที่รุนแรง เช่น แบ่งเขตเลือกตั้งอย่างไม่ยุติธรรม ฟ้องร้องคดีแพ่งว่าฝ่ายค้านหมิ่นประมาท หรือใช้การใส่ร้าย และพยายามสร้างความเสียหายใหญ่ ๆ ที่ทำให้ฝ่ายตรงข้ามล้มละลาย ผู้สังเกตการณ์ชาวตะวันตกมีความเห็นว่าระบบการเมืองสิงคโปร์นั้นค่อนไปทางอำนาจเผด็จการ แต่เป็นรัฐบาลที่มีประสิทธิภาพ ไม่ทุจริต มีความปลอดภัย และสร้างความก้าวหน้าให้ประชาชน บรรยากาศทางการเมืองได้รับการยอมรับจากหน่วยข่าวกรองเศรษฐศาสตร์ (The Economic Intelligence Unit) ว่าเป็นแบบลูกผสม คือ ผสมผสานระหว่างอำนาจเผด็จการกับประชาธิปไตย สิงคโปร์ใช้การปกครองโดยการควบคุมในหลายแง่มุมของชีวิตรวมถึงสื่อด้วย สิทธิบางอย่าง เช่น เสรีภาพในการชุมนุมและการปราศรัยยังค่อนข้างจำกัดสิงคโปร์ จัดอยู่ในอันดับที่ ๘๒ จากทั้งหมด ๑๖๗ ประเทศในดัชนีความเป็นประชาธิปไตย ค.ศ. ๒๐๐๘ ซึ่งจัดอันดับโดยนิตยสารข่าว The Economist ของลอนดอน และในค.ศ. ๒๐๐๙ องค์กรผู้สื่อข่าวไร้พรมแดน (Reporters without Borders) ได้จัดให้สิงคโปร์อยู่ในอันดับที่ ๑๓๓ จากทั้งหมด ๑๗๕ ประเทศ ในดัชนีด้านเสรีภาพของสื่อมวลชนทั่วโลกในด้านความสัมพันธ์กับต่างประเทศ สิงคโปร์เป็นประเทศกลุ่มที่ไม่ฝักใฝ่ฝ่ายใดอย่างเป็นทางการ สิงคโปร์เป็นสมาชิกองค์การสหประชาชาติ หรือ UN (United Nations) กลุ่มประเทศไม่ฝักใฝ่ฝ่ายใด หรือ NAM (Non - Aligned Movement) เป็นประเทศสมาชิกผู้ร่วมก่อตั้งอาเซียน และเข้าร่วมเป็นสมาชิกของเครือจักรภพอังกฤษ สิงคโปร์ดำรงตำแหน่งสมาชิกหมุนเวียนของคณะมนตรีความมั่นคงแห่งสหประชาชาติ (UN Security Council) ในช่วง ค.ศ. ๒๐๐๑ - ๒๐๐๒ และยังเข้าร่วมในภารกิจเป็นผู้สังเกตการณ์รักษาสันติภาพในคูเวต แองโกลา นามิเบีย กัมพูชา และติมอร์ตะวันออก ร่วมกับสหราชอาณาจักร ออสเตรเลีย นิวซีแลนด์ และมาเลเซีย ในฐานะส่วนหนึ่งของกลุ่มข้อตกลงการป้องกันประเทศร่วมกัน ๕ ชาติ หรือ FPDA (Five Power Defence Arrangements) ซึ่งแบ่งปันข้อมูลปรึกษาหารือ และช่วยเหลือกันในกรณีที่มีการรุกรานจากภายนอก

๒.๔.๑.๒ ระบบเศรษฐกิจ

สิงคโปร์เป็นประเทศสมาชิกอาเซียนที่มีเสรี รวมทั้งมีความก้าวหน้าและพัฒนามากที่สุดในกลุ่มอาเซียน สถาบันวิจัยฝ่ายอนุรักษ์นิยมของสหรัฐ (Heritage Foundation) ประเมินดัชนีชี้วัดเสรีภาพทางเศรษฐกิจ (Index of Economic Freedom) ใน ค.ศ. ๒๐๑๐ ของสิงคโปร์อยู่ที่ ๘๖.๒ ซึ่งนับว่ามีความเสรีเป็นอันดับที่ ๒ ของโลก สิงคโปร์ยังเป็นหนึ่งในประเทศเสือสี่ตัว (Four Tigers) ของเอเชียร่วมกับฮ่องกง ไต้หวัน และเกาหลีใต้ ซึ่งมีอัตราการเติบโตทางเศรษฐกิจที่โดดเด่น การเติบโตของเศรษฐกิจนี้เกิดขึ้นจากนโยบายของรัฐบาลที่สนับสนุนธุรกิจและการลงทุน และบทบาทหน้าที่ผ่านบริษัทที่ควบคุมโดยรัฐบาล ซึ่งเป็นกลไกในการเติบโตของเศรษฐกิจ นโยบายที่ได้รับการมุ่งเน้นจากรัฐบาลช่วยส่งเสริมการพัฒนาเศรษฐกิจ รวมถึงการกำจัดคอร์รัปชันในข้าราชการพลเรือน และธุรกิจสิงคโปร์ใช้ระบบความก้าวหน้าของงานโดยขึ้นอยู่กับความสามารถของบุคคลในการสรรหาบุคลากรและเรื่องค่าตอบแทน จัดตั้งสถาบันที่มีความมั่นคงและให้บริการประชาชนได้ดี และจัดเตรียมการศึกษาระดับโลก ฝึกทักษะความชำนาญร่วมกับการตั้งเป้าหมายของชาติและความต้องการของตลาด รายได้ของรัฐบาลคิดเป็นประมาณ ๖๐% ของผลิตภัณฑ์มวลรวมในประเทศ (GDP)

ซึ่งมาจากบริษัท ที่เชื่อมโยงกับรัฐบาลหรือ GLC (Government - Link Company) ซึ่งรัฐบาลเป็นหุ้นส่วน และคอยควบคุมอยู่ สิงคโปร์มีการสนับสนุนให้ประชาชนออมเงิน และกองทุนรวมเลี้ยงชีพหรือ CPF (Central Provident Fund) หรือก็คือแผนการออมเงินภาคบังคับ ซึ่งทำให้รัฐบาลมีทุนที่จำเป็นสำหรับการลงทุน สิงคโปร์มีกองทุนความมั่งคั่งแห่งชาติ ๒ ประเภท คือ องค์กรการลงทุนภาครัฐหรือ (Government Investment Corporation) และกองทุนเทมาเส็กโฮลดิงส์ ซึ่งดำเนินกิจการในเชิงพาณิชย์

การลงทุนจากต่างชาติมีบทบาทสำคัญต่อวิวัฒนาการเศรษฐกิจระดับต้นของสิงคโปร์ ซึ่งต้องอาศัยรัฐบาลที่มีเสถียรภาพและความร่วมมือ รวมถึงกำลังแรงงานที่มีทักษะ ซึ่งทั้งสองอย่างทำให้สิงคโปร์พร้อมรับบริษัทข้ามชาติ การสร้างแรงจูงใจ เช่น การเสนอวันหยุดภาษีเสรีให้แก่ นักลงทุนในการจัดตั้งอุตสาหกรรมการผลิตหรือการบริการในสิงคโปร์ มีองค์กรข้ามชาติจากสหรัฐอเมริกา ญี่ปุ่น และยุโรปกว่า ๗,๐๐๐ บริษัท นอกจากนั้นยังมีบริษัทจีน ๑,๕๐๐ บริษัท และบริษัทอินเดียในจำนวนพอ ๆ กับจีน รวมกันแล้วคิดเป็น ๒ ใน ๓ ของผลผลิตและการส่งออก มีการพัฒนาเขตนิคมอุตสาหกรรม เพื่อสิ่งปลูกสร้างที่จำเป็นสำหรับการอุตสาหกรรมขนาดใหญ่ ในระยะแรกสิงคโปร์ เน้นที่ผลผลิต เช่น ปิโตรเคมี อิเล็กทรอนิกส์ เครื่องจักรที่มีความแม่นยำ แต่ภายหลังมุ่งเน้นในการผลิตอุตสาหกรรมเทคโนโลยีชั้นสูง และอุตสาหกรรมการบริการ รวมถึงการเงินและการธนาคาร แบบอย่างการพัฒนาของสิงคโปร์มีพื้นฐานมาจากการประสบความสำเร็จในการสร้างพันธมิตรภาครัฐและเอกชน ซึ่งนโยบาย ระเบียบวาระ และการระดมทุน ทุกสิ่งได้มุ่งเน้นไปที่การพัฒนาเศรษฐกิจด้วยการบริหารจัดการที่มีประสิทธิภาพ ซื่อสัตย์ และให้การสนับสนุนนโยบายเหล่านี้ จึงส่งผลให้อัตราการเติบโตของเศรษฐกิจอยู่ที่ประมาณ ๘% ใน ค.ศ. ๑๙๖๐ - ๑๙๙๙ สิงคโปร์ฟื้นตัวได้ดีจากวิกฤติการณ์ทางการเงินของเอเชียใน ค.ศ. ๑๙๙๗ โดยใน ค.ศ. ๒๐๐๐ สิงคโปร์ก็กลับมาสู่เส้นทางเดิมอีกครั้ง กับอัตราการเติบโตของเศรษฐกิจถึง ๙% ต่อเนื่องจากภาวะเศรษฐกิจชะลอตัวทั่วโลกอัตราการเติบโตจึงเฉลี่ยอยู่ราว ๓% ใน ค.ศ. ๒๐๐๑ - ๒๐๐๓ และต่อมาในระหว่าง ค.ศ ๒๐๐๔ - ๒๐๐๗ อัตราการเติบโตก็ยังสูงถึง ๘% ทุกปีวิกฤติการณ์ทางการเงินโลกใน ค.ศ. ๒๐๐๘ - ๒๐๐๙ กระทบสิงคโปร์บ้าง แต่มีการพยากรณ์ว่าเศรษฐกิจจะฟื้นตัวใน ค.ศ. ๒๐๑๐ หรือนานกว่านี้ รัฐบาลได้เปิดเสรีบริการทางการเงิน การสื่อสาร โทรคมนาคม การผลิตกระแสไฟฟ้า และภาคการค้าปลีก เพื่อกระตุ้นเศรษฐกิจและการลงทุนใน ค.ศ. ๒๐๐๙ สิงคโปร์ใช้งบประมาณ ๒ หมื่นล้านในแผนกระตุ้นเศรษฐกิจของรัฐบาล

สิงคโปร์มีการสื่อสารโทรคมนาคมและเครือข่ายอินเทอร์เน็ตดีเยี่ยม รวมทั้งสายการบินและสนามบินที่ดีที่สุด ระบบขนส่งสาธารณะและระบบการศึกษาที่มีประสิทธิภาพ สภาพแวดล้อมเมืองสีเขียวที่มีความปลอดภัยและสะอาด รวมถึงการมีศักยภาพในการลงทุนชั้นยอด

๒.๔.๑.๓ ระบบกฎหมาย

ระบบกฎหมายของสิงคโปร์มีพื้นฐานมาจากกฎหมายจารีตประเพณีของอังกฤษ ซึ่งใช้ตั้งแต่เป็นอาณานิคม แม้ว่าสถาบันกฎหมายสุดท้ายที่เชื่อมโยงกับอังกฤษได้ถูกตัดออกใน ค.ศ. ๑๙๙๔ หรือเมื่อศาลอุทธรณ์ของสิงคโปร์ มาแทนที่สภาองคมนตรีอังกฤษ (English Privy Council) ในฐานะศาลอุทธรณ์ของประเทศก็ตาม แต่กฎหมายอังกฤษยังคงมีอำนาจอยู่ในนาม เช่นเดียวกันกับพัฒนาการในประเทศอื่น ๆ ที่ใช้กฎหมายจารีตประเพณี สิงคโปร์ก็มีแนวโน้มในการรวมหัวข้อที่สำคัญในกฎหมายรัฐบัญญัติระบบพิจารณาคดีโดยคณะลูกขุนได้ถูกยกเลิกใน ค.ศ. ๑๙๖๙ สิงคโปร์ใช้ระบบศาล ๓ ชั้น โดยมีศาลระดับล่างจำนวนหนึ่ง ศาลสูง และศาลอุทธรณ์ ศาลอุทธรณ์เป็นศาลสูงสุด

ในสิงคโปร์ ศาลอุทธรณ์และศาลสูงถือว่าเป็นศาลระดับสูงสุด ซึ่งตุลาการ ประกอบด้วย หัวหน้าผู้พิพากษาและผู้พิพากษาศาลอุทธรณ์ ผู้พิพากษาศาลสูง และคณะกรรมการพิจารณาคดี ศาลสูงมีหัวหน้าผู้พิพากษาเป็นประธานและมีผู้พิพากษาอุทธรณ์ ผู้พิพากษาทั้งหมดได้รับการแต่งตั้งจากรัฐบาล ศาลแขวงรับพิจารณาคดีสูงสุด ๖๐,๐๐๐ ดอลลาร์สหรัฐฯ และศาลเขตรับพิจารณาคดีสูงสุด ๒๕๐,๐๐๐ ดอลลาร์สหรัฐฯ

สิงคโปร์ประสบความสำเร็จในการสะสางคดีสะสม ๕ ปีที่คั่งค้างอยู่ด้วยการปฏิรูประบบศาลอย่างครอบคลุมใน ค.ศ. ๑๙๙๐ ปัจจุบันนี้การพิจารณาคดีแพ่งส่วนใหญ่ใช้เวลาประมาณ ๗ - ๘ เดือนนับตั้งแต่เริ่มต้นฟ้องร้อง และถึงแม้ว่าจะมีการยื่นอุทธรณ์ โดยปกติแล้วคดีจะจบภายในเวลา ๑ ปี คดีต่าง ๆ ได้รับการพิจารณาเร็วและไม่เกิดความล่าช้าไม่ว่าด้วยเหตุผลใด สิงคโปร์มีสิทธิทางกฎหมายบางประการสำหรับการปกป้องนักลงทุนที่แข็งแกร่งที่สุดในโลก โดยสิงคโปร์จัดอยู่ในอันดับที่ ๒ รองจากนิวซีแลนด์ในด้านการปกป้องนักลงทุนสิงคโปร์มีการบังคับใช้ทางสัญญาที่รวดเร็วที่สุดในโลก คือ ๑๕๐ วัน ค่าใช้จ่ายในการฟ้องร้องหรือการเรียกร้องทางสัญญาคิดเป็น ๒๕% กระบวนการของบริษัทในการเลิกกิจการ ล้มละลาย และการแสดงความจำนงของทนายหรือเจ้าหน้าที่นิติกรจะพิจารณาโดยศาลสูง ไม่นานมานี้สิงคโปร์ได้มีการจัดตั้ง ศาลแพ่งและการพาณิชย์เพื่อพิจารณาคดีเกี่ยวกับธุรกิจโดยเฉพาะ การระงับข้อพิพาทแบบทางเลือก หรือ ADR (Alternative Dispute Resolution) เป็นวิธีการที่นำมาใช้กับหลาย ๆ คดีโดยเฉพาะคดีการพาณิชย์ระหว่างประเทศ สิงคโปร์บังคับใช้กฎหมายคุ้มครองทรัพย์สินทางปัญญาอย่างเคร่งครัด เช่นเดียวกับกฎหมายสากลมีการจัดตั้งแผนกใหม่ในกรมตำรวจเพื่อคอยสอดส่อง การดำเนินคดีของผู้กระทำความผิด

สิงคโปร์จัดอยู่ในอันดับที่ ๑ ของโลกในการจัดอันดับความยากง่ายในการดำเนินธุรกิจ จากรายงาน การดำเนินธุรกิจ ค.ศ. ๒๐๑๐ โดยธนาคารโลก เสรีภาพโดยรวมในการดำเนินธุรกิจได้รับความคุ้มครองอย่างดี ภายใต้สภาพแวดล้อมโดยการกำกับดูแลของสิงคโปร์ การเริ่มต้นธุรกิจใช้เวลาเพียง ๓ วัน เทียบกับระยะเวลาโดยเฉลี่ยทั่วโลก คือ ๓๕ วัน การขอใบอนุญาตทางธุรกิจในสิงคโปร์ใช้เวลาน้อยกว่าระยะเวลาโดยเฉลี่ยของโลกมาก (๑๘ ขั้นตอนใน ๒๑๘ วัน) การล้มละลายก็สามารถทำได้อย่างเปิดเผย สิงคโปร์อยู่ในอันดับที่ ๔ ของโลกในการจัดอันดับความยากง่ายของการเริ่มต้นธุรกิจ สิงคโปร์มีการปฏิรูปเพื่อการเริ่มต้นธุรกิจใน ค.ศ. ๒๐๐๙ การขอใบอนุญาตการก่อสร้าง และการลงทะเบียนทรัพย์สินนั้นง่ายขึ้น รวมทั้งปรับปรุงกระบวนการเริ่มต้นธุรกิจโดยใช้ระบบออนไลน์ โดยเฉลี่ยแล้วการเริ่มต้นธุรกิจใช้เวลาเพียง ๓ วัน สิงคโปร์จัดอยู่ในอันดับ ๒ ของโลก ในเรื่องความยากง่ายในการขอใบอนุญาตการก่อสร้างใน ค.ศ. ๒๐๐๙ สิงคโปร์ได้นำการอนุมัติการก่อสร้างตามระดับความเสี่ยงมาใช้ และในการจัดอันดับความยากง่ายในการจ้างงาน สิงคโปร์อยู่ในอันดับที่ ๓ รองจากออสเตรเลียและสหรัฐอเมริกา สิงคโปร์อยู่ในอันดับที่ ๙ ของโลกในด้านความยากง่ายในการขอสินเชื่อ ซึ่งสหรัฐอเมริกาอยู่ในอันดับที่ ๑๐ อีกทั้งสิงคโปร์ยังเป็นหนึ่งในประเทศที่ส่งออกได้ง่ายที่สุดของโลก โดยการขนส่งต่อหนึ่งตู้คอนเทนเนอร์มีราคาถูกมาก

๒.๔.๒ ด้านอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

การกระทำผิดกฎหมายคอมพิวเตอร์และความปลอดภัยทางอินเทอร์เน็ต
(บทที่ ๕๐A)

(การตรากฎหมายดั้งเดิม:พระราชบัญญัติที่ ๑๙ ปี ๑๙๙๓)
ฉบับปรับปรุงปี ๒๐๐๗ (วันที่ ๓๑ กรกฎาคม ๒๕๕๐)

พระราชบัญญัติเพื่อให้มีการจัดหาวัสดุคอมพิวเตอร์เพื่อป้องกันการเข้าถึงหรือดัดแปลงที่ไม่ได้รับอนุญาต รับรองความปลอดภัยทางไซเบอร์และสำหรับเรื่องที่เกี่ยวข้อง

ส่วนที่ ๑
บทนำ
ชื่อย่อ

มาตรา ๑ พระราชบัญญัตินี้อาจอ้างถึงเป็นความผิดคอมพิวเตอร์และการรักษาความปลอดภัยทางการตีความ

มาตรา ๒

(๑) ในพระราชบัญญัตินี้เว้นแต่บริบทจะกำหนดเป็นอย่างอื่น -

"คอมพิวเตอร์" หมายถึง อุปกรณ์อิเล็กทรอนิกส์, แม่เหล็ก, ออปติคอล, ไฟฟ้า, หรืออื่น ๆ หรือ ฟังก์ชันลอจิคัลเลขคณิตหรือหน่วยเก็บข้อมูล และรวมถึงเครื่องมืออำนวยความสะดวกในการจัดเก็บข้อมูลหรือเครื่องมือสื่อสารที่เกี่ยวข้องโดยตรงหรือทำงานร่วมกับอุปกรณ์หรือกลุ่มของอุปกรณ์ที่เชื่อมต่อหรือเกี่ยวข้องดังกล่าว แต่ไม่รวมถึงกลุ่มอุปกรณ์ที่เชื่อมต่อ หรือเกี่ยวข้อง

(a) เครื่องพิมพ์ดีดหรือเครื่องพิมพ์ดีดอัตโนมัติ

(b) เครื่องคิดเลขพกพาแบบพกพา

(c) อุปกรณ์ที่คล้ายกันซึ่งไม่สามารถตั้งโปรแกรมได้หรือไม่มีอุปกรณ์เก็บข้อมูล หรือ

(d) อุปกรณ์อื่นเช่นรัฐมนตรีอาจประกาศกำหนดในราชกิจจานุเบกษา

"คอมพิวเตอร์เอาต์พุต" หรือเขียนพิมพ์ภาพแทนความจริง - "เอาต์พุต"

“กราฟิก” หมายถึง คำสั่งหรือการแสดง (ไม่ว่าจะในรูปแบบเขียน, พิมพ์, รูปภาพ, กราฟิก หรือในรูปแบบอื่น ๆ) ที่อ้างว่าเป็นปากคำหรือการนำเสนอความจริง

(a) ผลิตโดยคอมพิวเตอร์; หรือ

(b) แปลอย่างถูกต้องจากรายงานหรือการนำเสนอซึ่งผลิตภัณฑ์ใน;

"บริการคอมพิวเตอร์" รวมถึง เวลาของคอมพิวเตอร์, การประมวลผลข้อมูลและการจัดเก็บหรือการดึงข้อมูลผลิต;

"ความเสียหาย” หมายถึง ยกเว้นเพื่อจุดประสงค์ของมาตรา 13 การทำให้เสียใด ๆ กับคอมพิวเตอร์หรือความสมบูรณ์ของข้อมูลโปรแกรมหรือระบบหรือข้อมูลหรือ -

(a) ทำให้เกิดการสูญเสียรวมอย่างน้อย $๑๐,๐๐๐ ในมูลค่าหรือจำนวนเงินอื่น ๆ ตามที่รัฐมนตรีอาจประกาศโดยในราชกิจจานุเบกษากำหนดยกเว้นว่าการสูญเสียใด ๆ ที่เกิดขึ้นหรือเกิดขึ้นมากกว่าหนึ่งปีหลังจากวันที่ความผิดในคำถามจะไม่นำมาพิจารณา;

(b) ดัดแปลงหรือทำให้เสีย หรืออาจปรับเปลี่ยนหรือลดทอนหรือวินิจฉัย รักษาหรือดูแลคนหนึ่งคนหรือมากกว่านั้น

(c) สาเหตุหรือคุกคามมีการบาดเจ็บทางร่างกายหรือเกิดการเสียชีวิตกับบุคคลใด ๆ หรือ

(d) คุกคามสุขภาพของประชาชนหรือความปลอดภัยของประชาชน

"ข้อมูล" หมายถึง การนำเสนอข้อมูลหรือแนวคิดที่จัดทำในรูปแบบที่เหมาะสมสำหรับใช้ในคอมพิวเตอร์

"แม่เหล็กไฟฟ้าหรืออุปกรณ์อื่น ๆ" หมายถึง อุปกรณ์หรือเครื่องมือใด ๆ ที่ใช้หรือมีความสามารถในการใช้ เพื่อขัดขวางการทำงานของคอมพิวเตอร์ กำลังเตรียมหรือ

"ฟังก์ชัน" รวมถึง ตรรกะการควบคุมการคำนวณการลบการจัดเก็บและการดึงและการสื่อสารโทรคมนาคมไปยังจากหรือภายในคอมพิวเตอร์

“สกัดกั้น" ที่เกี่ยวข้องกับการทำงานของคอมพิวเตอร์รวมถึงการฟังหรือการทำงานของคอมพิวเตอร์หรือการรับสารความหมายหรือเจตนาของมัน

“โปรแกรมที่เมื่อใช้งานในคอมพิวเตอร์เครื่องคอมพิวเตอร์จะทำหน้าที่บันทึกโปรแกรมคอมพิวเตอร์" หมายถึงข้อมูลที่แสดงคำสั่งหรือข้อความหรือ

(๒) เพื่อความมุ่งประสงค์ของพระราชบัญญัตินี้บุคคลจะได้รับสิทธิ์ในการเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์หากโดยการทำให้คอมพิวเตอร์ทำหน้าที่ใด ๆ ก็ตาม

(a) แก้ไขหรือลบโปรแกรมหรือข้อมูล

(b) คัดลอกตำแหน่งอื่นในสื่อบันทึกที่จัดเก็บ หรือย้ายไปยังสื่อบันทึกข้อมูลอื่นนอกเหนือจากที่จัดเก็บหรือ

(c) ใช้งาน หรือ

(d) ที่จะเอาต์พุตจากคอมพิวเตอร์ที่มีการจัดขึ้น (ไม่ว่าจะมีมันแสดงหรือในลักษณะอื่นใด) และการอ้างอิงถึงการเข้าถึงโปรแกรมหรือข้อมูล (และการเข้าถึง) จะต้องอ่านตาม

(๓) เพื่อจุดประสงค์ของส่วนย่อย (๒) (c) ฟังก์ชันจะทำให้คอมพิวเตอร์ทำงานโดยมีเจตนาที่จะรักษาความปลอดภัยให้บุคคลดังกล่าวใช้โปรแกรม -

(a) ทำให้โปรแกรมถูกดำเนินการ หรือ

(b) เป็นฟังก์ชันของโปรแกรม

(๔) เพื่อจุดประสงค์ของส่วนย่อย (๒) (d) รูปแบบที่ข้อมูลโปรแกรมใด ๆ ถูกส่งออก (และโดยเฉพาะอย่างยิ่งว่ามันหมายถึง รูปแบบที่ในกรณีของโปรแกรมมันมีความสามารถในการเป็นดำเนินการหรือในกรณีของข้อมูลความสามารถในการประมวลผลโดยคอมพิวเตอร์) นั้นไม่มีสาระสำคัญ

(๕) เพื่อวัตถุประสงค์ของพระราชบัญญัตินี้การเข้าถึงใด ๆ โดยบุคคลใด ๆ ไปยังโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ไม่ได้รับอนุญาตหรือทำโดยไม่มีอำนาจถ้า

(a) เขาไม่มีสิทธิ์ควบคุมการเข้าถึงโปรแกรมหรือข้อมูลที่เป็นปัญหา และ (b) เขาไม่ได้รับความยินยอมจากเขาในการเข้าถึงโปรแกรมหรือข้อมูลจากบุคคลที่มีสิทธิ์

(๖) การอ้างอิงในพระราชบัญญัตินี้ไปยังโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ รวมถึงการอ้างอิงถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในสื่อบันทึกข้อมูลแบบถอดได้ใด ๆ ซึ่งเป็นเวลาที่อยู่ในคอมพิวเตอร์ และคอมพิวเตอร์จะถือว่าเป็นโปรแกรมหรือข้อมูลที่เก็บไว้ในสื่อดังกล่าว

(๗) เพื่อความมุ่งประสงค์ของพระราชบัญญัตินี้การแก้ไขเนื้อหาของคอมพิวเตอร์ใด ๆ จะเกิดขึ้นหากโดยการทำงานของฟังก์ชันใด ๆ ของคอมพิวเตอร์ที่เกี่ยวข้องหรือคอมพิวเตอร์อื่น ๆ

(a) โปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์ที่เกี่ยวข้องนั้นมีการเปลี่ยนแปลงหรือลบ

(b) โปรแกรมหรือข้อมูลใด ๆ จะถูกเพิ่มเข้าไปในเนื้อหาของมัน หรือ

(c) การกระทำใด ๆ ที่เกิดขึ้นซึ่งทำให้การทำงานปกติของคอมพิวเตอร์ใด ๆ เสียหายและการกระทำใด ๆ ที่ก่อให้เกิดการแก้ไขดังกล่าวจะถือเป็นการทำให้เกิดขึ้น

(๘) การดัดแปลงใด ๆ ที่อ้างถึงในส่วนย่อย (๗) ไม่ได้รับอนุญาตหาก -

(a) บุคคลที่มีการกระทำทำให้ไม่มีสิทธิ์ในการตัดสินใจว่าควรทำการแก้ไขหรือไม่ และ

(b) เขาไม่ได้รับความยินยอมให้แก้ไขจากบุคคลใด ๆ ที่มีสิทธิเช่นนั้น

(๙) การอ้างอิงในพระราชบัญญัตินี้ไปยังโปรแกรมรวมถึงการอ้างอิงถึงส่วนหนึ่งของโปรแกรม

ส่วนที่ ๒
ภาคความผิด
การเข้าถึงเนื้อหาคอมพิวเตอร์โดยไม่ได้รับอนุญาต

มาตรา ๓

(๑) ภายใต้หัวข้อย่อย (๒) บุคคลใด ๆ เจตนาที่ทำเพื่อให้คอมพิวเตอร์ทำหน้าที่ใด ๆ เพื่อวัตถุประสงค์ในการเข้าถึงการรักษาความปลอดภัยการโดยไม่มีอำนาจในโปรแกรมหรือข้อมูลใด ๆ ที่ถืออยู่ในคอมพิวเตอร์เครื่องใดก็ตามจะต้องมีความผิด ความเชื่อมั่นต่อการถูกปรับไม่เกิน ๕,๐๐๐ ดอลลาร์ หรือการจำคุกไม่เกิน ๒ ปี หรือทั้งจำทั้งปรับ และในกรณีที่มีครั้งที่สองหรือครั้งต่อไปหรือปรับไม่เกิน ๑๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๓ ปี หรือทั้งจำทั้งปรับ

(๒) หากความเสียหายใด ๆ เกิดขึ้นเนื่องจากความผิดตามมาตรานี้บุคคลที่ถูกตัดสินว่ามีความผิดต้องระวางโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๗ ปี หรือทั้งจำทั้งปรับ

(๓) เพื่อจุดประสงค์ของส่วนนี้มันเป็นสาระสำคัญที่การกระทำที่เป็นปัญหาไม่ได้กำกับที่ –

(a) โปรแกรมหรือข้อมูลใด ๆ

(b) ข้อมูลโปรแกรมทุกชนิด หรือ

(c) โปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ได้

เข้าถึงด้วยความตั้งใจที่จะกระทำหรืออำนวยความสะดวกในการกระทำความผิด

มาตรา ๔

(๑) บุคคลใด ๆ ที่ทำให้คอมพิวเตอร์ทำหน้าที่ใด ๆ เพื่อวัตถุประสงค์ในการเข้าถึงรักษาความปลอดภัยโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์เครื่องใด ๆ โดยมีเจตนาที่จะกระทำความผิด ซึ่งส่วนนี้มีผลใช้บังคับความผิดเกี่ยวกับทรัพย์สินการฉ้อโกงความไม่ซื่อสัตย์

(๒) มาตรานี้จะนำไปใช้หรือที่ก่อให้เกิดอันตรายต่อร่างกายและมีโทษต่อความเชื่อมั่นที่มีโทษจำคุกไม่น้อยกว่า ๒ ปี

(๓) บุคคลใดที่กระทำความผิดตามมาตรานี้ต้องระวางโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๑๐ ปีหรือทั้งจำทั้งปรับ

(๔) เพื่อจุดประสงค์ของส่วนนี้ ไม่สำคัญว่า -

(a) ไม่ว่าการเข้าถึงที่อ้างถึงในส่วนย่อย (๑) จะได้รับอนุญาตหรือไม่ได้รับอนุญาต;

(b) ความผิดที่ส่วนนี้มีผลในเวลาเดียวกันเมื่อการเข้าถึงนั้นปลอดภัยหรือในเวลาอื่น ๆ

การดัดแปลงวัสดุคอมพิวเตอร์โดยไม่ได้รับการอนุญาต

มาตรา ๕

(๑) ภายใต้หัวข้อย่อย (๒) บุคคลใด ๆ ที่กระทำการใด ๆ ที่เขารู้ว่าจะทำให้เกิดการดัดแปลงเนื้อหาของคอมพิวเตอร์ใด ๆ โดยไม่ได้รับอนุญาตจะต้องมีความผิดและจะต้องระวางโทษปรับไม่เกิน ๑๐,๐๐๐ ดอลลาร์ หรือการจำคุกไม่เกิน ๓ ปี หรือทั้งจำทั้งปรับ และในกรณีที่ครั้งที่สองหรือตัดสินว่ามีความผิดภายหลัง ครั้งต่อมามีโทษปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๕ ปี หรือทั้งจำทั้งปรับ

(๒) หากความเสียหายใด ๆ เกิดขึ้นเนื่องจากความผิดตามมาตรานี้บุคคลที่ถูกตัดสินว่ามีความผิดต้องระวางโทษ ปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๗ ปี หรือทั้งจำทั้งปรับ

(๓) สำหรับส่วนของวัตถุประสงค์มีความสำคัญอย่างยิ่งที่การกระทำที่เป็นปัญหาไม่ได้มุ่งไปที่

(a) โปรแกรมหรือข้อมูลเฉพาะใด ๆ

(b) โปรแกรมหรือข้อมูลประเภทใด ๆ หรือ

(c) โปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เฉพาะเครื่องใด ๆ

(๔) จุดประสงค์ของส่วนนี้ไม่ว่าจะเป็นการดัดแปลงหรือตั้งใจ ที่จะเป็นแบบถาวรหรือชั่วคราว

การใช้หรือการสกัดกั้นบริการคอมพิวเตอร์โดยไม่ได้รับอนุญาต

มาตรา ๖

(๑) ภายใต้หัวข้อย่อย (๒) บุคคลใด ๆ ที่รู้ดีว่า -

(a) การเข้าถึงการรักษาความปลอดภัยโดยไม่มีอำนาจซึ่งคอมพิวเตอร์เครื่องใด ๆ เพื่อวัตถุประสงค์ในการได้มาโดยตรงหรือโดยอ้อม

(b) โดยสาเหตุใด ๆ ทั้งทางตรงหรือทางอ้อม การสกัดกั้นโดยไม่มีสิทธิ์อำนาจโดยตรง หรือการทำงานของคอมพิวเตอร์โดยอุปกรณ์อื่น หรือวิธีการของแม่เหล็กไฟฟ้า หรือ

(c) การใช้หรือสาเหตุที่จะนำไปใช้โดยตรงเพื่อความมุ่งประสงค์ในการกระทำความผิดจะต้องมีความผิด และจะต้องรับผิดในความผิดที่ต้องโทษไม่ว่าทางตรงหรือทางอ้อม คอมพิวเตอร์หรืออุปกรณ์อื่นใดเป็นความผิดตามวรรค (a) หรือ (b) เกิน $ ๑๐,๐๐๐ หรือถูกจำคุกเป็นระยะเวลาไม่เกิน ๓ ปี หรือทั้งจำทั้งปรับ และในกรณีครั้งที่สอง หรือตัดสินว่ามีความผิดภายหลังต้องปรับ ๒๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๕ ปี หรือทั้งจำทั้งปรับ

(๒) หากความเสียหายใด ๆ เกิดขึ้นเนื่องจากความผิดตามมาตรานี้บุคคลที่ถูกตัดสินว่ามีความผิดต้องระวางโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๗ ปี หรือทั้งจำทั้งปรับ

(๓) เพื่อวัตถุประสงค์แห่งมาตรานี้ เป็นสิ่งสำคัญที่การเข้าถึงที่ไม่ได้รับอนุญาตหรือการสกัดกั้นไม่ได้กำกับที่เฉพาะ

(a) โปรแกรมหรือข้อมูลเฉพาะใด ๆ

(b) โปรแกรมหรือข้อมูลประเภทใด ๆ หรือ

(c) โปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เฉพาะเครื่องใดก็ได้

การขัดขวางการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต

มาตรา ๗

(๑) บุคคลใด ๆ ที่มีเจตนาหรือไม่มีข้อแก้ตัวตามกฎหมาย

(a) รบกวนหรือขัดขวางหรือขัดขวางการใช้คอมพิวเตอร์อย่างถูกกฎหมาย หรือ

(b) ขัดขวางหรือป้องกันการเข้าถึงหรือลดทอนประโยชน์หรือประสิทธิผลของโปรแกรม หรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์จะต้องมีความผิดและต้องระวางโทษปรับไม่เกิน ๑๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๓ ปี หรือทั้งจำทั้งปรับ และในกรณีที่มีครั้งที่สองหรือมีความเชื่อมั่นภายหลังจะต้องเสียค่าปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๕ ปีหรือทั้งจำทั้งปรับ

(๒) หากส่วนความเสียหายใด ๆ บุคคลที่ถูกตัดสินว่ามีความผิดต้องระวางโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๗ ปี หรือทั้งจำทั้งปรับ

การเปิดเผยรหัสการเข้าถึงโดยไม่ได้รับอนุญาต

มาตรา ๘

(๑) บุคคลใด ๆ ที่เจตนาเปิดเผยรหัสผ่านรหัสการเข้าถึงหรือใช้วิธีการอื่นใดในการเข้าถึงโดยไม่มีอำนาจซึ่งโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ตามจะต้องมีความผิดถ้าเขาทำเช่นนั้น

(a) เพื่อผลประโยชน์โดยมิชอบใด ๆ

(b) เพื่อจุดประสงค์ที่ผิดกฎหมาย หรือ

(c) รู้ว่ามันมีแนวโน้มที่จะสูญเสียผิดพลาดให้กับบุคคลใด ๆ

(๒) บุคคลใดที่มีความผิดตามหมวด (๑) จะต้องรับผิดในความผิดที่ปรับไม่เกิน ๑๐,๐๐๐ ดอลลาร์ หรือจำคุกในระยะที่ไม่เกินกว่า ๓ ปี หรือทั้งจำทั้งปรับ และในกรณีที่มีครั้งที่สองหรือมีการตัดสินความผิดภายหลังจากนั้น ครั้งต่อไปจะถูกปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๕ ปี หรือ ทั้งจำทั้งปรับ

มาตรา ๙

(๑) ในกรณีที่ได้รับการเข้าถึงคอมพิวเตอร์ที่ได้รับความคุ้มครองในระหว่างการกระทำความผิดตามมาตรา ๓, ๕, ๖ หรือ ๗ ผู้ถูกตัดสินว่ากระทำความผิดดังกล่าวจะต้องได้รับโทษตามที่กำหนดไว้ในส่วนนั้น ต้องระวางโทษปรับไม่เกิน $๑๐๐,๐๐๐ หรือจำคุกไม่เกิน ๒๐ ปี หรือทั้งจำทั้งปรับ

(๒) เพื่อจุดประสงค์ของส่วนย่อย (๑) คอมพิวเตอร์จะได้รับการปฏิบัติในฐานะ "คอมพิวเตอร์ที่ได้รับการป้องกัน" หากผู้ที่กระทำความผิดรู้หรือสมควรทราบว่ามีการใช้คอมพิวเตอร์

หรือโปรแกรมหรือข้อมูลโดยตรงในการเชื่อมต่อด้วยหรือจำเป็นสำหรับ – การลงโทษขั้นสูงสำหรับความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ที่ได้รับการป้องกัน

(a) ความปลอดภัย, รั้วและความสัมพันธ์ระหว่างประเทศของสิงคโปร์;

(b) การมีอยู่หรือเอกลักษณ์ของแหล่งข้อมูลลับที่เกี่ยวข้องกับการบังคับใช้กฎหมายอาญา

(c) การให้บริการที่เกี่ยวข้องโดยตรงกับโครงสร้างพื้นฐานด้านการสื่อสาร การธนาคารและบริการทางการเงินสาธารณูปโภคการขนส่งสาธารณะหรือโครงสร้างพื้นฐานกุญแจสาธารณะ หรือ

(d) การป้องกันความปลอดภัยสาธารณะรวมถึงระบบที่เกี่ยวข้องกับบริการฉุกเฉินที่จำเป็น เช่น ตำรวจ การป้องกันพลเรือน และการบริการทางการแพทย์

(๓) เพื่อความมุ่งประสงค์ของการดำเนินคดีตามมาตรานี้จะถูกสันนิษฐานไว้ก่อนจนกว่าจะมีการพิสูจน์ว่าผู้ถูกกล่าวหามีความรู้ที่จำเป็นซึ่งอ้างถึงในส่วนย่อย (๒) หากมีในส่วนที่เกี่ยวกับคอมพิวเตอร์โปรแกรม หรือข้อมูลคำเตือนทางอิเล็กทรอนิกส์ หรืออื่น ๆ ที่แสดงแก่ผู้ถูกกล่าวหาระบุว่าการเข้าถึงคอมพิวเตอร์ โปรแกรม หรือข้อมูล โดยไม่ได้รับอนุญาตจะได้รับโทษเพิ่มภายใต้หัวข้อนี้

การช่วยเหลือและพยายาม ถือลงโทษเป็นความผิด

มาตรา ๑๐

(๑) บุคคลใด ๆ ที่สนับสนุนหรือเป็นตัวการหรือเป็นผู้ที่พยายามกระทำ หรือกระทำการใด ๆ ที่เตรียมการ หรือเพื่อดำเนินการต่อการกระทำความผิดใด ๆ ตามพระราชบัญญัตินี้จะมีความผิดในความผิดนั้น และจะต้องรับผิดชอบต่อการลงโทษที่กำหนดไว้เป็นความผิด

(๒) สำหรับความผิดที่ภายใต้หัวข้อนี้สถานที่ที่การกระทำเกิดขึ้นนั้นไม่ใช่สาระสำคัญ

ส่วนที่ ๓
เบ็ดเตล็ดและทั่วไป
การกระทำความผิดตามพระราชบัญญัตินี้

มาตรา ๑๑

(๑) ภายใต้หมวด (๒) บทบัญญัติของพระราชบัญญัตินี้จะมีผลบังคับใช้ในส่วนที่เกี่ยวกับบุคคลใด ๆ ไม่ว่าจะเป็นสัญชาติหรือเป็นพลเมืองนอกหรือภายในสิงคโปร์

(๒) ในกรณีที่มีการกระทำความผิดตามพระราชบัญญัตินี้โดยบุคคลใดก็ตามในสถานที่ใดนอกสาธารณรัฐสิงคโปร์บุคคลนั้นอาจได้รับการจัดการเช่นเดียวกับว่ามีการกระทำความผิดที่เกิดขึ้นภายในสิงคโปร์

(๓) เพื่อความมุ่งประสงค์ของมาตรานี้พระราชบัญญัตินี้จะใช้บังคับหากมีการฝ่าฝืนกฎหมายดังกล่าว

(a) ผู้ต้องหาในเวลาสำคัญอยู่ที่สิงคโปร์; หรือ

(b) คอมพิวเตอร์ โปรแกรม หรือข้อมูล อยู่ในสิงคโปร์ตามเวลาสำคัญ

เขตอำนาจศาล

มาตรา ๑๒

ศาลแขวงหรือผู้พิพากษาศาลมีอำนาจตัดสินความผิดทั้งหมดตามพระราชบัญญัตินี้ และแม้จะมีสิ่งใดที่ขัดกับประมวลกฎหมายวิธีพิจารณาความอาญา (Cap. ๖๘) ก็จะมีอำนาจกำหนดบทลงโทษหรือการลงโทษเต็มรูปแบบตามความผิดตามพระราชบัญญัตินี้

องค์ประกอบของความผิด

มาตรา ๑๒ A

(๑) ผู้บัญชาการตำรวจหรือบุคคลที่ได้รับอนุญาต อาจใช้ดุลพินิจประกอบตรวจสอบการกระทำความผิดตามพระราชบัญญัตินี้ซึ่งกำหนดให้เป็นความผิดอันยอมความได้ โดยการรวบรวมจากบุคคลต้องสงสัยว่ามีความผิดรวมไม่เกิน ๓,๐๐๐ ดอลลาร์

(๒) รัฐมนตรีอาจกำหนดระเบียบความผิดซึ่งอาจทบต้น

คำสั่งให้จ่ายเงินชดเชย

มาตรา ๑๓

(๑) ก่อนที่บุคคลซึ่งถูกพิพากษาว่ามีความผิดตามพระราชบัญญัตินี้ศาลอาจมีคำสั่งให้เขาชำระเงินจำนวนรวมที่ศาลจะกำหนดโดยวิธีชดเชยแก่บุคคลใด ๆ สำหรับความเสียหายใด ๆ ที่เกิดขึ้นกับคอมพิวเตอร์โปรแกรมหรือข้อมูลของเขา โดยความผิดที่ประโยคถูกส่งผ่าน

(๒) การเรียกร้องใด ๆ โดยบุคคลสำหรับความเสียหายที่ยั่งยืนด้วยเหตุผลของความผิดจะถือว่ามีความพึงพอใจในขอบเขตของจำนวนเงินใด ๆ ที่ได้รับการจ่ายให้เขาภายใต้คำสั่งของการชดเชย แต่คำสั่งจะไม่กระทบกระเทือนสิทธิ การรักษาทางแพ่งสำหรับการกู้คืนความเสียหายที่เกินจำนวนเงินค่าชดเชยที่จ่ายตามคำสั่ง

(๓) คำสั่งของค่าตอบแทนตามมาตรานี้จะได้รับการชำระคืนในฐานะหนี้พลเรือน

การออมเพื่อการสืบสวนโดยตำรวจและเจ้าหน้าที่บังคับใช้กฎหมาย

มาตรา ๑๔

ไม่มีสิ่งใดในพระราชบัญญัตินี้ที่ห้ามมิให้เจ้าหน้าที่ตำรวจผู้มีอำนาจตามความหมายของมาตรา ๓๙ แห่งประมวลกฎหมายวิธีพิจารณาความอาญาปี ๒๐๑๐ หรือเจ้าหน้าที่บังคับใช้กฎหมายที่ได้รับมอบอำนาจจากการสอบสวนตามกฎหมายภายใต้กฎหมายใด ๆ

อำนาจของเจ้าหน้าที่ตำรวจในการเข้าถึงคอมพิวเตอร์และข้อมูล

มาตรา ๑๕ [ถูกยกเลิกโดย พระราชบัญญัติ ๔๒ ปี ๒๐๐๕]

มาตรการและข้อกำหนดด้านความปลอดภัยของไซเบอร์

มาตรา ๑๕ A

(๑) ในกรณีที่รัฐมนตรีพึงพอใจว่ามีความจำเป็นเพื่อวัตถุประสงค์ในการป้องกันตรวจจับหรือตอบโต้การคุกคามต่อความมั่นคงของประเทศการบริการที่จำเป็น หรือการป้องกันสาธารณรัฐสิงคโปร์หรือความสัมพันธ์ระหว่างประเทศของสิงคโปร์รัฐมนตรีอาจรับรองโดยใบรับรองตามมอบอำนาจหรือ

ส่งต่อบุคคลหรือองค์กรใด ๆ ที่ระบุในใบรับรอง (อ้างถึงในส่วนนี้เป็นบุคคลที่ระบุ) เพื่อใช้มาตรการดังกล่าวหรือปฏิบัติตามข้อกำหนดดังกล่าวตามที่จำเป็นเพื่อป้องกันตรวจจับหรือตอบโต้การคุกคามคอมพิวเตอร์หรือคอมพิวเตอร์บริการ หรือคอมพิวเตอร์หรือบริการคอมพิวเตอร์ใด ๆ

(๒) มาตรการและข้อกำหนดที่อ้างถึงในส่วนย่อย (๑) อาจรวมถึง แต่ไม่จำกัดเพียง -

(a) การใช้โดยบุคคลที่ระบุอำนาจที่อ้างถึงในส่วน ๓๙ (๑) (a) และ (b) และ (๒) (a) และ (b) และ ๔๐ (๒) (a), (b) และ (c) ของประมวลกฎหมายวิธีพิจารณาความอาญา (Cap. ๖๘);

(b) กำหนดหรืออนุญาตบุคคลที่ระบุเพื่อชี้นำบุคคลอื่นเพื่อให้ข้อมูลใด ๆ ที่จำเป็นในการรวม - ระบุตรวจจับหรือตอบโต้การคุกคามดังกล่าว

(i) ข้อมูลที่เกี่ยวข้องกับการออกแบบการกำหนดค่าโปรแกรมคอมพิวเตอร์หรือบริการคอมพิวเตอร์ และหรือการทำงานของคอมพิวเตอร์เครื่องใดก็ได้

(ii) ข้อมูลที่เกี่ยวข้องกับความปลอดภัยของคอมพิวเตอร์โปรแกรมคอมพิวเตอร์หรือบริการคอมพิวเตอร์

(c) การจัดหาให้รัฐมนตรีหรือเจ้าหน้าที่สาธารณะที่ได้รับอนุญาตจากเขาข้อมูลใด ๆ (รวมถึงข้อมูลเรียลไทม์) ที่ได้รับจากคอมพิวเตอร์ที่ควบคุมหรือดำเนินการโดยบุคคลที่ระบุหรือได้รับจากบุคคลที่ระบุจากบุคคลอื่นตามมาตรการหรือข้อกำหนดตามวรรค b) จำเป็นต้องระบุตรวจจับหรือตอบโต้การคุกคามใด ๆ รวมถึง -

(i) ข้อมูลที่เกี่ยวข้องกับการออกแบบการกำหนดค่าหรือการทำงานของคอมพิวเตอร์โปรแกรมคอมพิวเตอร์หรือบริการคอมพิวเตอร์ และ

(ii) ข้อมูลที่เกี่ยวข้องกับความปลอดภัยของคอมพิวเตอร์โปรแกรมคอมพิวเตอร์หรือบริการคอมพิวเตอร์ และ

(d) มอบให้รัฐมนตรีหรือการพยายามรักษาความปลอดภัยของคำอธิบายที่ระบุไว้ในใบรับรองภายใต้ส่วนย่อย (๑) ที่เกี่ยวข้องกับคอมพิวเตอร์ที่ควบคุมหรือดำเนินการโดยบุคคลที่ระบุ หรือเจ้าหน้าที่สาธารณะที่ได้รับอนุญาตจากเขารายงานการฝ่าฝืน

(๓) มาตรการหรือข้อกำหนดใด ๆ ที่อ้างถึงในส่วนย่อย (๑) และทิศทางใด ๆ ที่กำหนดโดยบุคคลที่ระบุเพื่อจุดประสงค์ในการใช้มาตรการดังกล่าวหรือปฏิบัติตามข้อกำหนดดังกล่าว -

(a) จะไม่มอบสิทธิ์ใด ๆ ในการผลิตหรือการเข้าถึงข้อมูลภายใต้สิทธิ์ตามกฎหมาย และ

(b) ภายใต้วรรค (a) จะมีผลแม้จะมีข้อผูกพันหรือข้อจำกัดใด ๆ ที่กำหนดหรือสิทธิพิเศษหรือภูมิคุ้มกันที่กำหนดโดยหรือภายใต้กฎหมายสัญญาหรือกฎของการดำเนินการทางวิชาชีพใด ๆ รวมถึงการจำกัดการเปิดเผยข้อมูลที่กำหนดโดยกฎหมาย กฎของการดำเนินการอย่างมืออาชีพ

(๔) บุคคลที่ระบุซึ่งไม่มีข้อแก้ตัวตามสมควรไม่สามารถใช้มาตรการใด ๆ หรือปฏิบัติตามข้อกำหนดที่รัฐมนตรีกำหนดภายใต้ส่วนย่อย (๑) ต้องมีความผิดและจะต้องถูกปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือต้องระวางโทษจำคุกไม่เกิน ๑๐ ปีหรือทั้งจำทั้งปรับ

(๕) บุคคลใด ๆ ที่ไม่มีข้อแก้ตัวที่เหมาะสม

(a) ขัดขวางบุคคลที่ระบุในการรับมาตรการใด ๆ หรือปฏิบัติตามข้อกำหนดใด ๆ ภายใต้ส่วนย่อย (๑) หรือ

(b) ล้มเหลวในการปฏิบัติตามทิศทางที่กำหนดโดยบุคคลที่ระบุเพื่อวัตถุประสงค์ของบุคคลที่ระบุการใช้มาตรการดังกล่าว หรือปฏิบัติตามข้อกำหนดดังกล่าวใด ๆ จะต้องมีความผิดและจะต้องรับผิดชอบต่อความผิดที่ต้องปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์ หรือจำคุกไม่เกิน ๑๐ ปี หรือ ทั้งจำทั้งปรับ

(๖) มีข้อยกเว้นความรับผิดทางแพ่งหรือทางอาญาที่เกิดขึ้นสำหรับ -

(a) บุคคลที่ระบุสำหรับการทำหรือละเว้นการกระทำใด ๆ หากบุคคลที่ระบุได้ทำหรือละเว้นการกระทำ โดยสุจริตและเพื่อวัตถุประสงค์หรือหรือเป็นผลมาจากมาตรการหรือปฏิบัติตามข้อกำหนดใด ๆ ภายใต้ส่วน (๑); หรือ

(b) บุคคลที่กระทำการโดยสุจริตและเพื่อจุดประสงค์หรือเป็นผลมาจากการปฏิบัติตามทิศทางที่กำหนด โดยหรือปฏิบัติตามข้อกำหนดดังกล่าว ละเว้นการกระทำใด ๆ หากบุคคลนั้นได้กระทำหรือละเว้นที่จะทำหรือบุคคลที่ระบุ เพื่อจุดประสงค์ในการใช้มาตรการดังกล่าว

(๗) บุคคลดังต่อไปนี้จะไม่ถูก จำกัด การเปิดเผยข้อมูลตามกฎหมายสัญญาหรือกฎของการประกอบวิชาชีพ:

(a) บุคคลที่ระบุซึ่งโดยสุจริตใจได้รับข้อมูลใด ๆ เพื่อจุดประสงค์ในการดำเนินมาตรการใด ๆ ภายใต้ส่วนย่อย (๑) หรือส่วนย่อยนั้นปฏิบัติตามข้อกำหนดใด ๆ ภายใต้หรือเปิดเผยข้อมูลใด ๆ ต่อรัฐมนตรีหรือเจ้าหน้าที่สาธารณะที่รัฐมนตรีมอบหมายปฏิบัติตามข้อกำหนดใด ๆ ภายใต้ส่วนย่อยนั้น

(b) บุคคลที่ระบุซึ่งโดยสุจริตใจได้รับข้อมูลใด ๆ หรือเปิดเผยข้อมูลใด ๆ โดยสุจริตใจให้กับบุคคลที่ระบุ โดยเป็นไปตามทิศทางที่กำหนดโดยบุคคลที่ระบุเพื่อจุดประสงค์ในการใช้มาตรการใด ๆ ภายใต้ส่วนย่อย (๑) หรือปฏิบัติตามข้อกำหนดใด ๆ ภายใต้ส่วนย่อยนั้น

(๘) บุคคลต่อไปนี้ ได้แก่:

(a) บุคคลที่ระบุซึ่งบุคคลให้ข้อมูลตามทิศทางที่กำหนดโดยบุคคลที่ระบุเพื่อจุดประสงค์ในการใช้มาตรการใด ๆ ภายใต้ส่วนย่อย (a) หรือปฏิบัติตามข้อกำหนดใด ๆ ภายใต้ส่วนย่อยนั้น

(b) บุคคลที่บุคคลที่ระบุให้ข้อมูลตามข้อกำหนดใด ๆ ภายใต้ส่วนย่อย (a) จะต้องไม่ใช้หรือเปิดเผยข้อมูลยกเว้น -

(i) ได้รับอนุญาตเป็นลายลักษณ์อักษรจากบุคคลที่ได้รับข้อมูลหรือในกรณีที่ข้อมูลนั้นเป็นข้อมูลลับของบุคคลที่สาม โดยได้รับอนุญาตเป็นลายลักษณ์อักษรจากบุคคลที่สาม

(ii) บริการตอบโต้หรือคอมพิวเตอร์ภัยคุกคามต่อเพื่อวัตถุประสงค์ในการป้องกันตรวจจับบริการคอมพิวเตอร์หรือคอมพิวเตอร์หรือคอมพิวเตอร์

(iii) เพื่อเปิดเผยต่อเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายอื่น ๆ ซึ่งข้อมูลใด ๆ ที่เปิดเผยการกระทำความผิดตามพระราชบัญญัตินี้หรือกฎหมายอื่นใดที่เป็นลายลักษณ์อักษร หรือ

(iv) เพื่อให้เป็นไปตามข้อกำหนดของศาลหรือข้อกำหนดของพระราชบัญญัตินี้หรือกฎหมายอื่นใดที่เป็นลายลักษณ์อักษร

(๙) บุคคลใดที่ฝ่าฝืนหมวด (๘) จะมีความผิดและต้องรับผิดในความผิดที่ต้องโทษปรับไม่เกิน ๑๐,๐๐๐ ดอลลาร์หรือจำคุกไม่เกิน ๑๒ เดือน หรือทั้งจำทั้งปรับ

(๑๐) เมื่อมีการเปิดเผยความผิดในหลักสูตรหรือตามการใช้อำนาจใด ๆ ภายใต้หัวข้อนี้ -

(a) ไม่มีข้อมูลสำหรับความผิดนั้นจะต้องยอมรับในหลักฐานในกระบวนการทางแพ่งหรือทางอาญา และ

(b) ไม่มีพยานในกระบวนการทางแพ่งหรือทางอาญาใด ๆ

(i) เพื่อเปิดเผยชื่อที่อยู่หรือรายละเอียดอื่น ๆ ของผู้แจ้งที่ให้ข้อมูลเกี่ยวกับความผิดนั้น หรือ

(ii) เพื่อตอบคำถามใด ๆ หากคำตอบจะนำไปสู่หรือมีแนวโน้มที่จะนำไปสู่การค้นพบชื่อที่อยู่หรือรายละเอียดอื่น ๆ ของผู้แจ้ง

(๑๑) หากหนังสือเอกสารข้อมูลหรือเอาต์พุตคอมพิวเตอร์ที่ยอมรับในหลักฐานหรือมีแนวโน้มที่จะตรวจสอบในการดำเนินคดีทางแพ่งหรือทางอาญาใด ๆ ที่มีรายการใด ๆ ที่มีชื่อหรือคำอธิบายใด ๆ หรืออาจนำไปสู่การค้นพบของเขาศาล ทำให้รายการเหล่านั้นถูกปกปิดจากการดูหรือถูกลบล้างเท่าที่จำเป็นเพื่อปกป้องผู้แจ้งจากการค้นพบ

(๑๒) ในส่วนย่อย (๑) "บริการที่จำเป็น" หมายถึง -

(a) บริการที่เกี่ยวข้องโดยตรงกับโครงสร้างพื้นฐานการสื่อสารการธนาคารและการเงินสาธารณูปโภค การขนส่งสาธารณะโครงสร้างพื้นฐาน การขนส่งทางบก การบินการขนส่งหรือโครงสร้างพื้นฐานกุญแจสาธารณะ หรือ

(b) บริการฉุกเฉิน เช่น ตำรวจป้องกันพลเรือน หรือบริการสุขภาพ

การจับกุมของเจ้าหน้าที่ตำรวจโดยไม่มีหมายจับ

มาตรา ๑๖

เจ้าหน้าที่ตำรวจอาจจับกุมได้โดยไม่ต้องมีหมายจับบุคคลใด ๆ ที่ต้องสงสัยว่ามีความผิดตามพระราชบัญญัตินี้

๒.๕ ข้อมูลและสภาพทั่วไปเกี่ยวกับอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้องของสาธารณรัฐฟิลิปปินส์

๒.๕.๑ ด้านสังคมการเมือง ความมั่นคง และด้านเศรษฐกิจ

๒.๕.๑.๑ ระบบการเมืองการปกครอง

รัฐบาลฟิลิปปินส์ใช้รูปแบบตัวแทนระบอบประชาธิปไตยตามระบบของสหรัฐอเมริกา แต่มีสิ่งหนึ่งที่แตกต่างกันมาก คือ สหรัฐอเมริกาเป็นสหพันธ์สาธารณรัฐ โดยมีอำนาจสำคัญสงวนไว้สำหรับรัฐ แต่สำหรับฟิลิปปินส์เป็นระบบเอกรัฐ ซึ่งรัฐบาลแห่งชาติไม่อาจถูกท้าทายอำนาจโดยหน่วยงานท้องถิ่น รัฐธรรมนูญฟิลิปปินส์ได้รับการปรับปรุงแก้ไขถึง ๔ ครั้งใน ค.ศ. ๑๙๘๗ หลังกฎอัยการศึกสิ้นสุดลงพร้อมกับการล้มสลายของระบบการปกครองของมาร์กอส ประธานาธิบดี

เป็นประมุขของรัฐ และเป็นหัวหน้าฝ่ายบริหารมาจากการเลือกตั้งวาระละ ๖ ปี สภานิติบัญญัติเป็น ๒ สภา และตุลาการอิสระ สมาชิกวุฒิสภา ๒๔ ที่นั่ง จะได้รับเลือกมาดำรงตำแหน่งวาระละ ๖ ปี (ดำรงตำแหน่งติดต่อกันได้สูงสุด ๒ วาระ) ซึ่งครึ่งหนึ่งของสมาชิกวุฒิสภาจะมีการเลือกตั้งใหม่ทุก ๆ ๓ ปี สมาชิกสภาผู้แทนราษฎรฟิลิปปินส์มีสมาชิกสูงสุด ๒๕๐ ที่นั่ง ๘๐% มาจากการเลือกตั้งจากเขตเลือกตั้งต่าง ๆ และ ๒๐% ที่เหลือมาจากตัวแทนในบัญชีรายชื่อของพรรคทุกที่นั่งดำรงตำแหน่งวาระละ ๔ ปี โดยดำรงตำแหน่งติดต่อกันได้สูงสุด ๓ วาระ การเลือกตั้งผู้แทนครึ่งหนึ่งของจำนวนที่นั่ง ๆ ๓ ปี ฟิลิปปินส์มีพรรคการเมืองหลัก ๘ พรรค และมีพรรคเล็ก ๆ อีกหลายพรรค ศาลสูงสุดของฟิลิปปินส์มีอำนาจในการตรวจสอบประเด็นเกี่ยวกับรัฐธรรมนูญ ศาลสูงสุดประกอบด้วย หัวหน้าผู้พิพากษา และ ผู้พิพากษาสมทบอีก ๑๔ คน ผู้พิพากษาไม่จำเป็นต้องเข้าร่วมการตัดสินทุกคน ในด้านการบริหารฟิลิปปินส์แบ่งออกเป็นเขต (๑๗) จังหวัด (๘๐) นคร (๑๒๐) เทศบาล (๑,๕๐๐) และบารังไกย์ (ประมาณ ๔,๒๐๐ หมู่บ้าน)

ฟิลิปปินส์ยังคงมีการสู้รบภายในจาก ๒ ฝ่ายอย่างต่อเนื่อง ฝ่ายแรก คือ พรรคคอมมิวนิสต์ฟิลิปปินส์ หรือ CPP (Communist Party of the Philippines) และกองกำลังติดอาวุธฝ่ายซ้าย หรือก็คือกองกำลังใหม่ของประชาชน หรือ NPA (New People's Army) มีความต้องการปฏิวัติประชาธิปไตยแห่งชาติ (National Democratic Revolution) โดยดำเนินการในเขตพื้นที่ชนบท ส่วนอีกฝ่าย คือ กลุ่มกองกำลังสู้รบ ๓ กลุ่มในภาคใต้ ที่ต้องการจัดตั้งรัฐมุสลิมที่เกาะทางตอนใต้ของหมู่เกาะมินดาเนา สหรัฐอเมริกาได้เข้ามามีส่วนร่วมในการช่วยเหลือรัฐบาลฟิลิปปินส์ต่อสู่กับกลุ่มกบฏอาบูไซยาฟ หรือ ASG (Abu Sayyaf Group) และกลุ่มกบฏเจมาห์ หรือ JI (Jamaah Islamiyah) โดยประสบความสำเร็จอย่างเป็นรูปธรรม และได้มีข้อตกลงหยุดยิงกับฝ่ายแบ่งแยกดินแดน หรือแนวร่วมปลดปล่อยอิสลามโมโร หรือ MILF (Moro Islamic Liberation Front) ใน ค.ศ. ๒๐๐๙ ในด้านความสัมพันธ์กับต่างประเทศ ฟิลิปปินส์ได้ปลูกฝังความร่วมมืออันใกล้ชิดกับประเทศเพื่อนบ้านโดยเฉพาะประเทศสมาชิกอาเซียน การเป็นประเทศสมาชิกร่วมก่อตั้งอาเซียนนับเป็นบทบาทสำคัญอย่างหนึ่ง และยังเป็นสมาชิกของ UN (รวมถึงเป็นสมาชิกคณะมนตรีความมั่นคง (Security Council) สมาชิกองค์กรความร่วมมือเศรษฐกิจเอเชีย - แปซิฟิก (APEC) และกลุ่มประเทศไม่ฝักใฝ่ฝ่ายใด หรือ NAM (Non Aligned Movement) ฟิลิปปินส์เข้าร่วมการพยายามรักษาสันติภาพในติมอตะวันออกในฐานะกองกำลังของ UN และปัจจุบันได้มีกองกำลังทหารในต่างประเทศถึง ๘ ภารกิจ

๒.๕.๑.๒ ระบบเศรษฐกิจ

หลังจากสงครามโลกครั้งที่ ๒ สิ้นสุดลง ฟิลิปปินส์มีการขยายตัวทางเศรษฐกิจมากขึ้น และกลายเป็นหนึ่งประเทศที่เศรษฐกิจแข็งแกร่งที่สุดในเอเชีย อย่างไรก็ตามหลังจากนั้นเศรษฐกิจของฟิลิปปินส์ก็ทรุดตัวลง และกลายเป็นประเทศที่ยากจนที่สุดในภูมิภาค เนื่องจากระยะเวลาอันยาวนานของการบริหารจัดการที่ไม่ได้ผล และไม่มีประสิทธิภาพ ความวุ่นวายและความผันผวนทางการเมือง รวมทั้งการจัดสรรทรัพยากรที่ขาดแคลนอย่างผิดพลาด ตลาดมีการผูกขาดโดยผู้ขาย เพียงน้อยราย ซึ่งมาจากสมัยที่สหรัฐอเมริกาปกครองพื้นที่การเกษตรรวมอยู่ในที่ดินขนาดใหญ่เท่านั้น และมีนโนบายอัตราภาษีศุลกากรสูง เพื่อป้องกันการนำเข้าและออกจำกัด เพื่อป้องกันไม่ให้ชาวต่างชาติเป็นเจ้าของที่ดินและสินทรัพย์อื่น ๆ นโยบายนี้ทวีความรุนแรงมากขึ้นจากการระบาดของคอร์รัปชัน และรายได้จากภาษียังคงอยู่ต่ำเพียง ๑๕% ของผลิตภัณฑ์มวลรวมในประเทศ (GDP)

มีการลงทุนและโครงสร้างพื้นฐานไม่เพียงพอ และการพัฒนาทางเศรษฐกิจไม่สมดุล โดยเขตรอบ ๆ มะนิลาให้ผลผลิตออกมาคิดเป็น ๓๖% จากผลผลิตทั้งหมดของประเทศ ซึ่งได้มาจากประชากรเพียง ๑๒% เท่านั้น ปัญหานี้เป็นผลมาจากเศรษฐกิจหยุดชะงักในยุคของมาร์กอส ทำให้เกิดภาวะเศรษฐกิจตกต่ำอย่างรุนแรงในช่วงกลาง ค.ศ. ๑๙๘๐ และเกิดความไม่เสถียรภาพทางการเมืองในช่วงการปกครองของอากีโน (ค.ศ. ๑๙๘๖ - ๑๙๙๒) การเติบโตทางเศรษฐกิจระยะยาวถูกขัดขวางโดยโครงสร้างพื้นฐานที่ล้มเหลว กำแพงการค้าและการลงทุน และการขาดศักยภาพในการแข่งขัน มูลค่ากว่าครึ่งของ GDP นั้นมาจากภาคบริการ (๕๓.๓%) ภาคอุตสาหกรรม ๓๑.๗% ส่วนภาคการเกษตร ป่าไม้ และการประมง เป็น GDP ส่วนที่เหลือ ๑๔.๘% กำลังแรงงานกว่า ๑๑% มีความจำเป็นต้องไปทำงานต่างประเทศ แล้วส่งเงินกลับมาจุลเจือครอบครัว ซึ่งใน ค.ศ. ๒๐๐๗ คิดเป็นมูลค่าถึง ๑.๔ พันล้านดอลลาร์สหรัฐฯ นับเป็น ๑๐% ของมูลค่า GDP

การปฏิรูปเศรษฐกิจหลายครั้งในสมัยประธานาธิบดีรามอส เพื่อเรียกเสถียรภาพกลับคืนมา และเศรษฐกิจฟิลิปปินส์ก็เริ่มมีเสถียรภาพมากขึ้น แม้ว่าใน ค.ศ. ๑๙๙๗ วิกฤติการณ์ทางการเงินได้ขัดขวางการเติมโตอยู่ช่วงหนึ่ง เสถียรภาพของเศรษฐกิจมหาภาคของฟิลิปปินส์เริ่มฟื้นกลับคืนมาอีกครั้ง แต่การเติบโตในระยะยาวยังคงเป็นที่กังขา เนื่องจากยังขาดโครงสร้างพื้นฐานและการศึกษา GDP เติบโต ๗.๑% ใน ค.ศ. ๒๐๐๗ ซึ่งถือว่าสูงสุดในรอบ ๓๐ ปี ใน ค.ศ. ๒๐๐๘ อัตราการเติบโตของ GDP ทรุดตัวลงมาอยู่ที่ ๓.๗% ซึ่งเป็นเหตุมาจากภาวะเงินเฟ้อสูงประกอบกับการชะลอตัวของอุปสงค์การส่งออกทั่วโลก นอกจากนั้นภาคการบริการเติบโตขึ้น ๓.๑% ใน ค.ศ. ๒๐๐๘ และเติบโตขึ้น ๒.๘% ใน ค.ศ. ๒๐๐๙ ภาคการผลิตเติบโตขึ้นเล็กน้อย แม้ว่าการสั่งซื้อจะลดลงในไตรมาสที่ ๔ การก่อสร้างมีการเติบโตที่แข็งแกร่ง ขณะที่เหมืองแร่ งานโลหะ และเกษตรกรรมค่อนข้างซบเซา

ฟิลิปปินส์ขาดดุลงบประมาณทุกปี ตั้งแต่ ค.ศ. ๑๙๙๘ แต่แนวโน้มในช่วง ๑๐ ปีหลังนั้นเริ่มดีขึ้น การขาดทุนเป็นผลโดยตรงมาจากการใช้งบประมาณฟุ่มเฟือย และการเก็บรวบรวมได้ที่ไม่มีประสิทธิภาพ ฟิลิปปินส์พยายามลดอัตราส่วนหนี้สิน การเพิ่มภาษีใหม่ ๆ ซึ่งช่วยได้บ้าง การเก็บภาษีมูลค่าเพิ่ม (VAT) ใน ค.ศ. ๒๐๐๕ และเพิ่มขึ้นจาก ๑๐% เป็น ๑๒% และขยายให้ครอบคลุมยิ่งขึ้น มีการใช้กฎหมายเพื่อเพิ่มรายได้ให้รัฐโดยใช้ระบบการเก็บภาษีตามเกณฑ์ประสิทธิภาพการทำงาน แต่รัฐยังคงขาดดุลอยู่ แม้จะมีความพยายามรักษาดุลงบประมาณมาถึง ๕ ปีติดต่อกัน การจ่ายขาดดุลเป็นเรื่องขาดดุลเป็นเรื่องสำคัญในการรับมือกับวิกฤติการณ์ทางเศรษฐกิจ ใน ค.ศ. ๒๐๐๘ ฟิลิปปินส์ขาดดุล ๐.๙% ของ GDP และขาดดุล ๓.๒% ใน ค.ศ. ๒๐๐๙ แหล่งรายได้อีกแห่งที่ต้องการปรับปรุง คือ อุตสาหกรรมเชิงสกัด มีการประเมินว่าฟิลิปปินส์ครอบครองแร่ธาตุที่ไม่ได้ใช้เป็นมูลค่าถึง ๘๔๐ พันล้านดอลลาร์สหรัฐฯ อุตสาหกรรมเหมืองแร่ลดลงจาก ๓๐% เหลือเพียง ๑% ของ GDP แม้ว่าฟิลิปปินส์เคยเป็นประเทศที่ผลิตแร่ชั้นนำในช่วง ค.ศ. ๑๙๗๐ - ๑๙๘๐ ใน ค.ศ. ๒๐๐๔ ศาลสูงสุดออกกฎว่าบริษัทต่างชาติจะได้รับอนุญาตให้ทำสัญญากับรัฐบาลฟิลิปปินส์ เพื่อเข้ามาทำอุตสาหกรรมเหมืองแร่และอุตสาหกรรมด้านพลังงาน ในปัจจุบันบริษัทต่างชาติได้รับอนุญาตให้เป็นเจ้าของหุ้นและการลงทุนได้ ๑๐๐% ในธุรกิจขนาดใหญ่ เพื่อการสำรวจ พัฒนา การนำแร่ธาตุ น้ำมัน และก๊าซ มาใช้ประโยชน์

GDP ของฟิลิปปินส์เติบโต ๑.๑% ใน ค.ศ. ๒๐๐๙ และ ๓.๕% ใน ค.ศ. ๒๐๑๐ รัฐบาลมีแผนที่จะกระตุ้นเศรษฐกิจอย่างรวดเร็ว โดยใช้แผนกระตุ้นเศรษฐกิจมูลค่าประมาณ ๗ พันล้านดอลลาร์สหรัฐฯ งบประมาณที่จะใช้ในส่วนเพิ่มสวัสดิการ ปรับปรุงโครงสร้างพื้นฐาน ให้ลดหย่อนภาษี แก่ประชาชนและองค์กรเอกชน ฟิลิปปินส์เริ่มมีศักยภาพที่เริ่มแข็งแกร่งขึ้น โดยเฉพาะด้านอุตสาหกรรมเหมืองแร่ การผลิตก๊าซธรรมชาติ อุตสาหกรรมการผลิต กระบวนการของการจ้างที่ไม่ใช่ธุรกิจหลักของบริษัท หรือ BPO (Business Process Outsourcing) และการท่องเที่ยว ภาวะเงินเฟ้อและปัญหาการว่างงานยังคงเป็นปัญหาหลัก โครงสร้างพื้นฐานต้องได้รับการพัฒนา รวมทั้งการปฏิรูปเพื่อเพิ่มผลผลิตและความสามารถในการแข่งขัน รายได้จากภาษีต้องเพิ่มขึ้น และการแก้ปัญหาความยากจนเป็นสิ่งที่ต้องให้ความสำคัญสูงสุด ต้องเปิดเสรีทางการค้าเพื่อกระตุ้นการลงทุน เพื่อเพิ่มการแข่งขันและผลผลิต ซึ่งจะช่วยให้เศรษฐกิจเติบโตยิ่งขึ้น การปฏิรูปเศรษฐกิจจะช่วยลดค่าใช้จ่ายในการดำเนินธุรกิจและกำจัดอุปสรรคในการเติบโตของเศรษฐกิจ

๒.๕.๑.๓ ระบบกฎหมาย

กฎหมายของฟิลิปปินส์นั้นส่วนใหญ่มีรากฐานมาจากกฎหมายของสเปนและกฎหมายแองโกล - อเมริกา สเปนได้บังคับให้ประเทศในอาณานิคมใช้ประมวลกฎหมายแพ่งและอาญาของสเปน และอเมริกันยังคงระบบกฎหมายนี้ไว้ในช่วงที่ปกครองฟิลิปปินส์ แม้ว่าระบบกฎหมายของอเมริกันจะมีพื้นฐานมาจากจารีตประเพณีก็ตาม อย่างไรก็ตาม มาตรฐานในการพิจารณาคดีของศาลสูงสุดฟิลิปปินส์ได้ผูกรวมกับระบบกฎหมายจารีตประเพณี ใน ค.ศ. ๑๙๓๐ ประมวลกฎหมายอาญาได้รับการปรับปรุงใหม่ และกฎหมายแพ่งฉบับใหม่ได้ประกาศใช้ใน ค.ศ. ๑๙๕๐ ประมวลกฎหมายฟิลิปปินส์ประกาศใช้หลังจากได้ผ่านการพิจารณาจากสภานิติบัญญัติ กฎหมายจารีตประเพณีได้ใช้ในกฎหมายรัฐธรรมนูญ กฎหมายหุ้นส่วนบริษัท ภาษี แรงงาน กฎหมายอื่น ๆ ที่เกี่ยวข้องกับธุรกิจในฟิลิปปินส์ไม่มีการพิจารณาโดยคณะลูกขุน ระบบตุลาการของฟิลิปปินส์ประกอบด้วย ศาลสูงสุด ศาลอุทธรณ์ ศาลเขต ศาลอุทธรณ์ภาษี ศาลนคร และเทศบาล ผู้พิพากษาจะได้รับการแต่งตั้งจากประธานาธิบดี โดยความเห็นชอบของฝ่ายตุลาการเนติบัณฑิตสภา ซึ่งจะทำหน้าที่จนถึงอายุ ๗๐ ปี ศาลระดับล่าง ประกอบด้วย ศาลอุทธรณ์ ซึ่งแบ่งออกเป็น ๑๗ หมวด ศาลท้องถิ่น และศาลเขต ระบบศาลท้องถิ่นที่ไม่เป็นทางการเพื่อยุติข้อพิพาทนอกระบบศาล ศาลพิเศษ Sandiganbayan (ศาลต่อต้านการรับสินบน) ซึ่งจัดตั้งขึ้นใน ค.ศ. ๑๙๗๙ ประกอบด้วย ประธานผู้พิพากษาและผู้พิพากษาสมทบ ๘ คน ซึ่งพิจารณาเฉพาะคดีการละเมิดกฎหมายต่อต้านสินบน (Anti - Graft Act) และรัฐบัญญัติคอร์รัปชัน (Corrupt Practice Act) รัฐบัญญัติความร่ำรวยที่ไม่สามารถชี้แจงได้ (Unexplained Wealth Act) และความผิดอาญาอย่างอื่น หรือความผิดอาญาที่กระทำโดยเจ้าหน้าที่รัฐหรือลูกจ้างที่เกี่ยวข้อง รวมถึงลูกจ้างในกิจการของรัฐ หรือบริษัทที่ควบคุมโดยรัฐด้วย ใน ค.ศ. ๑๙๘๕ มีการจัดตั้งระบบกฎหมายอิสลาม (ชารีอะห์) แยกออกมาต่างหากในเขตภาคใต้ โดยพิจารณาคดีเกี่ยวกับครอบครัว ความเกี่ยวข้องตามสัญญาในหมู่ชาวมุสลิม ผู้พิพากษาจังหวัด ๓ คน และผู้พิพากษาเชอร์กิต (ผู้มีอำนาจพิจารณาคดี ในเขตหลายท้องที่) จำนวน ๖ คน เป็นฝ่ายควบคุมระบบกฎหมายอิสลาม ศาลพิเศษอีกอย่างหนึ่ง คือ ศาลอุทธรณ์ภาษี ประกอบด้วย ประธานผู้พิพากษาและผู้พิพากษาสมทบ ๒ คน มีอำนาจพิจารณาการอุทธรณ์ในการตัดสินใจของคณะกรรมการภาษีสรรพากร คณะกรรมการภาษีศุลกากร เกี่ยวกับปัญหาเฉพาะกรณีกฎหมายธุรกิจเป็นกฎหมายเฉพาะ

เรียกว่าประมวลกฎหมายเชิงพาณิชย์ฟิลิปปินส์ โดยลักษณะแล้วเป็นกฎหมายแบบตะวันตก (โดยดั้งเดิมเป็นของสเปน) ครอบคลุมเรื่องสัญญาการปฏิบัติตามภาระผูกพัน การต่อต้านการผูกขาดและออกหลักทรัพย์ การเงินและการธนาคาร การเรียกร้องความปลอดภัยและคุณภาพของผลิตภัณฑ์ การโฆษณาและหลักการขาย รัฐบัญญัติการลงทุนของต่างชาติ ค.ศ. ๑๙๙๑ และประมวลกฎหมายมาตรการลงทุน ค.ศ. ๑๙๘๗ ควบคุมกระบวนการ และมีเงื่อนไขภายใต้หัวข้อที่ว่า บุคคลที่ไม่ได้มีสัญชาติฟิลิปปินส์สามารถลงทุนและดำเนินกิจการภายในประเทศ ภาครัฐที่ติดต่อกับนักลงทุนต่างประเทศคือ คณะกรรมการลงทุนฟิลิปปินส์ หรือ BOI (Philippines Board of Investment) การปฏิรูปใน ค.ศ. ๒๐๐๙ ช่วยให้รับสินเชื่อในการเริ่มต้นธุรกิจง่ายขึ้น

ฟิลิปปินส์จัดอยู่อันดับค่อนข้างต่ำในข้อมูลของธนาคารโลก และถูกจัดอันดับความยากง่ายในการดำเนินธุรกิจใน ค.ศ. ๒๐๑๐ อยู่อันดับที่ ๑๔๔ จากทั้งหมด ๑๘๓ ประเทศ และอยู่ในอันดับต่ำลงไปอีก ในการจัดอันดับความยากง่ายในการเริ่มต้นธุรกิจ คืออยู่อันดับ ๑๖๒ ถ้าเทียบกับกลุ่มประเทศอาเซียน ๙ ประเทศแล้ว ฟิลิปปินส์ถือว่ามาเป็นอันดับสุดท้าย ขั้นตอนในการเริ่มต้นธุรกิจในฟิลิปปินส์มี ๑๕ ขั้นตอนด้วยกัน ซึ่งใช้เวลาประมาณ ๕๒ วัน และค่าใช้จ่ายประมาณ ๒๘% ของรายได้เฉลี่ยต่อหัวของประชากร การขอใบอนุญาตก่อสร้างต้องใช้เวลานาน โดยเฉลี่ยประมาณ ๒๐๐ วัน การเลิกจ้างพนักงานนั้นค่าใช้จ่ายค่อนข้างสูง โดยค่าชดเชยการเลิกจ้างนั้นสูงเท่ากับเงินค่าจ้างถึง ๙๑ สัปดาห์ ฟิลิปปินส์อยู่ในอันดับที่ ๑๒๗ ในด้านความยากง่ายในด้านขอสินเชื่อโดยมีระดับความคุ้มครองต่ำ และมีข้อมูลน้อยสำหรับผู้ที่สนใจลงทุนในประเทศ การบังคับใช้สัญญาเรียกร้องสิทธิก็ใช้เวลามากเช่นเดียวกัน ใช้เวลาเฉลี่ยถึง ๘๔๒ วัน และค่าใช้จ่ายในการเรียกร้องสิทธิต่อครั้งคิดเป็น ๒๖% ของมูลค่าการเรียกร้องทั้งหมด อัตราภาษีคือ ๓๐% ของกำไร

กฎหมายด้านทรัพย์สินทางปัญญา (Intellectual Property) ในฟิลิปปินส์กำหนดให้เป็นสิทธิส่วนบุคคล ในการลงทะเบียนคุ้มครองและบังคับใช้สิทธินั้นอยู่ในการรับผิดชอบของผู้ถือสิทธิเอง ฟิลิปปินส์มีการคุ้มครองทรัพย์สินทางปัญญายาวนานที่สุดในอาเซียน ซึ่งเป็นผลมาจากกฎหมายสมัยภายใต้การปกครองของสเปน หลังจากช่วงการคุ้มครองทรัพย์สินทางปัญญาผ่านคำสั่งภายใต้การปกครองของมาร์กอส ฟิลิปปินส์เป็นชาติแรกในอาเซียนที่นำเอกสารมาตรการทรัพย์สินทางปัญญาแบบครอบคลุม ตามแบบองค์กรทรัพย์สินทางปัญญาโลก หรือ WPO (World Intellectual Property Organization) ค.ศ. ๑๙๙๕ มาใช้ มาตรการนี้ครอบคลุมเรื่องสิทธิบัตร ผลิตภัณฑ์อรรถประโยชน์ เครื่องหมายการค้า และสิ่งบ่งชี้ทางภูมิศาสตร์ ลิขสิทธิ์ การออกแบบอุตสาหกรรม การออกแบบผังภูมิของวงจรรวม และข้อมูลที่ไม่เปิดเผย อย่างไรก็ตาม การบังคับใช้กฎหมายทางทรัพย์สินทางปัญญานั้นยังคงไม่เต็มที่ และระบบตุลาการมักวินิจฉัยข้อพิพาทค่อนข้างช้า

๒.๕.๒ ด้านอาชญากรรมคอมพิวเตอร์และกฎหมายที่เกี่ยวข้อง

กฎและข้อบังคับที่ใช้สาธารณรัฐหมายเลข ๑๐๑๗๕ หรือที่รู้จักกันในชื่อ
"พระราชบัญญัติป้องกันอาชญากรรมทางไซเบอร์ของปี ๒๐๑๒"

ตามอำนาจหน้าที่ของกระทรวงยุติธรรม กรมมหาดไทย และรัฐบาลท้องถิ่น และกรมวิทยาศาสตร์และเทคโนโลยีตามพระราชบัญญัติสาธารณรัฐหมายเลข ๑๐๑๗๕ หรือที่รู้จักกันในนาม "พระราชบัญญัติป้องกันอาชญากรรมทางไซเบอร์ของปี ๒๕๕๕" มีการประกาศใช้กฎและข้อบังคับต่อไปนี้ ปฏิบัติตามบทบัญญัติของพระราชบัญญัติดังกล่าว

หมวด ๑ ข้อกำหนดเบื้องต้น

มาตราที่ ๑ หัวข้อ - กฎเหล่านี้จะเรียกว่ากฎการดำเนินการและข้อบังคับของสาธารณรัฐหมายเลข ๑๐๑๗๕ หรือ "พระราชบัญญัติป้องกันอาชญากรรมทางไซเบอร์ของปี ๒๐๑๒"

มาตราที่ ๒ การประกาศนโยบาย – รัฐตระหนักถึงบทบาทที่สำคัญของอุตสาหกรรมข้อมูลและการสื่อสาร เช่น การผลิตเนื้อหาการสื่อสารโทรคมนาคมการกระจายเสียงการพาณิชย์อิเล็กทรอนิกส์และการประมวลผลข้อมูลในการพัฒนาทางสังคม และเศรษฐกิจโดยรวมของรัฐ

รัฐยังตระหนักถึงความสำคัญของการจัดหาสภาพแวดล้อมที่เอื้อต่อการเร่งความเร็วในการพัฒนาและการประยุกต์ใช้อย่างมีเหตุผลและการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้ได้รับการแลกเปลี่ยนและ/หรือการส่งข้อมูลอย่างเสรีง่ายและเข้าใจได้และความจำเป็นในการปกป้องและปกป้องความสมบูรณ์ของคอมพิวเตอร์คอมพิวเตอร์และระบบสื่อสารเครือข่ายและฐานข้อมูล และการรักษาความลับความสมบูรณ์และความพร้อมของข้อมูลและข้อมูลที่จัดเก็บจากการใช้ในทางที่ผิดการละเมิด และการเข้าถึงที่ผิดกฎหมายทุกรูปแบบ กฎหมายการกระทำหรือการดำเนินการดังกล่าว

รัฐจะต้องใช้อำนาจที่เพียงพอในการป้องกันและต่อสู้กับความผิดดังกล่าวอย่างมีประสิทธิภาพโดยอำนวยความสะดวกในการตรวจสอบการสอบสวนและการดำเนินคดีทั้งในระดับประเทศและระหว่างประเทศ

มาตราที่ ๓ คำจำกัดความของข้อกำหนด – ข้อกำหนดต่อไปนี้ถูกกำหนดดังนี้

a) การเข้าถึง หมายถึง คำสั่งการสื่อสารกับการจัดเก็บข้อมูลในการดึงข้อมูลจากหรือใช้ประโยชน์จากทรัพยากรใด ๆ ของระบบคอมพิวเตอร์หรือเครือข่ายการสื่อสาร;

b) พระราชบัญญัติ หมายถึง พระราชบัญญัติของสาธารณรัฐหมายเลข ๑๐๑๗๕ หรือ "พระราชบัญญัติป้องกันอาชญากรรมทางไซเบอร์ของปี ๒๐๑๒"

c) การเปลี่ยนแปลง หมายถึง การดัดแปลงหรือเปลี่ยนแปลงข้อมูลหรือโปรแกรมคอมพิวเตอร์ที่มีอยู่ในรูปแบบหรือสาร;

d) Central Authority หมายถึง DOJ - Office of Cybercrime

e) ภาพอนาจารเด็ก หมายถึง การกระทำที่ผิดกฎหมายหรือต้องห้ามซึ่งกำหนดและลงโทษโดยพระราชบัญญัติสาธารณรัฐฉบับที่ ๙๗๗๕ หรือ "พระราชบัญญัติภาพอนาจารเด็กต่อต้านการกระทำของปี ๒๐๐๙" ที่กระทำผ่านระบบคอมพิวเตอร์: โดยมีเงื่อนไขว่าการลงโทษจะต้องเป็นหนึ่ง (๑) ระดับที่สูงกว่าที่กำหนดไว้ในพระราชบัญญัติสาธารณรัฐฉบับที่ ๙๗๗๕

f) การรวบรวม หมายถึง การรวบรวมและรับข้อมูล

g) การสื่อสาร หมายถึง การส่งข้อมูลผ่านสื่อข้อมูลและเทคโนโลยีการสื่อสาร (๑CT) รวมถึงข้อมูลเสียง วิดีโอ และรูปแบบอื่น ๆ

h) เจ้าหน้าที่ผู้มีอำนาจ หมายถึง ศูนย์สอบสวนและประสานงานอาชญากรรมไซเบอร์หรือสำนักงาน DOJ - Cybercrime แล้วแต่กรณี

i) คอมพิวเตอร์ หมายถึง อุปกรณ์อิเล็กทรอนิกส์, แม่เหล็ก, ออปติคัล, เคมีไฟฟ้า, หรือการประมวลผลข้อมูลหรืออุปกรณ์สื่อสารอื่น ๆ หรือการจัดกลุ่มของอุปกรณ์ดังกล่าวที่มีความสามารถในการดำเนินการทางตรรกะคณิตศาสตร์การกำหนดเส้นทางหรือฟังก์ชันการจัดเก็บ

สิ่งอำนวยความสะดวกหรืออุปกรณ์ที่เกี่ยวข้องโดยตรงกับหรือใช้งานร่วมกับอุปกรณ์ดังกล่าว ครอบคลุมอุปกรณ์คอมพิวเตอร์ทุกประเภทรวมถึงอุปกรณ์ที่มีความสามารถในการประมวลผลข้อมูล เช่น โทรศัพท์มือถือ สมาร์ทโฟนเครือข่ายคอมพิวเตอร์ และอุปกรณ์อื่น ๆ ที่เชื่อมต่อกับอินเทอร์เน็ต

j) ข้อมูลคอมพิวเตอร์ หมายถึง การเป็นตัวแทนของข้อเท็จจริงข้อมูลหรือแนวคิดในรูปแบบที่เหมาะสมสำหรับการประมวลผลในระบบคอมพิวเตอร์รวมถึงโปรแกรมที่เหมาะสมที่จะทำให้ระบบคอมพิวเตอร์ทำงานได้และรวมถึงเอกสารอิเล็กทรอนิกส์และ/หรือข้อความอิเล็กทรอนิกส์ ในระบบคอมพิวเตอร์ในพื้นที่หรือออนไลน์

k) โปรแกรมคอมพิวเตอร์ หมายถึง ชุดคำสั่งที่ดำเนินการโดยคอมพิวเตอร์เพื่อให้ได้ผลลัพธ์ที่ต้องการ

l) ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือกลุ่มใด ๆ ของอุปกรณ์เชื่อมต่อหรืออุปกรณ์ที่เกี่ยวข้อง ซึ่งอย่างน้อยหนึ่งอย่างซึ่งตามโปรแกรมจะทำการประมวลผลข้อมูลโดยอัตโนมัติ ครอบคลุมอุปกรณ์ทุกประเภทที่มีความสามารถในการประมวลผลข้อมูล รวมถึงแต่ไม่จำกัดเฉพาะคอมพิวเตอร์และโทรศัพท์มือถือ อุปกรณ์ที่ประกอบด้วยฮาร์ดแวร์ และซอฟต์แวร์อาจประกอบด้วยส่วนประกอบอินพุตเอาต์พุตและหน่วยเก็บข้อมูลซึ่งอาจแยกต่างหากหรือเชื่อมต่อกับเครือข่ายหรืออุปกรณ์อื่นที่คล้ายคลึงกัน นอกจากนี้ยังรวมถึงอุปกรณ์จัดเก็บข้อมูลคอมพิวเตอร์หรือสื่อ

m) ข้อมูลเนื้อหา หมายถึง เนื้อหาการสื่อสารของการสื่อสารความหมายหรือความหมายของการสื่อสารหรือข้อความหรือข้อมูลที่ถูกสื่อความหมายโดยการสื่อสารนอกเหนือจากข้อมูลการจราจร

n) โครงสร้างพื้นฐานที่สำคัญ หมายถึง ระบบคอมพิวเตอร์และ/หรือเครือข่ายไม่ว่าจะเป็นทางกายภาพหรือเสมือนและ/หรือโปรแกรมคอมพิวเตอร์ข้อมูลคอมพิวเตอร์และ/หรือข้อมูลการจราจรที่มีความสำคัญต่อประเทศนี้ ซึ่งการไร้ความสามารถหรือทำลายหรือรบกวนระบบและทรัพย์สินดังกล่าว จะส่งผลกระทบที่เลวร้ายต่อความมั่นคงความมั่นคงของชาติหรือทางเศรษฐกิจสุขภาพและความปลอดภัยสาธารณะแห่งชาติหรือการรวมกันของสิ่งเหล่านั้น

o) ความปลอดภัยทางไซเบอร์ หมายถึง การรวบรวมเครื่องมือนโยบายแนวทางการจัดการความเสี่ยงการกระทำการฝึกอบรมแนวปฏิบัติที่ดีที่สุดการรับรองและเทคโนโลยีที่สามารถใช้เพื่อปกป้องสภาพแวดล้อมในโลกไซเบอร์ และทรัพย์สินขององค์กรและผู้ใช้

p) แผนการรักษาความปลอดภัยทางไซเบอร์แห่งชาติ หมายถึง แผนปฏิบัติการที่ครอบคลุมซึ่งออกแบบมาเพื่อปรับปรุงความปลอดภัย และเพิ่มความยืดหยุ่นให้กับโลกไซเบอร์ของโครงสร้างพื้นฐานและบริการ มันเป็นวิธีการจากบนลงล่างสู่ความปลอดภัยบนโลกไซเบอร์ที่มีคำแถลงนโยบายในวงกว้างและกำหนดชุดวัตถุประสงค์และลำดับความสำคัญระดับชาติที่ควรทำภายในระยะเวลาที่กำหนด

q) Cybersex หมายถึง การมีส่วนร่วมโดยจงใจการบำรุงรักษาการควบคุมหรือการดำเนินงานไม่ว่าทางตรงหรือทางอ้อมใด ๆ ของการจัดแสดงนิทรรศการอวัยวะเพศหรือกิจกรรมทางเพศใด ๆ ด้วยความรักใคร่ด้วยความช่วยเหลือของระบบคอมพิวเตอร์

r) หมายถึง คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์สื่ออิเล็กทรอนิกส์ที่ใช้ในการสื่อสารออนไลน์

s) ฐานข้อมูล หมายถึง การเป็นตัวแทนของข้อมูลความรู้ข้อเท็จจริงแนวคิด หรือคำแนะนำที่จัดทำประมวลผลหรือจัดเก็บหรือได้จัดเตรียมประมวลผลหรือจัดเก็บในลักษณะที่เป็นทางการและมีวัตถุประสงค์เพื่อใช้ในระบบคอมพิวเตอร์

t) หลักฐานดิจิทัล หมายถึง ข้อมูลดิจิทัลที่อาจใช้เป็นหลักฐานในกรณีการรวบรวมข้อมูลดิจิทัล อาจดำเนินการโดยการยึดสื่อเก็บข้อมูล (ผู้ให้บริการข้อมูล) การแตะหรือตรวจสอบการรับส่งข้อมูลเครือข่ายหรือการทำสำเนาดิจิทัล (เช่น ภาพนิติวิทยาศาสตร์ สำเนาไฟล์ ฯลฯ) ของจัดเก็บข้อมูล

u) หลักฐานทางอิเล็กทรอนิกส์ หมายถึง หลักฐานการใช้งานซึ่งได้รับการอนุมัติโดยกฎของหลักฐานที่มีอยู่ในการสืบหาในกระบวนการพิจารณาคดีความจริงเกี่ยวกับเรื่องของความจริงที่ได้รับหลักฐานบันทึก ส่ง ถ่าย เก็บ ประมวลผลดึง หรือผลิตอิเล็กทรอนิกส์

v) Forensics หมายถึง การประยุกต์ใช้เทคนิคการสืบสวนและการวิเคราะห์ที่สอดคล้องกับมาตรฐาน หลักฐานและใช้ในหรือเหมาะสมสำหรับศาลของกฎหมายหรือบริบททางกฎหมายอื่น ๆ

w) ภาพทางนิติวิทยาศาสตร์หรือที่เรียกว่าสำเนาทางนิติเวช หมายถึง สำเนาที่แน่นอนของผู้ให้บริการข้อมูล รวมถึงการหย่อนพื้นที่ที่ไม่ได้ถูกจัดสรรและพื้นที่ที่ไม่ได้ใช้ มีเครื่องมือทางนิติวิทยาศาสตร์สำหรับการทำภาพเหล่านี้ เครื่องมือส่วนใหญ่ผลิตข้อมูล เช่น ค่าแฮช เพื่อให้มั่นใจถึงความสมบูรณ์ของภาพ

x) Hash หมายถึง อัลกอริทึมทางคณิตศาสตร์ที่สร้างขึ้นจากข้อมูลดิจิทัล (ไฟล์ดิสก์ทางกายภาพหรือดิสก์ แบบลอจิคัล) ดังนั้นการสร้าง "ลายนิ้วมือดิจิทัล" หรือ "ดิจิทัลดีเอ็นเอ" สำหรับข้อมูลนั้น เป็นอัลกอริทึมทางเดียว ดังนั้นจึงไม่สามารถเปลี่ยนหลักฐานดิจิทัลโดยไม่ต้องเปลี่ยนค่าแฮช ที่เกี่ยวข้อง

y) ข้อมูลระบุตัวตน หมายถึง ชื่อหรือหมายเลขใด ๆ ที่อาจถูกใช้เพียงอย่างเดียวหรือใช้ร่วมกับข้อมูล อื่นใดเพื่อระบุตัวบุคคลใดบุคคลหนึ่งโดยเฉพาะรวมถึงรายการใด ๆ ต่อไปนี้

๑. ชื่อ, วันเดือนปีเกิด, หมายเลขใบขับขี่, หมายเลขหนังสือเดินทางหรือหมายเลขประจำตัวผู้เสียภาษี

๒. ข้อมูลไบโอเมตริกซ์ที่ไม่ซ้ำกัน เช่น ลายนิ้วมือ หรือการเป็นตัวแทนทางกายภาพเฉพาะอื่น ๆ

๓. หมายเลขประจำตัวอิเล็กทรอนิกส์ที่ไม่ซ้ำกันที่อยู่หรือรหัสเส้นทาง และ

๔. ข้อมูลที่ระบุตัวตนทางโทรคมนาคมหรืออุปกรณ์เข้าถึง

z) ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ระบบที่มีไว้สำหรับและสามารถสร้างส่งรับจัดเก็บหรือประมวลผลข้อความข้อมูลอิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์ และรวมถึงระบบคอมพิวเตอร์หรืออุปกรณ์อื่น ๆ ที่คล้ายกันโดยหรือที่ข้อมูลถูกบันทึกหรือจัดเก็บและขั้นตอนใด ๆ ที่เกี่ยวข้องกับการบันทึกหรือจัดเก็บข้อมูลอิเล็กทรอนิกส์หรือเอกสารอิเล็กทรอนิกส์

aa) การสกัดกั้น หมายถึง การฟังบันทึกตรวจสอบหรือเฝ้าระวังเนื้อหาของการสื่อสาร รวมถึงการจัดหาเนื้อหาของข้อมูลไม่ว่าโดยตรงผ่านการเข้าถึง และการใช้ระบบคอมพิวเตอร์

หรือโดยอ้อมผ่านการใช้อุปกรณ์ดักฟังอิเล็กทรอนิกส์หรืออุปกรณ์ดักฟังทางอิเล็กทรอนิกส์ในเวลาเดียวกันที่มีการสื่อสารเกิดขึ้น

bb) โฮสต์เนื้อหาอินเทอร์เน็ต หมายถึง บุคคลที่เป็นเจ้าภาพหรือผู้เสนอที่จะโฮสต์เนื้อหาอินเทอร์เน็ตในฟิลิปปินส์

cc) หน่วยงานบังคับใช้กฎหมาย หมายถึง สำนักงานสืบสวนกลางแห่งชาติ (NBI) และตำรวจแห่งชาติฟิลิปปินส์ (PNP) ภายใต้มาตรา ๑๐ ของพระราชบัญญัติ

dd) ผู้แต่งดั้งเดิม หมายถึง บุคคลที่สร้างหรือเป็นที่มาของคำแถลงอิเล็กทรอนิกส์หรือโพสต์อิเล็กทรอนิกส์ที่ถูกโจมตีโดยใช้ระบบคอมพิวเตอร์

ee) การเก็บรักษา หมายถึง การเก็บรักษาข้อมูลที่มีอยู่แล้วในรูปแบบการจัดเก็บได้รับการคุ้มครองจากสิ่งที่จะทำให้คุณภาพหรือสภาพปัจจุบันของการเปลี่ยนแปลงหรือเสื่อมสภาพ เป็นกิจกรรมที่ช่วยให้ข้อมูลที่เก็บไว้ปลอดภัยและปลอดภัย

ff) ผู้ให้บริการ หมายถึง

๑. หน่วยงานของรัฐหรือเอกชนที่ให้บริการแก่ผู้ใช้ด้วยความสามารถในการสื่อสารด้วยระบบคอมพิวเตอร์ และ

๒. หน่วยงานอื่นใดที่ประมวลผลหรือเก็บข้อมูลคอมพิวเตอร์ในนามของบริการสื่อสารดังกล่าวหรือ ผู้ใช้บริการดังกล่าว

gg) ข้อมูลของสมาชิก หมายถึง ข้อมูลใด ๆ ที่อยู่ในรูปแบบของข้อมูลคอมพิวเตอร์หรือรูปแบบอื่นใดที่จัดขึ้นโดยผู้ให้บริการที่เกี่ยวข้องกับสมาชิกของบริการของตน นอกเหนือจากข้อมูลการจราจรหรือเนื้อหาและสิ่งใดต่อไปนี้สามารถที่จัดตั้งขึ้น

ประเภทของบริการสื่อสารที่ใช้ข้อกำหนดทางเทคนิคที่ได้รับและระยะเวลาของบริการ

ข้อมูลประจำตัวของสมาชิกไปรษณีย์ หรือที่อยู่ทางภูมิศาสตร์ โทรศัพท์ และหมายเลขการเข้าถึงอื่น ๆ ที่อยู่เครือข่ายที่ได้รับมอบหมายใด ๆ ข้อมูลการเรียกเก็บเงิน และการชำระเงินที่มีอยู่บนพื้นฐานของข้อตกลงการบริการ หรือการจัดการหรือข้อมูลอื่นใดที่มีอยู่บนเว็บไซต์ของการติดตั้งอุปกรณ์สื่อสารที่มีอยู่บนพื้นฐานของข้อตกลงการบริการหรือการจัดการ

hh) ข้อมูลการจราจรหรือข้อมูลที่ไม่ใช่เนื้อหา หมายถึง ข้อมูลคอมพิวเตอร์อื่น ๆ นอกเหนือจากเนื้อหาของการสื่อสาร รวมถึงแต่ไม่จำกัดเพียงที่มาของต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ขนาดระยะเวลา หรือประเภทของบริการพื้นฐาน และ

ii) การไม่มีสิทธิ หมายถึง: (i) การดำเนินการที่ดำเนินการโดยไม่มีอำนาจมากเกินไป; หรือ (ii) การดำเนินการที่ไม่ครอบคลุมโดยการป้องกันทางกฎหมายข้อแก้ตัวคำสั่งศาลเหตุผลหรือหลักการที่เกี่ยวข้องภายใต้กฎหมาย

หมวดที่ ๒

การกระทำที่มีโทษและบทลงโทษทางอาชญากรรม

มาตราที่ ๔ ความผิดอาญาไซเบอร์ – การกระทำต่อไปนี้เป็นความผิดฐานอาชญากรรมไซเบอร์ที่มีโทษตามพระราชบัญญัติ

A. ความผิดต่อการรักษาความลับความสมบูรณ์และความพร้อมของข้อมูลคอมพิวเตอร์และระบบจะถูกลงโทษด้วยการจำคุก Prision นายกเทศมนตรีหรือปรับไม่น้อยกว่าสองแสนเปโซ (P๒๐๐,๐๐๐.๐๐) สูงสุดถึงอัตราสูงสุดต่อความเสียหายที่เกิดขึ้นหรือ ทั้งสองยกเว้นที่เกี่ยวกับหมายเลข ๕ ในที่นี้

๑. Illegal access – การเข้าถึงทั้งหมดหรือบางส่วนของระบบคอมพิวเตอร์โดยไม่ถูกต้อง

๒. Illegal Interception การสกัดกั้นด้วยวิธีการทางเทคนิคและไม่ถูกต้องของการส่งผ่านข้อมูลคอมพิวเตอร์ที่ไม่ใช่แบบสาธารณะไปยังจากหรือภายในระบบคอมพิวเตอร์รวมถึงการปล่อยคลื่นแม่เหล็กไฟฟ้าจากระบบคอมพิวเตอร์ที่มีข้อมูลคอมพิวเตอร์ดังกล่าว: อย่างไรก็ตามจะต้องไม่ผิดกฎหมายสำหรับเจ้าหน้าที่ลูกจ้างหรือตัวแทนของผู้ให้บริการที่ใช้สิ่งอำนวยความสะดวกในการส่งการสื่อสารเพื่อสกัดกั้นเปิดเผยหรือใช้การสื่อสารนั้นตามปกติในการจ้างงานในขณะที่มีส่วนร่วมในกิจกรรมใด ๆ ที่จำเป็นต่อการให้บริการหรือการปกป้องสิทธิ์หรือทรัพย์สินของผู้ให้บริการยกเว้นบริการหลังนั้นจะไม่ใช้บริการการสังเกตหรือตรวจสอบแบบสุ่มนอกเหนือจากวัตถุประสงค์ของการตรวจสอบคุณภาพเชิงกลหรือบริการควบคุม

๓. การแทรกแซงข้อมูล – การแก้ไขโดยเจตนาหรือโดยประมาทการทำลายการลบหรือการเสื่อมสภาพของข้อมูลคอมพิวเตอร์เอกสารอิเล็กทรอนิกส์หรือข้อความข้อมูลอิเล็กทรอนิกส์โดยไม่มีสิทธิ์รวมถึงการแนะนำหรือส่งไวรัส

๔. การแทรกแซงระบบการเปลี่ยนแปลงโดยเจตนาหรือการขัดขวางโดยประมาทหรือการรบกวนการทำงานของคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์โดยการป้อนส่งส่งทำลาย ทำลาย ลบ เสื่อมสภาพ แก้ไข หรือระงับข้อมูลคอมพิวเตอร์หรือโปรแกรมเอกสารอิเล็กทรอนิกส์หรือข้อความข้อมูลอิเล็กทรอนิกส์ หรือสิทธิอำนาจรวมถึงการแนะนำหรือการส่งไวรัส

๕. การใช้อุปกรณ์ในทางที่ผิดซึ่งจะถูกลงโทษด้วยการจำคุกนายกเทศมนตรีส่วนที่ถูกปรับหรือปรับไม่เกินห้าแสนเปโซ (P500,000.00) หรือทั้งสองอย่างกระทำ ผ่านการกระทำดังต่อไปนี้

a. การใช้การผลิตการขายการจัดหาการนำเข้าการกระจายหรือการทำให้เป็นอย่างอื่นโดยเจตนา และโดยไม่มีสิทธิใด ๆ ต่อไปนี้

i) อุปกรณ์รวมถึงโปรแกรมคอมพิวเตอร์ออกแบบหรือปรับใช้เป็นหลักเพื่อจุดประสงค์ในการกระทำความผิดใด ๆ ภายใต้กฎนี้; หรือ

ii) รหัสผ่านคอมพิวเตอร์รหัสการเข้าถึงหรือข้อมูลที่คล้ายกันซึ่งระบบคอมพิวเตอร์ทั้งหมดหรือบางส่วนสามารถเข้าถึงได้โดยมีเจตนาที่จะใช้เพื่อจุดประสงค์ในการกระทำความผิดใด ๆ ภายใต้กฎนี้

b การครอบครองรายการที่อ้างถึงในวรรคย่อย ๕ (a) (i) หรือ (ii) ข้างต้นด้วยความตั้งใจที่จะใช้อุปกรณ์ดังกล่าวเพื่อจุดประสงค์ในการกระทำความผิดใด ๆ ภายใต้ส่วนนี้โดยมีเงื่อนไขว่าจะไม่มีความรับผิดทางอาญาใด ๆ เกิดขึ้นเมื่อการใช้การผลิตการขายการจัดหาการนำเข้าการจัดจำหน่ายมิฉะนั้นทำให้มีอยู่หรือครอบครองอุปกรณ์คอมพิวเตอร์หรือข้อมูลที่อ้างถึง

ในส่วนนี้ หากมีการลงโทษอย่างใดอย่างหนึ่งที่ระบุไว้ในส่วนที่ ๔ (A) กับโครงสร้างพื้นฐานที่สำคัญ การลงโทษของการรวมชั่วคราวหรือปรับอย่างน้อยห้า Hund แดงพันเปโซ (P๕๐๐,๐๐๐.๐๐) สูงสุดเท่ากับความเสียหายสูงสุดที่เกิดขึ้น หรือทั้งสองจะถูกกำหนด

B. ความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งจะถูกลงโทษด้วยการจำคุกนายกเทศมนตรีเมืองหรือปรับอย่างน้อยสองแสนเปโซ (P๒๐๐,๐๐๐.๐๐) สูงสุดตามจำนวนที่เหมาะสมกับความเสียหายที่เกิดขึ้นหรือทั้งสองอย่างดังนี้:

๑. การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์

a. การป้อนข้อมูลการเปลี่ยนแปลงหรือการลบข้อมูลคอมพิวเตอร์ใด ๆ โดยไม่ถูกต้องส่งผลให้เกิดข้อมูลที่ไม่ได้รับอนุญาตโดยมีเจตนาที่จะพิจารณาหรือดำเนินการเพื่อวัตถุประสงค์ทางกฎหมายราวกับว่าเป็นข้อมูล จริงไม่ว่าข้อมูลนั้นจะสามารถอ่านได้หรือไม่ หรือ

b. การกระทำของการใช้ข้อมูลคอมพิวเตอร์อย่างรู้เท่าทันซึ่งเป็นผลิตภัณฑ์ของการปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์ตามที่กำหนดไว้ในที่นี้เพื่อวัตถุประสงค์ในการขยายเวลาการออกแบบที่หลอกลวงหรือไม่ซื่อสัตย์

๒. การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์ –

การป้อนข้อมูลการเปลี่ยนแปลงหรือการลบข้อมูลคอมพิวเตอร์ หรือโปรแกรมหรือการรบกวนการทำงานของระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตก่อให้เกิดความเสียหายดังนั้นด้วยเจตนาฉ้อโกง: ให้หากไม่มีความเสียหายเกิดขึ้น โทษที่เป็นโทษจะต้องลดลงหนึ่งอัตรา

๓. การขโมยข้อมูลประจำตัวที่เกี่ยวกับคอมพิวเตอร์

การได้มาการใช้การใช้ผิดวัตถุประสงค์การถ่ายโอนการครอบครองการเปลี่ยนแปลงหรือการลบข้อมูลที่ระบุว่าเป็นของผู้อื่นไม่ว่าจะเป็นทางธรรมชาติหรือทางกฎหมายโดยไม่มีสิทธิ์: มีไว้ว่าหากไม่มีความเสียหายใด ๆ imposable จะต้องลดลงหนึ่งอัตรา

C. ความผิดเกี่ยวกับเนื้อหา

๑. บุคคลใดก็ตามที่พบว่ามีความผิดฐานลามกอนาจารของเด็กจะต้องถูกลงโทษตามพระราชบัญญัติที่กำหนดไว้ในพระราชบัญญัติหมายเลข ๙๗๗๕ ของสาธารณรัฐหรือพระราชบัญญัติต่อต้านการลามกอนาจารของเด็กในปี ๒๐๐๙: มีเงื่อนไขว่าการลงโทษจะต้องเป็นหนึ่งระดับที่สูงกว่าที่กำหนดไว้ในกฎหมายสาธารณรัฐฉบับที่ ๙๗๗๕ หากกระทำผ่านระบบคอมพิวเตอร์

มาตรา ๕ อาชญากรรมอื่น ๆ - ข้อมูลต่อไปนี้เป็นความผิดทางอาญาอื่น ๆ ที่มีโทษตามพระราชบัญญัติ

๑. Cyber – squatting การได้มาซึ่งชื่อโดเมนผ่านอินเทอร์เน็ตโดยไม่สุจริตเพื่อผลกำไรทำให้เข้าใจผิด ทำลายชื่อเสียง และกีดกันผู้อื่นจากการจดทะเบียนชื่อเดียวกัน หากชื่อโดเมนนั้นเป็น

a. ที่เหมือนกันหรือคล้ายกันสับสนกับหน่วยงานของรัฐในเวลาที่ชื่อโดเมนที่มีอยู่จดทะเบียนเครื่องหมายการค้าที่มีการลงทะเบียนที่เหมาะสม;

b. สำคัญหรือในลักษณะใด ๆ ที่คล้ายกับชื่อของบุคคลอื่นที่ไม่ใช่ผู้จดทะเบียนในกรณีของชื่อส่วนบุคคล; และ

c. ได้มาโดยไม่ถูกต้องหรือมีทรัพย์สินทางปัญญาอยู่ในนั้น

๒. Cyber - squatting จะต้องถูกลงโทษด้วยการจำคุกมากกว่า ๕ ปีขึ้นไป (Prision Mayor) หรือปรับอย่างน้อยสองร้อยพันเปโซ (P๒๐๐,๐๐๐.๐๐) จนถึงจำนวนสูงสุดที่เทียบเท่ากับความเสียหายที่เกิดขึ้น หรือทั้งสองอย่าง: หากว่ามีความมุ่งมั่นต่อวิกฤตโครงสร้างพื้นฐาน, การลงโทษของการรวมชั่วคราวหรือปรับอย่างน้อยห้าร้อยพันเปโซ (P๕๐๐,๐๐๐.๐๐) ถึงจำนวนสูงสุดเทียบเท่ากับความเสียหายที่เกิดขึ้น หรือทั้งสองจะถูกกำหนด

๓. Cybersex การมีส่วนร่วมอย่างจงใจการบำรุงรักษาการควบคุมหรือการดำเนินงานไม่ว่าทางตรงหรือทางอ้อมจากการจัดแสดงนิทรรศการอวัยวะเพศหรือกิจกรรมทางเพศใด ๆ ที่มีความใคร่ด้วยความช่วยเหลือจากระบบคอมพิวเตอร์ บุคคลใดก็ตามที่พบว่ามีความผิดไซเบอร์เท็กซ์จะต้องถูกลงโทษด้วยการจำคุกนายกเทศมนตรีส่วนหนึ่ง หรือปรับอย่างน้อยสองแสนเปโซ (P๒๐๐,๐๐๐.๐๐) แต่ไม่เกินหนึ่งล้านเปโซ (P๑,๐๐๐,๐๐๐.๐๐) หรือทั้งสองอย่าง

Cybersex ที่เกี่ยวข้องกับเด็กจะถูกลงโทษตามบทบัญญัติเกี่ยวกับภาพอนาจารเด็กของพระราชบัญญัติในกรณีที่การบำรุงรักษาการควบคุมหรือการดำเนินงานของไซเบอร์เท็กซ์นั้นเป็นความผิดที่มีโทษตามพระราชบัญญัติสาธารณรัฐฉบับที่ ๙๒๐๘ ซึ่งแก้ไขเพิ่มเติมการดำเนินคดีตามพระราชบัญญัตินี้จะต้องปราศจากอคติต่อความรับผิดใด ๆ หรือกฎหมายพิเศษรวมถึง RA ฉบับที่ ๙๒๐๘ สอดคล้องกับมาตรา ๘ ในที่นี้

๔. Libel การกระทำที่ผิดกฎหมายหรือต้องห้ามของการหมิ่นประมาทตามที่กำหนดไว้ในมาตรา ๓๕๕ แห่งประมวลกฎหมายอาญาที่แก้ไขแล้ว, ๓. การหมิ่นประมาทที่แก้ไขเพิ่มเติม, ได้กระทำผ่านระบบคอมพิวเตอร์หรือวิธีการอื่นใดที่คล้ายคลึงกันซึ่งอาจมีการวางแผนในอนาคต ระยะเวลาสูงสุดในการเรียกเก็บเงินนายกเทศมนตรีในหรือปรับตั้งแต่หกพันเปโซ (P๖,๐๐๐.๐๐) จนถึงระยะเวลาขั้นต่ำสูงสุดที่กำหนดโดยศาลหรือทั้งสองนอกเหนือจากการดำเนินการทางแพ่งซึ่งอาจนำโดยฝ่ายที่ถูกละเมิด: มีให้, ว่าบทบัญญัตินี้มีผลเฉพาะกับผู้เขียนต้นฉบับของการโพสต์หรือการกลั่นแกล้งทางออนไลน์และไม่ให้กับผู้อื่นเพียงแค่ได้รับการโพสต์และตอบสนองต่อมัน

๕. other offences ความผิดอื่น ๆ การกระทำต่อไปนี้จะเป็นความผิดที่ต้องระวางโทษจำคุกไม่เกินหนึ่ง (๑) ระดับต่ำกว่าโทษที่กำหนดไว้สำหรับความผิด หรือปรับอย่างน้อยหนึ่งแสนพัน (P๑๐๐,๐๐๐.๐๐) แต่ไม่เกินห้าแสนเปโซ (P๕๐๐,๐๐๐.๐๐) หรือทั้งสอง:

A. บุคคลใดก็ตามที่จงใจสนับสนุนช่วยเหลือหรือ ก. ช่วยเหลือหรือช่วยเหลือในการกระทำความผิดทางอาญาทางการเงินในการกระทำความผิดใด ๆ ที่ระบุในพระราชบัญญัติจะต้องรับผิดเว้นแต่ในส่วนที่ ๔ (c) (๒) ในภาพอนาจารของเด็กและ ๔ (c) (๔) บน Libel ออนไลน์

B. พยายามกระทำความผิดทางอาญา - บุคคลใดที่พยายามกระทำความผิดใด ๆ ในพระราชบัญญัติโดยเจตนาจะต้องรับผิดยกเว้นส่วนที่ ๔ (c) (๒) ในสื่อลามกเด็กและ ๔ (c) (๔) บน Libel ออนไลน์

หนี้สินและการลงโทษอื่น ๆ

มาตรา ๖ ความรับผิดของบริษัท – เมื่อใดก็ตามที่การลงโทษที่กำหนดไว้ในที่นี้มีความมุ่งมั่นอย่างรู้เท่าทันในนามของหรือเพื่อประโยชน์ของนิติบุคคลโดยบุคคลธรรมดาทำหน้าที่เป็นรายบุคคล

หรือเป็นส่วนหนึ่งของอวัยวะของนิติบุคคลที่มีตำแหน่งผู้นำภายในตาม บน: (a) อำนาจการเป็นตัวแทนของนิติบุคคล; (b) อำนาจในการตัดสินใจในนามของนิติบุคคล หรือ (c) ผู้มีอำนาจ ในการควบคุมภายในนิติบุคคลให้นิติบุคคลและจะต้องรับผิดชอบค่าปรับเท่ากับค่าปรับอย่างน้อยสองเท่าที่ปรับได้ในมาตรา ๗ สูงสุดไม่เกินสิบล้านเปโซ (P๑๐,๐๐๐,๐๐๐.๐๐)

หากคณะกรรมการของการกระทำที่มีโทษใด ๆ ที่กำหนดไว้นี้เป็นไปได้เนื่องจากการขาดหรือควบคุมโดยบุคคลธรรมดาที่อ้างถึงและอธิบายไว้ในวรรคก่อน เพื่อประโยชน์ในการกำกับดูแลของนิติบุคคลโดยบุคคลธรรมดาที่ทำหน้าที่ภายใต้อำนาจของตน นิติบุคคลจะต้องรับผิดชอบค่าปรับเท่ากับอย่างน้อยสองเท่าของค่าปรับที่กำหนดไม่ได้ในมาตรา ๗ สูงสุดไม่เกิน ห้าล้านเปโซ (P๕,๐๐๐,๐๐๐.๐๐)

ความรับผิดที่กำหนดไว้ในนิติบุคคลจะต้องไม่มีอคติต่อความรับผิดทางอาญาของบุคคลธรรมดาที่ได้กระทำความผิด

มาตรา ๗ การละเมิดประมวลกฎหมายอาญาที่แก้ไขผ่านการแก้ไขโดยผ่านและการใช้ข้อมูลอาชญากรรมทั้งหมดที่กำหนดและลงโทษตามประมวลกฎหมายอาญาที่แก้ไขและเทคโนโลยีการสื่อสารที่แก้ไขเพิ่มเติม และกฎหมายอาชญากรรมพิเศษ ที่กระทำโดยผ่านและด้วยการใช้เทคโนโลยีสารสนเทศและการสื่อสารจะถูกครอบคลุมโดยบทบัญญัติที่เกี่ยวข้องของพระราชบัญญัติ: หากว่าการลงโทษจะถูกกำหนดให้เป็นหนึ่ง (๑) ระดับสูงกว่าที่กำหนดไว้โดยประมวลกฎหมายอาญาที่แก้ไขเพิ่มเติมซึ่งแก้ไขเพิ่มเติมและกฎหมายพิเศษแล้วแต่กรณี อาจจะ

มาตรา ๘ ความรับผิดตามกฎหมายอื่น - การฟ้องคดีตามพระราชบัญญัตินี้ไม่เป็นการกระทบกระเทือนต่อการละเมิดความรับผิดของบทบัญญัติใด ๆ ของประมวลกฎหมายอาญาที่แก้ไขเพิ่มเติมหรือกฎหมายพิเศษ: โดยมีเงื่อนไขว่าบทบัญญัตินี้จะไม่ใช้บังคับกับการฟ้องร้องผู้กระทำความผิดตาม (๑) ทั้งสองมาตรา ๔ (c) (๔) ของ RA ๑๐๑๗๕ และมาตรา ๓๕๓ ของประมวลกฎหมายอาญา ที่แก้ไข; และ (๒) ทั้งสองส่วน ๔ (c) (๒) ของอาร์เอ ๑๐๑๗๕ และร. ๙๗๗๕ หรือ "พระราชบัญญัติ ภาพอนาจารเด็กต่อต้านการกระทำของปี ๒๐๐๙"

หมวด ๓

การบังคับใช้และการดำเนินการ

มาตรา ๙ สำนักสืบสวนแห่งชาติ (NBI) และมาตรา ๙ เจ้าหน้าที่ผู้รักษากฎหมาย ตำรวจแห่งชาติฟิลิปปินส์ (PNP) จะต้องรับผิดชอบต่อการบังคับใช้กฎหมายที่มีประสิทธิภาพและประสิทธิผลของบทบัญญัติของพระราชบัญญัติ NBI และ PNP จะจัดหน่วยงานอาชญากรรมไซเบอร์หรือหน่วยงาน ที่จะดำเนินการโดยผู้ตรวจสอบพิเศษเพื่อจัดการเฉพาะกรณีที่เกี่ยวข้องกับการละเมิดพระราชบัญญัติ

NBI จะสร้างส่วนอาชญากรรมไซเบอร์เพื่อให้มีหัวหน้าเป็นหัวหน้าอย่างน้อยที่สุด PNP จะสร้างหน่วยต่อต้านอาชญากรรมไซเบอร์โดยอย่างน้อยผู้อำนวยการตำรวจสำนักงาน DOJ-Cybercrime (๐๐C) ที่สร้างขึ้นภายใต้พระราชบัญญัตินี้จะประสานงานความพยายามของ NBI และ PNP ในการบังคับใช้บทบัญญัติของพระราชบัญญัติ

มาตรา ๑๐ อำนาจและหน้าที่ของหน่วยงานบังคับใช้กฎหมาย - NBI และ PNP หน่วยอาชญากรรมไซเบอร์หรือส่วนแบ่งจะมีอำนาจและหน้าที่ดังต่อไปนี้:

a. ตรวจสอบอาชญากรรมทั้งหมดที่เกี่ยวข้องกับระบบคอมพิวเตอร์

b. ทำการกู้คืนข้อมูลและการวิเคราะห์ทางนิติเวชในระบบคอมพิวเตอร์และหลักฐานทางอิเล็กทรอนิกส์อื่น ๆ ที่ถูกยึด

c. กำหนดแนวทางในการตรวจสอบการกู้คืนหลักฐานทางนิติเวชและการวิเคราะห์ข้อมูลทางนิติวิทยาศาสตร์ให้สอดคล้องกับแนวปฏิบัติมาตรฐานอุตสาหกรรม

d. ให้การสนับสนุนด้านเทคโนโลยีแก่หน่วยสืบสวนภายใน PNP และ NBT รวมถึงการค้นหาการยึด การเก็บรักษาหลักฐาน และการกู้คืนข้อมูลทางนิติวิทยาศาสตร์จากสถานที่เกิดเหตุ และ

e. ระบบอาชญากรรมที่ใช้ในการก่ออาชญากรรม พัฒนาความสัมพันธ์ระหว่างภาครัฐภาคเอกชน และหน่วยงานบังคับใช้กฎหมายในการจัดการกับอาชญากรรมไซเบอร์

f. รักษาฐานข้อมูลที่จำเป็นและเกี่ยวข้องสำหรับสถิติและ/หรือวัตถุประสงค์ในการติดตามตรวจสอบ

g. พัฒนาศักยภาพภายในองค์กรเพื่อปฏิบัติหน้าที่ดังกล่าวที่จำเป็นสำหรับการบังคับใช้พระราชบัญญัติ ชั่วโมง

h. สนับสนุนการกำหนดและบังคับใช้แผนความมั่นคงทางไซเบอร์แห่งชาติ และ

i. ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัติกำหนด

มาตรา ๑๑ หน้าที่ของเจ้าหน้าที่ผู้รักษากฎหมาย – เพื่อให้มั่นใจว่าลักษณะทางเทคนิคของอาชญากรรมไซเบอร์และการป้องกันนั้นได้รับความสนใจและพิจารณาขั้นตอนที่เกี่ยวข้องกับความร่วมมือระหว่างประเทศหน่วยงานบังคับใช้กฎหมายโดยเฉพาะแผนกคอมพิวเตอร์หรือเทคโนโลยีอาชญากรรมหรือหน่วยงานที่รับผิดชอบในการสืบสวนอาชญากรรมไซเบอร์ และรายงานปกติรวมถึงการเตรียมการล่วงหน้าหลังการปฏิบัติการและผลการสอบสวนและเอกสารอื่น ๆ ที่อาจจำเป็นต้องใช้กับกระทรวงยุติธรรม (DOJ) Office of Cybercrime สำหรับการตรวจสอบและตรวจสอบ หน่วยงานบังคับใช้กฎหมายจะต้องปฏิบัติตามแนวทางคำแนะนำและกระบวนการที่ออกและประกาศใช้โดยเจ้าหน้าที่ผู้มีอำนาจในทุกเรื่องที่เกี่ยวข้องกับอาชญากรรมไซเบอร์และใช้แบบฟอร์มและแม่แบบที่กำหนดรวมถึง แต่ไม่จำกัดเพียงคำสั่งการสงวนห่วงโซ่ เพื่อค้นหายินยอมให้แสดงตัวตนของบัญชี/ออนไลน์และร้องขอการตรวจสอบทางคอมพิวเตอร์

มาตรา ๑๒ การดูแลรักษาและการเก็บรักษาข้อมูลคอมพิวเตอร์ ความสมบูรณ์ของข้อมูลการจราจรและข้อมูลสมาชิกจะต้องเก็บรักษาและเก็บรักษาไว้โดยผู้ให้บริการเป็นระยะเวลาอย่างน้อยหก (๖) เดือนนับจากวันที่ทำธุรกรรม ข้อมูลเนื้อหาจะถูกเก็บรักษาไว้ในทำนองเดียวกันเป็นเวลาหก (๖) เดือนนับจากวันที่ได้รับคำสั่งจากหน่วยงานบังคับใช้กฎหมายที่ต้องการเก็บรักษาไว้

หน่วยงานบังคับใช้กฎหมายอาจสั่งให้ขยายเวลาเพียงครั้งเดียวสำหรับอีกหก (๖) เดือน: ให้เมื่อข้อมูลคอมพิวเตอร์ที่ถูกเก็บรักษาส่งหรือจัดเก็บโดยผู้ให้บริการจะถูกใช้เป็นหลักฐานในกรณีการกระทำของบริการดังกล่าวเท่านั้น ผู้ให้บริการที่มีสำเนาเอกสารส่งต่อไปยังสำนักงานอัยการถือเป็นการแจ้งให้เก็บรักษาข้อมูลคอมพิวเตอร์ไว้จนกว่าจะมีการยุติคดีและ/หรือตามคำสั่งของศาล

แล้วแต่กรณีผู้ให้บริการที่ได้รับคำสั่งให้เก็บรักษาข้อมูลคอมพิวเตอร์จะต้องรักษาคำสั่งซื้อและการปฏิบัติตามนั้นเป็นความลับ หมวดที่ ๑๓ การรวบรวมข้อมูลคอมพิวเตอร์ หน่วยงานบังคับใช้กฎหมายเมื่อมีการออกหมายศาลจะได้รับอนุญาตให้รวบรวมหรือบันทึกโดยวิธีการทางเทคนิคหรือทางอิเล็กทรอนิกส์และ ผู้ให้บริการจะต้องรวบรวมหรือบันทึกโดยวิธีการทางเทคนิคหรือทางอิเล็กทรอนิกส์และ/หรือให้ความร่วมมือและ

มาตรา ๑๓ การรวบรวมข้อมูลคอมพิวเตอร์ หน่วยงานบังคับใช้กฎหมายเมื่อมีการออกหมายศาลจะได้รับอนุญาตให้รวบรวมหรือบันทึกโดยวิธีการทางเทคนิคหรือทางอิเล็กทรอนิกส์และผู้ให้บริการจะต้องรวบรวมหรือบันทึกโดยวิธีการทางเทคนิคหรือทางอิเล็กทรอนิกส์และ/หรือให้ความร่วมมือและช่วยเหลือในการรวบรวม หรือบันทึกข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสื่อสารที่ระบุส่งโดยระบบคอมพิวเตอร์ ศาลจะต้องออกหมายจับตามมาตรานี้ให้ออกหรือได้รับเมื่อมีการยื่นคำร้องเป็นลายลักษณ์อักษรหลังจากการตรวจสอบภายใต้คำสาบานหรือการยืนยันของผู้สมัครและพยานที่เขาสามารถผลิตได้และการแสดงว่า: (๑) มีเหตุอันควรเชื่อว่า อาชญากรรมที่แจกแจงไว้ในที่นี้มีการกระทำเกิดขึ้นหรือกำลังจะเกิดขึ้น (๒) มีเหตุอันควรเชื่อได้ว่าหลักฐานที่จะได้รับนั้นมีความสำคัญต่อความเชื่อมั่นของบุคคลใด ๆ หรือเพื่อแก้ปัญหาหรือเพื่อป้องกันอาชญากรรมดังกล่าว และ (๓) ไม่มีวิธีอื่นใดที่พร้อมสำหรับการได้รับหลักฐานดังกล่าว

มาตรา ๑๔ การเปิดเผยข้อมูลคอมพิวเตอร์ เมื่อผู้รักษากฎหมายได้รับหมายศาลจะต้องออกคำสั่งให้บุคคลหรือผู้ให้บริการเปิดเผยหรือส่งภายในเจ็ดสิบสอง (๗๒) ชั่วโมงหลังจากได้รับคำสั่งดังกล่าวข้อมูลของสมาชิกข้อมูลการจราจรหรือข้อมูลที่เกี่ยวข้องในตัวเขา/การครอบครองหรือการควบคุมที่เกี่ยวข้องกับการร้องเรียนที่ถูกต้องอย่างเป็นทางการ docketed และมอบหมายให้สอบสวนโดยหน่วยงานบังคับใช้กฎหมายและการเปิดเผยข้อมูลที่จำเป็นและเกี่ยวข้องกับวัตถุประสงค์ของการสอบสวน หน่วยงานบังคับใช้กฎหมายจะต้องบันทึกคำร้องเรียนทั้งหมดที่สาบานไว้ในระบบการเชื่อมต่ออย่างเป็นทางการ

มาตรา ๑๕ ค้นหายึดและตรวจสอบข้อมูลคอมพิวเตอร์ ในกรณีที่มีการออกหมายจับค้นหาและยึดเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมายจะต้องมีอำนาจและหน้าที่ดังต่อไปนี้: ภายในระยะเวลาที่ระบุในใบสำคัญแสดงสิทธิเพื่อทำการสกัดกั้นตามที่กำหนดไว้ในกฎนี้และไปที่:

๑. ค้นหาและยึดข้อมูลคอมพิวเตอร์

๒. รักษาความปลอดภัยระบบคอมพิวเตอร์หรือสื่อบันทึกข้อมูลคอมพิวเตอร์

๓. แม่และเก็บสำเนาของข้อมูลคอมพิวเตอร์ที่ปลอดภัย

๔. รักษาความสมบูรณ์ของข้อมูลคอมพิวเตอร์ที่เก็บไว้ที่เกี่ยวข้อง

๕. ทำการวิเคราะห์ทางนิติเวชหรือตรวจสอบสื่อบันทึกข้อมูลคอมพิวเตอร์

๖. ทำให้ไม่สามารถเข้าถึงหรือลบข้อมูลคอมพิวเตอร์เหล่านั้นในคอมพิวเตอร์ที่เข้าถึงหรือคอมพิวเตอร์และเครือข่ายการสื่อสาร

b. หน่วยงานบังคับใช้กฎหมายอาจสั่งให้บุคคลใด ๆ ที่มีความรู้เกี่ยวกับการทำงานของระบบคอมพิวเตอร์และมาตรการในการปกป้องและเก็บรักษาข้อมูลคอมพิวเตอร์ในนั้นเพื่อให้ข้อมูลที่จำเป็นเพื่อให้สามารถดำเนินการ ค้นหา การยึด และตรวจร่างกาย

c. หน่วยงานบังคับใช้กฎหมายอาจขอขยายเวลาเพื่อดำเนินการตรวจสอบสื่อบันทึกข้อมูลคอมพิวเตอร์และส่งคืนได้ แต่จะไม่นานกว่าสามสิบ (๓๐) วันนับจากวันที่ศาลอนุมัติ มาตรา ๑๖ การดูแลข้อมูลคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ทั้งหมดรวมถึงเนื้อหาและข้อมูลการจราจรที่ถูกตรวจสอบภายใต้หมายจับที่เหมาะสม

จะต้องฝากภายในศาลในบรรจุภัณฑ์ที่ปิดผนึกภายในสี่สิบแปด (๔๘) ชั่วโมง ภายใน ๔๘ ชั่วโมง โดยหนังสือรับรอง

มาตรา ๑๖ การดูแลข้อมูลคอมพิวเตอร์ – ข้อมูลคอมพิวเตอร์ทั้งหมดรวมถึงเนื้อหาและข้อมูลการจราจรที่ตรวจสอบภายใต้หมายจับที่เหมาะสมจะต้องฝากภายในศาลในภาชนะบรรจุที่ปิดผนึกภายในสี่สิบแปด (๔๘) ชั่วโมง พร้อมกับหนังสือรับรองของหน่วยงานบังคับใช้กฎหมายที่ดำเนินการระบุวันที่และเวลาที่ครอบคลุม โดยการตรวจสอบและหน่วยงานบังคับใช้กฎหมายที่อาจเข้าถึงเงินฝากท่ามกลางข้อมูลอื่น ๆ ที่เกี่ยวข้องหน่วยงานบังคับใช้กฎหมายจะต้องรับรองด้วยว่าสำเนาทั้งหมดหรือส่วนหนึ่งส่วนใดนั้นได้ถูกทำขึ้นหรือถ้าทำไว้ว่ามีการทำซ้ำหรือสำเนาทั้งหมดดังกล่าวในแพ็คเกจที่ฝากไว้กับศาล หีบห่อที่ฝากนั้นจะต้องไม่เปิดออกหรือมีการบันทึกซ้ำหรือใช้เป็นหลักฐานหรือเนื้อหาที่เปิดเผยยกเว้นตามคำสั่งของศาลซึ่งจะไม่ได้รับยกเว้นเมื่อมีการเคลื่อนไหวโดยมีการแจ้งเตือนและโอกาสที่จะได้รับ บุคคลหรือบุคคลที่มีการบันทึกการสนทนาหรือการสื่อสาร

มาตรา ๑๗ การทำลายข้อมูลคอมพิวเตอร์ เมื่อพ้นกำหนดระยะเวลาตามที่กำหนดในส่วนที่ ๑๒ และ ๑๕ หรือจนกว่าคดีจะถึงที่สุดและ/หรือตามคำสั่งของศาลแล้วแต่กรณีผู้ให้บริการและหน่วยงานบังคับใช้กฎหมายแล้วแต่กรณี จะต้องทำลายข้อมูลคอมพิวเตอร์ในทันทีที่ถูกเก็บรักษาและตรวจสอบคำสั่งหรือรับประกัน

มาตรา ๑๘ กฎพิเศษ หลักฐานใด ๆ ที่ได้รับโดยไม่มีหมายจับที่ถูกต้องหรือเกินอำนาจของสิ่งเดียวกันจะไม่สามารถยอมรับได้สำหรับการดำเนินการใด ๆ ต่อหน้าศาลหรือศาลใด ๆ กฎของศาลจะมีการใช้งานเพิ่มเติมในการดำเนินการตามพระราชบัญญัติ

มาตรา ๑๙ การไม่ปฏิบัติตาม - ไม่ปฏิบัติตามบทบัญญัติในหมวดที่สี่ของพระราชบัญญัติและกฎ ๗ และ ๘ ของหมวดที่ ๗ นี้ โดยเฉพาะคำสั่งจากหน่วยงานบังคับใช้กฎหมายจะต้องถูกลงโทษตามคำสั่งของประธานาธิบดีหมายเลข ๑๘๒๙ (มีชื่อว่า "การขัดขวางการลงโทษในฐานะที่เป็นความเข้าใจและการฟ้องร้องคดีอาญา") โดยจำคุกระยะเวลาสูงสุด หรือปรับหนึ่งแสนเปโซ (P๑๐๐,๐๐๐.๐๐) หรือทั้งสองอย่างสำหรับการไม่ปฏิบัติตามคำสั่งของเจ้าหน้าที่ผู้รักษากฎหมาย

มาตรา ๒๐ ขอบเขตของความรับผิดของผู้ให้บริการ ยกเว้นที่ระบุไว้เป็นอย่างอื่นในมาตรานี้ไม่มีบุคคลหรือภาคีจะต้องรับผิดทางแพ่งหรือทางอาญาใด ๆ ที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ที่บุคคลหรือฝ่ายที่ทำหน้าที่เป็นผู้ให้บริการเพียงการเข้าถึงหากความรับผิดดังกล่าวเกิดขึ้นเมื่อ:

a. ภาระผูกพันและความรับผิดของคู่กรณีภายใต้ข้อมูลคอมพิวเตอร์

b. การเผยแพร่ตีพิมพ์หรือแจกจ่ายข้อมูลคอมพิวเตอร์ดังกล่าวหรือคำแถลงใด ๆ ที่ทำขึ้นในข้อมูลคอมพิวเตอร์ดังกล่าวรวมถึงการละเมิดสิทธิ์ในการให้สิทธิ์ในหรือที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ดังกล่าว: โดยมีเงื่อนไขว่า:

๑. ผู้ให้บริการไม่มีจริง ความรู้หรือไม่ตระหนักถึงข้อเท็จจริงหรือสถานการณ์ที่ปรากฏว่าการเผยแพร่ตีพิมพ์หรือเผยแพร่เนื้อหาดังกล่าวนั้นผิดกฎหมายหรือเป็นการละเมิดสิทธิ์ใด ๆ ที่มีอยู่ในหรือเกี่ยวข้องกับเนื้อหาดังกล่าว

๒. ผู้ให้บริการไม่ได้รับผลประโยชน์ทางการเงินโดยตรงจากกิจกรรมที่ผิดกฎหมายหรือละเมิด; และ

๓. ผู้ให้บริการไม่กระทำการละเมิดใด ๆ หรือการกระทำที่ผิดกฎหมายโดยตรงไม่ชักจูงหรือทำให้บุคคลหรือพรรคอื่นกระทำการละเมิดหรือการกระทำที่ผิดกฎหมายอื่น ๆ และ/หรือ ไม่ได้รับผลประโยชน์ทางการเงินโดยตรงจากกิจกรรมที่ละเมิดหรือการกระทำที่ผิดกฎหมายของบุคคลหรือพรรคอื่น: ให้เพิ่มเติมไม่มีอะไรในส่วนนี้จะมีผล

i. ภาระผูกพันใด ๆ ที่เกิดขึ้นจากสัญญา

ii. ภาระหน้าที่ของผู้ให้บริการภายใต้การออกใบอนุญาตหรือระบอบการปกครองอื่น ๆ ที่จัดตั้งขึ้นภายใต้กฎหมาย

iii. ภาระผูกพันใด ๆ ที่กำหนดภายใต้กฎหมายใด ๆ หรือ

iv. ความรับผิดทางแพ่งของฝ่ายใดฝ่ายหนึ่งในกรณีที่ความรับผิดดังกล่าวเป็นพื้นฐานสำหรับการบรรเทาความเสียหายโดยศาลซึ่งออกโดยกฎหมายใด ๆ ที่กำหนดให้ผู้ให้บริการใช้ หรือละเว้นจากการกระทำที่จำเป็นในการลบบล็อกหรือปฏิเสธการเข้าถึงข้อมูลคอมพิวเตอร์ใด ๆ เก็บรักษาหลักฐานการละเมิดกฎหมาย

หมวด ๔

เขตอำนาจศาล

มาตรา ๒๑ เขตอำนาจศาล – ศาลพิจารณาคดีส่วนภูมิภาคจะมีเขตอำนาจศาลเหนือการฝ่าฝืนบทบัญญัติของพระราชบัญญัติรวมถึงการฝ่าฝืนโดยสาธารณรัฐฟิลิปปินส์ โดยไม่คำนึงถึงสถานที่ของคณะกรรมาธิการ เขตอำนาจศาลจะต้องอยู่ภายใต้องค์ประกอบใด ๆ ที่เกิดขึ้นภายในสาธารณรัฐฟิลิปปินส์หรือกระทำการใช้ระบบคอมพิวเตอร์ใด ๆ ที่ตั้งอยู่ทั้งหมดหรือบางส่วนในประเทศหรือเมื่อคณะกรรมาธิการดังกล่าวเกิดความเสียหายใด ๆ ต่อบุคคลธรรมดาหรือนิติบุคคลที่ในเวลาที่มีการกระทำความผิดเกิดขึ้นในฟิลิปปินส์

มาตรา ๒๒ สถานที่ - การดำเนินการทางอาญาสำหรับการละเมิดพระราชบัญญัติอาจถูกยื่นต่อ RTC ของจังหวัดหรือเมืองที่อาชญากรรมไซเบอร์หรือองค์ประกอบใด ๆ ของมันมีการกระทำหรือในกรณีที่ส่วนใดส่วนหนึ่งของระบบคอมพิวเตอร์ที่ใช้อยู่หรือในกรณีที่ความเสียหาย บุคคลธรรมดาหรือนิติบุคคลเกิดขึ้นโดยมีเงื่อนไขว่าศาลที่มีการฟ้องคดีอาญาครั้งแรกจะได้รับเขตอำนาจศาลในการยกเว้นศาลอื่น

หมวด ๒๓ การกำหนดของศาลอาชญากรรม – จะมีการกำหนดศาลอาชญากรรมทางไซเบอร์พิเศษ ซึ่งจัดการโดยผู้พิพากษาที่ได้รับการฝึกอบรมมาเป็นพิเศษเพื่อจัดการคดีอาชญากรรมทางไซเบอร์

หมวด ๒๔ การแต่งตั้งอัยการพิเศษและนักลงทุน กำหนดอัยการและผู้ตรวจสอบ ซึ่งประกอบด้วย กองกำลังฝ่ายอัยการหรือหน่วยงานภายใต้สำนักงาน DOJ-Cybercrime ซึ่งจะจัดการกับคดีไซเบอร์ในกรณีที่ฝ่าฝืนพระราชบัญญัติ

หมวด ๕
ความร่วมมือระหว่างประเทศ

มาตรา ๒๕ ความร่วมมือระหว่างประเทศ ความร่วมมือในเรื่องคดีอาญาและการที่ตกลงกันบนพื้นฐานของกฎหมายที่เป็นรูปแบบเดียวกันหรือซึ่งกันและกันและกฎหมายในประเทศจะได้รับการบังคับและผลอย่างเต็มที่ในขอบเขตที่กว้างที่สุดเท่าที่เป็นไปได้เพื่อวัตถุประสงค์ในการสอบสวนหรือดำเนินคดี เครื่องมือระหว่างประเทศที่เกี่ยวข้องในระดับนานาชาติ เพื่อรวบรวมหลักฐานทางอิเล็กทรอนิกส์ของอาชญากรรม กรมสรรพสามิตจะร่วมมือและให้ความช่วยเหลือแก่ภาคีผู้ทำสัญญาอื่น ๆ รวมทั้งขอความช่วยเหลือจากต่างประเทศ เพื่อวัตถุประสงค์ในการตรวจจับการสอบสวนและดำเนินคดีความผิดที่ได้รับการกล่าวถึงในพระราชบัญญัติและในการรวบรวมพยานหลักฐานในรูปแบบอิเล็กทรอนิกส์หลักการที่มีอยู่ในพระราชกฤษฎีกาประธานาธิบดีหมายเลข ๑๐๖๙ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง รวมถึงการส่งผู้ร้ายข้ามแดนและสนธิสัญญาความช่วยเหลือทางกฎหมายที่มีอยู่ให้ใช้บังคับในเรื่องนี้ ผู้มีอำนาจส่วนกลางจะต้อง:

a. ให้ความช่วยเหลือแก่รัฐที่ร้องขอในการรวบรวมข้อมูลการจราจรตามเวลาจริงที่เกี่ยวข้องกับการสื่อสารที่ระบุในประเทศที่ส่งผ่านระบบคอมพิวเตอร์ด้วยความเคารพต่อความผิดทางอาญาที่กำหนดไว้ในพระราชบัญญัติ ซึ่งการรวบรวมข้อมูลจราจรแบบเรียลไทม์ ที่มีอยู่ภายใต้บทบัญญัติของหมวด ๑๓ นี้

b. ให้ความช่วยเหลือแก่รัฐผู้ร้องขอในการรวบรวมบันทึกแบบเรียลไทม์หรือสกัดกั้นข้อมูลเนื้อหาของการสื่อสารที่ระบุที่ส่งผ่านระบบคอมพิวเตอร์ภายใต้เงื่อนไข บทบัญญัติของหมวด ๑๓

c. อนุญาตให้รัฐอื่น:

๑. เข้าถึงข้อมูลคอมพิวเตอร์ที่จัดเก็บแบบสาธารณะที่มีอยู่ในประเทศหรือที่อื่น ๆ หรือ

๒. เข้าถึงหรือรับผ่านระบบคอมพิวเตอร์ที่ตั้งอยู่ในประเทศข้อมูลคอมพิวเตอร์ที่เก็บอยู่ในประเทศ อื่นหากรัฐอื่นได้รับความยินยอมทางกฎหมายและความสมัครใจของบุคคลที่มีอำนาจตามกฎหมายในการเปิดเผยข้อมูลไปยังรัฐอื่น ๆ ดังกล่าว ผ่านระบบคอมพิวเตอร์นั้น

d. รับคำร้องขอจากรัฐอื่นเพื่อให้มีคำสั่งหรือขอรับการเก็บรักษาข้อมูลอย่างเร่งด่วนด้วยระบบคอมพิวเตอร์ที่ตั้งอยู่ภายในประเทศ ซึ่งสัมพันธ์กับที่รัฐผู้ร้องขอจะต้องยื่นคำร้องขอความช่วยเหลือซึ่งกันและกันสำหรับการค้นหาหรือการเข้าถึงที่คล้ายกัน หรือการรักษาความปลอดภัยที่คล้ายกันหรือการเปิดเผยข้อมูลคอมพิวเตอร์ที่จัดเก็บ: ให้ที่:

๑. คำขอเก็บรักษาข้อมูลในส่วนนี้จะต้องระบุ:

I. ผู้มีอำนาจในการค้นหาการเก็บรักษา;

II. ความผิดที่เป็นเรื่องของการสอบสวนทางอาญาหรือการดำเนินคดีและสรุปโดยย่อของข้อเท็จจริงที่เกี่ยวข้อง

III. ข้อมูลคอมพิวเตอร์ซึ่งปกป้องไว้และเกี่ยวข้องกับความผิดนั้น;

IV. ความจำเป็นของการเก็บรักษา; และ

V. ให้รัฐผู้ร้องขอส่งคำร้องขอความช่วยเหลือซึ่งกันและกัน สำหรับการค้นหาหรือการเข้าถึงการยึดหรือการรักษาความปลอดภัยที่คล้ายกันหรือการเปิดเผยข้อมูลคอมพิวเตอร์ที่เก็บไว้

๒. เมื่อได้รับการร้องขอจากรัฐอื่นหน่วยงาน DOJ และหน่วยงานบังคับใช้กฎหมายจะใช้มาตรการที่เหมาะสมทั้งหมดในการเก็บรักษาข้อมูลที่ระบุอย่างรวดเร็วตามกฎหมายและกฎหมายอื่น ๆ ที่เกี่ยวข้อง เพื่อวัตถุประสงค์ในการตอบสนองต่อการร้องขอเพื่อการสงวนรักษาความผิดทางอาญาคู่จะไม่จำเป็นต้องเป็นเงื่อนไข;

๓. คำขอการสงวนอาจถูกปฏิเสธได้ก็ต่อเมื่อ:

i. คำร้องขอเกี่ยวข้องกับความผิดที่รัฐบาลฟิลิปปินส์ถือว่าเป็นความผิดทางการเมืองหรือความผิดที่เกี่ยวข้องกับความผิดทางการเมือง หรือ

ii. รัฐบาลฟิลิปปินส์ถือว่าการดำเนินการตามคำขอนั้นมีอคติต่ออำนาจอธิปไตยความมั่นคง ความสงบเรียบร้อยของประชาชน หรือผลประโยชน์ของชาติอื่น ๆ

๔. ในกรณีที่รัฐบาลฟิลิปปินส์เชื่อว่าการเก็บรักษาจะไม่รับประกันความพร้อมใช้งานของข้อมูลในอนาคตหรือจะคุกคามความลับหรืออคติต่อการสอบสวนของรัฐที่ร้องขอประเทศนั้นจะต้องแจ้งให้รัฐผู้ร้องขอทราบโดยพลัน รัฐผู้ร้องขอจะพิจารณาว่าควรดำเนินการตามคำขอหรือไม่; และ

๕. การเก็บรักษาใด ๆ ที่มีผลในการตอบสนองต่อคำขอที่อ้างถึงในวรรค (d) จะต้องเป็นระยะเวลาไม่น้อยกว่าหกสิบ (๖๐) วัน เพื่อให้รัฐที่ร้องขอส่งการร้องขอสำหรับการค้นหาหรือการเข้าถึงที่คล้ายกัน หรือการรักษาความปลอดภัยที่คล้ายกันหรือการเปิดเผยข้อมูล หลังจากได้รับคำขอดังกล่าวแล้วข้อมูลจะยังคงถูกเก็บไว้ต่อไปเพื่อรอการตัดสินใจเกี่ยวกับคำขอนั้น

e. รองรับการร้องขอจากรัฐอื่นเพื่อค้นหาเข้าถึงยึดปลอดภัยหรือเปิดเผยข้อมูลที่จัดเก็บ โดยระบบคอมพิวเตอร์ที่ตั้งอยู่ภายในประเทศรวมถึงข้อมูลที่ถูกเก็บรักษาไว้ภายใต้ส่วนย่อย ก่อนหน้ารัฐบาลฟิลิปปินส์จะตอบสนองต่อคำร้องขอผ่านการใช้แอประหว่างประเทศการจัดการและกฎหมายที่เหมาะสมและเป็นไปตามกฎต่อไปนี้:

๑) คำขอจะได้รับการตอบกลับอย่างเร่งด่วนเมื่อ:

ii. เครื่องมือการจัดการและกฎหมายที่อ้างถึงในวรรค (b) ของหมวดนี้มิฉะนั้นให้ทำตามกันอย่างเร่งด่วน

๒) รัฐที่ร้องขอจะต้องรักษาความลับของข้อเท็จจริงหรือเรื่องที่ขอความช่วยเหลือและความร่วมมือ มันอาจใช้ข้อมูลที่ร้องขอภายใต้เงื่อนไขที่ระบุไว้ในการอนุญาต

f. ขอความช่วยเหลือจากต่างประเทศเพื่อขอความช่วยเหลือในการตรวจสอบสอบสวนและดำเนินคดีกับความผิดที่อ้างถึงในพระราชบัญญัติ

g. ความผิดทางอาญาที่อธิบายไว้ในบทที่สองของพระราชบัญญัติจะถูกพิจารณาว่าเป็นความผิดที่ส่งผู้ร้ายข้ามแดนในสนธิสัญญาส่งผู้ร้ายข้ามแดนใด ๆ ที่ฟิลิปปินส์เป็นภาคี: โดยมีเงื่อนไขว่าการกระทำนั้นมีโทษภายใต้กฎหมายของทั้งสองฝ่าย ระยะเวลาขั้นต่ำอย่างน้อยหนึ่งปีหรือโดยการลงโทษที่รุนแรงมากขึ้น ให้รัฐมนตรีว่าการกระทรวงยุติธรรมกำหนดคำแนะนำของรัฐที่เหมาะสม เพื่อจัดการเรื่องความร่วมมือระหว่างประเทศตามที่กำหนดไว้ในกฎนี้

หมวด ๖
เจ้าหน้าที่ผู้มีอำนาจ

มาตรา ๒๖ ศูนย์สืบสวนและประสานงานอาชญากรรมไซเบอร์ องค์ประกอบ - หน่วยงานระหว่างหน่วยงานที่รู้จักกันในชื่อศูนย์สอบสวนและประสานงานอาชญากรรมไซเบอร์ (CICC) ภายใต้การควบคุมดูแลของสำนักงานอธิการบดีจัดตั้งขึ้น เพื่อประสานนโยบายระหว่างหน่วยงานที่เกี่ยวข้องและเพื่อกำหนดและบังคับใช้แผนรักษาความปลอดภัยไซเบอร์แห่งชาติเป็นหัวหน้า โดยผู้อำนวยการบริหารสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร ภายใต้กรมวิทยาศาสตร์และเทคโนโลยี (ICTO-DOST) ในฐานะประธาน; ผู้อำนวยการ NBI ในฐานะรองประธาน; และหัวหน้า PNP หัวหน้าสำนักงาน DOJ ของอาชญากรรมไซเบอร์ และตัวแทนหนึ่ง (๑) คน จากภาคเอกชนองค์กรพัฒนาเอกชนและสถาบันการศึกษาในฐานะสมาชิก

สมาชิก CICC จะถูกจัดตั้งขึ้นเป็นคณะกรรมการบริหารและได้รับการสนับสนุนจากสำนักเลขาธิการ โดยเฉพาะอย่างยิ่งสำหรับอาชญากรรมไซเบอร์การบริหารและการรักษาความปลอดภัยทางไซเบอร์ สำนักเลขาธิการ จะต้องจัดการจากบุคลากรที่มีอยู่หรือตัวแทนของหน่วยงานที่มีส่วนร่วมของ CICC CICC อาจขอความช่วยเหลือจากหน่วยงานอื่น ๆ ของรัฐบาลรวมถึงบริษัทที่รัฐบาลเป็นเจ้าของและที่ควบคุมแล้วและต่อไปนี้:

a. สำนักตรวจคนเข้าเมือง;
b. สำนักงานปราบปรามยาเสพติดของฟิลิปปินส์
c. สำนักศุลกากร
d. บริการฟ้องร้องแห่งชาติ;
e. สภาต่อต้านการฟอกเงิน
f. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
g. คณะกรรมการกิจการโทรคมนาคมแห่งชาติ; และ
h. สำนักงานหน่วยงานและ/หรือหน่วยงานอื่น ๆ ดังกล่าวตามที่จำเป็น

สำนักงาน DOJ of Cybercrime จะทำหน้าที่เป็นศูนย์ปฏิบัติการไซเบอร์อาชญากรรมของ CICC และจะส่งรายงานเป็นระยะให้แก่ CICC การมีส่วนร่วมและการเป็นตัวแทนในสำนักเลขาธิการและ/หรือศูนย์ปฏิบัติการไม่ต้องการการมีอยู่จริง แต่อาจทำได้ผ่านโหมดอิเล็กทรอนิกส์ เช่น อีเมล การประชุมทางเสียงและภาพ และอื่น ๆ

มาตรา ๒๗ อำนาจและหน้าที่ - CICC จะมีอำนาจและหน้าที่ดังต่อไปนี้:

a. กำหนดแผนความปลอดภัยทางไซเบอร์แห่งชาติ และขยายความช่วยเหลือในทันทีเพื่อระงับการกระทำความผิดเกี่ยวกับอาชญากรรมไซเบอร์แบบเรียลไทม์ ผ่านทีมรับมือเหตุฉุกเฉินทางคอมพิวเตอร์ (CERT)

b. ประสานงานการจัดทำมาตรการที่เหมาะสมและมีประสิทธิภาพในการป้องกันและปราบปรามกิจกรรมอาชญากรรมไซเบอร์ตามที่กำหนดไว้ในพระราชบัญญัติ

c. ตรวจสอบกรณีอาชญากรรมทางไซเบอร์ที่ถูกจัดการโดยหน่วยงานบังคับใช้กฎหมายและการดำเนินคดีที่เข้าร่วม

d. อำนวยความสะดวกในการร่วมมือระหว่างประเทศด้านข่าวกรองการสืบสวน การฝึกอบรมและการเพิ่มขีดความสามารถที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์ การปราบปราม และการดำเนินคดีผ่านทางสำนักงาน DOJ - Cybercrime

e. ประสานงานการสนับสนุนและการมีส่วนร่วมของภาคธุรกิจหน่วยงานปกครองส่วนท้องถิ่นและ NGOS ในโครงการป้องกันอาชญากรรมไซเบอร์และโครงการอื่น ๆ ที่เกี่ยวข้อง

f. แนะนำการออกกฎหมายที่เหมาะสมการออกมาตรการและนโยบายที่เหมาะสม

g. Call ให้หน่วยงานของรัฐใด ๆ ให้ความช่วยเหลือในการบรรลุภารกิจและหน้าที่ของ CICC; การประสานงาน

h. จัดทำและดำเนินโครงการเพื่อสร้างความตระหนักในชุมชนเกี่ยวกับการป้องกันอาชญากรรมไซเบอร์กับหน่วยงานบังคับใช้กฎหมาย และผู้มีส่วนได้เสีย และ

I. ดำเนินการอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์รวมถึงการเสริมสร้างขีดความสามารถและหน้าที่และหน้าที่อื่น ๆ ตามที่จำเป็นเพื่อการดำเนินการตามพระราชบัญญัติ

มาตรา ๒๘ กระทรวงยุติธรรม (DOJ); หน้าที่และหน้าที่ - DOJ-Office of Cybercrime (OOC) ซึ่งได้รับมอบหมายให้เป็นหน่วยงานกลางในทุกเรื่องที่เกี่ยวข้องกับความช่วยเหลือ และการส่งผู้ร้ายข้ามแดนระหว่างประเทศและศูนย์ปฏิบัติการไซเบอร์อาชญากรรมของ CICC จะมีหน้าที่และหน้าที่ดังต่อไปนี้:

A. ทำหน้าที่เป็นเจ้าหน้าที่ผู้มีอำนาจสำหรับคำร้องขอความช่วยเหลือทั้งหมดเพื่อการสอบสวนหรือดำเนินคดีเกี่ยวกับอาชญากรรมทางอินเทอร์เน็ต อำนวยความสะดวกในการให้คำแนะนำทางกฎหมาย หรือทางเทคนิคการเก็บรักษา และการผลิตข้อมูลการรวบรวมพยานหลักฐานการให้ข้อมูลทางกฎหมาย

B. ดำเนินการเกี่ยวกับการร้องเรียน/การอ้างอิง และทำให้เกิดการสอบสวน และดำเนินคดีกับอาชญากรรมไซเบอร์ และการละเมิดอื่น ๆ ของพระราชบัญญัติ

C. ออกคำสั่งการสงวนรักษาที่ส่งถึงผู้ให้บริการ d ดูแลคำสาบานออกหมายเรียกพยานและหมายเรียกพยาน เพื่อให้ปรากฏในการสอบสวนหรือการดำเนินคดีทางอาชญากรรมไซเบอร์

E. ต้องมีการส่งรายงานที่ทันเวลา และสม่ำเสมอรวมถึงการเตรียมการล่วงหน้าหลังการผ่าตัดและผลการสอบสวนและเอกสารอื่น ๆ จาก PNP และ NBI สำหรับการติดตามและตรวจสอบ:

F. ตรวจสอบการปฏิบัติตามของผู้ให้บริการด้วยบทบัญญัติของหมวดที่ ๔ ของพระราชบัญญัติและกฎข้อ ๗ และ ๘ ในที่นี้

G. อำนวยความสะดวกในการร่วมมือระหว่างประเทศกับหน่วยงานบังคับใช้กฎหมายอื่น ๆ เกี่ยวกับข่าวกรองการสืบสวนการฝึกอบรม และการเสริมสร้างศักยภาพที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์การปราบปราม และการดำเนินคดี

H. แนวทางการออกและประกาศใช้คำแนะนำ และขั้นตอนในทุกเรื่องที่เกี่ยวข้องกับการสืบสวนอาชญากรรมไซเบอร์ การกู้หลักฐานทางนิติเวช และการวิเคราะห์ข้อมูลทางนิติวิทยาศาสตร์ที่สอดคล้องกับมาตรฐานอุตสาหกรรม

I. กำหนดรูปแบบและเทมเพลตรวมถึง แต่ไม่จำกัดเพียงการรักษาคำสั่งห่วงโซ่การดูแล ยินยอมให้ค้นหายินยอมให้แสดงตัวตนของบัญชี/ออนไลน์ และขอการตรวจสอบทางคอมพิวเตอร์

J. ปฏิบัติตามหน้าที่และความรับผิดชอบเฉพาะของ DOJ ที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ภายใต้กฎหมาย และระเบียบข้อบังคับของสาธารณรัฐที่บังคับใช้ฉบับที่ ๙๗๗๕ หรือพระราชบัญญัติต่อต้านการลามกอนาจารเด็ก ๒๕๕๒; และ

K. ปฏิบัติการอื่น ๆ ที่จำเป็นสำหรับการดำเนินการตามพระราชบัญญัติ

มาตรา ๒๙ คอมพิวเตอร์ฉุกเฉินทีมรับมือ (CERT) - สำนักงาน DOST-ICT จะต้องจัดตั้งและดำเนินงานทีมรับมือเหตุฉุกเฉินทางคอมพิวเตอร์ (CERT) ที่จะทำหน้าที่เป็นผู้ประสานงานกิจกรรมที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ รวมถึง แต่ไม่จำกัดเพียงหน้าที่และหน้าที่ดังต่อไปนี้:

a. ขยายความช่วยเหลือโดยทันทีไปยัง CICC เพื่อปฏิบัติตามคำสั่งภายใต้พระราชบัญญัติที่เกี่ยวข้องกับเรื่องที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์และแผนความมั่นคงทางไซเบอร์แห่งชาติ

b. คำแนะนำและขั้นตอนการออกคำแนะนำและขั้นตอนในทุกเรื่องที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์และแผนความมั่นคงทางไซเบอร์แห่งชาติ

c. อำนวยความสะดวกระหว่างประเทศกับหน่วยงานด้านความปลอดภัยอื่น ๆ ในด้านปัญญา การฝึกอบรม และการเสริมสร้างศักยภาพที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ และ

d. ทำหน้าที่เป็นจุดรวมสำหรับทุกกรณีของเหตุการณ์ความปลอดภัยทางไซเบอร์ โดย

๑. ให้การวิเคราะห์ทางเทคนิคของเหตุการณ์ความปลอดภัยของคอมพิวเตอร์

๒. ช่วยเหลือผู้ใช้ในการรายงานการละเมิดที่เพิ่มขึ้นไปยังฝ่ายที่เกี่ยวข้อง

๓. ดำเนินการวิจัยและพัฒนาเกี่ยวกับภัยคุกคามที่เกิดขึ้นกับความปลอดภัยของคอมพิวเตอร์

๔. การออกคำเตือนและคำแนะนำที่เกี่ยวข้องกับภัยคุกคามที่เกิดขึ้นกับความปลอดภัย ของคอมพิวเตอร์

๕. ประสานงานการตอบสนองเหตุการณ์ความปลอดภัยทางไซเบอร์กับบุคคลที่สามที่เชื่อถือได้ในระดับชาติและระดับนานาชาติ และ

๖. ดำเนินการฝึกอบรมด้านเทคนิคเกี่ยวกับความปลอดภัยทางไซเบอร์ และหัวข้อที่เกี่ยวข้อง ตำรวจแห่งชาติฟิลิปปินส์ และสำนักงานสืบสวนแห่งชาติ จะทำหน้าที่เป็นหน่วยปฏิบัติการภาคสนามของ CERT CERT อาจขอความช่วยเหลือจากหน่วยงานภาครัฐอื่น ๆ เพื่อทำหน้าที่ CERT

หมวด ๗
หน้าที่ของผู้ให้บริการ

มาตรา ๓๐ หน้าที่ของผู้ให้บริการ - หน้าที่ของผู้ให้บริการดังต่อไปนี้:

a. รักษาความสมบูรณ์ของข้อมูลการจราจรและข้อมูลสมาชิกเป็นเวลาหลายเดือนนับจากวันที่ทำธุรกรรม; ระยะเวลาขั้นต่ำหก (๖)

b. รักษาความถูกต้องของข้อมูลเนื้อหาเป็นเวลาหก (๖) เดือน นับจากวันที่ได้รับคำสั่งจากหน่วยงานบังคับใช้กฎหมายหรือเจ้าหน้าที่ผู้มีอำนาจที่ต้องการสงวนรักษา

c. รักษาความถูกต้องของข้อมูลคอมพิวเตอร์เป็นระยะเวลานานหก (๖) เดือน นับจากวันที่ได้รับคำสั่งจากหน่วยงานบังคับใช้กฎหมายหรือเจ้าหน้าที่ผู้มีอำนาจที่ต้องการยืดเวลาการเก็บรักษา

d. รักษาความถูกต้องของข้อมูลคอมพิวเตอร์จนกว่าคดีจะถึงที่สุดและ/หรือตามคำสั่งของศาลแล้วแต่กรณี เมื่อได้รับสำเนาของเอกสารส่งต่อสำนักงานอัยการ

e. รับรองความลับของคำสั่งการเก็บรักษาและการปฏิบัติตาม;

f. รวบรวมหรือบันทึกโดยวิธีการทางเทคนิคหรือทางอิเล็กทรอนิกส์และ/หรือร่วมมือและช่วยเหลือด้านการบังคับใช้กฎหมายหรือเจ้าหน้าที่ผู้มีอำนาจในการรวบรวมหรือบันทึกข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการสื่อสารที่ระบุที่ส่งโดยระบบคอมพิวเตอร์ตามส่วนที่ ๑๓

g. เปิดเผยหรือส่งข้อมูลของสมาชิกข้อมูลการจราจรหรือข้อมูลที่เกี่ยวข้องในการครอบครองหรือการควบคุมของเขาต่อการบังคับใช้กฎหมายหรือเจ้าหน้าที่ผู้มีอำนาจภายในเจ็ดสิบสอง (๗๒) ชั่วโมง หลังจากได้รับคำสั่งและ/หรือสำเนาของหมายศาล;

h. รายงานการปฏิบัติตาม DOJ-Office ของอาชญากรรมไซเบอร์ตามบทบัญญัติของหมวดที่ ๔ ของพระราชบัญญัติและกฎข้อ ๗ และ ๘ ในที่นี้;

I. ทำลายข้อมูลคอมพิวเตอร์ในทันทีที่มีการเก็บรักษา และตรวจสอบทันทีหลังจากสิ้นสุดระยะเวลาที่กำหนดไว้ในมาตรา ๑๓ และ ๑๕ ของพระราชบัญญัติ และ

J. ปฏิบัติหน้าที่อื่นตามที่จำเป็น และเหมาะสมเพื่อให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัติ

มาตรา ๓๑ หน้าที่ของผู้ให้บริการในกรณีภาพอนาจารเด็ก - สอดคล้องกับ RA ๙๗๗๕ หรือ “พระราชบัญญัติภาพอนาจารเด็กต่อต้านปี ๒๐๐๙” ต่อไปนี้ เป็นหน้าที่ของผู้ให้บริการในกรณีภาพลามกอนาจารของเด็ก:

๑. ผู้ให้บริการอินเทอร์เน็ต (ISP) /โฮสต์เนื้อหาอินเทอร์เน็ต ต้องติดตั้งเทคโนโลยีโปรแกรมหรือซอฟต์แวร์ที่มีอยู่ เช่น แต่ไม่จำกัดเฉพาะระบบ/เทคโนโลยีที่สร้างมูลค่าแฮชหรือการคำนวณที่คล้ายคลึงกันใด ๆ เพื่อให้แน่ใจว่าการเข้าถึงหรือการส่งผ่านของสื่อลามกอนาจารเด็กรูปแบบใด ๆ จะถูกบล็อกหรือกรอง

๒. ผู้ให้บริการจะต้องแจ้งเจ้าหน้าที่ผู้มีอำนาจตามกฎหมายทันทีภายในเจ็ด (๗) วันนับจากวันที่ข้อเท็จจริงและสถานการณ์ที่เกี่ยวข้องกับสื่อลามกอนาจารเด็กรูปแบบใด ๆ ที่ผ่านหรือมีความมุ่งมั่นในระบบของพวกเขา และ

๓. ผู้ให้บริการหรือบุคคลใด ๆ ที่ครอบครองข้อมูลการจราจรหรือข้อมูลของสมาชิกจะต้องแจ้งรายละเอียดของผู้ใช้ที่ได้รับหรือเข้าร่วม เพื่อเข้าถึงอินเทอร์เน็ตที่มีรูปแบบใด ๆ ตามคำขอของหน่วยงานบังคับใช้กฎหมายหรือเจ้าหน้าที่ผู้มีอำนาจ ของภาพอนาจารเด็ก ISPS จะเก็บรักษาบันทึกข้อมูลลูกค้า โดยเฉพาะเวลาแหล่งกำเนิดและปลายทางของการเข้าถึง เพื่อวัตถุประสงค์ในการตรวจสอบและดำเนินคดีโดยหน่วยงานที่เกี่ยวข้องภายใต้ส่วนที่ ๙ และ ๑๑ ของอาร์เอ ๙๗๗๕

หมวด ๘
แบบฟอร์มและขั้นตอนที่กำหนดไว้

มาตรา ๓๒ แบบฟอร์มและขั้นตอนที่กำหนดไว้ - สำนักงาน DOJ ของไซเบอร์ครอสจะออกและประกาศแนวทางคำแนะนำและขั้นตอนในทุกเรื่องที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ การสอบสวนการกู้หลักฐานทางนิติวิทยาศาสตร์และการวิเคราะห์ข้อมูลทางนิติเวชที่สอดคล้องกับแนวปฏิบัติสากลที่ดีที่สุด

ตามหมวด ๒๘ (h) และ (i) ของที่นี้ มันจะต้องกำหนดรูปแบบและแม่แบบ เช่น แต่ไม่จำกัดเพียงคำสั่งการเก็บรักษาห่วงโซ่การดูแลยินยอมให้ทำการค้นหายินยอมให้รับข้อมูลบัญชี/ออนไลน์ร้องขอความช่วยเหลือทางนิติเวชคอมพิวเตอร์

หมวด ๙
ข้อกำหนดขั้นสุดท้าย

มาตรา ๓๓ การจัดสรร - จำนวนเงินห้าสิบล้านเปโซ (P๕๐,๐๐๐,๐๐๐.๐๐) จะถูกจัดสรรเป็นประจำทุกปี เพื่อการดำเนินการตามพระราชบัญญัติภายใต้การจัดการทางการเงินของสำนักงาน DOJ ของอาชญากรรมไซเบอร์

มาตรา ๓๔ หากข้อกำหนดใด ๆ ของกฎเหล่านี้ไม่ถูกต้อง บทบัญญัติอื่น ๆ ที่ไม่ได้รับผลกระทบจะยังคงมีผลบังคับใช้อย่างสมบูรณ์

มาตรา ๓๕ การยกเลิกข้อ กฎ และข้อบังคับ ทั้งหมดที่ไม่สอดคล้องกับกฎเหล่านี้จะถูกยกเลิกหรือปรับเปลี่ยน

มาตรา ๓๖ ประสิทธิผล – กฎ และข้อบังคับเหล่านี้จะมีผลสิบห้า (๑๕) วัน หลังจากเสร็จสิ้นการเผยแพร่ในหนังสือพิมพ์หมุนเวียนอย่างน้อยสอง (๒) ฉบับ เสร็จสิ้นในกรุงมะนิลา วันที่ ๑๒ สิงหาคม ๒๕๕๘

บทที่ ๓
การศึกษาดูงาน

กองคดีเทคโนโลยีและสารสนเทศ ได้รับจัดสรรงบประมาณสำหรับโครงการอาเซียน ตั้งแต่ปี พ.ศ. ๒๕๕๙ จำนวน ๒๒๔,๑๐๐ บาท ปี พ.ศ. ๒๕๖๐ จำนวน ๗๕๗,๔๐๐ บาท ปี พ.ศ. ๒๕๖๑ จำนวน ๓๘๙,๕๐๐ บาท ซึ่งตั้งแต่ปีงบประมาณ พ.ศ. ๒๕๕๙ ได้ขออนุมัติศึกษาดูงานที่ประเทศมาเลเซีย โดยมี นายเกริกไชย ศรีศุกร์เจริญ ผู้เชี่ยวชาญคดีพิเศษ เป็นหัวหน้าคณะ และคณะรวมทั้งหมด ๑๐ คน

ปีงบประมาณ พ.ศ. ๒๕๖๐ ได้ขออนุมัติศึกษาดูงานที่สาธารณรัฐสิงคโปร์ โดยมี พันตำรวจโท วิชัย สุวรรณประเสริฐ ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ เป็นหัวหน้าคณะ และคณะรวมทั้งหมด ๑๙ คน

ปีงบประมาณ พ.ศ. ๒๕๖๑ ได้ขออนุมัติศึกษาดูงานที่สาธารณรัฐฟิลิปปินส์ โดยมี นางสาวปัทมาภรณ์ กฤษณายุทธ พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ เป็นหัวหน้าคณะ และคณะรวมทั้งหมด ๓ คน โดยมีผลการศึกษาดูงานดังนี้

๓.๑ การศึกษาดูงานประเทศมาเลเซีย

๓.๑.๑ สถานเอกอัครราชทูตไทย ณ กรุงกัวลาลัมเปอร์ (วันที่ ๑๗ มีนาคม ๒๕๕๙) โดยผลการประชุมหารือสามารถสรุปได้ดังนี้

๓.๑.๑.๑ ผู้เข้าร่วมประชุมจากสถานเอกอัครราชทูตไทย ณ กรุงกัวลาลัมเปอร์ จำนวน ๖ คน ประกอบด้วย

๑) นายอรรณพ	ศูนย์จันทร์	อัครราชทูตที่ปรึกษา
๒) นายไสว	โชคเจริญเลิศ	อัครราชทูตที่ปรึกษา
๓) นายอรรถพงศ์	พันธ์รัตน์	ที่ปรึกษา
๔) นายอับดุลฮาลิม	มาฮะ	เจ้าหน้าที่ล่าม
๕) นางสาวอามาณีย์	หะยีด๊ะ	เจ้าหน้าที่ช่วยปฏิบัติงานด้านกงสุล
๖) นางสาวสุกัญญา	สูเด็น	เจ้าหน้าที่ช่วยปฏิบัติงานด้านกงสุล

๓.๑.๑.๒ ผู้แทนจากสถานเอกอัครราชทูตไทยฯ ได้ให้ข้อมูลต่อที่ประชุมฯ ดังนี้

๑) โดยทั่วไปแล้ว สถานเอกอัครราชทูตไทยฯ จะระมัดระวังในการออก Visa ให้กับบุคคลต่างชาติ โดยเฉพาะอย่างยิ่งบุคคลที่มาจากทางทวีปแอฟริกา ซึ่งหากมีสัญชาติไนจีเรียแล้วแทบจะไม่มีการออกวีซ่าให้

๒) ในประเทศมาเลเซีย มีกลุ่มนักศึกษาชาวไนจีเรียประมาณ ๘,๐๐๐ คน ซึ่งบางคนก็มีวัตถุประสงค์ที่จะมาศึกษาต่อจริง ๆ แต่บางคนก็ใช้วีซ่านักเรียนเพื่อที่จะเข้ามาหลอกลวง ซึ่งคนมาเลเซียเองก็โดนหลอกเช่นกัน โดยทางสถานเอกอัครราชทูตไทยฯ เคยอ่านพบในหนังสือพิมพ์ว่าคนมาเลเซียถูกหลอกลวงโดยมีมูลค่าความเสียหายประมาณ ๒๐๐ ล้านบาท/ปี ดังนั้น สถานทูตของบางประเทศที่ตั้งอยู่ในประเทศมาเลเซีย เช่น สถานทูตสหรัฐฯ และสถานทูตอังกฤษ จึงได้ขึ้นข้อความแจ้งเตือนบนเว็บไซต์เพื่อให้คนสัญชาติของตนระวังการถูกหลอกลวง

๓) แม้ว่ากลุ่มคนไนจีเรียจะสร้างปัญหาให้กับประเทศมาเลเซียเป็นอย่างมาก ทางการมาเลเซียก็มิได้มีการเข้มงวดในการให้วีซ่ากับกลุ่มคนเหล่านี้มากขึ้นแต่อย่างใด จะเห็นได้ว่าประเทศมาเลเซียจะให้วีซ่ากับคนต่างชาติง่ายมาก ในขณะที่ประเทศเกือบทั้งหมดที่ตั้งอยู่ในบริเวณนี้จะเข้มงวดกับการให้วีซ่าคนต่างชาติ ส่งผลให้ประเทศมาเลเซียกลายเป็นแหล่งพักพิงของกลุ่มอาชญากรต่าง ๆ ซึ่งจะสังเกตได้ว่าไม่มีเหตุการณ์ร้ายแรงหรือการลอบวางระเบิดเกิดขึ้นในประเทศมาเลเซีย เนื่องจากอาชญากรเหล่านี้จะไม่ทำลายแหล่งพักพิงของตนเอง

๔) ที่ผ่านมามักจะมีหญิงไทยโทรศัพท์มาที่สถานเอกอัครราชทูตไทยฯ เพื่อขอให้ช่วยตรวจสอบว่า ชาวต่างชาติที่ตนเองรู้จักและพูดคุยผ่านทาง Social Media นั้น มีตัวตนอยู่จริงหรือไม่ (ชาวต่างชาติที่หลอกลวงส่วนใหญ่มักอ้างว่าตนเองมีสัญชาติอังกฤษ) และหญิงไทยที่โทรศัพท์มาขอตรวจสอบมักจะมีอายุมากกว่า ๔๐ ปีขึ้นไป และเป็นผู้ที่มีความรู้ภาษาอังกฤษในระดับหนึ่ง ทั้งนี้ ลักษณะการหลอกลวงที่พบ คือ เป็น Romance Scam ซึ่งเป็นการหลอกลวงโดยพูดคุยกับผู้เสียหายผ่าน Social Media ต่าง ๆ โดยเฉพาะอย่างยิ่ง Facebook และใช้ภาพถ่ายที่เป็นหน้าตาฝรั่งผิวขาวแต่ตัวตนจริง ๆ เป็นคนไนจีเรีย และจะแสดงทีท่าว่ามีความสนใจรักใคร่ผู้เสียหายและอยากจะแต่งงานด้วยแต่ติดขัดปัญหาบางอย่างจึงขอให้ช่วยโอนเงินมาให้ ซึ่งผู้เสียหายส่วนใหญ่ก็จะโอนเงินไปให้หลายครั้ง แต่เนื่องด้วยการพูดคุยดังกล่าวมักจะกระทำผ่านทาง Facebook และมักจะใช้ชื่อปลอมในการติดต่อพูดคุย จึงทำให้ไม่สามารถทราบตัวตนที่แท้จริงของผู้หลอกลวง นอกจากนี้เวลาที่ผู้เสียหายไปแจ้งความที่สถานีตำรวจท้องที่ ทางเจ้าหน้าที่ตำรวจมาเลเซียก็มักจะมิได้มีการดำเนินการใด ๆ ดังนั้นสถานเอกอัครราชทูตไทยฯ จึงมักจะแนะนำให้ผู้เสียหายไปติดต่อกับตำรวจที่รับผิดชอบคดีอาชญากรรมทางเทคโนโลยี

๕) ตัวอย่างการหลอกลวงคนไทยก็เช่น เมื่อปีที่ผ่านมาหัวหน้าพยาบาลของโรงพยาบาลแห่งหนึ่งในจังหวัดกาฬสินธุ์ ถูกชายต่างชาติหลอกลวงว่าทำงานอยู่ที่บริษัทน้ำมันเปโตรนาส และกำลังจะได้งานสัมปทาน แต่ขาดเงินอยู่อีกเท่านั้นเท่านี้ซึ่งฝ่ายหญิงไทยก็โอนเงินไปให้หลายครั้ง คิดรวมเป็นเงินประมาณ ๔ ล้านบาท โดยเชื่อว่าหากฝ่ายชายได้งานสัมปทานก็จะเอาเงินที่ยืมไปมาคืนและจะมาขอแต่งงาน แต่ทางสถานเอกอัครราชทูตไทยฯ ก็เชื่อว่าถูกหลอกลวงแน่นอน เนื่องจากได้ประสานตรวจสอบชื่อผู้ชายไปยังบริษัทน้ำมันเปโตรนาสแล้วได้รับแจ้งว่าทางบริษัทไม่มีพนักงานที่ใช้ชื่อดังกล่าว และล่าสุดก็ได้รับการติดต่อแจ้งว่าหัวหน้าพยาบาลของโรงพยาบาลอีกแห่งหนึ่งในจังหวัดเพชรบูรณ์ก็ถูกหลอกลวงในลักษณะดังกล่าวเช่นกัน นอกจากนี้ บางกรณีก็ถูกชายต่างชาติหลอกว่าถือเงินสดมาประเทศไทยคิดเป็นมูลค่าประมาณ ๒ ล้านบาท เพื่อนำมาขอแต่งงาน แต่ถูกเจ้าหน้าที่ไทยกักตัวไว้ที่สนามบินที่ภูเก็ต เนื่องจากถือเงินสดมาเป็นปริมาณมากจึงขอให้หญิงไทยช่วยโอนเงินมาให้ ๕๐,๐๐๐ บาท เพื่อใช้เคลียร์เรื่องกับทางเจ้าหน้าที่ ซึ่งหญิงไทยก็โอนเงินให้และด้วยความเป็นห่วงก็ได้ขับรถตามไปถึงภูเก็ตแต่ก็ไม่เจอใคร ซึ่งฝ่ายชายต่างชาติก็แก้ตัวในภายหลังว่าได้เคลียร์เรื่องและเดินทางออกนอกประเทศไปก่อน แต่อย่างไรก็ตามทางหญิงไทยก็ยังไม่ยอมปักใจเชื่อว่าตนเองถูกหลอกลวง

๖) ในช่วงที่ผ่านมาสถานเอกอัครราชทูตไทยฯ ได้เห็นประกาศรับสมัครหญิงไทยให้มาทำงานเดินแบบในมาเลเซีย โดยเชื่อว่าน่าจะเป็นการทำงานที่ไม่มีใบอนุญาตทำงาน (Work Permit) ซึ่งทางหน่วยงานตำรวจมาเลเซียก็ได้เพ่งเล็งที่จะทำการจับกุม โดยล่าสุดได้มีการ

จับกุมคนไทยประมาณ ๓๐ คน ที่รัฐยะโฮร์ (อยู่ใกล้ชายแดนสาธารณรัฐสิงคโปร์) และมีอีกคดีหนึ่งที่จับกุมได้ประมาณ ๑๐ กว่าคน ทั้งนี้ บทลงโทษของประเทศมาเลเซียในเรื่องการลักลอบทำงาน คือ จำคุก ๓ เดือน และปรับเงินประมาณ ๕,๐๐๐ – ๑๐๐,๐๐๐ บาท ซึ่งที่ผ่านมาเมื่อถูกเจ้าหน้าที่ตำรวจจับกุมเจ้าของร้านก็จะไปประกันตัวออกมาแล้วมาทำงานต่อ

๗) ที่ผ่านมามีหน่วยงานบังคับใช้กฎหมายไทยขอความร่วมมือหน่วยงานตำรวจมาเลเซียในเรื่องต่าง ๆ ผ่านทางช่องทางความร่วมมือระหว่างประเทศในเรื่องทางอาญา ซึ่งพบว่าหน่วยงานตำรวจมาเลเซียได้ให้ความร่วมมือเป็นอย่างดี

๘) ที่ผ่านมาสถานเอกอัครราชทูตไทยฯ ได้เคยประสานงานเรื่องคดีหลอกลวงคนไทยกับทางหน่วยงานตำรวจมาเลเซีย ๒ คดี โดยคดีแรกผู้เสียหายได้สูญเสียเงินไปประมาณ ๑๓ ล้านบาท จากการโอนเงินหลายครั้งในช่วงเวลา ๒ - ๓ เดือน ซึ่งทางเจ้าหน้าที่ตำรวจมาเลเซียได้ทำการปิดคดีไปแล้ว แต่ทางสถานเอกอัครราชทูตไทยฯ ได้ร้องขอให้มีการเปิดคดีขึ้นมาพิจารณาใหม่ซึ่งทางเจ้าหน้าที่ตำรวจมาเลเซียก็ดำเนินการให้ สำหรับคดีที่สองนั้นผู้เสียหายได้สูญเสียเงินไปประมาณ ๓ - ๔ ล้านบาท ซึ่งทางสถานเอกอัครราชทูตไทยฯ ก็ได้พาผู้เสียหายไปแจ้งความแต่ก็ไม่ทันการณ์

๙) การตรวจสอบคนไทยที่เข้ามาทำงานในประเทศมาเลเซียนั้นกระทำได้ลำบาก เนื่องจาก (๑) ส่วนใหญ่มักจะเข้ามาในประเทศมาเลเซียด้วยวีซ่าท่องเที่ยว และเมื่อวีซ่าหมดอายุก็จะมีตัวแทนไปดำเนินการต่อวีซ่าให้ที่ด่านชายแดน และ (๒) การเข้าออกบริเวณด่านชายแดนไทยมาเลเซียนั้นกระทำได้โดยง่าย แต่ได้รับทราบข้อมูลมาว่ากลุ่มคนไทยที่ถูกพาเข้ามาในประเทศมาเลเซียนั้นจะมีจุดแวะพักที่โรงแรมบางแห่งในอำเภอหาดใหญ่ และ/หรือในจังหวัดนราธิวาส ก่อนที่จะเดินทางเข้าประเทศมาเลเซียผ่านทางด่านสะเดา ทั้งนี้ หากกรมสอบสวนคดีพิเศษประสงค์จะตรวจสอบคนไทยที่เข้ามาทำงานในประเทศมาเลเซียโดยไม่ถูกต้องตามกฎหมาย อาจจะประสานไปยังหน่วยงานตำรวจตรวจคนเข้าเมือง เพราะเชื่อว่าน่าจะมีข้อมูลของบุคคลเหล่านี้อยู่ หรืออาจจะประสานไปที่เจ้าหน้าที่ตำรวจสันติบาล เนื่องจากมีการข่าวรวดเร็วและมีความคุ้นเคยกับกลุ่มร้านอาหารไทยที่ตั้งอยู่ในประเทศมาเลเซีย

๑๐) สถานเอกอัครราชทูตไทยฯ มีอาสาสมัครคนไทยที่อยู่ในรัฐต่าง ๆ ซึ่งส่วนใหญ่จะเป็นหญิงไทยที่เป็นแม่บ้านและอาศัยอยู่ในประเทศมาเลเซียมาเป็นระยะเวลานาน ซึ่งเป็นการทำงานด้วยจิตอาสา เนื่องจากสถานเอกอัครราชทูตไทยฯ ไม่มีงบประมาณสำหรับให้เป็นค่าตอบแทนหรือค่าใช้จ่ายใด ๆ (ในประเทศมาเลเซีย คนไทยส่วนใหญ่จะเข้ามาทำงานแล้วอาศัยอยู่ไม่นาน ดังนั้น คนไทยที่มาอาศัยอยู่ในประเทศมาเลเซียเป็นเวลานาน ๆ จนตั้งรกรากถิ่นฐานนั้นมีไม่มาก) สาเหตุหนึ่ง ที่จำเป็นต้องมีอาสาสมัครคนไทยก็เนื่องจากเวลาที่คนไทยถูกจับและถูกส่งตัวกลับนอกจากจะต้องมีหนังสือสำคัญประจำตัว (Certificate of Identity: CI) หรือหนังสือเดินทางแล้วยังต้องจ่ายค่า Special Pass อีกจำนวน ๑๐๐ ริงกิตมาเลเซีย (ประมาณ ๙๐๐ บาท) ด้วยจึงจะสามารถเดินทางกลับประเทศไทยได้ ซึ่งผู้ที่ถูกส่งตัวกลับก็มักจะไม่มีเงินติดตัวส่งผลให้สถานเอกอัครราชทูตไทยฯ ต้องขอให้ทางอาสาสมัครคนไทยที่อยู่ในรัฐต่าง ๆ ช่วยสำรองจ่ายแทนไปก่อน

๑๑) ปัจจุบันสถานเอกอัครราชทูตไทยฯ มีการทำโครงการประชาสัมพันธ์เพื่อให้คนไทยที่อาศัยอยู่ในแต่ละรัฐของประเทศมาเลเซียได้รู้จักกัน รู้จักผู้ที่เป็นอาสาสมัคร รู้ว่าเวลา

ที่ถูกทำร้าย หรือมีการค้ามนุษย์เกิดขึ้นจะต้องติดต่อใครวีซ่ามาเลเซียมีกี่ประเภทแบบใดบ้าง เนื่องจากบางคนก็ไม่ทราบว่าวีซ่าที่ตนเองถืออยู่นั้นเป็นวีซ่าปลอม ทั้งนี้เพื่อที่จะได้ดูแลและช่วยเหลือตนเองได้ในระดับหนึ่งนอกจากนี้ก็มีการเผยแพร่ข้อมูลต่าง ๆ ของสถานเอกอัครราชทูตไทยฯ ผ่าน “ชมรมสตรีไทยในมาเลเซีย” หรือ“ไทยคลับ” ด้วย เนื่องจากผู้เสียหายบางรายจะไม่กล้าติดต่อสถานเอกอัครราชทูตไทยฯ แต่จะติดต่อ “ไทยคลับ” แทน

๑๒) หากกรมสอบสวนคดีพิเศษ ต้องการให้สถานเอกอัครราชทูตไทยฯ ให้การสนับสนุนหรือช่วยเหลือในด้านใด ๆ ขอให้ดำเนินการแบบคู่ขนาน คือ มีหนังสือเป็นทางการจากปลัดกระทรวงยุติธรรมแจ้งไปยังปลัดกระทรวงการต่างประเทศ และในขณะเดียวกันก็ให้กรมสอบสวนคดีพิเศษประสานแจ้งให้สถานเอกอัครราชทูตไทยฯ ทราบด้วยอีกทางหนึ่ง

๑๒.๑) ผู้แทนจากกรมสอบสวนคดีพิเศษ ได้ให้ข้อมูลต่อที่ประชุมฯ ว่าบัญชีธนาคารที่รับโอนเงินจากการหลอกลวงประมาณร้อยละ ๘๐ ขึ้นไป มักจะเปิดบัญชีโดยหญิงไทยที่มาประกอบอาชีพนวด และ/หรือ ขายบริการทางเพศ ในประเทศมาเลเซีย โดยหญิงไทยเหล่านี้มักจะรับจ้างเปิดบัญชีเพื่อเป็นอาชีพเสริม และในบางกรณีหากมีการหลอกลวงเงินมาได้หญิงไทยเหล่านั้นก็จะได้ส่วนแบ่งด้วย ทั้งนี้จากการตรวจสอบพบว่าหญิงไทยเหล่านี้มักจะอาศัยอยู่ในอมันปุรีอพาร์ทเม้นท์ย่านเกปง และมักจะข้ามชายแดนไทย - มาเลเซีย เพื่อไปเปิดบัญชีธนาคารที่ใช้หลอกลองให้โอนเงินที่บริเวณด่านสะเดา

๑๒.๒) ผู้แทนกรมสอบสวนคดีพิเศษได้เสนอต่อที่ประชุมฯ ให้มีการสร้างสายข่าว โดยบุคคลที่เป็นสายข่าวนั้นอาจจะเป็นผู้ที่ถูกหลอกลวงหรือผู้ที่เกี่ยวข้องกับการกระทำความผิดโดยให้โอกาสบุคคลเหล่านั้นกลับมาให้ข้อมูลที่เป็นประโยชน์ในการสืบสวนสอบสวนต่อทางการไทย เพื่อที่จะได้กันตัวบุคคลดังกล่าวไว้เป็นพยาน ซึ่งก็จะเป็นประโยชน์ด้วยกันทั้งสองฝ่าย นอกจากนี้ ก็อาจจะให้อาสาสมัครคนไทยในมาเลเซียเป็นผู้แจ้งหรือให้ข้อมูลที่เป็นประโยชน์แก่กรมสอบสวนคดีพิเศษ โดยกรมสอบสวนคดีพิเศษจะให้การสนับสนุนค่าใช้จ่ายที่เกิดขึ้น

๓.๑.๒ หน่วยงาน Commercial Crime Investigation Department สังกัด Royal Malaysia Police (วันที่ ๑๘ มีนาคม ๒๕๕๙) โดยผลการประชุมหารือสามารถสรุปได้ดังนี้

๓.๑.๒.๑. รองผู้บัญชาการและผู้ช่วยผู้บัญชาการหน่วยงาน Commercial Crime Investigation Department เจ้าหน้าที่จากส่วนงาน Cyber & Multimedia Crime Investigation Division และเจ้าหน้าที่จากส่วนงานอื่น ๆ อาทิเช่น ส่วนปฏิบัติการและส่วนความร่วมมือระหว่างประเทศ รวมทั้งสิ้นประมาณ ๑๐ คน ได้ให้การต้อนรับบรรยายสรุปภาพรวมและแลกเปลี่ยนประสบการณ์ในการสืบสวนสอบสวนกับคณะเจ้าหน้าที่จากกรมสอบสวนคดีพิเศษ ดังนี้

๑) หน่วยงาน Commercial Crime Investigation Department มีเจ้าหน้าที่ทั้งหมดประมาณ ๓๐๐ กว่าคน โดยส่วนงานที่รับผิดชอบด้านอาชญากรรมทางคอมพิวเตอร์ คือ ส่วนงาน Cyber & Multimedia Crime Investigation Division ซึ่งมีเจ้าหน้าที่ จำนวน ๗๖ คน (ประกอบด้วยเจ้าหน้าที่ตำรวจ ๗๐ คน และเจ้าหน้าที่พลเรือนที่ทำงานด้านการตรวจพิสูจน์ ๖ คน)

๒) ในปี ค.ศ. ๒๐๑๕ มีผู้ใช้งานอินเทอร์เน็ตในประเทศมาเลเซีย ทั้งหมดประมาณ ๒๕ ล้านคน เพิ่มขึ้นมากจากปี ค.ศ. ๒๐๑๔ ซึ่งมีประมาณ ๑๘ ล้านคน (ประเทศมาเลเซียสนับสนุนให้ประชาชนสามารถเข้าถึงบริการทางอินเทอร์เน็ตได้ง่ายขึ้น เช่น มีการติดตั้งจุด Hotspot

ประมาณ ๓๑,๐๐๐ จุดทั่วประเทศ) ผู้ใช้งานส่วนใหญ่จะเป็นกลุ่มคนที่มีอายุ ๒๐ - ๒๔ ปี และใช้อินเทอร์เน็ตโดยเฉลี่ยสัปดาห์ละ ๒๒.๓ ชั่วโมง โดยผู้ที่เข้าใช้อินเทอร์เน็ตจำนวน ๘๘% จะเข้าเว็บไซต์ Facebook นอกจากนี้จากการศึกษาวิจัยยังพบว่าผู้ที่ใช้อินเทอร์เน็ตสัปดาห์ละ ๑ - ๒๔ ชั่วโมง จะมีความเสี่ยงที่ถูกหลอกลวงประมาณ ๖๔% ในขณะที่ผู้ที่ใช้อินเทอร์เน็ตสัปดาห์ละ ๔๙ ชั่วโมงขึ้นไป จะมีความเสี่ยงที่ถูกหลอกลวงเพิ่มสูงขึ้นเป็น ๗๙%

๓) กลุ่มชาวต่างชาติที่มาก่ออาชญากรรมหลอกลวงในประเทศมาเลเซียนั้น แบ่งออกได้เป็น ๓ กลุ่มใหญ่ ๆ คือ (๑) กลุ่มคนแอฟริกา (๒) กลุ่มคนไนจีเรีย และ (๓) กลุ่มคนมาเก๊า จีน และไต้หวัน

๔) คดีอาชญากรรมทางคอมพิวเตอร์หลักในมาเลเซียในปี ค.ศ. ๒๐๑๕ จะไม่ค่อยแตกต่างจากเมื่อสองปีก่อน ซึ่งได้แก่

๔.๑) คดี E-commerce (เช่น การซื้อขายสินค้าและการลงทุนผ่านทางอินเทอร์เน็ต) จำนวน ๔,๐๘๒ คดี

๔.๒) คดี ๔๑๙/Love or Romance Scam จำนวน ๑,๗๕๐ คดี

๔.๓) Telecommunication Fraud (เช่น การหลอกลวงผ่านทาง SMS และ E-mail) จำนวน ๑,๔๒๙ คดี

๔.๔) Phishing จำนวน ๑๖๓ คดี

๔.๕) ATM จำนวน ๖๕๑ คดี

๔.๖) Hacking จำนวน ๑๗๒ คดี

๔.๗) Intellectual Property (เป็นการแชร์หรือซื้อขายหนังภาพยนตร์และ/หรือเพลง โดยผิดกฎหมาย รวมถึงการละเมิดลิขสิทธิ์ต่างๆ บนอินเทอร์เน็ต) จำนวน ๗๕๒ คดี

๔.๘) ๒๓๓ AKM จำนวน ๘๑ คดี นอกจากนี้ก็มีคดีเกี่ยวกับภาพลามกอนาจารของเด็กที่เผยแพร่ลงบนอินเทอร์เน็ต สำหรับการดำเนินคดีนั้น ในบางครั้งหน่วยงานตำรวจมาเลเซียก็จะทำคดีร่วมกับธนาคารชาติมาเลเซีย

๕) ตัวอย่างคดี ๔๑๙/Love or Romance Scam เช่น เมื่อปี ค.ศ. ๒๐๑๓ มีผู้เสียหายถูกหลอกลวงผ่านทาง Social Network โดยฝ่ายชายอ้างว่า เป็นคนสหรัฐฯ (แต่จริงๆ แล้วเป็นคนแอฟริกา) บอกว่า จะส่งเงินสดมาให้ทางพัสดุภัณฑ์เป็นจำนวนมาก และก็มีใบแจ้งให้ฝ่ายหญิงที่ติดต่อคุยกันผ่านทาง Social Media ไปรับพัสดุภัณฑ์ แต่จะต้องโอนเงินเข้าบัญชีเพื่อใช้เคลียร์กับทางเจ้าหน้าที่ก่อน ซึ่งในคดีนี้สามารถจบคดีได้เร็วและจับกุมผู้กระทำความผิดได้ เนื่องจากผู้กระทำความผิดยังอยู่ในประเทศมาเลเซีย และบัญชีธนาคารที่ใช้รับโอนเงินก็เป็นบัญชีของแฟนสาวของผู้กระทำความผิด ส่งผลให้สามารถเชื่อมโยงหลักฐานมาถึงตัวผู้กระทำความผิดได้

๖) ภัยคุกคามทางคอมพิวเตอร์ในประเทศมาเลเซีย ได้แก่ การขโมยข้อมูล การขโมยข้อมูลที่ระบุถึงตัวตน Phishing และ Malware ต่าง ๆ ซึ่งปัญหาต่าง ๆ เหล่านี้มีสาเหตุมาจากระบบ Server ไม่มีความปลอดภัยเพียงพอ และมีการใช้โปรแกรมฟรีหรือโปรแกรมที่ผิดกฎหมาย

๗) ปัจจุบันกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ในมาเลเซียนั้น มี ๘ ฉบับ ได้แก่

๗.๑) Computer Crime Act ๑๙๙๗

๗.๒) Digital Signature Act ๑๙๙๗

๗.๓) Communication and Multimedia Act ๑๙๙๘

๗.๔) Copyright Act ๑๙๙๗

๗.๕) Telemedicine Act ๑๙๙๗

๗.๖) Optical Disk Act ๒๐๐๐

๗.๗) Electronic Commerce Act ๒๐๐๖

๗.๘) Personal Data Protection Act ๒๐๐๙

๘) ยุทธศาสตร์ที่หน่วยงานตำรวจมาเลเซียจะนำมาใช้เพื่อแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ คือ (๑) ให้การศึกษาและสร้างความตระหนักให้กับกลุ่มเสี่ยง (๒) บังคับใช้กฎหมายอย่างจริงจังและแก้ไขปรับปรุงกฎหมายในปัจจุบัน (๓) เสริมสร้างศักยภาพของเจ้าหน้าที่โดยการฝึกอบรมในด้านต่าง ๆ อาทิเช่น การสืบสวนสอบสวนทางอาชญากรรมคอมพิวเตอร์ VoIP ระบบสื่อสารแบบไร้สาย และการตรวจพิสูจน์ต่าง ๆ เป็นต้น (๔) จัดซื้อจัดจ้างอุปกรณ์และแอปพลิเคชันต่าง ๆ (เช่น ระบบการติดตาม IP หรือสื่อใหม่ ๆ และกล่องอุปกรณ์สำหรับการสืบสวน เป็นต้น) และ (๕) เสริมสร้างความร่วมมือระหว่างหน่วยงานในประเทศ/ความร่วมมือระหว่างประเทศ และการทำงานแบบกองกำลังร่วม (Task Force) เช่น หน่วยงาน Interpol, Europol และ Virtual Global Taskforce (VGT) เป็นต้น

๙) ในประเด็นเรื่องที่ชาวไนจีเรียเข้ามาอาศัยอยู่ในประเทศมาเลเซียโดยใช้วีซ่านักเรียนนั้น หน่วยงานตำรวจมาเลเซียไม่มีอำนาจในการดำเนินการใด ๆ ทั้งนี้ หน่วยงานที่มีอำนาจในเรื่องดังกล่าว คือ กระทรวงศึกษาธิการ

๑๐) ในประเด็นเรื่องการสืบสวนนั้น เมื่อมีการหลอกลวงกันทาง Facebook หรือ Social Media หน่วยงานตำรวจมาเลเซียจะทำการตรวจสอบ IP Address และระบุตัวผู้ต้องสงสัย และเมื่อรวบรวมพยานหลักฐานได้เพียงพอ (การรวบรวมพยานหลักฐานมักจะเน้นทางด้านการตรวจสอบสายการเงิน มิได้เน้นไปทางการตรวจสอบ IP Address เนื่องจาก Server ของ Facebook อยู่ที่ประเทศสหรัฐฯ) ก็จะส่งพนักงานอัยการเพื่อดำเนินคดีต่อไป

๑๑) ในประเทศมาเลเซียยังไม่มีการบัญญัติกฎหมายเรื่องระยะเวลาการเก็บรักษาข้อมูลย้อนหลังของบริษัทสื่อสาร ดังนั้น สภาวการณ์ในปัจจุบัน คือ แต่ละบริษัทจะจัดเก็บข้อมูลย้อนหลังไว้ตามแต่นโยบายของบริษัทตน บางบริษัทก็จัดเก็บย้อนหลัง ๒ เดือน บางบริษัทก็จัดเก็บย้อนหลัง ๗ วัน แต่อย่างไรก็ตามคาดว่าจะมีการแก้ไขกฎหมาย Communication and Multimedia Act ๑๙๙๘ ในเร็ว ๆ นี้ โดยจะมีการเสนอให้ต้องมีการจัดเก็บข้อมูลย้อนหลังไว้อย่างน้อย ๒ เดือน

๓.๑.๒.๒ หน่วยงานตำรวจมาเลเซีย แสดงท่าทีว่ามีความยินดีที่จะทำงานร่วมกับกรมสอบสวนคดีพิเศษ โดยแจ้งว่าหากมีสิ่งใดที่ต้องการให้หน่วยงาน Commercial Crime Investigation Department ช่วยเหลือ ก็สามารถประสานติดต่อมาได้โดยตรงและในอนาคต หากได้มีโอกาสมาเยือนประเทศไทย ก็จะมาเยือนกรมสอบสวนคดีพิเศษด้วย

๓.๒ การศึกษาดูงานสาธารณรัฐสิงคโปร์

๓.๒.๑ สถานเอกอัครราชทูตไทย ณ สาธารณรัฐสิงคโปร์ (วันที่ ๑๖ พฤษภาคม ๒๕๖๐) ได้มีผู้เข้าร่วมประชุมจากสถานเอกอัครราชทูตไทย ณ สาธารณรัฐสิงคโปร์ จำนวน ๒ ท่าน

ผลการเข้าหารือและดูงาน เอกอัครเอกอัครราชทูตไทยประจำสิงคโปร์ได้บรรยายสรุปภาพรวมของสาธารณรัฐสิงคโปร์โดยได้ระบุว่าในสาธารณรัฐสิงคโปร์ รัฐบาลจะเคร่งครัดในเรื่องการให้สัญชาติมาก เช่น หากพ่อแม่เป็นผู้ลี้ภัย ลูกหลานก็จะไม่มีสิทธิได้สัญชาติ เป็นต้น ปัญหาการละเมิดทรัพย์สินทางปัญญามีน้อยมากและการบริหารจัดการงบประมาณของประเทศนั้นก็มีความคล่องตัวสูง เนื่องจากใช้หลัก DBOO (Design – Build – Own - Operate) เช่น หากรัฐบาลต้องการน้ำดื่ม รัฐบาลก็จะกำหนดเพียงว่าต้องการปริมาณน้ำดื่มเท่าใดแล้วให้ภาคเอกชนไปดำเนินการออกแบบ ผลิตลงทุนและบริหารจัดการทั้งหมด สำหรับความร่วมมือระหว่างประเทศภายใต้กรอบ AEC นั้น เห็นว่าไม่ค่อยประสบผลสำเร็จเท่าไรนัก เนื่องจากทุกเรื่องจะต้องมีการประชุมและต้องเป็นฉันทามติ จึงส่งผลให้การขับเคลื่อนในเรื่องต่าง ๆ เป็นไปได้ช้าความร่วมมือแบบทวีภาคีจะเกิดผลและเดินหน้าได้เร็วกว่า

๓.๒.๒ Commercial Affairs Department: CAD

เป็นหน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติสิงคโปร์ โดยมีการแบ่งโครงสร้างองค์กรออกเป็น ๔ ส่วน ตามลักษณะงาน ดังนี้

๓.๒.๒.๑ งานบังคับใช้กฎหมายส่วน ๑ รับผิดชอบคดีการฉ้อโกงในการลงทุนและการฉ้อโกงในหลักทรัพย์

๓.๒.๒.๒ งานบังคับใช้กฎหมายส่วน ๒ รับผิดชอบคดีฉ้อโกงโดยผู้ประกอบวิชาชีพเฉพาะ (เช่น ทนายความ นักบัญชี) การฉ้อโกงที่เกี่ยวข้องกับเจ้าหน้าที่ของรัฐและองค์กรการกุศลต่าง ๆ และฉ้อโกงที่เกี่ยวข้องกับระบบชำระเงิน เช่น การฉ้อโกงบัตรเครดิต/ATM การฉ้อโกงประกันภัย)

๓.๒.๒.๓ งานบังคับใช้กฎหมายส่วน ๓ รับผิดชอบงานการสืบสวนทางการเงิน (รวมถึงการสืบสวนคดีฟอกเงิน และคดีการสนับสนุนทางการเงินแก่การก่อการร้าย) นโยบาย และการปฏิบัติการ

๓.๒.๒.๔ ส่วนการข่าวและความร่วมมือ รับผิดชอบงานด้านรายงานธุรกรรมที่มีเหตุอันควรสงสัยตามกฎหมายฟอกเงิน การข่าวทางการเงิน และการให้ความร่วมมือต่าง ๆ

ดังนั้น คดีทางด้านการเงินและคดีทางด้านการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายที่มีความสลับซับซ้อนที่ยากต่อการสืบสวนสอบสวนโดยเจ้าหน้าที่ตำรวจทั่วไป จะถูกส่งมาให้หน่วยงาน Commercial Affairs Department เป็นผู้ดำเนินการ

เรื่องการป้องกันและปราบปรามการฟอกเงินนั้น ส่วนงานหนึ่งของ Commercial Affairs Department ที่มีชื่อว่า STRO (สำนักงาน ปปง. ของสาธารณรัฐสิงคโปร์) จะมีภารกิจหน้าที่ในการป้องกันและปราบปรามการฟอกเงินของสาธารณรัฐสิงคโปร์ โดย STRO นี้ จะประกอบด้วยส่วนงานย่อย ๔ ส่วนงานคือ

๑) ส่วนงานที่ ๑. รับผิดชอบคดีทางเศรษฐกิจที่สำคัญ การก่อการร้าย และการรายงานธุรกรรมเงินสดในสถานการพนัน

๒) ส่วนงานที่ ๒. รับผิดชอบคดีอื่น ๆ และความร่วมมือระหว่างประเทศ

๓) ส่วนงานที่ ๓. รับผิดชอบคดีภาษี การรายงานธุรกรรมเงินสดผ่านแดน และการรายงานธุรกรรมเงินสดของผู้ค้าอัญมณีและโลหะมีค่า

๔) ส่วนงานที่ ๔. รับผิดชอบระบบข้อมูลสารสนเทศ การทำงานภาคสนาม และการวิจัย

โดยภารกิจหน้าที่หลักของ STRO คือ รับรายงานธุรกรรมฯ วิเคราะห์รายงานธุรกรรมฯ และส่งต่อผลการวิเคราะห์รายงานธุรกรรมฯ ให้กับหน่วยงานที่เกี่ยวข้อง โดยให้การสนับสนุนข้อมูลแก่หน่วยงานทั้งในและต่างประเทศ

รายงานข้อมูลธุรกรรมที่มีเหตุอันควรสงสัย (Suspicious Transaction Reports) จะประกอบด้วยการรายงานใน ๒ กรณี คือ

๑) กรณีที่บุคคลใดในสิงคโปร์ พบทรัพย์สินที่น่าเชื่อว่าเกี่ยวข้องกับการค้ายาเสพติดหรือการกระทำความผิดทางอาญา จะต้องรายงานธุรกรรมที่มีเหตุอันควรสงสัยมายังหน่วยงาน STRO ทั้งนี้หากมีการฝ่าฝืนไม่รายงาน จะมีโทษปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์สิงคโปร์

๒) กรณีที่บุคคลทุกคนในสิงคโปร์รวมถึงคนสิงคโปร์ที่อาศัยอยู่ในต่างประเทศ จะต้องรายงานธุรกรรมที่มีเหตุอันควรสงสัยไปยังเจ้าหน้าที่ตำรวจ หากพบทรัพย์สินหรือข้อมูลใด ๆ ที่เกี่ยวข้องกับการก่อการร้าย ทั้งนี้ หากมีการฝ่าฝืนไม่รายงาน จะมีโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์สิงคโปร์ หรือจำคุก ๕ ปี หรือทั้งจำและปรับ โดยรายงานธุรกรรมที่มีเหตุอันควรสงสัยนี้มีแนวโน้มเพิ่มขึ้นโดยตลอด โดยเพิ่มจาก ๑๓,๕๕๘ รายงาน ในปี ค.ศ. ๒๐๑๑ เป็น ๒๒,๔๑๗ รายงาน และ ๓๐,๕๑๑ รายงาน ในปี ค.ศ.๒๐๑๓ และ ๒๐๑๕ ตามลำดับ

รายงานธุรกรรมเงินสดข้ามแดน (Cash Movement Reports) นั้น จะประกอบด้วยการรายงานใน ๒ กรณี คือ

๑) กรณีที่บุคคลใดก็ตามมีการเคลื่อนย้ายเงินสดเข้า - ออกสาธารณรัฐสิงคโปร์ที่มีมูลค่าเทียบเท่ากับ ๒๐,๐๐๐ ดอลลาร์สิงคโปร์ขึ้นไป จะต้องกรอกแบบรายงาน (แบบฟอร์ม NP๗๒๗)

๒) กรณีที่บุคคลใดก็ตามได้รับเงินสดที่มีมูลค่าเทียบเท่ากับ ๒๐,๐๐๐ ดอลลาร์สิงคโปร์ขึ้นไป จะต้องกรอกแบบรายการ (แบบฟอร์ม NP๗๒๗) ทั้งนี้ หากมีการฝ่าฝืนไม่รายงาน จะมีโทษปรับไม่เกิน ๕๐,๐๐๐ ดอลลาร์สิงคโปร์ หรือ จำคุก ๓ ปี หรือทั้งจำทั้งปรับ โดยรายงานธุรกรรมเงินสดข้ามแดนในสาธารณรัฐสิงคโปร์นี้ มีแนวโน้มลดลงเป็นลำดับ โดยลดจาก ๑๐๐,๔๒๗ รายงาน ในปี ค.ศ. ๒๐๑๑ เป็น ๗๖,๘๒๓ รายงาน ในปี ค.ศ.๒๐๑๕

รายงานธุรกรรมเงินสดของผู้ค้าอัญมณีและโลหะมีค่า (Precious Stones and Metals Dealers: PSMD) นั้น จะประกอบด้วยการรายงานใน ๒ กรณี คือ

๑) กรณีที่ผู้ค้าอัญมณีฯ ได้รับเงินสดจากการขายอัญมณีฯ ที่มีมูลค่าเกินกว่า ๒๐,๐๐๐ ดอลลาร์สิงคโปร์

๒) กรณีที่ผู้ค้าอัญมณีฯ ได้รับเงินสดจากการขายอัญมณีฯ ภายใน ๑ วัน ที่มีมูลค่ารวมแล้วเกินกว่า ๒๐,๐๐๐ ดอลลาร์สิงคโปร์ ทั้งนี้ หากมีการฝ่าฝืนไม่รายงาน จะมีโทษปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์สิงคโปร์ หรือจำคุก ๒ ปี หรือทั้งจำทั้งปรับ

รายงานธุรกรรมเงินสดของสถานการณ์พนันนั้น จะประกอบด้วยการรายงานใน ๒ กรณี คือ

๑) กรณีที่มีการทำธุรกรรมเงินสดเข้าหรือออกที่มีมูลค่าเกินกว่า ๑๐,๐๐๐ ดอลลาร์สิงคโปร์/ธุรกรรม และ

๒) กรณีที่มีการทำธุรกรรมทางการเงินหลายครั้งและมียอดรวมของการทำธุรกรรมเหล่านั้นเกินกว่า ๑๐,๐๐๐ ดอลลาร์สิงคโปร์ ทั้งนี้ หากมีการฝ่าฝืนไม่รายงาน จะมีโทษปรับไม่เกิน ๒๐,๐๐๐ ดอลลาร์สิงคโปร์ โดยในปัจจุบันสาธารณรัฐสิงคโปร์มีสถานคาสิโน จำนวน ๒ แห่ง คือ Sentosa และ Marina Bay

ในเรื่องการแลกเปลี่ยนข้อมูลกับต่างประเทศนั้น ส่วนงาน STRO จะเป็นผู้ที่ทำหน้าที่รับข้อมูลจากต่างประเทศ โดยหาก STRO ประสงค์จะส่งต่อข้อมูลดังกล่าวให้กับหน่วยงานผู้มีอำนาจอื่นในสิงคโปร์ ส่วนงาน STRO จะต้องขอความยินยอมในการเปิดเผยข้อมูลจากหน่วยงานต่างประเทศผู้ให้ข้อมูลก่อนเมื่อได้รับความยินยอมแล้ว ส่วนงาน STRO จะทำการปกปิดแหล่งที่มาของข้อมูลนั้นก่อนที่จะส่งต่อและข้อมูลดังกล่าวจะใช้เพื่อวัตถุประสงค์ในทางการข่าวเท่านั้น

ตามมาตรา ๔๑ ของพระราชบัญญัติว่าด้วยการคอร์รัปชัน การลักลอบค้ายาเสพติดและอาชญากรรมร้ายแรงอื่น ๆ (การยึดทรัพย์จากผลประโยชน์ที่ได้รับ) Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act: CDSA นั้น หน่วยงาน STRO สามารถที่จะส่งข้อมูลธุรกรรมที่มีเหตุอันควรสงสัยให้กับหน่วยงานต่างประเทศโดยที่ไม่ต้องมีการร้องขอมาก่อน แต่การดำเนินการดังกล่าวจะต้องมีข้อตกลงที่ทำไว้ล่วงหน้าหรือต้องมีบันทึกความเข้าใจ (MOU) ระหว่างกัน โดยปัจจุบันส่วนงาน STRO มี MOU กับต่างประเทศทั้งสิ้น จำนวน ๓๙ ประเทศ (เช่น อาร์เจนตินา กัมพูชา อินเดีย มาเลเซีย อิตาลี ญี่ปุ่น เกาหลีใต้ สหรัฐอเมริกา และอังกฤษ) สำหรับในส่วนของประเทศไทยนั้น ปัจจุบันอยู่ในขั้นตอนของการเจรจาความตกลงฯ

สำหรับภารกิจหน้าที่ทางด้านการต่อต้านการฟอกเงินนั้น ความผิดมูลฐานที่เป็นความผิดตามกฎหมายฟอกเงินในสาธารณรัฐสิงคโปร์นั้นมีประมาณ ๓๐๐ กว่ามูลฐานความผิด ทั้งนี้องค์ประกอบความผิดหลักของการฟอกเงิน คือ การปกปิดซ่อนเร้น หรือแปลงสภาพ หรือจำหน่ายจ่ายโอนซึ่งทรัพย์สินที่ได้มาจากการกระทำความผิดมูลฐาน ซึ่งรวมถึงกรณีที่บุคคลที่สามให้ความช่วยเหลือในการกระทำดังกล่าวด้วย และการยึดทรัพย์ตามกฎหมายฟอกเงินของสาธารณรัฐสิงคโปร์นี้จะแตกต่างจากไทย คือ เป็นการยึดทรัพย์โดยใช้มาตรการในทางการอาญา (Criminal Asset Forfeiture) มิใช่การยึดทรัพย์โดยใช้มาตรการในทางแพ่ง (Civil Asset Forfeiture) เหมือนดังเช่นประเทศไทย ทั้งนี้ บทลงโทษความผิดฐานฟอกเงินคือ จำคุกไม่เกิน ๑๐ ปี ปรับไม่เกิน ๕๐๐,๐๐๐ ดอลลาร์สิงคโปร์ หรือทั้งจำทั้งปรับ (หากเป็นนิติบุคคล จะเป็นโทษปรับไม่เกิน ๑ ล้านดอลลาร์สิงคโปร์)

<u>ตัวอย่างคดีของหน่วยงาน CAD</u>

๑) คดีอาชญากรรมทางการเงินที่เกี่ยวข้องกับคอมพิวเตอร์ เช่น Email Hacking, Internet Love Scam และ Credit for Sex Scam เป็นต้น โดย Internet Love Scam หรือ Romance Scam นั้น พฤติการณ์แห่งคดีคือ เหยื่อหรือผู้เสียหายจะได้รับการติดต่อผ่านทางอินเทอร์เน็ต และอีกฝ่ายก็จะแสร้งทำว่าตกหลุมรักผู้เสียหาย จากนั้นผู้หลอกลวงก็จะแจ้งว่าจะเดินทางมาสาธารณรัฐสิงคโปร์เพื่อแต่งงานด้วย และจะหลอกว่าถูกกักตัวโดยเจ้าหน้าที่ตรวจคนเข้าเมือง จึงขอให้ผู้เสียหายโอนเงินให้เพื่อนำไปใช้เป็นหลักประกันในการปล่อยตัว หรือในบางกรณี

อาจจะหลอกว่า มีส่งของขวัญไปให้ผู้เสียหาย แต่ของขวัญถูกกักไว้โดยเจ้าหน้าที่ศุลกากร จึงขอให้ผู้เสียหายจ่ายเงินเพื่อเป็นหลักประกันในการปล่อยของ ซึ่งคดีประเภทนี้ในสิงคโปร์มีแนวโน้มเพิ่มขึ้น โดยในปี ค.ศ.๒๐๑๕ - ๒๐๑๖ มีจำนวนทั้งสิ้น ๓๘๕ คดี และ ๖๓๖ คดี ตามลำดับ

๒) คดี Internet Love Scam ในสาธารณรัฐสิงคโปร์ ซึ่งได้รับข้อมูลการข่าวว่ามีการหลอกลวง Internet Love Scam ซึ่งกระทำโดยกลุ่มเครือข่ายชาวแอฟริกันในประเทศมาเลเซีย จึงมีการติดต่อและแลกเปลี่ยนข้อมูลกับหน่วยงานตำรวจประเทศมาเลเซียและวางแผนที่จะทำการสืบสวนร่วมกัน ซึ่งจากการสืบสวนร่วมกันส่งผลให้มีการเปิดคดี จำนวน ๔๓ คดีสำหรับสาธารณรัฐสิงคโปร์ และ ๖๕ คดีในประเทศมาเลเซีย โดยมีมูลค่าความเสียหายประมาณ ๒๑.๖ ล้านริงกิตมาเลเซีย และมีการตรวจค้นใน ๕ รัฐของมาเลเซียในช่วงระหว่างวันที่ ๖ - ๘ กุมภาพันธ์ ๒๕๖๐ ส่งผลให้สามารถจับกุมบุคคลได้จำนวน ๒๑ คน ในประเทศมาเลเซียโดยเป็นชาวไนจีเรียถึง ๑๓ คน

๓) คดี Credit for Sex Scam ในสาธารณรัฐสิงคโปร์ คือการหลอกลวงเริ่มต้นจากผู้ชาย (ผู้เสียหาย) ได้รับข้อความจากผู้หญิง (ผู้หลอกลวง) ผ่านทาง Social Media Applications ต่าง ๆ เช่น WeChat จากนั้น ผู้หลอกลวงก็อ้างว่า อาศัยอยู่ในสาธารณรัฐสิงคโปร์ และเสนอที่จะให้บริการทางเพศโดยให้จ่ายค่าบริการผ่านทาง Alipay (ระบบการชำระเงินระบบหนึ่งที่มีรูปแบบเหมือนกับ PayPal) หรือผ่านทางบัตร iTunes Card ซึ่งผู้เสียหายก็จะไปซื้อบัตรดังกล่าวแล้วส่งให้กับผู้หลอกลวงทาง Email หลังจากนั้น ผู้เสียหายจะไม่สามารถติดต่อกับผู้หลอกลวงได้อีกเลย และในบางกรณีก็จะมีบุคคลที่ไม่รู้จักตัวตนมาติดต่อผู้เสียหายอีกครั้งโดยจะทำตัวเป็นมาเฟียเพื่อข่มขู่และรีดไถเงิน ซึ่งในคดีประเภทนี้ ทางสิงคโปร์ก็ได้ติดต่อหน่วยงานตำรวจประเทศจีนผ่านทางองค์การตำรวจสากล (INTERPOL) โดยได้ให้ข้อมูลกับทางตำรวจจีนเพื่อทำการสืบสวน ตลอดจนได้รับความร่วมมือจากภาคเอกชน (กลุ่มธุรกิจเครือ Alibaba) ที่ได้ให้ข้อมูลสนับสนุนอย่างทันท่วงที ส่งผลให้ในเดือนธันวาคม ค.ศ. ๒๐๑๕ ทางการจีนสามารถจับกุมผู้ต้องสงสัยได้ทั้งสิ้น ๔๓ คน และยึดเครื่องคอมพิวเตอร์/เครื่องมือสื่อสารได้เป็นจำนวนมาก ทั้งนี้ในปี ค.ศ. ๒๐๑๕ สาธารณรัฐสิงคโปร์มีคดีในลักษณะดังกล่าว จำนวน ๑,๑๙๔ คดี คิดเป็นมูลค่าความเสียหายประมาณ ๒.๙ ล้านดอลลาร์สิงคโปร์

๓.๒.๓ หน่วยงาน Cyber Security Agency of Singapore (CSA)

๓.๒.๓.๑ เป็นหน่วยงานระดับชาติในสังกัดสำนักนายกรัฐมนตรี แต่อยู่ภายใต้การบริหารจัดการของกระทรวงสารสนเทศและการสื่อสาร ก่อตั้งขึ้นเมื่อวันที่ ๑ เมษายน ค.ศ. ๒๐๑๕ โดยยุบรวมภารกิจหน้าที่ของหน่วยงาน Infocomm Development Authority (IDA) และหน่วยงาน Singapore Infocomm Technology Security Authority (SITSA ซึ่งอยู่สังกัดกระทรวงมหาดไทย) มาดำเนินการ เพื่อทำหน้าที่กำกับดูแลยุทธศาสตร์ปฏิบัติการเพื่อตอบสนองต่อภัยคุกคาม ให้ความรู้ วิจัยและพัฒนาเทคโนโลยี กำกับดูแลและกำหนดมาตรฐานในการทำงานทางด้านระบบสารสนเทศ เฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ สร้างความตระหนักเกี่ยวกับความมั่นคงปลอดภัยทางคอมพิวเตอร์ให้กับกลุ่มเสี่ยง และประสานความร่วมมือระหว่างประเทศเพื่อต่อต้านภัยคุกคามทางคอมพิวเตอร์ โดยมีส่วนงาน Singapore Computer Emergency Response Team (SingCERT) ทำหน้าที่เป็นทีมงานตอบสนองและอำนวยความสะดวกในการติดต่อสื่อสารต่อเหตุการณ์ฉุกเฉินทางด้านคอมพิวเตอร์ สำหรับทั้งประเทศ (SingCERT มิใช่หน่วยงานสืบสวนสอบสวนหรือหน่วยงานบังคับใช้กฎหมาย) โดยมีภารกิจหลักคือ ให้ความช่วยเหลือทางเทคนิคแก่หน่วยงานต่าง ๆ

จัดการฝึกอบรม รวมถึงการเผยแพร่ข้อมูล และแจ้งเตือนภัยต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางคอมพิวเตอร์

๓.๒.๓.๒ การดูแลระบบข้อมูลสารสนเทศของสาธารณรัฐสิงคโปร์ จะแบ่งออกเป็น ๒ ส่วนหลัก ๆ คือ ส่วนระบบข้อมูลสารสนเทศที่มีความสำคัญ ๑๑ ด้าน ซึ่งจะดูแลโดย CSA (ได้แก่ ระบบฐานข้อมูลสารสนเทศทางด้านการเงินการธนาคาร การบิน การขนส่งทางบก พลังงาน การติดต่อสื่อสาร หน่วยงานรัฐบาล ระบบน้ำทางทะเล สุขภาพ สื่อมวลชนและการติดต่อสื่อสาร) และส่วนระบบข้อมูลสารสนเทศที่ดูแลโดยหน่วยงานเฉพาะ (ได้แก่งานด้านอาชญากรรมทางคอมพิวเตอร์ ซึ่งรับผิดชอบโดยหน่วยงานตำรวจสิงคโปร์ และงานด้านการทหารซึ่งรับผิดชอบโดยกระทรวงกลาโหม)

๓.๒.๓.๓ ยุทธศาสตร์ความมั่นคงทางด้าน Cyber Security ของสิงคโปร์ที่ได้ประกาศไว้เมื่อวันที่ ๑๐ ตุลาคม ค.ศ. ๒๐๑๖ คือ มีความร่วมมือและประสานความกับหุ้นส่วนในระดับระหว่างประเทศเพื่อให้สภาพแวดล้อมของโลก Cyber มีความยืดหยุ่นปรับตัวได้เร็วและได้รับความไว้วางใจเพื่อประโยชน์ทางด้านเทคโนโลยีและความมั่นคงปลอดภัยของประชาชนสิงคโปร์ โดยมีแผนปฏิบัติการเพื่อสนับสนุนยุทธศาสตร์ดังกล่าว ๔ เรื่อง คือ

๑) สร้างระบบสาธารณูปโภคที่มีความยืดหยุ่นปรับตัวได้ง่าย คือ ดูแลและปกป้องระบบบริการที่มีความสำคัญมีนโยบายการตอบสนองต่อภัยคุกคามที่ชัดเจน แก้ไขกฎหมายให้มีประสิทธิภาพ และดูแลระบบเครือข่ายทางคอมพิวเตอร์ของหน่วยงานรัฐบาลให้มีความปลอดภัย

๒) สร้างโลก Cyber ให้มีความปลอดภัยมากขึ้น คือ ต่อต้านอาชญากรรมทางคอมพิวเตอร์ แสดงให้เห็นว่าสาธารณรัฐสิงคโปร์เป็นศูนย์รวม (Hub) ที่มีความน่าเชื่อถือและสนับสนุนความรับผิดชอบร่วมกัน

๓) สร้างนวัตกรรมที่เป็นมิตรกับสิ่งแวดล้อม คือ มีการสร้างผู้เชี่ยวชาญที่มีทักษะเฉพาะ สนับสนุนให้บริษัทต่าง ๆ ใช้เทคโนโลยีระดับสูง และสนับสนุนการวิจัยและพัฒนาร่วมกัน

๔) เสริมสร้างความร่วมมือกับหุ้นส่วนต่างประเทศ คือ สนับสนุนความร่วมมือทั้งในระดับภูมิภาคและระดับระหว่างประเทศ เสริมสร้างศักยภาพของเจ้าหน้าที่ทางด้าน Cyber ผ่านทางการฝึกอบรม และมีการแลกเปลี่ยนความรู้ทางด้านกฎหมายและแนวทางการทำงาน ซึ่งหน่วยงาน CSA มี MOU กับหลายประเทศ ได้แก่ ฝรั่งเศส อินเดีย สหรัฐอเมริกา อังกฤษ และเนเธอร์แลนด์

๓.๒.๓.๔ เมื่อปี ค.ศ. ๒๐๑๗ สาธารณรัฐสิงคโปร์มีการจัดงานประชุม/สัมมนาในระดับภูมิภาค/ระหว่างประเทศที่สำคัญหลายงาน อาทิเช่น การประชุมคณะกรรมาธิการระดับโลกเพื่อความมีเสถียรภาพในโลก Cyber การประชุมระดับโลกสำหรับผู้เชี่ยวชาญทางโลก Cyber การประชุมระดับโลกทางด้าน Cyber กิจกรรม Singapore International Cyber Week (โดยในปีนี้กิจกรรมดังกล่าวจะมีขึ้นในระหว่างวันที่ ๑๘ - ๒๕ กันยายน ๒๕๖๐) และการประชุมระดับรัฐมนตรีอาเซียนครั้งที่ ๒ ทางด้านความมั่นคงปลอดภัยทาง Cyber

๓.๒.๓.๕ SingCERT ก่อตั้งขึ้นครั้งแรกเมื่อเดือนตุลาคม ค.ศ. ๑๙๙๗ โดยความร่วมมือระหว่างหน่วยงาน IDA กับมหาวิทยาลัยแห่งชาติสิงคโปร์ ต่อมาเมื่อปี ค.ศ. ๑๙๙๙ SingCERT ได้โอนมาอยู่ภายใต้การดูแลของหน่วยงาน IDA แต่เพียงหน่วยเดียว และหลังจากที่มีการก่อตั้งหน่วยงาน CSA เมื่อปี ค.ศ. ๒๐๑๕ SingCERT ก็ถูกโอนมาเป็นส่วนหนึ่งของหน่วยงาน CSA

๓.๒.๓.๖ การตอบสนองต่อภัยคุกคามทางคอมพิวเตอร์ที่อยู่ในอำนาจของ SingCERT ได้แก่

๑) การฉ้อโกง (เช่น Email Scam, Business Email Compromise และ Phishing)

๒) การเข้าครอบงำระบบ (เช่น Bots, Defacement และ Ransomware)

๓) การทำให้ผู้ใช้งานคอมพิวเตอร์ไม่สามารถเข้าสู่ระบบได้ (DDos)

๓.๒.๓.๗ ตัวอย่างเหตุการณ์ภัยคุกคามทางคอมพิวเตอร์ที่ SingCERT เคยพบ คือ การฉ้อโกงโดยใช้ Email โดยพฤติการณ์แห่งคดี คือ ลูกค้าได้ติดต่อกับผู้ขายเพื่อขอทราบราคาและข้อมูลของสินค้า จากนั้นทั้งสองฝ่ายมีการตกลงกำหนดวันชำระเงินโดยผู้ขายจะออกใบสั่งซื้อให้กับลูกค้า เมื่อมีการกำหนดวันชำระเงินที่แน่นอนต่อมาลูกค้าได้รับ Email หลอกลวงจากผู้ฉ้อโกง โดยได้รับแจ้งให้โอนเงินเข้าบัญชีธนาคารของผู้ฉ้อโกงแทนบัญชีธนาคารของผู้ขาย นอกจากนี้ ก็มีกรณีของ DYRE Malware ซึ่งเป้าหมายคือกลุ่มลูกค้าของธนาคารต่าง ๆ ในสิงคโปร์ ซึ่งธนาคารสิงคโปร์ก็ได้มีการแจ้งเตือนลูกค้าทางอินเทอร์เน็ต

๓.๒.๓.๘ สำหรับในกรณีของ DDos นั้น มีผู้โจมตีระบบทีใช้ชื่อ DD๔BC โดยมีการโจมตีแบบ DDos เพื่อทำให้ระบบล่มไม่สามารถเข้าใช้งานได้ แล้วเรียกร้องให้โอน Bitcoin ให้ ทั้งนี้ จากรายงานพบว่ามีการโจมตีครั้งแรกเมื่อเดือนพฤศจิกายน ค.ศ. ๒๐๑๔ โดยมีเป้าหมายคือ Bitalo Bitcoin Exchange และมีรายงานว่า มีการโจมตีทั้งหมดประมาณ ๑๐ ครั้ง ในสิงคโปร์ คือ เดือนพฤษภาคม มิถุนายน และกรกฎาคม ค.ศ. ๒๐๑๕ จำนวน ๔ ครั้ง ๕ ครั้ง และ๑ ครั้ง ตามลำดับ ทั้งนี้ จากการสังเกต/วิเคราะห์พบว่า หมายเลขบัญชีที่ให้โอน Bitcoin ให้ที่ปรากฏใน Email แต่ละฉบับนั้น มิใช่เลขบัญชีเดียวกัน และจำนวนค่าไถ่ที่เรียกร้องใน Email แต่ละฉบับนั้นก็แตกต่างกันไป (๓๐, ๕๐ หรือ ๑๐๐ Bitcoin) นอกจากนี้ ก็ไม่ปรากฏว่ามีการโจมตีแบบ DDos รอบที่สองตามมา หากไม่มีการจ่ายเงินค่าไถ่ให้ตามคำขู่ที่ระบุไว้ใน Email และเขตเวลา (Time Zone) ของผู้ส่ง Email ก็เป็นคนละเขตเวลาของผู้รับ Email

๓.๒.๓.๙ สำหรับ Ransomware ในสิงคโปร์นั้นพบว่า มีแนวโน้มเพิ่มขึ้นเรื่อย ๆ ซึ่งหน่วยงาน CSA ได้รับรายงานหลายฉบับในเรื่องดังกล่าว ทั้งนี้ วิธีแก้ไขปัญหาเรื่อง Ransomware คือ ให้พยายาม Back-Up ข้อมูลให้เป็นปัจจุบันเป็นระยะ ๆ เพื่อกรณีมีปัญญาเรื่อง Ransomware ขึ้นมา จะได้ Restore ข้อมูลจาก Back-Up ที่ทำไว้ ซึ่งทางส่วนงาน SingCERT ได้จัดทำคำแนะนำไว้บน Website

๓.๒.๓.๑๐ สำหรับศูนย์ตอบสนองเหตุการณ์ฉุกเฉินทางคอมพิวเตอร์ระดับชาติ (National Cyber Incident Response Centre) นั้น จะมีห้อง Lab ขนาดใหญ่ที่สามารถจุคนได้สูงสุดไม่เกิน ๘๐ คน สามารถรองรับงานตรวจพิสูจน์ขนาดใหญ่ ห้อง Lab จะแบ่งพื้นที่การทำงานออกเป็น ๕ ส่วน ประกอบด้วย

๑) Evidence Processing Room (ห้องที่ทำหน้าที่รับพยานหลักฐาน และจัดการเรื่อง Chain of Custody)

๒) Evidence Analysis (วิเคราะห์พยานหลักฐานเพื่อการสืบสวน)

๓) Malware Analysis Lab (วิเคราะห์ Malware โดยเวลาที่วิเคราะห์การทำงานของ Malware ก็จะทำการส่ง Malware นั้นเข้า Sandbox เพื่อดูว่า Malware นั้นมีการทำงานอย่างไร)

๔) Sensitive Investigation Room (เป็นห้องที่สืบสวนคดีสำคัญที่เป็นความลับ ซึ่งเจ้าหน้าที่บางส่วนเท่านั้นที่สามารถเข้าห้องนี้ได้)

๕) Evidence Room (ห้องเก็บพยานหลักฐาน) โดยมีขั้นตอนตามลำดับดังนี้

๕.๑) Collection and Preservation (ลงทะเบียน และดำเนินกระบวนการเก็บรักษาพยานหลักฐาน)

๕.๒) Triage (ประเมิน คัดแยก และวิเคราะห์พยานหลักฐาน)

๕.๓) Forensics Examination (ตรวจพิสูจน์)

๕.๔) Malware Analysis (วิเคราะห์ Malware)

๕.๕) Assessment & Reporting (ประเมินผลการตรวจพิสูจน์และจัดทำรายงาน)

๓.๒.๓.๑๑ ในเรื่อง Advanced Persistent Threat (APT) นั้น เป็นเรื่องของการขโมยข้อมูลและโจมตีระบบเครือข่ายที่ปัจจุบันทั่วโลกมีความกังวลกันมาก ตัวอย่างคือ เมื่อปี ค.ศ. ๒๐๑๖ นั้น หน่วยงาน CSA พบว่ามีองค์กรหนึ่งในสิงคโปร์ที่มีความเป็นไปได้สูงสุดที่จะติด Malware จาก APT ซึ่งองค์กรนี้เคยถูกโจมตีระบบถึง ๓ ครั้งในปี ค.ศ. ๒๐๑๖ ทั้งนี้ ข้อมูลจากแหล่งข่าวรายงานว่า กรณีดังกล่าวมีความเกี่ยวข้องกับประเทศไทย ซึ่งปัจจุบัน หน่วยงาน CSA กำลังอยู่ในระหว่างการสืบสวนเพิ่มเติมร่วมกับหน่วยงานอื่น ๆ ในสิงคโปร์) แต่จากการตรวจพิสูจน์พบว่ามี Email ต้องสงสัยฉบับหนึ่งที่มีไฟล์แนบเป็นไฟล์ Microsoft Word แต่จากการตรวจดูเนื้อหาในไฟล์นั้นไม่พบว่ามีเนื้อหาผิดปกติอะไร โดยเป็นเนื้อหาเกี่ยวกับงานวิจัย อย่างไรก็ตาม พบว่าในไฟล์เอกสารนั้นมี Weaponized Macros ซ่อนอยู่ด้วย จึงได้ทำ Firewall Logs Analysis และได้มีการคัดแยกเครื่องคอมพิวเตอร์นั้นออกจากระบบ รวมถึงได้นำ Email ต้นฉบับมาทำการตรวจพิสูจน์อีกครั้งหนึ่งหลังจากที่ได้ทำการตรวจสอบ Logs และออกรายงานผลการสืบสวนแล้ว ทางหน่วยงาน CSA ก็ได้มีการจัดทำข้อเสนอแนะเพื่อลดความเสี่ยงและได้มีการแลกเปลี่ยนข้อมูลการสืบสวนที่ได้กับหน่วยงานที่เกี่ยวข้อง อาทิเช่น หน่วยงานการข่าว หน่วยงานในต่างประเทศที่เกี่ยวข้อง และหน่วยงานที่เกี่ยวข้องกับการกำหนดยุทธศาสตร์/กลยุทธ์ ทางด้าน Cyber

๓.๒.๔ หน่วยงาน Interpol Global Complex for Innovation (IGCI)

๓.๒.๔.๑ เป็นส่วนงานหนึ่งขององค์การตำรวจสากล (INTERPOL) ที่ได้เปิดทำการอย่างเป็นทางการแล้วเมื่อเดือนเมษายน พ.ศ. ๒๕๕๘ ที่ผ่านมา โดยมีภารกิจหน้าที่เกี่ยวกับการวิจัยและพัฒนาอุปกรณ์และเครื่องมือต่าง ๆ ที่ใช้ในการระบุอาชญากรรมและตัวตนของผู้กระทำความผิด สนับสนุนงานด้านการตรวจพิสูจน์ทางคอมพิวเตอร์ มีห้อง Lab ที่ทันสมัย ตลอดจนมีการจัดการฝึกอบรมเกี่ยวกับนวัตกรรมและเทคโนโลยีใหม่ที่ช่วยในการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ หน่วยงาน IGCI มีเจ้าหน้าที่ประจำประมาณ ๑๕๐ คน โดยมีเจ้าหน้าที่ที่เป็น Seconded Officers จำนวน ๔๐ คน จาก ๒๔ ประเทศ ได้แก่ ประเทศออสเตรเลีย อาร์เจนตินา ออสเตรีย บราซิล แคนาดา จีน อินโดนีเซีย เนเธอร์แลนด์ อิตาลี อิหร่าน อิสราเอล เคนย่า นอร์เวย์ กาตาร์ รวันดา สิงคโปร์ สเปน ไนจีเรีย เกาหลี สหรัฐอเมริกา คูเวต ฝรั่งเศส อังกฤษ และญี่ปุ่น

๓.๒.๔.๒ งานทางด้าน Cyber Crime นั้นแม้ว่าที่ผ่านมา หน่วยงานบังคับใช้กฎหมายประเทศต่าง ๆ จะสามารถจับกุมผู้กระทำความผิดได้ แต่ก็เป็นเพียงผู้กระทำผิดที่อยู่เบื้องหน้า

เท่านั้น มิใช่ผู้กระทำผิดที่อยู่เบื้องหลัง ดังนั้น การสืบสวนสอบสวนจึงต้องทำในส่วนที่เป็น Dark Side ของอินเทอร์เน็ตด้วย ซึ่งเป็นเหตุผลหนึ่งที่สนับสนุนให้มีการก่อตั้งหน่วยงาน IGCI ทั้งนี้ เพื่อที่จะได้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลซึ่งกันและกัน แม้ว่าจะพบเพียงคอมพิวเตอร์เครื่องเดียวในสถานที่เกิดเหตุ

๓.๒.๔.๓ นวัตกรรมที่สนับสนุนความร่วมมือระหว่างประเทศของหน่วยงานตำรวจนั้น มีหลายอย่าง เช่น Secure Communication System (VPN) หรือ ระบบ I๒๔/๗ ซึ่งเป็นระบบที่ให้บริการการติดต่อสื่อสารภายใต้ระบบความปลอดภัยแก่เจ้าหน้าที่ตำรวจทั่วโลก ระบบ INTERPOL SECURE CLOUD SERVICES และระบบฐานข้อมูลเพื่อการสืบสวนต่าง ๆ โดยมีฐานข้อมูลหลักที่สำคัญ ๖ ฐานข้อมูล ประกอบด้วย

๑) ฐานข้อมูล DNA มีประมาณ ๑๖๐,๐๐๐ records

๒) ฐานข้อมูลหนังสือเดินทางที่ถูกสูญหายและที่ถูกโจรกรรม มีประมาณ ๗๒,๙๗๐,๐๐๐ records

๓) ฐานข้อมูลลายพิมพ์นิ้วมือ มีประมาณ ๑,๖๘๗,๐๐๐ records

๔) ฐานข้อมูลอาชญากรทั่วไป (อาทิเช่น ชื่อและรูปถ่าย)

๕) รายละเอียดข้อมูลเกี่ยวกับพฤติการณ์แห่งคดี ลักษณะ และรูปแบบการคุกคามทางเพศต่อเด็ก

๖) รายละเอียดข้อมูลยานพาหนะที่ถูกโจรกรรม

๓.๒.๔.๔ หน่วยงาน IGCI มีการดำเนินโครงการ “Follow the Sun” ซึ่งเป็นโครงการที่ให้การสนับสนุนทางด้านการข่าวแก่ประเทศสมาชิกตลอด ๒๔ ชั่วโมง โดยมีศูนย์ดำเนินการกระจายอยู่ ๓ แห่งทั่วโลก คือ (๑) เมืองลียอง สาธารณรัฐฝรั่งเศส (๒) สาธารณรัฐสิงคโปร์ และ (๓) เมืองบัวโนสไอเรส ราชอาณาจักรสเปน (โดยแบ่งกะการทำงาน ศูนย์ละ ๘ ชั่วโมงครึ่ง)

๓.๒.๔.๕ หน่วยงาน IGCI มีผู้เชี่ยวชาญทางด้าน Cyber จำนวน ๙ คน จากองค์กรต่าง ๆ รวมถึงภาคเอกชนที่มาช่วยสนับสนุนการทำงาน ได้แก่ ๒ คน จากหน่วยงาน NEC และ ๑ คน จากหน่วยงานต่าง ๆ อีก ๘ แห่ง ได้แก่ LAC, Barclays, Trend Micro, CECOM, Cyber Defense, TNO Innovation for Life และ Kaspersky Lab ภารกิจหลักทางด้าน Cyber ของหน่วยงาน IGCI คือ พัฒนาปรับปรุงระบบการทำงาน ประเมินสถานการณ์ของอาชญากรรมทางคอมพิวเตอร์ กระตุ้นให้มีการแลกเปลี่ยนข้อมูลการข่าวระหว่างกันและสร้างความสมดุลระหว่างเรื่องข้อมูลส่วนตัวกับเรื่องความมั่นคงปลอดภัย

๓.๒.๔.๖ เรื่องการสืบสวนที่เกี่ยวข้องกับ Blockchain นั้น มีกระบวนการขั้นตอนดังนี้

๑) คัดแยก/แบ่งกลุ่ม ธุรกรรมและ IP ADDRESS ที่ต้องสงสัย

๒) ค้นหาข้อมูลในเชิงลึกเกี่ยวกับธุรกรรมและ IP ADDRESS ที่ต้องสงสัย

๓) หาความสัมพันธ์ของ IP ADDRESS โดยดูทิศทางการไหลเวียนของ Bitcoins ระหว่าง IP ADDRESS ๒ แห่ง

๔) ค้นหาความสัมพันธ์ของ IP ADDRESS เป้าหมายที่เกี่ยวข้องกับ IP ADDRESS อื่น ๆ

๕) จัดแบ่งกลุ่ม IP ADDRESS ที่ดำเนินการโดย Wallet Operator รายเดียวกัน การดำเนินการดังกล่าว จะทำให้เห็นทิศทางการเคลื่อนไหวว่า สุดท้ายแล้ว Bitcoin เข้าไปที่กระเป๋าของผู้ใด ซึ่งจะทำให้ทราบถึงผู้กระทำความผิดที่อยู่เบื้องหลัง

๓.๒.๔.๗ ในส่วนของ Digital Forensics Laboratory นั้น พบว่าการตรวจพิสูจน์โทรศัพท์มือถือนั้นมีปัญหามาก เนื่องจากมีหลายรุ่นหลายยี่ห้อ และมีแอปพลิเคชันต่าง ๆ เป็นจำนวนมาก บางแอปพลิเคชันก็จะใช้งานเฉพาะแต่ในประเทศนั้น ๆ ดังนั้น ประเทศอื่น ๆ ก็จะไม่มีข้อมูลเกี่ยวกับแอปพลิเคชันดังกล่าว ซึ่งหน่วยงาน INTERPOL พยายามที่จะเข้ามาช่วยเหลือโดยเป็นผู้เผยแพร่ข้อมูลเหล่านี้

<u>การทำคดี CYBER</u>

การทำคดี Cyber นั้น ควรที่จะมีเครือข่ายทางการข่าวมาสนับสนุนการทำงาน เนื่องจากเป็นอาชญากรรมที่เกิดขึ้นอย่างรวดเร็วและเกิดขึ้นที่ใดก็ได้ ดังนั้น จึงควรมีความร่วมมือกับภาคเอกชน รวมถึงควรมีการเก็บข้อมูลผ่านทาง Social Media เพื่อประโยชน์ในเรื่องของการรวบรวมข้อมูลเพื่อการวิเคราะห์ นอกจากนี้ ธุรกรรมทางการเงินที่เกี่ยวข้องกับอาชญากรรมก็มีแนวโน้มที่จะไปใช้ระบบเงินอิเล็กทรอนิกส์หรือ Bitcoin มากขึ้น

ความรู้เกี่ยวกับ Line ปัจจุบันมีผู้ใช้งาน Line ในกว่า ๒๓ ประเทศ โดยมีมากกว่า ๒๓๐ ล้าน users ระบบการใช้งานของ Line เป็นแบบการส่งข้อความแบบหนึ่งต่อหนึ่ง การส่งข้อความแบบกลุ่ม โดยสนับสนุนการใช้งาน ๑๙ ภาษา ข้อมูลที่ Line จัดเก็บมาจาก Address Book จะมีเพียงหมายเลขโทรศัพท์มือถือ และ Email Address เท่านั้น เพื่อให้เพื่อนสามารถที่จะเข้ามา Search และ Add Friend ได้ รวมถึงเพื่อป้องกันการเข้าใช้โดยไม่มีสิทธิ์ ในการ Search Friend บน Line โดยใช้ Line ID นั้น Line ID ที่พิมพ์จะต้องถูกต้องตรงกับ Line ID ที่ลงทะเบียนไว้ทุกตัวอักษรเท่านั้น จึงจะปรากฏให้สามารถ Add Friend ได้ เนื่องจาก Line จะไม่มีการค้นหาแบบ Partial Search บริษัท Line จะจัดเก็บข้อมูลที่เป็น Data/Record/History ไว้เป็นระยะเวลา ๙๐ วัน ในขณะที่ข้อมูลที่เป็น Text จะเก็บไว้เพียง ๓๐ วัน

ความรู้เกี่ยวกับ Facebook ปัจจุบันมีผู้ใช้งาน ๑.๒๘ พันล้านคนทั่วโลก โดยมีจำนวนผู้ใช้งานเฉลี่ย ๑.๙๔ พันล้านคน/เดือน (เป็นผู้ใช้งานผ่านมือถือจำนวน ๑.๗๔ พันล้านคน/เดือน) ในภูมิภาคเอเชียแปซิฟิก มีผู้ใช้งานที่ Active ประมาณ ๓๔๖ ล้านคน/วัน หรือประมาณ ๕๙๒ ล้านคน/เดือน ในประเทศไทย มีผู้ใช้งานเป็นจำนวนมากลำดับต้น ๆ ของโลก คือประมาณ ๓๑ ล้านคน/วัน (เป็นผู้ใช้งานผ่านมือถือ จำนวน ๓๐ ล้านคน/วัน) หรือประมาณ ๔๕ ล้านคน/เดือน (เป็นผู้ใช้งานผ่านมือถือจำนวน ๔๔ ล้านคน/เดือน) สำหรับประเทศมาเลเซียนั้น มีการใช้งานประมาณ ๑๔ ล้านคน/วัน ในขณะที่ประเทศอินเดียนั้นจะเป็นประเทศที่มีผู้ใช้งานมากที่สุดในโลก คือ ประมาณ ๙๙ ล้านคน/วัน สำหรับประเทศอื่น ๆ ที่มีการใช้งานเป็นลำดับต้น ๆ รองจากอินเดีย เช่น บราซิล สหรัฐอเมริกา และอินโดนีเซีย ทั้งนี้ ประเทศที่ไม่มีการใช้งานหรือเข้าถึง Facebook ได้แก่ ประเทศจีน อิหร่าน และเกาหลีเหนือ ธุรกิจขนาดกลางและขนาดย่อมมีแนวโน้มที่จะใช้ Facebook ในการสนับสนุนการประกอบธุรกิจของตน โดยใช้เป็นช่องทางในการเข้าถึงตัวลูกค้าหรือกลุ่มเป้าหมายต่าง ๆ หรือใช้เป็นช่องทางในการโฆษณา

๓.๓ การศึกษาดูงานสาธารณรัฐฟิลิปปินส์

๓.๓.๑ สถานเอกอัครราชทูตไทย ณ สาธารณรัฐฟิลิปปินส์

เมื่อวันอังคารที่ ๙ มกราคม ๒๕๖๑ ได้เข้าพบและเข้าร่วมประชุมหารือข้อราชการ กล่าวแนะนำบทบาทและภารกิจของของหน่วยงานกองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ และตอบข้อซักถาม พร้อมทั้ง หารือแนวทางการประสานความร่วมมือ การจัดทำหนังสือแสดงความเข้าใจ (MOU) กรณีมีคดีพิเศษด้านอาชญากรรมคอมพิวเตอร์ และการแลกเปลี่ยนข้อมูลกับเจ้าหน้าที่สถานเอกอัครราชทูตไทย ณ สาธารณรัฐฟิลิปปินส์

ผลการเข้าหารือและดูงาน

๑) เจ้าหน้าที่ทูตฯ บรรยายให้ข้อมูลว่าฟิลิปปินส์ประชาชน ๑๐๓ ล้านคน โครงสร้างพื้นฐานยังต่ำ ในปี ๒๐๑๖ ระบบคอมพิวเตอร์มีการถูกแฮคโจมตีจำนวนมาก จึงทำให้เกิดการตื่นตัวในเรื่อง IT Security

๒) ชาวฟิลิปปินส์จำนวนกว่า ๘ ล้านคน อยู่ต่างประเทศทำงานเป็นครูสอนภาษาอังกฤษ เนื่องจากมีทักษะภาษาอังกฤษดี เพราะเคยอยู่ในการปกครองของประเทศสหรัฐอเมริกา และไปทำงานเป็นแม่บ้านหาเงินเข้าประเทศ ๓.๖% ของ GDP

๓) ประชาชนชาวฟิลิปปินส์ ๕๐ กว่าล้านคน มีการใช้โทรศัพท์สมาร์ทโฟน และคอมพิวเตอร์ จึงมีความเสี่ยงในเรื่องความปลอดภัยทางไซเบอร์ ทั้งในการติดต่อสื่อสารและการค้าขาย และการที่ประเทศยังด้อยเรื่องโครงสร้างพื้นฐานและกลุ่มทุนผูกขาดระบบการสื่อสารจึงทำให้การสื่อสารไม่เสถียร บางช่วงเวลาโทรศัพท์เคลื่อนที่สัญญาณเต็มก็จะทำให้สัญญาณถูกตัดเป็นระยะ ๆ

๔) ฟิลิปปินส์มีปัญหายาเสพติด การค้ามนุษย์ การฟอกเงินจากยาเสพติด เนื่องจากเจ้าหน้าที่บังคับใช้กฎหมายรายได้น้อย ทำให้มีเหตุการณ์เจ้าหน้าที่ตำรวจฝ่ายต่อต้านการจับตัวเรียกค่าไถ่ ไปทำการจับนักธุรกิจเกาหลีใต้จากบ้านพักไปเป็นตัวประกันเรียกค่าไถ่ ๑ ล้านเหรียญสหรัฐฯ เมื่อได้รับเงินค่า ๕ แสนเหรียญสหรัฐฯ ยังได้ทำการฆาตรกรรมนักธุรกิจภายในกองต่อต้านการจับตัวเรียกค่าไถ่ภายในพื้นที่สำนักงานตำรวจแห่งชาติฟิลิปปินส์ จึงทำให้ประธานาธิบดีดูเตเต้ เข้ามาจัดการปัญหาดำเนินคดีเจ้าหน้าที่ตำรวจ และไล่เจ้าหน้าที่ตำรวจออกกว่า ๖๐ นาย และได้แก้ไขปัญหาโดยเพิ่มเงินเดือนข้าราชการให้ถึง ๘๐% เพื่อแก้ไขปัญหาคอร์รัปชัน

๕) ฟิลิปปินส์กำลังเผชิญกับปัญหาการก่อการร้ายจากกลุ่มไอสิส โดยเฉพาะในเกาะมินดาเนาพื้นที่ประเทศในภาคใต้ที่มีข้อมูลการรับสมัครบุคคลไปเป็นสมาชิกไอสิส แต่ด้วยทางการฟิลิปปินส์มีระบบและแผนดี ทำให้สามารถเข้าจัดการแก้ไขปัญหาดำเนินการตรวจค้นจับกุมกลุ่มบุคคลที่เกี่ยวข้องได้ และเหตุการณ์การเกิดกบฏบนเกาะมาลาวี ที่ต้องมีการนำกองกำลังทหารเข้าสู้รบเพื่อปลดปล่อยเมืองจากกลุ่มกบฏ

๖) สมาชิกไอสิสถูกจับตัวได้ในกรุงมะนิลาจำนวนหนึ่ง แต่จากการวิเคราะห์ข้อมูลอาจไม่สัมพันธ์กับกลุ่มผู้ก่อการฯ ในพื้นที่สามจังหวัดชายแดนภาคใต้ เนื่องจากหลักนิยมและอุดมการณ์ที่ไม่เหมือนกัน

๓.๓.๒ สำนักงานสืบสวนแห่งชาติฟิลิปปินส์

เมื่อวันพุธที่ ๑๐ มกราคม ๒๕๖๑ ประชุมหารือและดูงานที่ National Bureau of investigation (เทียบเท่าหน่วยกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม) ได้เข้าพบและประชุมหารือกับ Mr. Dante Gierran ตำแหน่ง NBI Directors เทียบเท่าอธิบดีกรมสอบสวนคดีพิเศษ และ Mrs. Emelyn M. Aoanan ตำแหน่ง Chief of IT Division เทียบเท่าตำแหน่ง ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ และคณะผู้บริหารสำนักงานสืบสวนแห่งชาติฟิลิปปินส์

ผลการเข้าหารือ

๑) แลกเปลี่ยนแนวทางป้องกันและแก้ไขปัญหาคดีความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ Inter - Cyber Fraud และได้ทักษะการตรวจจับข้อมูลแนวร่วมของกลุ่มไอสิสในสาธารณรัฐฟิลิปปินส์จนสามารถเข้าตรวจค้นจับกุมกลุ่มแนวร่วมได้หลายคน โดยวิธีการทำ Data Analysis เทคโนโลยี Google Street View และการเฝ้าจุดสะกดรอย

๒) การบริหารงานเพื่อควบคุมอาชญากรรมที่เป็นคดีพิเศษนั้น ผู้อำนวยการสำนักงานสืบสวนแห่งชาติฟิลิปปินส์ หรือ NBI Directors บรรยายให้ฟังว่า NBI (National Bureau of Investigation (Philippines)) เริ่มต้นจากหน่วยงานชื่อ BI (The Bureau of Investigation) ซึ่งก่อตั้งเมื่อ ๑๙ มิถุนายน ๒๔๗๙ ในชื่อแรกเริ่มว่า DI (Division of Investigation) เป็นหน่วยสืบสวนสังกัดกระทรวงยุติธรรม มีอำนาจหน้าที่สืบสวนสอบสวน ดำเนินคดี ดำเนินการจัดหา เก็บรวบรวม จัดการให้ได้มาซึ่งพยานหลักฐาน จัดทำบัญชีและรักษาพยานหลักฐาน จัดการเพื่อให้ได้ข้อมูลทั้งหลายเพื่อรักษาผลประโยชน์ของสาธารณะ ซึ่งได้รับอิทธิพลมาจากหน่วยงาน FBI ของประเทศสหรัฐอเมริกา

๓) มีผลงานที่สำคัญในการติดตามสืบสวนตรวจค้นจับกุมกลุ่มไอสิสที่มีการรับสมัครสมาชิกไปเป็นนักรบไอสิสออนไลน์ จนพิสูจน์ทราบที่อยู่ของกลุ่มได้และเข้าตรวจค้นจับกุมโดยเริ่มจากประเทศอินเดียลงข่าวเกี่ยวข้องกับประเทศฟิลิปปินส์ โดยเฉพาะจากเมืองมาลาวี ซึ่งจากการสืบสวนสอบสวนของเจ้าหน้าที่ NBI สามารถขอหมายค้นเข้าทำการตรวจค้นอุปกรณ์ข้อมูลมือถือ ข้อมูลออนไลน์ พบพยานหลักฐานที่สามารถดำเนินคดีข้อหาร้ายแรงแก่กลุ่มบุคคลดังกล่าวได้

๔) เพื่อประโยชน์ในการร่วมมือในอนาคต แม้จะยังไม่ได้ทำ MOU ผู้อำนวยการสำนักงานสืบสวนฯ ก็มีความยินดีที่จะร่วมมือกันในการปกป้องและรักษาประโยชน์คุ้มครองประชาชนของทั้งสองประเทศ โดยเฉพาะความร่วมมือในคดี Cybercrime ซึ่งผู้อำนวยการฯ ได้มอบให้รองผู้อำนวยการฯ ชื่อ Mr. Judy Guzman ซึ่งรับผิดชอบในคดี Cybercrime และสามารถติดต่อประสานกับ Mrs. Emelyn M. Aoanan ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศได้ต่อไปอีกทั้งพร้อมที่จะทำ MOU กับ DSI ด้าน Cybercrime and Cyber Security ในอนาคต

๕) สาธารณรัฐฟิลิปปินส์มีคดีอาชญากรรมไซเบอร์ เช่น แก๊ง Call Center และอาชญากรรมข้ามชาติ การค้ามนุษย์ด้วย ในอนาคตหากพบ IP Address ของผู้ต้องสงสัยปรากฏในสาธารณรัฐฟิลิปปินส์การทำ MOU เพื่อให้ตรวจสอบ IP Address ชื่อสกุลหรืออีเมลจะเป็นประโยชน์เพื่อการปกป้องประชาชนของทั้งสองประเทศ ซึ่งผู้อำนวยการสำนักงานสืบสวนฯ และคณะผู้บริหารฯ แจ้งว่ามีความยินดีเพราะผู้ร้ายเดี๋ยวนี้มีเครื่องมือที่ดีกว่าหากได้รับความร่วมมือกับทางการไทยก็เป็นเรื่องที่น่ายินดี ซึ่งในอนาคตจะทำ MOU ก็เป็นเรื่องที่น่ายินดีแต่ หากมีกรณีเร่งด่วนก็ให้ใช้ช่องทางการติดต่อประสานก่อนได้

๓.๓.๓ สำนักงานตำรวจแห่งชาติฟิลิปปินส์

เมื่อวันพฤหัสบดีที่ ๑๑ มกราคม ๒๕๖๑ ประชุมหารือและดูงานที่ Philippine national police (เทียบเท่าหน่วยงานสำนักงานตำรวจแห่งชาติ ประเทศไทย) ได้เข้าพบและประชุมหารือกับพันตำรวจเอก Ronaldo F DE JESUS ตำแหน่ง Deputy Director Anti - Cybercrime ผู้แทน PDG Ronald M. Dela Rosa ตำแหน่ง Police Director General เทียบเท่าผู้บัญชาการสำนักงานตำรวจแห่งชาติและพันตำรวจเอก Marni C Marcos JR. CESE ตำแหน่งเทียบเท่าผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และคณะ

ผลการเข้าหารือ

๑) มีกฎหมายที่รับผิดชอบ คือ กฎหมายป้องกันอาชญากรรมทางไซเบอร์ พ.ศ. ๒๕๕๕ หรือ The Cybercrime Prevention Act of ๒๐๑๒ ที่มี ๘ หมวด ๓๑ มาตรา บัญญัติให้สามารถดำเนินคดีไซเบอร์โดยเฉพาะจริง ๆ คือ Cybersquatting, Cybersex, Child Pornography, Identity Theft, Illegal Access to Data and Libel โดยคำว่า Cybersquatting: ซึ่งเป็นการจดทะเบียนชื่อโดเมนโดยเจตนามิชอบ เป็นการจดทะเบียนชื่อโดเมนโดยการนำเอาชื่อบุคคล ชื่อทางการค้า หรือเครื่องหมายการค้าที่มีชื่อเสียงของผู้อื่นไปจดทะเบียนชื่อโดเมนเพื่อแสวงหากำไร โดยการนำมาขายคืนแก่ผู้มีส่วนได้ส่วนเสียที่แท้จริงในชื่อดังกล่าวในราคาที่สูง โดยเป็นกฎหมายที่ออกมาเสริมกับกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ฯ The Electronic Commerce Act of ๒๐๐๐ ทั้งนี้ เนื่องจากสาธารณรัฐฟิลิปปินส์ประสบปัญหาที่ไม่มีกฎหมายที่จะสามารถเอาผิดกับผู้ที่สร้างไวรัสคอมพิวเตอร์ประเภทเวิร์มชื่อ ILOVEYOU โดยบุคคลที่ชื่อ Onel de Guzman สำนักงานสืบสวนแห่งชาติฟิลิปปินส์ จึงได้เสนอร่างกฎหมายฉบับดังกล่าว จนประกาศใช้เป็นกฎหมาย

๒) มีการติดตามจับกุมแก๊งคอลเซ็นเตอร์ในสาธารณรัฐฟิลิปปินส์ด้วย และล่าสุดเมื่อวันที่ ๑๓ มกราคม ๒๕๖๑ ตำรวจฟิลิปปินส์สามารถทลายแก๊งชาวจีนและจีนไต้หวันในกรุงมะนิลาได้จำนวน ๑๕๑ คน

๓) จัดการร่วมฝึกกับ FBI, INTERPOL ทั้งการฝึกฝนทักษะด้าน Digital Forensic และทบทวนการปฏิบัติงาน โดยยกตัวอย่างกรณีคดีที่เคยประสบผลสำเร็จ (Cybercrime Case Study) มาร่วมศึกษาเรียนรู้อย่างสม่ำเสมอหน่วยงานตำรวจสาธารณรัฐฟิลิปปินส์ มีหลักสูตร ISDE ที่จะฝึกอบรมบุคลากรของหน่วยให้พร้อมเผชิญเหตุได้อย่างมีประสิทธิภาพ (Identification and Seizure of Digital Evidence for First Responder)

๔) มีการทำงานเชิงรุกประชาสัมพันธ์แจ้งเตือน อธิบายสิทธิของประชาชนผ่านหน้าเว็บไซต์ เว็บเพจ Facebook ของ PNP ให้ประชาชนเข้าใจ เข้าถึงได้อย่างเป็นรูปธรรม

๓.๓.๔ สำนักงานอาชญากรรมทางคอมพิวเตอร์ กระทรวงยุติธรรมสาธารณรัฐฟิลิปปินส์

เมื่อวันศุกร์ที่ ๑๒ มกราคม ๒๕๖๑ ประชุมหารือและดูงานที่ Department of Justice Republic of the Philippine (เทียบเท่ากับหน่วยงานกระทรวงยุติธรรม) ได้เข้าพบและประชุมหารือกับ Mr. JED SHERWIN G. UY ผู้อำนวยการสำนักงานอาชญากรรมทางคอมพิวเตอร์ (Office of Cybercrime (OOC)) และผู้แทนกระทรวงยุติธรรม

ผลการเข้าหารือ

๑) มีความยินดีที่จะทำข้อตกลงความร่วมมือ หรือ MOU ในเรื่อง Cybercrimes + Cyber Security

๒) DOJ มีความยินดีจะรับส่งข้อมูลให้แก่กันและกัน

๓) สาธารณรัฐฟิลิปปินส์ มีปัญหาก่อการร้ายในมินดาเนา และมีคดี Cyber Terrorist ด้วย

๔) เจ้าหน้าที่ของหน่วยมีการร่วมฝึกกับ FBI INTERPOL และตำรวจ รวมทั้งมีการฝึกฝนทักษะด้าน Digital Forensic ทบทวนการปฏิบัติงาน Cybercrime Case Study อย่างสม่ำเสมอเช่นกัน

๕) กรณีบิทคอยน์สาธารณรัฐฟิลิปปินส์ก็ไม่ได้รับรองเงินดิจิทัล และได้มีธนาคารแห่งชาติและกระทรวงการคลังของฟิลิปปินส์ออกเตือนประชาชน เช่นเดียวกันกับประเทศไทย

๖) สาธารณรัฐฟิลิปปินส์ยังไม่มีคดีฉ้อโกงทางบิทคอยน์ และมีเพียงการฉ้อโกงโดยใช้อินเทอร์เน็ตเป็นสื่อกลางซึ่งก็จะใช้กระบวนการยุติธรรมทางอาญาปกติ ในการดำเนินคดี

๓.๔ สรุปผลการศึกษาดูงานต่างประเทศ

จากการเข้าศึกษาดูงานในแต่หน่วยของประเทศทั้ง ๓ ประเทศ ในแต่ละประเทศมีภัยด้านอาชญากรรมทางคอมพิวเตอร์ในรูปแบบที่คล้ายคลึงกัน แต่แนวทางการป้องกันและรับมือต่างกัน ซึ่งอาจจะเกิดจากปัจจัยพื้นฐานในด้านต่าง ๆ เช่น ความพร้อมในด้านสาธารณูปโภค เช่น ระบบการติดต่อสื่อสาร การคมนาคม ความเป็นอยู่ของประชาชน บุคลากรของรัฐ ความพร้อมด้านเทคโนโลยี ส่วนใหญ่แล้ว จะมีแนวทางการแก้ไขและป้องกันโดยการออกกฎหมาย ประสานความร่วมมือระหว่างประเทศ และจัดตั้งหน่วยเฝ้าระวังภัยจากอาชญากรรมคอมพิวเตอร์

๓.๕ สรุปผลสัมมนาในประเทศ

เป็นการนำความรู้ ความเข้าใจที่ได้ไปศึกษาดูงานในต่างประเทศทั้ง ๓ ประเทศ มาต่อยอดในการสัมมนาโดยได้ผลดังนี้

การจัดสัมมนาในครั้งนี้ (รูปแบบของการปาฐกถาพิเศษและการเสวนา) ในหัวข้อ “การปรับตัวกับ Cyber Warfare ในอนาคต และการเสวนาในหัวข้อ “การเผชิญหน้ากับ Cyber Crime ในปัจจุบันและปัญหาที่เกิดขึ้นในอาเซียน”

๓.๕.๑ วิทยากรที่เข้าร่วมการเสวนามีจำนวน ๕ ท่าน ประกอบด้วย ๑) คุณอาจารีย์ ศุภพิโรจน์ ตำแหน่งผู้อำนวยการฝ่ายส่งเสริมเทคโนโลยีการเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ๒) พันตำรวจเอกดุสิต วารีประโคน ตำแหน่งรองผู้กำกับการ ๑ กองบัญชาการตำรวจท่องเที่ยว ๓ สำนักงานตำรวจแห่งชาติ ๓) Mr. Alexandru Caciuloiu ตำแหน่ง Cybercrime Project Coordinator สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ (UNODC) ๔) Mr. Joseph Thorn ตำแหน่ง Liaison Officer Australian Federal Police (AFP) กรมตำรวจแห่งสหพันธรัฐออสเตรเลีย ๕) พันตำรวจเอกสถิตย์ พรหมอุทัย ตำแหน่งผู้กำกับการตำรวจภูธรบ่อผุด สำนักงานตำรวจแห่งชาติ

๓.๕.๒ ผู้เข้าร่วมการสัมมนา มีจำนวนทั้งสิ้น ๑๑๐ คน จากหน่วยงานต่าง ๆ ประกอบด้วย กรมสอบสวนคดีพิเศษ สำนักงานตำรวจแห่งชาติ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ กรมตำรวจแห่งสหพันธรัฐออสเตรเลีย และผู้แทนจากสถานทูตของกลุ่มประเทศสมาชิกอาเซียนทั้ง ๔ ประเทศ สาธารณรัฐประชาธิปไตยประชาชนลาว สาธารณรัฐแห่งสหภาพเมียนมา สาธารณรัฐฟิลิปปินส์ และสาธารณรัฐอินโดนีเซีย

สรุปผลการเสวนาจากวิทยากร ๕ ท่าน ดังนี้

๑) พ.ต.อ.ดุสิต วาลีประโคน

การจัดตั้งศูนย์ป้องกันปราบปรามการฉ้อโกงประชาชนผ่านระบบโทรศัพท์และสื่ออิเล็กทรอนิกส์ (ศปท.ฉปทน.ตร) ขึ้นมาเพื่อรับผิดชอบการสืบสวนสอบสวนคดีความผิดเกี่ยวกับกลุ่มผู้กระทำความผิดโดยการใช้โทรศัพท์หลอกลวง หรือแก๊ง Call Center โดยมี พล.ต.อ.ธนิตศักดิ์ ธีระสวัสดิ์ ที่ปรึกษาพิเศษ ตร. เป็น ผอ.ศป.ฉปทน.ตร.

ศูนย์ป้องกันและปราบปรามการฉ้อโกงประชาชนผ่านระบบโทรศัพท์และสื่ออิเล็กทรอนิกส์ สำนักงานตำรวจแห่งชาติ (ศป.ฉปทน.ตร.) มีผลการดำเนินการตั้งแต่วันที่ ๘ ธันวาคม ๒๕๖๑ ดังนี้

<u>ด้านการสอบสวน</u>

<u>ข้อมูลที่แจ้งมายัง ศป.ฉปทน.ตร.</u>	จำนวน	๔๕๒ คดี
- ผู้เสียหายมาแจ้งที่ศูนย์ฯ ด้วยตนเอง	จำนวน	๑๐๔ คดี
- รับแจ้งผ่านสายด่วน ๑๑๕๕	จำนวน	๓๔๘ คดี
- รวมมูลค่าความเสียหายทั้งสิ้น	จำนวน	๒๔๕,๕๙๗,๐๖๕.๙๒ บาท
- การรับแจ้งเบาะแสและเหตุอื่น ๆ	จำนวน	๑๒๙ เรื่อง

<u>ด้านการปราบปราม</u>

- ยอดหมายจับทั้งหมด	จำนวน	๕๘๖ หมาย
- จับกุมแล้ว	จำนวน	๔๑๗ หมาย
- ไม่มีคุณภาพและอยู่ต่างประเทศ	จำนวน	๑๐๕ หมาย
คงเหลือ	จำนวน	๖๑ หมาย

<u>ด้านการเยียวยาผู้เสียหาย</u>

- มาตรการเยียวยาคืนเงินผู้เสียหายแล้ว	จำนวน	๑๘ ครั้ง
- สามารถอายัดเงินคืนผู้เสียหายได้	จำนวน	๑๑๔ ราย
- รวมเป็นเงินทั้งสิ้น	จำนวน	๒๒,๖๑๒,๒๔๖.๘๗ บาท

จากการวิเคราะห์แผนประทุษกรรมของผู้กระทำความผิด ผู้กระทำความผิดจะใช้ ๒ ช่องทางในการหลอกลวงผู้เสียหาย คือ

๑.๑) การใช้โทรศัพท์หลอกลวงผู้เสียหาย โดยโทรศัพท์ผ่านเครือข่ายอินเทอร์เน็ต VoIP (Voice Over Internet Protocol) แอบอ้างว่าเป็นเจ้าหน้าที่ของหน่วยงานภาครัฐ

๑.๒) การหลอกลวงให้ผู้เสียหายโอนเงินเข้าบัญชีธนาคารของผู้กระทำความผิดที่เปิดไว้รับโอนเงินทางศูนย์ ได้มีการประสานงานความร่วมมือระหว่างประเทศ จำนวน ๘ ครั้ง

โดยสามารถจับกุมผู้ต้องหาเป็นคนไต้หวัน ๔๒ คน คนไทย ๙๒ คน คนมาเลเซีย ๒ คน และคนกัมพูชา ๕ คน ในการดำเนินการส่งผู้ร้ายข้ามแดน ทางศูนย์ฯ ได้มีการประสานงานกับกรมการกงสุล และได้มีการประสานงานกับต่าง ๆ ได้ผลตอบรับอยู่ในเกณฑ์ที่ดี ส่วนในเรื่องของ Call Center ช่วงแรก ๆ ศูนย์ได้ทราบว่าผู้กระทำความผิดมีนำ Cryptocurrency มาใช้ในการ trade กัน ทางศูนย์ฯ ได้ประสานงานกับบริษัทฯที่มีซื้อขาย Cryptocurrency ในประเทศไทย และทำ MOU ร่วมกันในการทำ KYC ในการพิสูจน์ตัวบุคคลเพื่อจะทราบถึงบุคคลที่ทำการซื้อขาย ปัจจุบันทางศูนย์ฯ ไม่ได้รับรายงานเกี่ยวกับการนำ Cryptocurrency มาใช้ในเกี่ยวกรณีของ Call Center และทางศูนย์ฯ มีการเฝ้าระวังเกี่ยวกับเรื่องดังกล่าวไว้แล้ว

สำหรับเรื่องแก๊ง Call Center ในกรณีของคนรับจ้างเปิดบัญชีเพื่อเปิดรับโอนเงินจากผู้เสียหายนั้น ปัจจุบันมีน้อยเนื่องจากผู้กระทำความผิดใช้รูปแบบในการหลอกลวงแบบใหม่ คือ การให้ผู้เสียหาย สมัครใช้ Internet Banking และหลอกลวงเอา OTP ของผู้เสียหายไป โดยจะมีการโอนเงินไปต่างประเทศ ผู้กระทำจะใช้จิตวิทยาในการโทรศัพท์หลอกผู้เสียหาย โดยแอบอ้างเป็นเจ้าหน้าที่รัฐ และส่วนใหญ่ผู้กระทำความผิดจะทำการหลอกลวงผู้เสียหายที่เป็นผู้สูงอายุ โสด และมีฐานะ

๒) พ.ต.อ.สถิตย์ พรหมอุทัย

สำหรับพฤติการณ์ของการกระทำความผิดของแก๊ง Call Center จะมีการหลอกลวงผู้เสียหายที่เป็นคนไทย และคนต่างประเทศ ทางศูนย์ฯ ได้ดำเนินสืบสวนสอบสวนจนพบว่าสถานที่ตั้งที่ใช้ในการกระทำความผิดส่วนใหญ่ตั้งอยู่ที่ต่างประเทศ เช่น ประเทศจีน (จีนแผ่นดินใหญ่) มาเลเซีย กัมพูชา ฟิลิปปินส์ และสหรัฐอาหรับเอมิเรตส์ (ดูไบ) โดยมีหลักการว่า ถ้าหลอกลวงคนประเทศไหน คนประเทศนั้นจะเป็นคนโทรศัพท์หลอกลวงเพื่อสะดวกในการติดต่อสื่อสาร เช่น ผู้กระทำความผิดต้องการโทรศัพท์หลอกลวงคนไทย คนไทยที่เป็นผู้รวมขบวนการจะโทรศัพท์หลอกลวงผู้เสียหาย และใช้บัญชีธนาคารของคนไทยที่เปิดไว้รับโอนเงิน

การสืบสวนสอบสวนเส้นทางความเชื่อมโยงทางการเงินที่ได้จากการหลอกลวงพบว่า ผู้กระทำความผิดจะมีการส่งเงินให้กับคนไต้หวันโดยไม่ผ่านธนาคาร (ใช้วิธีของโพยก๊วน) และอีกช่องทางหนึ่งที่ผู้กระทำความผิดใช้คือ การนำเงินที่ได้จากการหลอกลวงไปซื้อ Bitcoin ซึ่งเป็นเงินสกุลดิจิทัลใน Cryptocurrency ซึ่งทางศูนย์ฯ ได้มีการอายัดเงิน Bitcoin ดังกล่าวไว้ โดยจะเป็นการอายัดบัญชีเงินในส่วนที่เข้าไปซื้อ Bitcoin ทั้งบัญชีบุคคล และบริษัทที่ทำการซื้อขาย Bitcoin นั้น ปัจจุบันไม่พบว่า กลุ่มผู้กระทำความผิดมีการซื้อขายเงินสกุลดิจิทัลใน Cryptocurrency อีก

สำหรับแก๊ง Call Center จะทำงานเป็นองค์กรที่เข้มแข็ง ผู้กระทำความผิดที่ทำหน้าที่เป็น Call Center ส่วนใหญ่จะมีการอบรมกันก่อนที่จะมีการโทรศัพท์ผู้เสียหาย โดยส่วนใหญ่จะอ้างเป็นเจ้าหน้าที่ไปรษณีย์ เจ้าหน้าที่กรมสอบสวนคดีพิเศษและเจ้าหน้าที่อื่นของรัฐในหลายหน่วยงาน สำหรับความร่วมมือระหว่างประเทศเป็นหลัก ทางศูนย์ฯ จะใช้ช่องทางที่มีการประสานงานไว้ โดยทางศูนย์ฯ ได้มีการร่วมจับกุม แก๊ง Call Center กับต่างประเทศหลายครั้ง

๓) คุณอาจารีย์ ศุภพิโรจน์

ในเรื่องของ Cryptocurrency เป็นเทคโนโลยีที่ไม่ใช่นำมาใช้ในเรื่องของการหลอกลวงเพียงอย่างเดียว แต่ Cryptocurrency ก็มีประโยชน์ในเรื่องการโอนเงินที่มีความรวดเร็ว

ไม่ยุ่งยาก และซับซ้อน อยู่ที่ว่าผู้ใช้จะใช้วิธีการที่ถูกหรือไม่ ส่วนในเรื่องของ ICO (Initial Coin Offering) หรือการระดมทุนไม่ใช่เป็นเรื่องที่หลอกลวง แต่เป็นผลพวงจากความนิยมใน Cryptocurrency ที่เติบโตขึ้นอย่างมาก และมีผู้ให้ความสนใจอย่างกว้างขวาง กลายเป็นแหล่งระดมทุนที่สามารถระดมทุนทั้งที่เป็นเงินดิจิทัลและเงินตราสกุลต่าง ๆ ได้อย่างรวดเร็ว ลดขั้นตอนการระดมทุน เปิดโอกาสให้กับผู้ต้องการระดมทุนและผู้ต้องการลงทุนพบกันโดยตรงอย่างรวดเร็วทั่วโลกผ่านเครือข่ายอินเทอร์เน็ต

ก.ล.ต. ในฐานะหน่วยงานกำกับดูแล มีหน้าที่ในการแยก ICO ที่น่าเชื่อถือออกจาก ICO ที่ไม่น่าเชื่อถือ เพื่อป้องกันผู้ระดมทุนนำเงินที่ได้ไปใช้อย่างไม่เหมาะสม เป็นการปกป้องนักลงทุนที่จะเข้าไป โดย ก.ล.ต. มีแนวทางในการกำกับดูแล โดยมองเฉพาะ ICO ที่มีลักษณะเข้าข่ายเป็นการเสนอขายหลักทรัพย์ โดยเตรียมเสนอนิยามหลักทรัพย์ทั่วไปประเภทใหม่ คือ “ส่วนแบ่งร่วมลงทุน” ตามความหมายที่ร่างขึ้นมา ซึ่งยังไม่ออกบังคับใช้ ระบุว่า หมายถึง “ตราสารหรือหลักฐานแสดงสิทธิ ที่แบ่งเป็นหน่วยแต่ละหน่วยมีข้อตกลงที่เป็นสาระสำคัญเป็นอย่างเดียวกัน ซึ่งตราสารหรือหลักฐานดังกล่าวออกเพื่อการจัดการเงินทุนจากประชาชน และให้สิทธิแก่ผู้ถือในการได้รับส่วนแบ่งในผลประโยชน์ที่เกิดจากการร่วมลงทุนในทรัพย์สินใดหรือการดำเนินการใดโดยผู้ถือไม่มีส่วนในการบริหาร การจัดการ หรือการดำเนินการในลักษณะประจำ ทั้งนี้ ไม่รวมถึง กรณีที่เข้าลักษณะใดลักษณะหนึ่งดังต่อไปนี้

๓.๑) หลักทรัพย์ที่มีการประกาศกำหนดไว้แล้วภายใต้ พ.ร.บ.หลักทรัพย์ฯ

๓.๒) ตราสารหรือหลักฐานแสดงสิทธิตามข้อตกลงหรือสัญญาที่มีวัตถุประสงค์หลักเพื่อให้สิทธิในการใช้ทรัพย์สินหรือการรับบริการ

ตามนิยามที่ร่างขึ้นมา สามารถครอบคลุม Token ที่เกิดจากการทำ ICO ได้ด้วย เปิดช่องให้หน่วยงานกำกับดูแลสามารถเข้ามาดูแล ICO ได้ด้วย โดยมีร่างเกี่ยวกับกระบวนการไอซีโอที่ระบุว่าเป็นการออกและเสนอขายหลักทรัพย์ที่ใช้วิธีการทางดิจิทัลกำหนดสิทธิของผู้ถือหลักทรัพย์ จัดเก็บทะเบียน และบังคับข้อตกลงโดยอัตโนมัติเพื่อมารองรับการทำธุรกรรม

สำหรับสถาบันการเงิน และที่ไม่ใช่สถาบันการเงิน (Non-Bank) หันมาออกเทคโนโลยีทางการเงิน ที่เรียกว่า Financial Technology หรือ Fintech จะเป็นเรื่องของการ Disturb หรือการพัฒนา Operation ให้ตอบ Plan Point ให้เยอะ ๆ นั้นเป็นสิ่งที่ดี และสำหรับการออก Cryptocurrency ชนิดต่าง ๆ นั้นจะทำให้เกิด ปรากฏการณ์ที่เรียกว่า Bubble Risks ก็เป็นเรื่องที่เป็นไปได้ และสำหรับมาตรการในการควบคุม ทั้ง Fintech และ Cryptocurrency ทาง ก.ล.ต. ให้คำแนะนำไปที่รัฐมนตรีกระทรวงการคลัง โดยมีการออกมาตรการที่จะมาช่วยเกี่ยวกับการกระทบเสถียรภาพได้

๔) Mr. Alexandru Caciuloiu

UNODC เป็นหน่วยงานขององค์การสหประชาชาติ ทำงานกับชาติสมาชิกในการต่อสู้กับอาชญากรรมต่าง ๆ สนับสนุนการดำเนินการ การปรับปรุงกฎหมายให้สอดคล้องกับสนธิสัญญาอนุสัญญาต่าง ๆ เกี่ยวกับเรื่องการปราบปรามอาชญากรรม นอกจากนี้ UNODC มีจัดการอบรม และพัฒนาให้กับผู้พิพากษา เจ้าหน้าที่รักษากฎหมายและหน่วยงานที่เกี่ยวข้อง มีการศึกษาค้นคว้าวิจัยว่าอาชญากรรมมีการพัฒนาและมีศึกษาถึงแนวโน้มเกี่ยวกับอาชญากรรมเป็นอย่างไร มีการศึกษาในเรื่องของ Cyber Crime, Internet Frauds, Call Center และสนับสนุนในเรื่องของการวิเคราะห์วัตถุพยาน เป็นต้น

Cyber Crime เป็นเรื่องที่มีความซับซ้อน และแต่ละภูมิภาคมีความแตกต่างกัน ทั้งในเรื่องของภาษาวัฒนธรรม และระบบกฎหมาย ซึ่งเป็นสิ่งที่ท้าทายที่จะวิเคราะห์ในเรื่องของอาชญากรรมที่เกิดขึ้นในการต่อสู้กับ Cyber Crime มีปัจจัยอยู่ ๒ ประการ คือ ปัจจัยแรกเป็นเรื่องของกฎระเบียบจะต้องมีการพัฒนาถึงแนวทางการร่างกฎหมายและกฎระเบียบ เนื่องจาก Cyber Crime มีการพัฒนาและมีความเปลี่ยนแปลงอย่างรวดเร็ว จึงทำให้เป็นสิ่งที่ท้าทายสำหรับรัฐบาลและผู้รักษากฎหมาย ปัจจัยที่ ๒ เป็นเรื่องของเทคโนโลยี ข้อจำกัดต่าง ๆ ของเครื่องมือที่ใช้สำหรับเจ้าหน้าที่ควรมีการพัฒนาให้เหมาะสม เราควรคำนึงเรื่องสิทธิมนุษยชนและตระหนักรู้ของประชาชนในเรื่องของอาชญากรรม และรัฐบาลจะต้องมีความรู้ความเข้าใจเกี่ยวกับเรื่องเทคโนโลยีว่ามีการพัฒนาและปรับเปลี่ยนไปทิศทางใด ส่งผลกระทบอย่างไรกับชีวิตรวมไปถึงเรื่องของขีดความสามารถ และเครื่องมือที่ใช้ในการปฏิบัติงาน เช่น เครื่องคอมพิวเตอร์ เครื่องมือในการพิสูจน์พยานหลักฐาน รวมไปถึงตำรวจ อัยการ และผู้พิพากษา ควรมีการจัดอบรมให้ความรู้ความเข้าใจในเรื่องอาชญากรรมไซเบอร์ และสิ่งสำคัญอีกประการหนึ่ง ก็คือ การส่งเสริมเกี่ยวกับความร่วมมือในระหว่างประเทศทั้งระดับภาคี ทวิภาคี และนานาชาติ และความร่วมมือระหว่างหน่วยงานในประเทศ เช่น DSI สตช. ปปง. และ ป.ป.ส. เป็นต้น

ในส่วนการของการพัฒนาขีดความสามารถเป็นสิ่งหนึ่งที่สอดคล้องกันกับการประชุม CCPCJ ซึ่งเป็นการประชุมเหมือนกับสภาในการป้องกันอาชญากรรมและการส่งเสริมให้เกิดความยุติธรรมทางอาญาเป็นการประชุมประจำปี และชาติสมาชิกเป็นส่งผู้แทนเข้าร่วมประชุมจะมีการประชุมถึงการศึกษาวิธีการต่อสู้กับอาชญากรรม การพิจารณาถึงขีดความสามารถ ศักยภาพของชาติสมาชิก ในปีนี้การประชุมพูดถึงเรื่องของ Cyber Crime ซึ่งเป็นเรื่องที่มีการหารือในระดับนานาชาติเป็นจำนวนมาก สิ่งหนึ่งที่ในที่ประชุมเห็นด้วยในการประชุม CCPCJ คือ ต้องมีการดำเนินการในเรื่องการส่งเสริมและพัฒนาศักยภาพให้มากขึ้น ซึ่งลักษณะของอาชญากรรมไซเบอร์นั้นไม่มีพรมแดน เราจึงต้องยกระดับเรื่องขีดความสามารถของผู้ที่เกี่ยวข้องให้ถึงระดับที่จะสามารถระบุและต่อสู้กับอาชญากรรมทางไซเบอร์ให้ได้ โดยต้องได้รับการสนับสนุนจากทุกฝ่ายและเป็นที่ทราบกันดีว่าหน่วยงานด้านการบังคับใช้กฎหมายมีความท้าทายต่าง ๆ ทั้งในเรื่องของการฝึกอบรมการให้ความรู้กับเจ้าหน้าที่ทางด้าน Cyber Crime รวมไปถึงเจ้าหน้าที่อื่น ๆ ให้สามารถทำงานออนไลน์ได้รู้ถึงวิธีการทำงาน และการแก้ไขปัญหาที่เกิดขึ้น เนื่องจากอาชญากรรมต่าง ๆ จะมีหลักฐานที่เป็นดิจิทัล เราจะต้องรู้จักวิธีการใช้อุปกรณ์ที่จะทำการตรวจยึดของผู้กระทำความผิดได้อย่างเหมาะสม เพื่อไม่ให้ส่งผลเสียต่อพยานหลักฐาน และสามารถนำพยานหลักฐานที่ตรวจยึดได้สามารถนำไปใช้เป็นพยานในศาลได้โดยไม่ให้มีการเปลี่ยนแปลง

๕) Mr. Joseph Thorn

หน่วยงาน AFP มีการทำคดีที่เกี่ยวกับ Cyber Crime เป็นจำนวนมาก ทั้งในส่วนของการแลกเปลี่ยนข้อมูลของ Cyber Crime, การค้ามนุษย์ต่าง ๆ เป็นต้น ในเรื่องของ Cyber Crime นั้นจะต้องใช้เวลาในการหาแหล่งข้อมูล ต้องมีเจ้าหน้าที่ประสานงานทั่วโลกทั้งภาครัฐและภาคเอกชนเพื่อพิสูจน์ให้ทราบว่าอาชญากรรมที่เกิดขึ้นเป็นของประเทศไหน มีการสืบสวนสอบสวน และมีการวางแผนการดำเนินการ ในส่วนเรื่องของ Cryptocurrency ก่อนหน้านี้ประเทศออสเตรเลียได้มีการติดตามเกี่ยวกับกรณีของการฟอกเงิน โดยเฉพาะเรื่องของ Bitcoin ถ้าเราติดตามในเรื่องของข้อมูลได้เราก็จะสามารถทราบถึงการแลกเปลี่ยน และความเชื่อมโยงของ Bitcoin ได้

ส่วน Blockchain ก็เป็นเทคโนโลยีหนึ่งที่ยากจะติดตามหาร่องรอย เราจำเป็นต้องใช้เครื่องมือในสำหรับติดตาม Cryptocurrency จะมีหลายสกุล เช่น Bitcoin เป็นเงินสกุลแรก ๆ ที่ออกมา และเป็นเงินสกุลเงินกลางไม่มีธนาคารกลางที่คอยควบคุมส่วนต่าง ๆ ของเครือข่ายจะเป็นตัวสนับสนุนระบบโดยรวม เพราะฉนั้นสกุลเงิน Bitcoin หรือ Cryptocurrency จะเป็นระบบ Blockchain ที่มีความล้ำหน้ามากจะมีบัญชีที่อัพเดตอยู่ตลอดเวลาจะมีบัญชีรับจ่ายสาธารณะ ผู้ซื้อขายจะสามารถทราบว่าใครมีการซื้อขาย Bitcoin กันในกลุ่มของผู้ซื้อขาย แต่จะไม่สามารถทราบได้ว่าใครอยู่เบื้องหลังในการทำธุรกรรมนั้นถ้าอยากจะทราบ เราจะต้องทำการสืบสวนขึ้นไปอีกระดับหนึ่ง เราสามารถนำ Bitcoin ไปแลกเงินสกุลอื่นได้ ในสหรัฐอเมริกาคนที่จะซื้อขาย Cryptocurrency จะต้องมีบัตรประชาชนแสดงตัวตน พาสปอร์ต รูปถ่าย ซึ่งจะมีการคัดกรองที่สามารถตรวจสอบได้ กรณีของประเทศไทยตัวกลาง หรือนายหน้า ก็ต้องปฏิบัติตามกฎระเบียบ ต้องมีการบันทึกข้อมูลของบุคคลไว้ เพื่อสามารถนำมาติดตามตัวบุคคลนั้นได้

บทที่ ๔
วิเคราะห์การบูรณาการการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์

๔.๑ แนวโน้มภัยคุกคามทางอาชญากรรมคอมพิวเตอร์ในปัจจุบันและในอนาคต

เทคโนโลยี Internet of Things (IoT) หรือ “อินเทอร์เน็ตในทุกสิ่ง”หมายถึง การที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การสั่งเปิด - ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น โดยเทคโนโลยีนี้จะเป็นทั้งประโยชน์อย่างมหาศาล หรือ บางแห่งเรียก M๒M ย่อมาจาก Machine to Machine คือ เทคโนโลยีอินเทอร์เน็ตที่เชื่อมอุปกรณ์กับเครื่องมือต่าง ๆ เช่น โทรศัพท์มือถือ รถยนต์ ตู้เย็น โทรทัศน์และอื่น ๆ เข้าไว้ด้วยกัน โดยการเชื่อมโยงช่วยให้สื่อสารกันได้ผ่านระบบอินเทอร์เน็ต จากการคาดการณ์ ในปี ค.ศ. ๒๐๒๐ สิ่งต่าง ๆ กว่าแสนล้านชิ้นจะสามารถเชื่อมต่อกันได้ด้วยระบบ (IoT) ซึ่งจะส่งผลให้ผู้บริโภคทั่วไปจะเริ่มคุ้นเคยกับเทคโนโลยีที่ทำให้พวกเขา สามารถควบคุมสิ่งของต่าง ๆ ทั้งจากในบ้านและสำนักงานหรือจากที่ไหนก็ได้ทั้งนั้น

ในปี ๒๐๑๘ มีเรื่องราวเกิดขึ้นบนโลกไซเบอร์มากมาย เริ่มต้นจากอัตราการละเมิดข้อมูลผ่านโลกออนไลน์เพิ่มขึ้นอย่างชัดเจน รวมถึงเกิดการก่ออาชญากรรมทางไซเบอร์ไม่เว้นแต่ละสัปดาห์ ทำให้การหาวิธีการป้องกันภัยกลายเป็นปัจจัยหลักที่สำคัญสำหรับธุรกิจ และผู้บริหารองค์กร ไม่ว่าจะขนาดเล็ก หรือใหญ่ ต่างต้องคำนึงถึงเรื่องความปลอดภัยเป็นอันดับแรก ดังนั้น มาเตรียมพร้อมสำหรับปี ๒๐๑๙ กับ ๑๐ เทรนด์ความปลอดภัยในโลกไซเบอร์ ที่ทุกส่วนที่เกี่ยวข้องควรจะต้องนำมาพิจารณา เพื่อที่จะสามารถป้องกันและรับมือกับอาชญากรบนโลกไซเบอร์ได้อย่างมีประสิทธิภาพ

๔.๑.๑ เทคโนโลยีบล็อกเชนจะได้รับความนิยมอย่างแพร่หลายมากขึ้น[๑]

เทคโนโลยี Blockchain เป็นระบบการทำธุรกรรมที่ไม่อิงศูนย์กลาง ทำให้ไม่สามารถเปลี่ยนแปลงความถูกต้องของข้อมูลได้ จะไม่มีใครมาละเมิด เปลี่ยนแปลง หรือ พยายาม หลอกลวงผ่านระบบ Blockchain ได้ จึงสามารถนำมาแก้ปัญหาต่าง ๆ ด้านความปลอดภัยได้

๔.๑.๒ แฮกเกอร์เก่งขึ้น

ความสามารถในการเขียนโค้ดแบบซับซ้อนเพื่อใช้โจมตีของแฮกเกอร์ คือ ภัยอันดับแรกเมื่อมีการพูดถึงภัยคุกคามเกิดขึ้นบนโลกไซเบอร์ เนื่องจากพวกเขามีการพัฒนาความสามารถและเรียนรู้ตามการเปลี่ยนแปลงที่เกิดขึ้นอยู่ตลอดเวลา ซึ่งนั่นแสดงให้เห็นว่าเหล่าแฮกเกอร์นั้นอาจเดินเร็วกว่าระบบรักษาความปลอดภัยอยู่ก้าวหนึ่งเสมอ

๔.๑.๓ การป้องกันการจู่โจมบนโลกไซเบอร์จะมีความยากมากขึ้น

อาชญากรรมบนโลกไซเบอร์ กำลังเติบโต และมีปริมาณเพิ่มสูงขึ้นอย่างมาก ส่งผลให้การป้องกันทำได้ยากขึ้นด้วยเช่นกัน เนื่องจากตัวแฮกเกอร์เองมีความเข้าใจในตัวระบบและสามารถ

---

[๑]CAT cyfence. (๒๕๖๒). *๑๐ เทรนด์ความปลอดภัยในโลกไซเบอร์ที่ต้องจับตามองในปี ๒๐๑๙*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: https://www.catcyfence.com/it-security/it-๓๖๐/๑๐-cyber-security-trend-๒๐๑๙

เข้าถึงระบบเพื่อเจาะข้อมูลได้ง่ายไม่แพ้กับเจ้าของระบบหรือเจ้าของธุรกิจเลยทีเดียว อีกทั้งรูปแบบของอาชญากรรมทางไซเบอร์จะมีความหลากหลายมากขึ้น ส่งผลทำให้การเตรียมการเพื่อรับมือ หรือป้องกันได้ยากขึ้นเช่นกัน

๔.๑.๔ ธุรกิจประกันภัยความเสี่ยงบนโลกไซเบอร์จะเป็นที่ต้องการมากขึ้น

ในปี ๒๐๑๙ อุตสาหกรรมประกันภัยจะมีการพัฒนา และมีการนำเสนอผลิตภัณฑ์ด้านการประกันภัยบนโลกไซเบอร์เพิ่มมากขึ้น เพื่อตอบสนองความต้องการของกลุ่มลูกค้า โดยเฉพาะในกลุ่มธุรกิจที่เกี่ยวข้องกับโลกดิจิทัล และออนไลน์ ซึ่งดูจะเป็นความหวัง ในการช่วยป้องกัน และช่วยลดความเสียหายที่จะเกิดขึ้นจากการโจรกรรมได้

๔.๑.๕ การขาดแคลนบุคลากรทางด้านไอที

การขาดแคลนบุคลากรทางด้านไอทีนั้นถือเป็นปัญหาสำคัญสำหรับองค์กร และธุรกิจ เพราะว่าบุคลากรในสาขานี้มีความเกี่ยวข้องกับปัญหาอาชญากรรมบนโลกไซเบอร์โดยตรง

๔.๑.๖ กฎหมายทางไซเบอร์จะถูกนำมาใช้อย่างเคร่งครัด

แม้ว่าจะมีกฎหมาย และกฎระเบียบที่บังคับใช้เกี่ยวกับความปลอดภัยบนโลกไซเบอร์อยู่แล้ว แต่ในปี ๒๐๑๙ นี้คาดว่าจะมีการบังคับใช้กฎหมายที่เข้มงวดมากขึ้น รัฐบาลทั่วโลกต่างกำลังดำเนินการตามกฎหมายเพื่อตรวจสอบกิจกรรมที่ส่อความไม่ชอบมาพากลที่เกิดขึ้นบนโลกไซเบอร์ กฎหมายจึงถือว่าเป็นอีกปัจจัยสำคัญที่จะมีบทบาทอย่างจริงจังเพิ่มมากขึ้น

๔.๑.๗ การติดตามผู้โจมตีบนโลกไซเบอร์จะทำได้ยากขึ้น

กลุ่มอาชญากรทางไซเบอร์เป็นกลุ่มคนที่มีความเข้าใจเกี่ยวกับโลกไซเบอร์อย่างลึกซึ้ง ซึ่งทำให้การติดตามการกระทำผิดทางไซเบอร์จะทำได้ยากขึ้น เนื่องจากคนกลุ่มนี้รู้จักการหาทางหนีทีไล่ เพื่อหลีกเลี่ยงการติดตามจากเจ้าหน้าที่ ดังนั้นในปี ๒๐๑๙ นี้อาชญากรทางไซเบอร์อาจจะ “ล้ำหน้า” กว่าระบบการป้องกันการก่ออาชญากรรมได้

๔.๑.๘ ผู้ดูแลระบบไอทีจะต้องเข้าใจระบบอย่างถ่องแท้

ผู้ที่รับผิดชอบทางด้าน Cyber Security ในองค์กร หรือธุรกิจ ต้องมีความเข้าใจในระบบไอทีของตัวเองอย่างถ่องแท้ มีการตรวจสอบระบบอยู่เสมอ เพราะบางครั้งความผิดพลาดอาจเกิดขึ้นจากบุคคลภายในองค์กรเอง หรือเกิดจากคนในองค์กรที่ทำการก่อการโจรกรรมทางไซเบอร์เพื่อหาผลประโยชน์จากช่องโหว่ที่เกิดขึ้นในระบบได้

๔.๑.๙ การเพิ่มเติมระบบป้องกันการโจมตีบนโลกไซเบอร์

ปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) จะเป็นสิ่งที่ถูกใช้เพื่อเพิ่มการป้องกันการโจมตี เพราะไม่ใช่แค่เพียงประสิทธิภาพในการแจ้งล่วงหน้าว่าการโจมตีจะเกิดขึ้นเท่านั้น แต่ AI ยังสามารถระบุได้ว่า ผู้ที่โจมตีมีวัตถุประสงค์ได้อีกด้วย

๔.๑.๑๐ Internet of Things ยังคงเป็นจุดอ่อน

Internet of Things เป็นอุปกรณ์ เครื่องใช้ต่าง ๆ ที่สามารถเชื่อมต่อกับอินเทอร์เน็ตได้ซึ่งอุปกรณ์เหล่านี้มีอัตราการโจมตีเพิ่มขึ้นตลอดเวลาด้วยเช่นกัน นั่นจึงเป็นสาเหตุที่ผู้เชี่ยวชาญพบว่าอุปกรณ์เหล่านี้เป็นจุดอ่อนที่ทำให้ผู้ใช้งานเสี่ยงต่อการถูกแฮก เพื่อใช้แสวงหาผลประโยชน์ในทางที่ผิดได้ ซึ่งในปี ๒๐๑๙ จะมีการโจรกรรมข้อมูลผ่านอุปกรณ์เหล่านี้เพิ่มขึ้น ผู้ใช้งานจึงควรเพิ่ม

ความปลอดภัยให้กับการใช้งานโดยการป้องกันขั้นพื้นฐานคือ การตั้งค่ารหัสผ่านของระบบให้ปลอดภัยเพื่อยากต่อการโจมตีได้โดยง่าย

การเปลี่ยนแปลงที่เกิดขึ้นบนโลกไซเบอร์ จะยิ่งทวีคูณความรวดเร็วขึ้นไปตามเวลา ดังนั้น ผู้เขียนเห็นว่าการเรียนรู้ ปรับตัว เพื่อรับมือ แก้ไข และป้องกัน จึงถือเป็นปัจจัยที่จะทำให้ธุรกิจ องค์กรต่าง ๆ ปลอดภัยจากการจู่โจมบนโลกไซเบอร์ได้ หรืออย่างน้อยก็ช่วยทำให้เกิดความเสียหายต่อทรัพย์สินดิจิทัลให้น้อยที่สุด

แนวโน้มทางสถิติสำหรับ Cyber security ในอีก ๕ ปีข้างหน้า มีดังนี้[๒]

๑) ความเสียหายจากอาชญากรรมไซเบอร์จะแตะ $๖ ล้านล้านต่อปีในปี ๒๐๒๑ Community และสื่อยักษ์ใหญ่หลายรายมีความเห็นตรงกันเกี่ยวกับความเสียหายที่เกิดขึ้นจากการโจมตีไซเบอร์ โดยคาดการณ์มูลค่าความเสียหายทั้งโลกจะพุ่งสูงถึง $๖ ล้านล้าน (ประมาณ ๒๑๖ ล้านล้านบาท) ในปี ๒๐๒๑ ซึ่งเพิ่มขึ้นถึง ๑๐๐% เมื่อเทียบกับปีที่ผ่านมาที่มีมูลค่าความเสียหายที่ $๓ ล้านล้าน

๒) การลงทุนทางด้าน Cybersecurity จะทะลุ $๑ ล้านล้าน จากปี ๒๐๑๗ ถึง ๒๐๒๑ ผลสำรวจของ Gartner ระบุว่า ปี ๒๐๑๖ การเติบโตของอาชญากรรมไซเบอร์เป็นแรงผลักดันให้เกิดการลงทุนทางด้าน Cyber security ไม่ว่าจะเป็นผลิตภัณฑ์หรือบริการ ซึ่งมีมูลค่ามากกว่า $๘๐,๐๐๐ ล้าน (ประมาณ ๒.๙ ล้านล้านบาท) ซึ่งยังไม่ชัดเจนว่ารวมการป้องกันอุปกรณ์ IoT และอุปกรณ์ระดับ Consumer ด้วยหรือไม่ แต่การลงทุนทั่วโลกในอีก ๕ ปีข้างหน้านี้ถูกคาดการณ์ไว้ว่าจะสูงเกิน $๑ ล้านล้าน (ประมาณ ๓๖ ล้านล้านบาท) อย่างแน่นอน

๓) ความต้องการบุคลากรทางด้าน Cybersecurity จะเพิ่มขึ้นถึง ๑.๕ ล้านตำแหน่ง ในปี ๒๐๑๙ นักวิเคราะห์และสื่อหลายรายต่างให้ความเห็นตรงกันว่า ขณะนี้ทั้งโลกกำลังขาดแคลนบุคลากรผู้เชี่ยวชาญด้าน Cybersecurity ปี ๒๐๑๖ นี้เปิดรับตำแหน่งงานด้าน Cybersecurity มากถึง ๑,๐๐๐,๐๐๐ ตำแหน่ง ในขณะที่ปี ๒๐๑๙ คาดว่าจะรับเพิ่มมากถึง ๑.๕ ล้านตำแหน่ง นั่นหมายความว่า บุคลากรสาย Cybersecurity จะไม่มีคำว่าตกงานแน่นอน

๔) มนุษย์จะตกเป็นเป้าหมายของภัยคุกคามไซเบอร์สูงถึง ๔,๐๐๐ ล้านคน ในปี ๒๐๒๐ โลกกำลังเข้าสู่ยุคดิจิทัลที่ทุกอย่างจะมีการนำเทคโนโลยีเข้ามาสนับสนุน ส่งผลให้มนุษย์จะกลายเป็นเป้าหมายของอาชญากรไซเบอร์แทนที่จะเป็นอุปกรณ์คอมพิวเตอร์ เนื่องจากเป็นองค์ประกอบที่อ่อนแอมากที่สุด Microsoft ประมาณการณ์ไว้ว่า ในปี ๒๐๒๐ คนจำนวน ๔,๐๐๐ ล้านคนจะอยู่ในโลกออนไลน์ ซึ่งสูงกว่าปัจจุบันถึง ๒ เท่า แน่นอนว่ามีเหยื่อให้แฮ็กเกอร์โจมตีเยอะจนเลือกไม่ถูก

๕) อุปกรณ์ IoT กว่า ๒๐๐,๐๐๐ ล้านชิ้นจำเป็นต้องได้รับการปกป้อง ในปี ๒๐๒๐ คาดการณ์ว่าจะมีอุปกรณ์ IoT เป็นจำนวนมากถึง ๒๐๐,๐๐๐ ล้านเครื่อง เพิ่มขึ้นจาก ๑๕,๐๐๐ ล้านเครื่อง ในปี ๒๐๑๕ ถึง ๑๓ เท่า นั่นหมายความว่า แฮคเกอร์มีช่องทางให้เลือกโจมตีมากขึ้นอย่างมหาศาลในอีก ๕ ปีข้างหน้า นอกจากนี้ Microsoft ยังพยากรณ์ไว้อีกว่า ภายในปี ๒๐๒๐ ปริมาณข้อมูลที่อยู่ในโลกออนไลน์จะเพิ่มขึ้นมากกว่าปัจจุบันถึง ๕๐ เท่า

---

[๒]Josh Fruhlinger. (๒๕๖๓). *Top cybersecurity facts, figures and statistics.* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: www.csoonline.com/article/๓๑๕๓๗๐๗/security/top-๕-cybersecurity-facts-figures-and-statistics-for-๒๐๑๗.html

ประเทศไทยถึงแม้จะมียุทธศาสตร์ Thailand ๔.๐ แต่ก็ต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์ เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง อีกทั้งต้องสมดุลกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่เข้มแข็ง การเติบโตและความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชากรในประเทศไทยเพิ่มขึ้นอย่างก้าวกระโดดในช่วง ๒-๓ ปีที่ผ่านมา จึงทำให้ความเสี่ยงด้านภัยคุกคามไซเบอร์มีสูงขึ้นหลายเท่าตัวและจะเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศอย่างหลีกเลี่ยงไม่ได้

ความสามารถของอาชญากรทางไซเบอร์ที่มีจำนวนเพิ่มมากขึ้น ผู้โจมตีจะมีความสามารถในการเข้าถึงข้อมูลขององค์กรที่สำคัญ การโจมตีมีความซับซ้อนมากกว่าเดิม และผู้โจมตีจะมองหาช่องโหว่ในสภาพแวดล้อมการทำงานในองค์กรได้อย่างง่ายดาย ซึ่งจากการสำรวจที่ผ่านมาพบว่าบุคลากรในองค์กรมีโอกาสถูกโจมตีได้มากที่สุด โดยผู้โจมตีที่มาจากภายนอกองค์กร เพราะองค์กรเหล่านั้นไม่มีความคล่องตัวในการดำเนินการ องค์กรไม่มีงบประมาณสำหรับความมั่นคงปลอดภัยไซเบอร์ และขาดทักษะด้านความมั่นคงปลอดภัยไซเบอร์

๔.๒ วิเคราะห์หน่วยงานและรูปแบบการบริหารจัดการอาชญากรรมคอมพิวเตอร์ (กฎหมาย)

๔.๒.๑ ประเทศมาเลเซีย จากการเข้าไปศึกษาดูงานของผู้เขียนและคณะพบว่า ประเทศมาเลเซียถือว่าเป็นแหล่งซ่องสุมของผู้กระทำความผิดชาวต่างชาติผิวดำที่มาจากกลุ่มประเทศทวีปแอฟริกา ซึ่งพฤติการณ์ในการกระทำความผิดเหล่านี้มีลักษณะการหลอกลวงที่พบคือเป็น Romance Scam ซึ่งเป็นการหลอกลวงโดยพูดคุยกับผู้เสียหายผ่าน Social Media ต่าง ๆ โดยเฉพาะอย่างยิ่ง Facebook และใช้ภาพถ่ายที่เป็นหน้าตาฝรั่งผิวขาวแต่ตัวตนจริง ๆ เป็นคนไนจีเรีย และจะแสดงทีท่าว่ามีความสนใจรักใคร่ผู้เสียหายและอยากจะแต่งงานด้วย แต่ติดขัดปัญหาบางอย่างจึงขอให้ช่วยโอนเงินมาให้ ซึ่งผู้เสียหายส่วนใหญ่ก็จะโอนเงินไปให้หลายครั้ง แต่เนื่องด้วยการพูดคุยดังกล่าวมักจะกระทำผ่านทาง Facebook และมักจะใช้ชื่อปลอมในการติดต่อพูดคุย จึงทำให้ไม่สามารถทราบตัวตนที่แท้จริงของผู้หลอกลวง นอกจากนี้เวลาที่ผู้เสียหายไปแจ้งความที่สถานีตำรวจท้องที่ แต่ทางเจ้าหน้าที่ตำรวจมาเลเซียก็มักจะมิได้มีการดำเนินการใด ๆ ดังนั้น สถานเอกอัครราชทูตไทยฯ จึงมักจะแนะนำให้ผู้เสียหายไปติดต่อกับตำรวจที่รับผิดชอบคดีอาชญากรรมทางเทคโนโลยี แต่ทว่าประเทศมาเลเซียกลับให้วีซ่ากับชาวต่างชาติเหล่านี้อย่างง่ายดาย หากผู้เขียนและคณะซึ่งเป็นเจ้าหน้าที่ของกรมสอบสวนคดีพิเศษต้องการให้สถานเอกอัครราชทูตไทยฯ ให้การสนับสนุนหรือช่วยเหลือในด้านใด ๆ ขอให้ดำเนินการแบบคู่ขนาน คือ มีหนังสือเป็นทางการจากปลัดกระทรวงยุติธรรมแจ้งไปยังปลัดกระทรวงการต่างประเทศและในขณะเดียวกัน ก็ให้กรมสอบสวนคดีพิเศษประสานแจ้งให้สถานเอกอัครราชทูตไทยฯ ทราบด้วยอีกทางหนึ่ง

แนวทางการบริหารจัดการอาชญากรรมคอมพิวเตอร์ของประเทศมาเลเซีย ซึ่งกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ในมาเลเซียนั้นมี ๘ ฉบับ ยุทธศาสตร์ที่หน่วยงานตำรวจมาเลเซียจะนำมาใช้เพื่อแก้ไขปัญหาอาชญากรรมคอมพิวเตอร์ คือ (๑) ให้การศึกษาและสร้างความตระหนักให้กับกลุ่มเสี่ยง (๒) บังคับใช้กฎหมายอย่างจริงจังและแก้ไขปรับปรุงกฎหมายในปัจจุบัน (๓) เสริมสร้างศักยภาพของเจ้าหน้าที่โดยการฝึกอบรมในด้านต่าง ๆ อาทิเช่น การสืบสวนสอบสวนทางอาชญากรรมคอมพิวเตอร์ VoIP ระบบสื่อสารแบบไร้สาย และการตรวจพิสูจน์ต่าง ๆ

เป็นต้น (๔) จัดซื้อจัดจ้างอุปกรณ์และแอปพลิเคชันต่าง ๆ (เช่น ระบบการติดตาม IP หรือสื่อใหม่ ๆ และกล่องอุปกรณ์สำหรับการสืบสวน เป็นต้น) และ (๕) เสริมสร้างความร่วมมือระหว่างหน่วยงานในประเทศ/ความร่วมมือระหว่างประเทศ และการทำงานแบบกองกำลังร่วม (Task Force) เช่น หน่วยงาน Interpol, Europol และ Virtual Global Taskforce (VGT) เป็นต้น

๔.๒.๒ สาธารณรัฐสิงคโปร์ จากการเข้าไปศึกษาดูงานของผู้เขียนและคณะพบว่า หน่วยงานบังคับใช้กฎหมายของสาธารณรัฐสิงคโปร์ก็พบปัญหาอาชญากรรมคอมพิวเตอร์หลากหลาย ไม่ต่างจากอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในประเทศไทย เช่น Internet Love Scam หรือ Romance Scam, Credit for Sex Scam และอื่นๆ

แนวทางการบริหารจัดการอาชญากรรมคอมพิวเตอร์ของสาธารณรัฐสิงคโปร์ งานทางด้าน Cyber Crime นั้นแม้ว่าที่ผ่านมา หน่วยงานบังคับใช้กฎหมายประเทศต่าง ๆ จะสามารถจับกุมผู้กระทำความผิดได้ แต่ก็เป็นเพียงผู้กระทำผิดที่อยู่เบื้องหน้าเท่านั้น มิใช่ผู้กระทำผิดที่อยู่เบื้องหลัง ดังนั้น การสืบสวนสอบสวนจึงต้องทำในส่วนที่เป็น Dark Side ของอินเทอร์เน็ตด้วย ซึ่งเป็นเหตุผลหนึ่งที่สนับสนุนให้มีการก่อตั้งหน่วยงาน IGCI ทั้งนี้ เพื่อที่จะได้มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลซึ่งกันและกัน โดยหน่วยงาน IGCI มีเจ้าหน้าที่ประจำประมาณ ๑๕๐ คน โดยมีเจ้าหน้าที่ที่เป็น Seconded Officers จำนวน ๔๐ คน จาก ๒๔ ประเทศ ได้แก่ ประเทศออสเตรเลีย อาร์เจนตินา ออสเตรีย บราซิล แคนาดา จีน อินโดนีเซีย เนเธอร์แลนด์ อิตาลี อิหร่าน อิสราเอล เคนย่า นอร์เวย์ กาตาร์ รวันดา สิงคโปร์ สเปน ไนจีเรีย เกาหลี สหรัฐอเมริกา คูเวต ฝรั่งเศส อังกฤษ และญี่ปุ่น มีภารกิจหน้าที่เกี่ยวกับการวิจัยและพัฒนาอุปกรณ์และเครื่องมือต่าง ๆ ที่ใช้ในการระบุอาชญากรรมและตัวตนของผู้กระทำความผิด สนับสนุนงานด้านการตรวจพิสูจน์ทางคอมพิวเตอร์ มีห้อง Lab ที่ทันสมัยตลอดจนมีการจัดการฝึกอบรมเกี่ยวกับนวัตกรรมและเทคโนโลยีใหม่ที่ช่วยในการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์

การทำคดี Cyber นั้น ควรที่จะมีเครือข่ายทางการข่าวมาสนับสนุนการทำงาน เนื่องจากเป็นอาชญากรรมที่เกิดขึ้นอย่างรวดเร็วและเกิดขึ้นที่ใดก็ได้ ดังนั้น จึงควรมีความร่วมมือกับภาคเอกชน รวมถึงควรมีการเก็บข้อมูลผ่านทาง Social Media เพื่อประโยชน์ในเรื่องของการรวบรวมข้อมูลเพื่อการวิเคราะห์

๔.๒.๓ สาธารณรัฐฟิลิปปินส์ จากการเข้าไปศึกษาดูงานของผู้เขียนและคณะพบว่า สาธารณรัฐฟิลิปปินส์ยังเป็นประเทศที่กำลังพัฒนาในด้านเทคโนโลยี จึงขาดการป้องกันภัยในด้านนี้ จะสังเกตเห็นว่ามีผู้ก่อเหตุในลักษณะของแก๊ง Call Center ในระดับแรกของประเทศในกลุ่มอาเซียน มีผู้ที่สร้างไวรัสคอมพิวเตอร์ประเภทเวิร์มชื่อ ILOVEYOU โดยบุคคลที่ชื่อ Onel de Guzman จนทำให้มีกฎหมายในด้านป้องกันภัยอาชญากรรมคอมพิวเตอร์มากขึ้น

แนวทางการบริหารจัดการอาชญากรรมคอมพิวเตอร์ของสาธารณรัฐฟิลิปปินส์ สำหรับหน่วยงานบังคับใช้กฎหมาย โดยการจัดบุคลากรและเครื่องมือให้มีหน้าที่เฝ้าระวังภัยจากอาชญากรรมคอมพิวเตอร์ และออกกฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์

๔.๓ ความร่วมมือระว่างประเทศของประเทศ มาเลเซีย สาธารณรัฐฟิลิปปินส์ และสาธารณรัฐสิงคโปร์[๓]

๔.๓.๑ แบบทางการ ปัจจุบันประเทศไทยมีสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในคดีอาญาที่เรียกว่า Treaty on Mutual Legal Assistance in Criminal Matters กับประเทศต่าง ๆ รวม ๑๒ ประเทศ ได้แก่ สหรัฐอเมริกา แคนาดา ฝรั่งเศส นอร์เวย์ เกาหลีใต้ จีน อินเดีย โปแลนด์ ศรีลังกา เปรู ออสเตรเลีย เบลเยี่ยม ส่วนประเทศ สหราชอาณาจักร ฝรั่งเศส และนอร์เวย์ ที่ไม่มีสนธิสัญญาก็จะถือหลักต่างตอบแทนสนธิสัญญาก็จะถือหลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัติ

ในส่วนของประชาคมอาเซียน ประเทศไทยยังไม่มีสนธิสัญญาในเรื่องดังกล่าวกับประเทศสมาชิกอาเซียนโดยตรงในลักษณะทวิภาคี แต่ในกลุ่มประชาคมอาเซียนด้วยกันได้มีการลงนามสนธิสัญญาว่าด้วย ช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาของภูมิภาคอาเซียน (The Treaty on Mutual Legal Assistance In Criminal Matters among Like-minded ASEAN Member Countries) ซึ่งเป็นเครื่องมือทางกฎหมายสำคัญระดับภูมิภาคที่กำหนดมาตรการทางกฎหมายสำหรับหน่วยงานบังคับใช้กฎหมาย ในการให้ความช่วยเหลือและการขอความช่วยเหลือระหว่างรัฐต่อรัฐในภูมิภาคอาเซียนในเรื่องทางอาญาไว้หลายรูปแบบสนธิสัญญาฯ ได้เปิดโอกาสระหว่างผู้ประสานงานกลางของแต่ละรัฐ สามารถส่งคำร้องขอความช่วยเหลือและการติดต่อประสานงานผ่านทางช่องทางตำรวจสากล (International Criminal Police Organization หรือ INTERPOL) หรือองค์การตำรวจอาเซียน (ASEANAPOL) ในสถานการณ์เร่งด่วนได้ จึงทำให้ข้อมูลและพยานหลักฐานที่ได้จากการประสานงานทางคดีผ่านช่องทางดังกล่าว รอรับการยอมรับในกระบวนพิจารณาชั้นศาลมากขึ้น (ชิตพล, ๒๕๕๖) สนธิสัญญาดังกล่าวได้ร่วมลงนามโดยประเทศสมาชิกอาเซียนแล้ว โดยไทยได้ให้สัตยาบันสนธิสัญญานี้เมื่อวันที่ ๓๑ มกราคม ๒๕๕๖

๔.๓.๒ แบบไม่เป็นทางการ (Informal Channel) การดำเนินการประสานความร่วมมือดังกล่าวสามารถ แบ่งได้ ดังนี้[๔]

๔.๓.๒.๑ การประสานการปฏิบัติระหว่างหน่วยงานต่อหน่วยงาน (Agency to Agency) เป็นรูปแบบของความร่วมมือทวิภาคีระหว่างหน่วยงานบังคับใช้กฎหมายของประเทศไทยและหน่วยงานบังคับใช้กฎหมายต่างประเทศ มีวัตถุประสงค์ในการแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการสืบสวนสอบสวนเพื่อให้การบังคับใช้กฎหมายมีความเข้มแข็ง มากขึ้น ส่งผลให้การทำงานของหน่วยงานทั้งสองฝ่ายมีความแนบแน่นและมีประสิทธิภาพมากขึ้น การประสาน การปฏิบัติระหว่างหน่วยงาน ต่อหน่วยงานที่กล่าวถึงนี้ ส่วนใหญ่แล้วจะมีการดำเนินการในรูปแบบของการลงนามบันทึกความเข้าใจระหว่างหน่วยงาน โดยกำหนดเนื้อหาสาระสำคัญเฉพาะหัวข้อ และเป็นการดำเนินการที่ไม่ขัดกับกฎหมายภายในประเทศ ซึ่งกรมสอบสวนคดีพิเศษมีการลงนามในบันทึกความเข้าใจระหว่างหน่วยงานกับหน่วยงาน บังคับใช้กฎหมายต่างประเทศหลายหน่วยงาน เช่น บันทึกความเข้าใจระหว่างกรมสอบสวนคดีพิเศษกับสำนักงานตำรวจเครือรัฐออสเตรเลีย หรือบันทึกความเข้าใจ

---

[๓]กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๓๓

[๔]กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๒๑-๑๒๒

ระหว่างกรมสอบสวนคดีพิเศษกับสำนักงานปราบปรามอาชญากรรม แห่งสหราชอาณาจักร ในเรื่องการต่อต้านอาชญากรรมข้ามชาติ ในส่วนของประเทศสมาชิกภูมิภาคอาเซียนยังอยู่ในระหว่างการดำเนินการขอความเห็นชอบตามมติคณะรัฐมนตรี เรื่องการลงนามบันทึกความเข้าใจระหว่างกรมสอบสวนคดีพิเศษ กับสำนักงานตำรวจแห่งชาติกัมพูชาว่าด้วยการค้ามนุษย์ข้ามพรมแดน

๔.๓.๒.๒ การประสานการปฏิบัติโดยผ่านความร่วมมือขององค์กรความร่วมมือระหว่างประเทศ การประสานการปฏิบัติผ่านองค์กรความร่วมมือระหว่างประเทศ ได้แก่ องค์กรสหประชาชาติ (UN) องค์กรตำรวจสากล (INTERPOL) องค์กรตำรวจอาเซียน (ASEANAPOL) เป็นการประสานการปฏิบัติ ในรูปแบบที่ไม่เป็นทางการ กล่าวคือ ข้อมูลที่ได้รับสามารถนำมาใช้ในขั้นตอนการสืบสวนสอบสวนได้ แต่ไม่สามารถใช้เป็นพยานต่อศาลในกระบวนการพิจารณาคดี แต่ในส่วนของสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาของอาเซียน พ.ศ. ๒๕๔๗ ซึ่งเป็นเครื่องมือทางกฎหมายสำคัญระดับภูมิภาคที่ได้กำหนดมาตรการทางกฎหมายสำหรับหน่วยงานบังคับใช้กฎหมายในการให้ความช่วยเหลือและการขอความช่วยเหลือระหว่างรัฐต่อรัฐ ในภูมิภาคอาเซียนในเรื่องทางอาญาไว้หลายรูปแบบ อย่างไรก็ตามสนธิสัญญาอาเซียนฉบับนี้มีข้อจำกัดที่คล้ายคลึงกับสนธิสัญญาระหว่างประเทศ ในเรื่องทางอาญาทั่วไป โดยรัฐผู้รับคำร้องสามารถปฏิเสธการให้ความช่วยเหลือได้ หากคำร้องดังกล่าวเกี่ยวข้องกับประเด็นการเมือง เชื้อชาติ เพศ ศาสนา ชาติกำเนิด สัญชาติ และความผิดทางทหาร หรือความมั่นคงในลักษณะอื่น ๆ โดยสนธิสัญญาได้เปิดโอกาสให้ผู้ประสานงานกลางส่งคำร้องขอความช่วยเหลือ และการติดต่อประสานงานผ่านช่องทางตำรวจสากล (INTERPOL) หรือ องค์การตำรวจอาเซียน (ASEANAPOL) ในสถานการณ์เร่งด่วนได้ จึงทำให้ข้อมูลและพยานหลักฐานที่ได้จากการประสานงานทางคดีผ่านทางช่องทางนี้ ได้รับการยอมรับในกระบวนการพิจารณาคดีในชั้นศาลด้วย เนื่องจากมีการระบุให้เป็นช่องทางการประสานงานใน สนธิสัญญาดังกล่าว

๔.๓.๒.๓ การประสานการปฏิบัติผ่านเจ้าหน้าที่ประสานงานประจำสถานเอกอัครราชทูต (LEGATS, Attache, Liaison) สำหรับประเทศสมาชิกประชาคมอาเซียน มีประเทศที่มีผู้ช่วยทูตฝ่ายตำรวจ (Police Attaché) ประจำ ณ สถานทูต ในประเทศไทย ๒ ประเทศ คือ มาเลเซีย และอินโดนีเซีย

๔.๓.๓ ความร่วมมือระหว่างประเทศในทางอาญา ความร่วมมือระหว่างประเทศในเรื่องทางอาญา Mutual Legal Assistance in Criminal Matters หรือที่เรียก MLAT เป็นการดำเนินการให้หรือขอความช่วยเหลือจากต่างประเทศในเรื่องทางอาญาระหว่างรัฐต่อรัฐ ในเรื่องเกี่ยวกับการดำเนินการสืบสวนสอบสวน ฟ้องคดี ริบทรัพย์สินและการดำเนินการ อื่น ๆ ที่เกี่ยวเนื่องกับคดีอาญา[๕]

๔.๓.๓.๑ หลักกฎหมายที่เกี่ยวข้องกับความร่วมมือระหว่างประเทศในเรื่องทางอาญา

๑) หลักความผิดสองรัฐ (Double Criminality/Dual Criminality) หลักการนี้แต่เดิมใช้ในเรื่องส่งผู้ร้ายข้ามแดน ส่วนการให้ความร่วมมือระหว่างประเทศในเรื่องทางอาญานั้นก็ได้นำหลักความผิดสองรัฐนี้มาด้วยเช่นกัน แต่อาจไม่เคร่งครัดเท่ากับในเรื่องการส่งผู้ร้ายข้ามแดน โดยจะเป็นการให้ความร่วมมือกันในเรื่องอื่น ซึ่งอาจเป็นเพียงขั้นตอนวิธีการของการดำเนินคดีอาญา ซึ่งอาจมีผลกระทบต่อสิทธิบุคคลอยู่บ้าง แต่ก็ไม่ใช่สิทธิต่อตัวร่างกายของบุคคลนั้นโดยตรง

---

[๕] กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๓๐-๑๓๓

๒) หลักต่างตอบแทนหรือหลักถ้อยทีถ้อยปฏิบัติ (Reciprocity) หลักการนี้เป็นหลักพื้นฐานในเรื่องความร่วมมือระหว่างประเทศในเรื่องทางอาญาโดยเป็นการที่รัฐหนึ่งยอมรับในการบังคับให้ตามคำร้องขอของรัฐ ภายใต้เงื่อนไขว่าหากรัฐตนได้ร้องขอให้รัฐอื่นนั้นดำเนินการเช่นเดียวกันแล้ว รัฐนั้นจะยอมปฏิบัติเช่นเดียวกัน หลักต่างตอบแทนนี้ทำให้รัฐทั้งสองต่างมีความผูกพันตามกฎหมายระหว่างประเทศมากกว่าหลักไมตรีจิต (Comity)

๔.๓.๓.๒ สรุปสาระสำคัญของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. ๒๕๓๕ และที่แก้ไขเพิ่มเติม

๑) ความหมายของความช่วยเหลือและวิธีการร้องขอความช่วยเหลือ

มาตรา ๔ “ความช่วยเหลือ หมายความว่า ความช่วยเหลือในเรื่องเกี่ยวกับการดำเนินการสืบสวน สอบสวน ฟ้องคดี ริบทรัพย์สิน และการดำเนินการอื่น ๆ ที่เกี่ยวเนื่องกับคดีอาญา”

จากบทบัญญัติมาตรา ๔ ความช่วยเหลือระหว่างประเทศในเรื่องทางอาญาจึงหมายถึง ความช่วยเหลือในการสืบสวนสอบสวนฟ้องคดีริบทรัพย์สินและการดำเนินการอื่น ๆ ที่เกี่ยวเนื่องกับคดีอาญา ซึ่งหากประสงค์จะขอความช่วยเหลือนี้จากประเทศไทยจะต้องทำคำร้องขอความช่วยเหลือส่งไปยังอัยการสูงสุดผู้ประสานงานกลาง แต่สำหรับประเทศที่ไม่มีสนธิสัญญาในเรื่องความร่วมมือระหว่างประเทศในเรื่องทางอาญากับประเทศไทย ให้จัดส่งคำร้องขอโดยวิถีทางการทูตตามที่ได้บัญญัติไว้ในมาตรา ๑๐

“มาตรา ๑๐ ประเทศที่มีสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญากับประเทศไทยหากประสงค์จะขอความช่วยเหลือตามที่บัญญัติไว้ในหมวดนี้จากประเทศไทย ให้ทำคำร้องขอความช่วยเหลือส่งไปยังผู้ประสานงานกลาง แต่สำหรับประเทศที่ไม่มีสนธิสัญญาดังกล่าวกับประเทศไทยให้ส่งคำร้องขอโดยวิถีทางการทูต คำร้องขอความช่วยเหลือให้ทำตามแบบ หลักเกณฑ์ วิธีการและเงื่อนไข ที่ผู้ประสานงานกลางกำหนด”

๒) หลักเกณฑ์การให้ความช่วยเหลือทางอาญาแก่ต่างประเทศ (มาตรา ๔)

๒.๑) การร้องขอความช่วยเหลือนั้นจะดำเนินการตามสนธิสัญญาว่าด้วยความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาระหว่างประเทศผู้ร้องขอกับประเทศไทย กรณีที่ประเทศ ผู้ร้องขอไม่มีสนธิสัญญาดังกล่าว ก็ต้องปรากฏว่าประเทศผู้ร้องขอจะให้ความช่วยเหลือทำนองเดียวกันเมื่อประเทศไทยร้องขอ

๒.๒) การกระทำความผิดที่เป็นมูลฐานในการร้องขอต้องเป็นความผิดตามกฎหมายไทย เว้นแต่จะมีสนธิสัญญาระบุเป็นอย่างอื่น

๒.๓) ประเทศไทยอาจปฏิเสธการให้ความช่วยเหลือได้หากการช่วยเหลือดังกล่าวจะกระทบกระเทือนอธิปไตย ความมั่นคง หรือสาธารณประโยชน์ที่สำคัญของประเทศไทย หรือเกี่ยวกับความผิดทางการเมือง หรือการทหาร

๓) ประเภทของความช่วยเหลือ ประเภทของความช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาโดยลักษณะความร่วมมือระหว่างประเทศในขั้นตอนสืบสวนสอบสวน การพิจารณาคดี ซึ่งถือว่ามีขอบเขตในการพิจารณาให้ความช่วยเหลือค่อนข้างกว้าง โดยความช่วยเหลือซึ่งกันและกันที่ยอมรับในระดับสากล ได้แก่

๓.๑) การสืบพยานบุคคลและการสอบปากคำบุคคล

๓.๒) การจัดหาให้ซึ่งเอกสาร บันทึก และพยานหลักฐาน

๓.๓) การส่งเอกสาร

๓.๔) การปฏิบัติตามคำร้องขอในการค้นและยึด

๓.๕) การโอนตัวบุคคลที่ถูกคุมขังเพื่อการสืบพยานบุคคล

๓.๖) การสืบหาตัวบุคคล

๓.๗) การเริ่มกระบวนการทางอาญาตามคำร้องขอ

๓.๘) การให้ความช่วยเหลือเกี่ยวกับการดำเนินการริบทรัพย์สิน

๔) วิธีการให้ความช่วยเหลือ กฎหมายกำหนดให้อัยการสูงสุดในฐานะผู้ประสานงานกลางเป็นผู้รับคำร้องขอจากต่างประเทศแล้ว พิจารณาเบื้องต้นว่าการร้องขอดังกล่าวเป็นไปตามหลักเกณฑ์ที่กำหนดไว้ในกฎหมายหรือไม่ ถ้าเห็นว่าไม่เป็นไปตามหลักเกณฑ์ก็ให้แจ้งให้ประเทศผู้ร้องขอทราบ แต่หากเป็นไปตามหลักเกณฑ์ที่กำหนดในกฎหมายก็ส่งเรื่องให้ผู้มีอำนาจหน้าที่ดำเนินการ ซึ่งหมายถึงเจ้าหน้าที่ตามที่กฎหมายกำหนดอำนาจหน้าที่ไว้

๔.๑) คำร้องขอให้สอบปากคำพยาน จัดหาให้ซึ่งเอกสารหรือสิ่งของอันเป็นพยานหลักฐาน ซึ่งเป็นการดำเนินการนอกศาล คำร้องขอให้จัดส่งเอกสาร คำร้องขอให้ค้น คำร้องขอให้สืบหาบุคคล และคำร้องขอให้อายัดหรือยึดเอกสารหรือสิ่งของ เพื่อประโยชน์ในการรวบรวมพยานหลักฐาน ให้ส่งให้ผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษ เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ หรือเลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ

๔.๒) คำร้องขอให้สืบพยานบุคคล พยานเอกสาร หรือพยานวัตถุ ซึ่งเป็นการดำเนินการในศาล และคำร้องขอให้อายัดหรือยึดทรัพย์สิน เพื่อประโยชน์ในการริบทรัพย์สินหรือในการบังคับบุคคลใดให้ชำระเงินแทนการริบทรัพย์สินและคำร้องขอให้อายัด ยึด หรือริบทรัพย์สินหรือบังคับชำระเงินแทนการริบทรัพย์สินตามคำพิพากษาหรือคำสั่งของศาลต่างประเทศ ให้ส่งพนักงานอัยการ

๔.๓) คำร้องขอให้โอนหรือรับโอนบุคคลซึ่งถูกคุมขังเพื่อช่วยเหลือในการดำเนินคดีชั้นเจ้าพนักงานหรือชั้นศาล ให้ส่งอธิบดีกรมราชทัณฑ์

๔.๔) คำร้องขอให้เริ่มกระบวนการคดีทางอาญา ให้ส่งให้ผู้บัญชาการตำรวจแห่งชาติ อธิบดีกรมสอบสวนคดีพิเศษ หรือพนักงานอัยการ

เมื่อเจ้าหน้าที่ผู้มีอำนาจดำเนินการเสร็จก็จะส่งเรื่องกลับมาให้อัยการสูงสุดผู้ประสานงานกลาง เพื่อส่งให้ประเทศผู้ร้องขอต่อไป

๕) คำวินิฉัยของผู้ประสานงานกลางเป็นยุติ ตามพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. ๒๕๓๕ กำหนดให้คำวินิจฉัยของผู้ประสานงานกลางเป็นยุติ เว้นแต่นายกรัฐมนตรีจะมีคำสั่งเป็นอย่างอื่น

๖) การขอความช่วยเหลือจากต่างประเทศ หน่วยงานของรัฐอาจขอความช่วยเหลือทางอาญาจากต่างประเทศได้โดยมีหลักการทำนองเดียวกัน กับการให้ความช่วยเหลือแก่ต่างประเทศโดยผ่านอัยการสูงสุดผู้ประสานงานกลาง

ปัจจุบันได้มีการออกพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. ๒๕๕๙ ซึ่งแก้ไขเพิ่มเติมพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ. ต่าง ๆ เช่น ให้ผู้ประสานงานกลางมีอำนาจส่งคำร้องขอความช่วยเหลือจากต่างประเทศไปให้เจ้าพนักงานหรือพนักงาน เจ้าหน้าที่ตามกฎหมายอื่น เพื่อดำเนินการในส่วนที่เกี่ยวข้องกับคำร้องขอได้ให้ผู้ประสานงานกลางมีอำนาจส่งข้อมูลเกี่ยวกับการกระทำความผิดหรือทรัพย์สินใดไปให้ต่างประเทศเพื่อประโยชน์ในการสืบสวน สอบสวน การฟ้องคดี หรือการพิจารณาคดีในศาลแม้ยังมิได้รับการร้องขอกำหนดกระบวนการค้นหรือยึดทรัพย์สิน เพื่อประโยชน์ในการรวบรวมพยานหลักฐานและเพื่อประโยชน์ชั้นที่สุดในการริบทรัพย์สิน เพื่อป้องกันการยักย้ายถ่ายเททรัพย์สินที่ได้มาจากการกระทำความผิดให้มีการเจรจาตกลงเพื่อให้มีการรับรองว่าจะไม่มีการประหารชีวิตถือเป็นกลไกในการร้องขอความช่วยเหลือในความผิดอันเป็นมูลเหตุแห่งการร้องขอความช่วยเหลือนั้น ต้องระวางโทษถึงประหารชีวิตตามกฎหมายไทย แต่ไม่ถึงโทษประหารชีวิตตามกฎหมายของประเทศผู้รับร้องขอการโอนบุคคลซึ่งถูกคุมขัง เพื่อช่วยเหลือในการดำเนินคดีในชั้นเจ้าพนักงาน เป็นต้น

สำหรับในส่วนที่เกี่ยวข้องกับกรมสอบสวนคดีพิเศษโดยตรง คือ อธิบดีกรมสอบสวนคดีพิเศษ เป็นเจ้าหน้าที่ผู้มีอำนาจดำเนินการตามคำร้องขอความช่วยเหลือจากต่างประเทศตามมาตรา ๑๒ วงเล็บหนึ่ง กล่าวคือ อัยการสูงสุดซึ่งเป็นผู้ประสานงานกลาง มีอำนาจส่งคำร้องขอให้สอบปากคำพยานหรือจัดหาให้ซึ่งกฎหมายหรือสิ่งของอันเป็นพยานหลักฐานซึ่งเป็นการดำเนินการนอกศาล คำร้องขอ ให้จัดส่งเอกสาร คำร้องขอให้ค้น คำร้องขอให้สืบหาบุคคล และคำร้องขอให้อายัดหรือยึดเอกสารหรือสิ่งของเพื่อประโยชน์ในการรวบรวมพยานหลักฐาน ให้อธิบดีกรมสอบสวนคดีพิเศษดำเนินการได้ ซึ่งกรมสอบสวนคดีพิเศษอยู่ระหว่างการประสานอัยการสูงสุด เพื่อให้การปฏิบัติงานดังกล่าวเป็นไปอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ต่อไป

๔.๓.๓.๓ การส่งผู้ร้ายข้ามแดน (Extradition)[๖]

๑) หลักกฎหมายที่เกี่ยวข้องกับการส่งผู้ร้ายข้ามแดน

๑.๑) ต้องเป็นความผิดที่อาจมีการส่งผู้ร้ายข้ามแดนได้ (Extradition Offences) คือ หลักการที่ระบุให้มีการส่งผู้ร้ายข้ามแดนได้เฉพาะกรณีการกระทำความผิดซึ่งได้ระบุไว้โดยเฉพาะในสนธิสัญญา

๑.๒) หลักต่างตอบแทน (Reciprocity) หลักการนี้จะใช้บังคับในกรณีที่ประเทศที่ผู้ร้ายข้ามแดนได้หลบหนีไปอาศัยนั้นไม่มีสนธิสัญญาหรือข้อตกลงในเรื่องความร่วมมือทางอาญาระหว่างกัน แต่ประเทศผู้ร้องขอและประเทศผู้รับคำร้องขอได้พิจารณาแล้วว่า จะดำเนินการให้ความช่วยเหลือการดำเนินคดีอาญาแก่กัน และเป็นการตอบแทนในลักษณะเดียวกัน

๑.๓) ต้องเป็นความผิดที่สามารถลงโทษได้ทั้งตามกฎหมายของรัฐผู้ร้องขอและรัฐผู้รับคำร้องขอ (Double Criminality) ความผิดอาญาที่รัฐผู้รับคำร้องขอจะดำเนินการส่งผู้ร้ายข้ามแดนนั้นจะต้องเป็นความผิดอาญาที่ปรากฏในกฎหมายของประเทศผู้ร้องขอ และประเทศที่ส่งตัวตามหลัก “ไม่มีความผิด ถ้าไม่มีกฎหมาย” (Nullapeona Sine Lege) เนื่องจากการดำเนินการ

---

[๖]กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๒๒-๑๒๘

ในทางอาญาเป็นเรื่องที่ส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ดังนั้น การกระทำที่จะเป็นความผิดอาญาที่ส่งผู้ร้ายข้ามแดนได้จะต้องเป็นมูลฐานความผิดตามกฎหมายทั้งสองประเทศ

๑.๔) การไม่ลงโทษซ้ำในความผิดเดียวกัน (Double Jeopardy) หลักเกณฑ์ตรงกับหลักกฎหมายทั่วไป ที่ว่า “การไม่พิจารณาหรือลงโทษซ้ำในคดีเดียวกัน” (Non Bis in Idem) กล่าวคือ จะไม่มีการส่งผู้ร้ายข้ามแดนในกรณีถ้าหากบุคคลที่ถูกขอให้ส่งตัวได้รับการพิจารณาคดี และถูกพิพากษาลงโทษหรือปล่อยตัวในรัฐที่รับคำร้องขอแล้ว โดยเป็นความผิดเดียวกันกับความผิดที่ขอให้ส่งผู้ร้ายข้ามแดน ทั้งนี้อาจรวมไปถึงการที่บุคคลที่ถูกขอให้ส่งตัวกำลังถูกดำเนินคดีในรัฐที่ได้รับคำร้องขอสำหรับความผิดที่ขอให้ส่งผู้ร้ายข้ามแดนด้วย

๑.๕) รัฐผู้ร้องขอจะดำเนินคดีได้เฉพาะความผิดที่ได้ระบุในคำร้องขอ “หลักความผิดเฉพาะเรื่อง” (Rule of Speciality) รัฐผู้ร้องขอไม่อาจดำเนินคดีในความผิดอื่นแก่บุคคล ผู้ถูกส่งตัวเป็นผู้ร้ายข้ามแดนได้ หากไม่ใช่ความผิดที่ได้กล่าวอ้างไว้ในคำร้องขอให้ส่งผู้ร้ายข้ามแดน อีกทั้งรัฐผู้ร้องขอไม่สามารถส่งผู้ร้ายข้ามแดนต่อไปยังรัฐที่สามอีกด้วย หากรัฐที่ได้รับคำร้องขอไม่ยินยอม

๑.๖) การไม่ส่งผู้ร้ายข้ามแดนในคดีเล็กน้อย เนื่องจากการส่งผู้ร้ายข้ามแดนเป็นความร่วมมือระหว่างประเทศ ซึ่งมีพิธีการและค่าใช้จ่ายในการดำเนินการ ดังนั้นความผิดเล็กน้อยจึงมักไม่มีการขอให้ส่งผู้ร้ายข้ามแดน คดีที่จะดำเนินการขอให้ส่งผู้ร้ายข้ามแดนนั้นจึงพิจารณาจากฐานความผิดที่มีอัตราโทษจำคุกหรือกักขังเกินกว่า ๑ ปี

๑.๗) ต้องไม่เป็นคดีที่ขาดอายุความ สำหรับอายุความนั้นให้ถือเอาอายุความในฐานความผิดของทั้งสองประเทศทั้งในประเทศผู้ร้องขอและประเทศผู้รับคำร้องขอ

๑.๘) บุคคลต้องปรากฏตัวอยู่ในรัฐที่รับการร้องขอ การที่จะร้องขอให้มีการส่งผู้ร้ายข้ามแดนนั้นต้องปรากฏข้อเท็จจริงว่าบุคคลผู้กระทำความผิดนั้นข้ามแดนไป และได้ปรากฏตัวอยู่ในรัฐที่รับคำร้องขอดังกล่าว

๒) ข้อยกเว้นของการส่งผู้ร้ายข้ามแดน

๒.๑) หลักไม่ส่งผู้ร้ายข้ามแดนในความผิดทางการเมือง (Political Offences) เนื่องจากความผิดทางการเมืองเป็นเพียงการกระทำความผิดเพราะมีแนวคิดไม่ตรงกันกับผู้มีอำนาจบริหารประเทศในเวลานั้น

๒.๒) หลักการไม่ส่งคนชาติข้ามแดน (Non - Extradition of Nationals) ในประเทศกลุ่มระบบกฎหมายลายลักษณ์อักษร (Civil Law) จะไม่ส่งบุคคลสัญชาติตนข้ามแดนไปเพื่อดำเนินคดีในต่างรัฐ เนื่องจากเป็นหน้าที่ของรัฐในขณะเดียวกันก็ไม่มั่นใจในกระบวนการยุติธรรมทางอาญาของรัฐต่างประเทศ แต่ในกลุ่มระบบกฎหมายแบบจารีตประเพณี (Common Law) ไม่มีข้อห้ามในเรื่องดังกล่าว เพราะถือหลักว่าผู้กระทำความผิด ณ ที่ใดจะต้องถูกพิจารณาคดี ณ ที่ที่กระทำความผิด เนื่องจากเห็นว่ากระบวนการยุติธรรมจะดำเนินไปได้อย่างดีในรัฐที่ความผิดเกิดขึ้น ไม่ว่าจะเป็นด้านพยานหลักฐาน พยานบุคคล และผู้เสียหาย

๒.๓) หลักการไม่ส่งผู้ร้ายข้ามแดนในโทษประหารชีวิต (Death Penalty) สนธิสัญญาสหประชาชาติว่าด้วยการส่งผู้ร้ายข้ามแดน มาตรา ๔ (United Nations Model Treaty on Extradition (d)) เป็นแม่แบบในข้อยกเว้นเรื่องความผิดโทษประหารชีวิต โดยยกเว้นในกรณี

ที่ประเทศ ผู้ร้องขอตกลงว่าจะไม่ตัดสินลงโทษประหารชีวิต หรือไม่จัดให้มีการประหารชีวิตบุคคลที่ร้องขอให้ส่งผู้ร้ายข้ามแดนในทางปฏิบัติประเทศต่าง ๆ ในทวีปยุโรปจะปฏิเสธไม่ส่งผู้ร้ายข้ามแดนหากบุคคลดังกล่าวต้องเสี่ยงกับการรับโทษประหารชีวิตในประเทศผู้ร้องขอ เนื่องจากประเทศเหล่านั้นได้ยกเลิกโทษประหารชีวิตตามกฎหมายภายในประเทศแล้วเป็นส่วนใหญ่

๒.๔) หลักการไม่ส่งผู้ร้ายข้ามแดนหากพยานหลักฐานไม่เพียงพอ (Insufficiency of Evidence) หลักข้อยกเว้นนี้มาจากสนธิสัญญาสหประชาชาติว่าด้วยการส่งผู้ร้ายข้ามแดน (United Nations Model Treaty on Extradition) ข้อ ๓ ซึ่งกำหนดข้อยกเว้นให้ประเทศภาคีสมาชิกสามารถปฏิเสธไม่ส่งผู้ร้ายข้ามแดนได้หากพยานหลักฐานไม่เพียงพอ ตามมาตรฐานกฎหมายลักษณะพยานของประเทศผู้รับคำร้องขอ

๓) พระราชบัญญัติการส่งผู้ร้ายข้ามแดน พ.ศ. ๒๕๕๑

ประเทศไทยมีมาตรการให้ความร่วมมือในการส่งผู้ร้ายข้ามแดนตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. ๒๕๕๑ (เดิมมีพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. ๒๔๗๒ แต่ภายหลังถูกยกเลิกไป) โดยกำหนดให้มีผู้ประสานงานกลาง คือ อัยการสูงสุดหรือผู้ซึ่งอัยการสูงสุดมอบหมาย เพื่อทำหน้าที่ในการประสานงานการส่งผู้ร้ายข้ามแดนให้ประเทศผู้ร้องขอ และการร้องขอให้ส่งผู้ร้ายข้ามแดนแก่ประเทศไทย

การร้องขอให้ส่งผู้ร้ายข้ามแดนจากประเทศผู้รับคำร้องขอมายังประเทศไทยให้พนักงานอัยการ หรือหน่วยงานที่ประสงค์จะให้มีการส่งผู้ร้ายข้ามแดน เสนอเรื่องต่อผู้ประสานงานกลาง ในกรณีที่ผู้ประสานงานกลางมีคำวินิจฉัยว่าสมควรที่จะจัดคำร้องขอให้ส่งผู้ร้ายข้ามแดนจากประเทศผู้รับคำร้องขอให้ผู้ประสานงานกลางส่งเรื่องให้พนักงานอัยการจัดทำคำร้องขอส่งให้ผู้ร้ายข้ามแดนและเอกสารประกอบต่อไปคำวินิจฉัยของผู้ประสานงานกลาง เกี่ยวกับการขอให้ส่งผู้ร้ายข้ามแดนให้ถือเป็นยุติ เว้นแต่คณะรัฐมนตรีมีมติเป็นอย่างอื่น

ความผิดที่จะขอให้มีการส่งผู้ร้ายข้ามแดนได้ต้องเป็นความผิดอาญาที่กฎหมายทั้งสองประเทศบัญญัติไว้เป็นความผิด ซึ่งมีโทษประหารชีวิตหรือโทษจำคุกหรือโทษจำกัดเสรีภาพในรูปแบบอื่น ตั้งแต่หนึ่งปีขึ้นหรือหากมีโทษน้อยกว่าหนึ่งปี แต่เป็นความผิดเกี่ยวพันกับความผิดที่ให้มีการส่งผู้ร้ายข้ามแดนตามร้องขอแล้ว ก็อาจร้องขอให้ส่งผู้ร้ายข้ามแดนแก่กันได้ ยกเว้นความผิดที่มีลักษณะทางการเมืองหรือเป็นความผิดทางทหาร

การส่งผู้ร้ายข้ามแดนจะเริ่มด้วยการมีคำร้องขอ ถ้าเป็นประเทศที่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับ ประเทศไทยก็ต้องส่งไปยังผู้ประสานงานกลาง หากมิได้มีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศไทยก็ต้องส่งคำร้องขอดังกล่าวโดยผ่านวิถีทางการทูต ทั้งนี้ รัฐบาลไทยอาจพิจารณาส่งผู้ร้ายข้ามแดนให้เมื่อประเทศผู้ร้องขอจะต้องแสดงโดยชัดแจ้งว่าจะส่งผู้ร้ายข้ามแดนให้แก่ประเทศไทย ในทำนองเดียวกันเมื่อประเทศไทยร้องขอคำร้องขอให้ส่งผู้ร้ายข้ามแดนและเอกสารหลักฐานให้เป็นไปตามหลักเกณฑ์วิธีการและเงื่อนไขที่กำหนดในกฎกระทรวง กล่าวคือคำร้องขอให้ส่งผู้ร้ายข้ามแดนจะต้องทำเป็นลายลักษณ์อักษร โดยมีรายละเอียดและเอกสารหลักฐานดังต่อไปนี้

๓.๑) รายละเอียดเกี่ยวกับบุคคลซึ่งถูกร้องขอให้ส่งข้ามแดน โดยระบุชื่อ รูปพรรณ สัญชาติ และที่อยู่ บุคคลดังกล่าวหรือสถานที่ที่มีเหตุอันควรเชื่อได้ว่าบุคคลนั้นอยู่ในราชอาณาจักร

๓.๒) ข้อเท็จจริงเกี่ยวกับคดีและรายละเอียดเกี่ยวกับวัน เวลา และสถานที่กระทำความผิด

๓.๓) กฎหมายที่บัญญัติให้การกระทำนั้นเป็นความผิด ฐานความผิด อัตราโทษ และอายุความ

๓.๔) ถ้าร้องขอให้ส่งตัวเพื่อไปดำเนินคดี จะต้องมีหมายจับที่ออกโดยศาลหรือเจ้าหน้าที่ผู้มีอำนาจ หรือสำเนาหมายจับซึ่งรับรองความถูกต้อง รวมทั้งพยานหลักฐานที่แสดงว่าคดีมีมูลที่ศาลจะรับฟ้องไว้พิจารณา หากความผิดนั้นได้กระทำในราชอาณาจักร หรือมีกฎหมายบัญญัติให้ถือว่าได้กระทำในราชอาณาจักร

๓.๕) ถ้าเป็นกรณีร้องขอให้ส่งตัวเพื่อรับโทษตามคำพิพากษา จะต้องมีสำเนาคำพิพากษาของศาล ของประเทศผู้ร้องขอซึ่งรับรองความถูกต้อง และคำแถลงที่แสดงว่าบุคคลซึ่งถูกร้องขอให้ส่งข้ามแดนต้องรับโทษตามคำพิพากษาอีกเพียงใด

คำร้องขอและเอกสารทั้งหมดจะต้องได้รับการรับรองโดยเจ้าหน้าที่ผู้มีอำนาจของประเทศผู้ร้องขอพร้อมคำแปลเป็นภาษาไทยและรับรองความถูกต้องด้วย

๔) ข้อจำกัดในการส่งผู้ร้ายข้ามแดน

๔.๑) คดีความผิดที่มีลักษณะทางการเมืองหรือเป็นความผิดทางทหาร ซึ่งความผิดที่ลักษณะทางการเมือง ไม่หมายรวมถึง

๔.๑.๑) การปลงพระชนม์ ประทุษร้ายต่อพระองค์ หรือเสรีภาพของพระมหากษัตริย์ พระราชินีหรือรัชทายาท

๔.๑.๒) การฆ่า ประทุษร้ายต่อร่างกาย หรือเสรีภาพของประมุขแห่งรัฐ ผู้นำรัฐบาล หรือสมาชิกโดยตรงในครอบครัวของบุคคลนั้น

๔.๑.๓) การกระทำความผิดที่ไม่ถือว่าเป็นความผิดทางการเมือง เพื่อวัตถุประสงค์ในการส่งผู้ร้ายข้ามแดนตามสนธิสัญญาซึ่งประเทศไทยเป็นภาคี

๔.๒) บุคคลซึ่งถูกร้องขอให้ส่งข้ามแดนนั้นได้รับการพิจารณาคดีในความผิดนั้น และมีคำพิพากษาถึงที่สุดให้ปล่อยตัวไป หรือให้ลงโทษและพ้นโทษไปแล้ว หรือได้รับการอภัยโทษ หรือนิรโทษกรรม หรือคดีขาดอายุความ หรือมีเหตุอื่นใดซึ่งไม่สามารถดำเนินคดีแก่บุคคลนั้นตามกฎหมายของประเทศผู้ร้องขอ

๔.๓) ในกรณีที่จะส่งผู้ร้ายข้ามแดนซึ่งเป็นบุคคลสัญชาติไทยไปยังประเทศอื่นจะดำเนินการได้เมื่อผู้นั้นให้ส่งข้ามแดนหรือเป็นการปฏิบัติต่างตอบแทน ตามหลักถ้อยทีถ้อยปฏิบัติกับประเทศที่ร้องขอหรือกรณีระบุไว้ในสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยกับประเทศที่ร้องขอ

๔.๔) หากความผิดที่ประเทศไทยจะร้องขอให้ส่งผู้ร้ายข้ามแดนนั้น ต้องระวางโทษประหารชีวิตตามกฎหมายไทยแต่ไม่ถึงโทษประหารชีวิตตามกฎหมายของประเทศผู้รับคำร้องขอ และรัฐบาลจำเป็นต้องให้คำรับรองว่าจะไม่มีการประหารชีวิต ก็ต้องจัดให้มีการเจรจาเพื่อให้มี

การรับรอง ในกรณีนี้หากศาลพิพากษาลงโทษประหารชีวิตให้รัฐบาลไทยดำเนินการตามบทบัญญัติของกฎหมายเพื่อให้มีการบังคับตามคำพิพากษาโดยวิธีการจำคุกตลอดชีวิตแทนการประหารชีวิต และห้ามมิให้ลดหย่อนผ่อนโทษไม่ว่าด้วยเหตุใด ๆ เว้นแต่เป็นการพระราชทานอภัยโทษ

๔.๕) การพิจารณาคดีส่งผู้ร้ายข้ามแดนจะเป็นกระบวนการพิจารณาในศาล ในกรณีจำเป็นเร่งด่วน ประเทศผู้ร้องขออาจมีคำร้องขอให้จับกุมและคุมขังบุคคลที่ต้องการตัวไว้ชั่วคราวก่อนก็ได้ (มาตรา ๑๕) เมื่อจับกุมตัวบุคคลได้ให้นำส่งพนักงานอัยการโดยมิชักช้า เพื่อยื่นคำร้องต่อศาล มีคำสั่งขังบุคคลซึ่งถูกร้องขอไว้ในระหว่างรอคำร้องขอส่งผู้ร้ายข้ามแดนอย่างเป็นทางการและเอกสารหลักฐานจากประเทศผู้ร้องขอหากศาลมิได้รับคำฟ้อง เพื่อดำเนินคดีส่งผู้ร้ายข้ามแดนภายในหกสิบวันนับแต่วันที่บุคคลซึ่งถูกร้องขอถูกจับหรือภายในเวลาที่ศาลกำหนด แต่ต้องไม่เกินเก้าสิบวันนับแต่วันที่บุคคลนั้นถูกจับให้ปล่อยตัวบุคคลนั้นไป

๔.๖) ภายหลังจากศาลมีคำสั่งถึงที่สุดให้ขังบุคคลซึ่งถูกร้องขอให้เป็นผู้ร้ายข้ามแดนและรัฐบาลไทยพิจารณาให้ส่งบุคคลนั้นเป็นผู้ร้ายข้ามแดนแล้ว จะต้องดำเนินการให้เสร็จสิ้นภายในเก้าสิบวันนับแต่วันที่ศาลมีคำสั่งถึงที่สุด

๕) การดำเนินการส่งผู้ร้ายข้ามแดนของประเทศไทย

ไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดนกับประเทศต่าง ๆ ๑๔ ประเทศ บางฉบับก็มีข้อจำกัดระบุเฉพาะ บางฐานความผิดเท่านั้นที่จะส่งผู้ร้ายข้ามแดนได้ อย่างไรก็ตาม กรณีที่ไม่มีความตกลงเรื่องการส่งผู้ร้ายข้ามแดนก็เป็นดุลยพินิจของรัฐบาลที่จะส่งผู้ร้ายข้ามแดนให้หรือไม่ก็ได้ ซึ่งเป็นไปตามหลักต่างตอบแทน ซึ่งยังมีปัจจัยที่ต้องพิจารณาอยู่ ๒ ประการ คือ ประการแรก กฎหมายของประเทศนั้นต้องเปิดช่องให้ทำได้ด้วย ประการที่สอง คือ การที่จะได้รับความร่วมมือจากประเทศนั้นหรือไม่ขึ้นอยู่กับเจตจำนงทางการเมือง บรรยากาศทางการเมือง และผลประโยชน์ของประเทศนั้นในเรื่องนี้ด้วย

๕.๑) ความร่วมมือระหว่างประเทศในกรณีมีสนธิสัญญาระหว่างกัน ปัจจุบันประเทศไทยมีสนธิสัญญาส่งผู้ร้ายข้ามแดน (Extradition Treaty) กับ ๑๔ (๑๐ ฉบับ) ได้แก่ อังกฤษ แคนาดา ออสเตรเลีย มาเลเซีย ฟิจิ เบลเยียม อินโดนีเซีย ฟิลิปปินส์ สหรัฐอเมริกา จีน เกาหลีใต้ ลาว บังคลาเทศ และกัมพูชา โดยในกลุ่มประชาคมอาเซียน ๑๐ ประเทศนั้น ไทยมีสนธิสัญญากับ ๕ ประเทศ คือ มาเลเซีย อินโดนีเซีย ฟิลิปปินส์ ลาว และกัมพูชา

ในสนธิสัญญาฯ ที่ไทยทำไว้กับประเทศต่าง ๆ นอกจากจะมีหลักทั่วไปของการส่งผู้ร้ายข้ามแดนตามที่กล่าวไปแล้ว บางสนธิสัญญาอาจมีการระบุฐานความผิดไว้โดยเฉพาะเจาะจงที่จะส่งผู้ร้ายข้ามแดนให้แก่กันได้ อาทิ สนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างประเทศไทยกับอังกฤษ ร.ศ. ๑๒๙ (ค.ศ. ๑๙๑๑) อนุสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนระหว่างสยามกับเบลเยี่ยม ค.ศ. ๑๙๓๗ สนธิสัญญาระหว่างรัฐบาลแห่งราชอาณาจักรไทยกับรัฐบาลแห่งสาธารณรัฐอินโดนีเซียว่าด้วยการส่งผู้ร้ายข้ามแดน ค.ศ. ๑๙๗๖ สนธิสัญญาระหว่างรัฐบาล แห่งราชอาณาจักรไทยกับรัฐบาลแห่งสาธารณรัฐฟิลิปปินส์ว่าด้วยการส่งผู้ร้ายข้ามแดน ค.ศ. ๑๙๘๑ หรือบางสนธิสัญญาจะกำหนดโทษขั้นต่ำของความผิดที่จะส่งผู้ร้ายข้ามแดนได้ กล่าวคือ ต้องเป็นความผิดที่มีโทษจำคุกหรือทำให้ปราศจากเสรีภาพหรือการกักขังในรูปแบบอื่นเป็นระยะเวลามากกว่าหนึ่งปีหรือโดยการลงโทษ

ที่หนักกว่า ซึ่งมักปรากฏอยู่ในการทำสนธิสัญญาในระยะหลัง ๆ อาทิ สนธิสัญญาระหว่างรัฐบาลแห่งราชอาณาจักรไทยกับรัฐบาลแห่งสหรัฐอเมริกาว่าด้วยการส่งผู้ร้ายข้ามแดน ค.ศ. ๑๙๘๓

๕.๒) ความร่วมมือตามหลักถ้อยทีถ้อยปฏิบัติต่อกันระหว่างประเทศ (Reciprocity) กรณีไม่มีสนธิสัญญา

ในกรณีที่ไม่มีสนธิสัญญาส่งผู้ร้ายข้ามแดนระหว่างกันจะต้องดำเนินการจัดส่งคำร้องขอพร้อมเอกสาร ที่เกี่ยวข้องโดยผ่านวิถีทางการทูต ซึ่งกระทรวงการต่างประเทศจะเป็นผู้พิจารณาหากไม่กระทบต่อสัมพันธไมตรีระหว่างประเทศ และไม่มีเหตุผลอื่นใดที่จะไม่ดำเนินการให้ก็ให้ส่งคำร้องนั้นให้ผู้ประสานงานกลางดำเนินการต่อไป ทั้งนี้ในทางปฏิบัติจะต้องพิจารณาด้วยว่าในคำร้องขอดังกล่าวประเทศผู้ร้องขอจะต้องแสดงโดยชัดแจ้งว่าจะส่งผู้ร้ายข้ามแดนให้แก่ประเทศไทยในทำนองเดียวกันเมื่อประเทศไทยร้องขอตามหลักถ้อยทีถ้อยปฏิบัติ แต่หากกระทรวงการต่างประเทศพิจารณาเห็นว่าคำร้องขอนั้นอาจกระทบกระเทือนความสัมพันธ์ระหว่างประเทศหรือมีเหตุผลอื่นใดที่ไม่อาจดำเนินการให้ได้ ก็ให้เสนอความเห็นพร้อมคำร้องนั้นให้คณะรัฐมนตรีพิจารณาโดยเร็ว หากคณะรัฐมนตรี เห็นตามความเห็นของกระทรวงการต่างประเทศก็ให้พิจารณาสั่งการตามที่เห็นสมควร แต่หากเห็นชอบให้ส่งผู้ร้ายข้ามแดนตามคำร้องขอก็ให้กระทรวงการต่างประเทศส่งเรื่องให้ ผู้ประสานงานกลางดำเนินการต่อไป

๕.๓) มาตรการเร่งด่วนเพื่อการจับกุมนอกเหนือจากการดำเนินการตามข้อ ๕.๑) หรือข้อ ๕.๒) ก็อาจใช้ความร่วมมือโดยการติดต่อสื่อสารผ่านองค์การตำรวจสากลซึ่งเป็นองค์การระหว่างประเทศหน่วยงานหนึ่งที่มีสมาชิก ๑๗๙ ประเทศทั่วโลก มีหน้าที่เป็นสื่อกลางติดต่อประสานงานด้านการข่าวและความร่วมมือระหว่างประเทศสมาชิก เพื่อเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมสำหรับประเทศไทย สำนักงานกลางแห่งชาติ ตำรวจสากล (National Central Bureau - NCB) ตั้งอยู่ที่กองการต่างประเทศ สำนักงานตำรวจแห่งชาติ โดยมีผู้บังคับการกองการต่างประเทศเป็นหัวหน้า โดยผ่านสำนักงานกลางแห่งชาติตำรวจสากลประเทศไทย (NCB Bangkok) เป็นการช่วยเหลือซึ่งกันและกันในเรื่องทางอาญาในรูปแบบกึ่งทางการ โดยไม่ต้องมีความสัมพันธ์กันเป็นกรณีพิเศษ หากเป็นไปตามความตกลงหรือความร่วมมือภายใต้หน่วยงานระหว่างประเทศที่รับผิดชอบ ในเรื่องทางกระบวนการยุติธรรมต่าง ๆ

ในทางปฏิบัติก่อนที่จะดำเนินกรรมวิธีร้องขอให้ส่งผู้ร้ายข้ามแดน จะต้องทราบสถานที่หรือประเทศที่ผู้นั้นหลบหนีเข้าไป ในการสืบหาบุคคลที่จะขอให้ส่งตัวผู้ร้ายข้ามแดนนั้นจะดำเนินการขอให้องค์การตำรวจสากลออกหมายแดง (Red Notice) ซึ่งเป็นใบแจ้งรูปพรรณของคนร้ายเพื่อที่จะได้ดำเนินกรรมวิธีการส่งผู้ร้ายข้ามแดนต่อไป ซึ่งองค์การตำรวจสากลเปิดโอกาสให้ประเทศสมาชิกยื่นคำร้องขอให้ออกหมายแดง เพื่อสืบหาติดตามจับกุมตัวชั่วคราวบุคคลที่ได้กระทำความผิดในประเทศผู้ยื่นคำร้อง โดยบางประเทศถือว่าหมายแดงเป็นเสมือนหนึ่งหมายจับนานาชาติ ทำให้เจ้าหน้าที่ตำรวจในประเทศนั้น สามารถจับกุมชั่วคราวบุคคลดังกล่าวได้ แต่ในบางประเทศรวมทั้งประเทศไทยเจ้าหน้าที่ตำรวจไม่สามารถที่จะจับกุมชั่วคราวบุคคลที่ปรากฏอยู่ในหมายแดงได้ในทุกกรณี

เพื่อให้การประสานงานกับสำนักเลขาธิการองค์การตำรวจสากลในการสืบสวนหาตัวบุคคลที่กระทำผิดในประเทศไทยนั้น เป็นไปด้วยความละเอียดรอบคอบและรัดกุม

และเพื่อให้การประสานงานกับพนักงานอัยการในการดำเนินการเพื่อให้ได้ตัวผู้ต้องหาข้ามแดนมาดำเนินคดีหรือรับโทษในประเทศไทยมีประสิทธิภาพมากยิ่งขึ้น กองการต่างประเทศ สำนักงานตำรวจแห่งชาติ จึงได้วางหลักเกณฑ์ในการดำเนินการดังนี้

แนวทางการปฏิบัติในการออกหมายแดงขององค์การตำรวจสากล (ตามคำสั่งกองการต่างประเทศที่ ๑๗๕/๒๕๔๔ ลงวันที่ ๒๑ ธันวาคม ๒๕๔๔)

๑) วัตถุประสงค์

๑.๑) เพื่อเป็นการสืบหาติดตามจับกุมตัวผู้ต้องหาซึ่งกระทำผิด ในประเทศไทยแล้วหลบหนีไปต่างประเทศกลับมาดำเนินคดีในประเทศไทยผ่านช่องทางการประสานงานขององค์การตำรวจสากล

๑.๒) เพื่อสนับสนุนการดำเนินการของพนักงานอัยการและกระทรวงการต่างประเทศ ในการขอส่งผู้ร้ายข้ามแดนมาดำเนินคดีในประเทศไทย

๒) หลักปฏิบัติในการดำเนินการร้องขอหมายแดงในกรณีดังต่อไปนี้

๒.๑) กรณีพนักงานอัยการมีคำสั่งฟ้องผู้ต้องหา ให้ถือเป็นหลักปฏิบัติทั่วไป

๒.๒) กรณีผู้ต้องหามีหมายจับในชั้นพนักงานสอบสวน หรือกรณีที่พนักงานอัยการยังไม่ได้มีความเห็นสั่งฟ้อง ควรให้ใช้ใช้วิธีแจ้งเวียนให้สืบสวนหาข่าวถึงแหล่งที่พักพิงหรือหลบซ่อนตัวทาง INTERPOL Diffusion เป็นลำดับแรก และจะต้องเสนอสำนักงานตำรวจแห่งชาติสั่งการเป็นราย ๆ ไป

๓) เงื่อนไขเบื้องต้นในการร้องขอให้ออกหมายแดง

๓.๑) บุคคลที่ต้องการตัวกระทำผิดกฎหมายที่มีโทษทางอาญา

๓.๒) มีการออกหมายจับบุคคลดังกล่าวแล้ว

๓.๓) พนักงานสอบสวนมีความเห็นควรสั่งฟ้อง หรือพนักงานอัยการได้สั่งฟ้องผู้ต้องหาแล้ว

๓.๔) ได้รับการประสานจากพนักงานอัยการ หรือกระทรวงการต่างประเทศว่าจะมีการร้องขอให้มีการส่งผู้ร้ายข้ามแดนต่อไป

แนวทางดังกล่าวเบื้องต้น กรมสอบสวนคดีพิเศษได้ประสานความร่วมมือระหว่างหน่วยงานดำเนินการในการออกหมายแดงโดยใช้แนวทางปฏิบัติเดียวกัน หากไม่ครบเงื่อนไขทั้ง ๔ ข้อ ตามแนวทางการปฏิบัติดังกล่าวจะไม่มีการออกหมายแดง แต่อาจขอให้สำนักเลขาธิการองค์การตำรวจสากลออกหมายประเภทอื่นให้ได้

๔) วิธีการในการร้องขอให้ออกหมาย

๔.๑) กรอกแบบฟอร์มการร้องขอหมายแดง ส่งถึงสำนักเลขาธิการองค์การตำรวจสากล โดยเสนอผู้บังคับการกองการต่างประเทศ หรือรองผู้บังคับการ กองการต่างประเทศที่ได้รับมอบหมายเป็นผู้ลงนามในแบบฟอร์มการร้องขอ การร้องขอควรระบุข้อมูลเกี่ยวกับบุคคลที่ต้องการตัว ให้มากที่สุด เช่น

ก) ชื่อเต็ม วันเดือนปี และสถานที่เกิด บิดามารดา และสัญชาติ

ข) ตำหนิรูปพรรณ

ค) เจ้าหน้าที่ที่ออกหมายจับ

ง) เลขที่หมายจับ

จ) ข้อหาโดยละเอียด

ฉ) พฤติการณ์แห่งคดีโดยย่อ

ช) คำยืนยันว่าจะมีการขอส่งผู้ร้ายข้ามแดนต่อมา

ซ) จะมีคำขอส่งผู้ร้ายข้ามแดนจากประเทศใดบ้าง

๔.๒) แจ้งข้อมูลตามแบบฟอร์มดังกล่าวไปยังสมาชิกองค์การตำรวจสากลประเทศต่าง ๆ โดยผ่านทาง INTERPOL Diffusion

๔.๓) แจ้งให้สำนักเลขาธิการองค์การตำรวจสากลทราบ หากมีการแก้ไขเปลี่ยนแปลงข้อมูลตามหมาย

๕) การดำเนินการหลังการจับกุมตามหมายแดง

๕.๑) กรณีที่จับกุมผู้ต้องหาได้ภายในประเทศ หรือกรณีหมายจับถูกยกเลิก

๕.๑.๑) แจ้งการยกเลิกหมายไปยังประเทศต่าง ๆ โดยวิทยุตำรวจสากล (X-๔๐๐)

๕.๑.๒) แจ้งให้สำนักเลขาธิการองค์การตำรวจสากล จัดทำหมายยกเลิก

๕.๒) กรณีที่จับกุมผู้ต้องหาได้ในประเทศอื่น ๆ

๕.๒.๑) มีคำขอหมายจับเฉพาะกาล (Provisional Arrest) ส่งถึงทางการประเทศที่พบตัวผู้ต้องหาโดยเร็วที่สุดเท่าที่จะทำได้ ในทางเดียวกันก็ดำเนินการให้มีการจัดส่งคำขอ ส่งผู้ร้ายข้ามแดนระหว่างประเทศนั้นกับประเทศไทย

๕.๒.๒) หลังจากที่ผู้ต้องหาถูกส่งข้ามแดนเรียบร้อยแล้ว ให้ประเทศที่ร้องขอมีวิทยุถึงประเทศสมาชิกต่าง ๆ แจ้งยกเลิกหมายต้องการตัว แล้วแจ้งสำนักเลขาธิการองค์การตำรวจสากลเพื่อยกเลิกหมาย

๖) หน้าที่อื่น ๆ

ประเทศที่ร้องขอต้องดำเนินการตรวจสอบทุก ๆ ๕ ปี ว่าผู้ต้องหาตามหมายยังเป็นที่ต้องการตัวหรือไม่ และแจ้งให้สำนักเลขาธิการองค์การตำรวจสากลทราบ

ทั้งนี้ ในการสืบสวนหาตัวผู้ต้องหาที่กระทำผิดในประเทศไทยแล้วหลบหนีไปอยู่ต่างประเทศ เมื่อได้รับแจ้งจากพนักงานสอบสวนเจ้าของคดีหรือหน่วยงานหนึ่งหน่วยงานใดให้กองการต่างประเทศพิจารณาดำเนินการออกหนังสือแจ้งเวียนไปยังประเทศสมาชิกองค์การตำรวจสากลเพื่อขอความร่วมมือในการสืบสวนหาตัวและแจ้งเบาะแสที่อยู่ของผู้ต้องหาดังกล่าวให้ทราบโดยเร็ว

ส่วนการดำเนินการเพื่อนำตัวผู้กระทำผิดในประเทศไทยที่ได้หลบหนีไปต่างประเทศอื่นมาดำเนินคดีหรือรับโทษตามคำพิพากษาของศาล กรณีที่พนักงานอัยการได้สั่งฟ้องผู้ต้องหาหรือกรณีที่ศาลได้ตัดสินลงโทษผู้กระทำผิดแล้ว เมื่อได้รับแจ้งจากพนักงานอัยการหรือหน่วยงานหนึ่งหน่วยงานใดให้กองการต่างประเทศพิจารณาดำเนินการร้องขอหมายแดงจากองค์การตำรวจสากลได้ตามหลักเกณฑ์ที่องค์การตำรวจสากลกำหนด แล้วแจ้งให้ทางพนักงานอัยการหรือหน่วยงานนั้น ๆ ทราบ เพื่อเป็นทางประสานการปฏิบัติต่อไป ส่วนกรณีอื่น ๆ นอกเหนือจากที่กล่าวไว้ให้กองการต่างประเทศพิจารณาดำเนินการร้องขอหมายแดงจากองค์การตำรวจสากลได้ต่อเมื่อได้รับ

ความเห็นชอบจากสำนักงานตำรวจแห่งชาติแล้ว หรือเมื่อสำนักงานตำรวจแห่งชาติได้สั่งการไว้โดยเฉพาะเท่านั้นในการปฏิบัติที่ผ่านมา กรมสอบสวนคดีพิเศษพบว่าการจะดำเนินการดังกล่าว พนักงานสอบสวนที่รับผิดชอบจะต้องทราบแนวทางปฏิบัติในการติดตามตัวผู้ต้องหามาดำเนินคดี โดยการรายงานให้กองการต่างประเทศทราบ

แนวปฏิบัติในการร้องขอให้ส่งผู้ร้ายข้ามแดน และการขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาของกรมสอบสวนคดีพิเศษ การดำเนินการเกี่ยวกับการส่งผู้ร้ายข้ามแดนและความร่วมมือระหว่างประเทศในเรื่องทางอาญาเป็นหน้าที่ของกองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ (กตท.) ตามกฎกระทรวงแบ่งส่วนราชการ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ. ๒๕๕๔ ข้อ ๔ (๑) การดำเนินความร่วมมือระหว่างประเทศ ในเรื่องการส่งผู้ร้ายข้ามแดนและความร่วมมือระหว่างประเทศในเรื่องทางอาญาของกรมสอบสวนคดีพิเศษที่ผ่านมาส่วนใหญ่เป็นกรณีที่ประเทศไทยร้องขอความร่วมมือไปยังต่างประเทศ ซึ่งในช่วงปี พ.ศ. ๒๕๕๘ - ๒๕๕๙ มีการดำเนินการร้องขอให้ส่งผู้ร้ายข้ามแดนรวม ๑๒ คดี และร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา ๘ คดี และเมื่อเดือนกรกฎาคม ๒๕๕๙ ผู้แทนกรมสอบสวนคดีพิเศษพร้อมด้วยสำนักงานอัยการสูงสุดได้เดินทางไปรับตัวผู้ต้องหาที่หลบหนีไปยังมาเลเซียกลับมาดำเนินคดีในไทย โดยผ่านกระบวนการร้องขอให้ส่งผู้ร้ายข้ามแดนตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. ๒๕๕๑ จำนวน ๑ ราย คือ คดี นายปาค เนจัด ซาเยส รามิน ชาวอิหร่าน ผู้ต้องหาในคดีพิเศษ ที่ ๘๔/๒๕๕๕ กระทำความผิดฐานครอบครองยาเสพติด ปลอมเอกสาร ปลอมและจำหน่ายหนังสือเดินทางต่างประเทศปลอม และร่วมกันลักทรัพย์และรับของโจร[๗]

อย่างไรก็ตามการดำเนินการที่ผ่านมา มีกระบวนการขั้นตอนมากมาย ทำให้การดำเนินงานไม่เป็นเอกภาพและเกิดความล่าช้า ดังนั้น เพื่อให้การร้องขอให้ส่งผู้ร้ายข้ามแดนและการร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาเป็นไปอย่างมีประสิทธิภาพ กตท. จึงได้จัดทำแนวปฏิบัติในเรื่องดังกล่าว ซึ่งเน้นขบวนการดำเนินงานภายในของกรมสอบสวนคดีพิเศษ เพื่อที่ผู้ที่เกี่ยวข้องสามารถนำไปใช้ปฏิบัติในเบื้องต้น จนกว่าจะมีการกำหนดแนวปฏิบัติที่เป็นทางการต่อไป

๑) แนวปฏิบัติในการร้องขอให้ส่งผู้ร้ายข้ามแดน

๑.๑) เมื่อหน่วยงานหรือพนักงานสอบสวนคดีพิเศษเจ้าของคดี พบว่าผู้ต้องหาหลบหนีไปต่างประเทศ และมีความประสงค์จะร้องขอให้ส่งผู้ร้ายข้ามแดน และ/หรือได้รับแจ้งว่าอัยการสูงสุดเห็นสมควรสั่งฟ้องผู้ต้องหา และขอให้กรมสอบสวนคดีพิเศษจัดการให้ได้ตัวผู้ต้องหามาดำเนินคดี ให้หัวหน้าหน่วยงานเจ้าของคดีดำเนินการขออนุมัติต่ออธิบดีกรมสอบสวนคดีพิเศษผ่านรองอธิบดีที่กำกับดูแลพร้อมแนบแบบขอให้ดำเนินการร้องขอให้ส่งผู้ร้ายข้ามแดน (สตท ๐๐๑) พร้อมเอกสารหลักฐานตามที่กำหนด ซึ่งได้ลงลายมือชื่อรับรองความถูกต้องทุกแผ่นแล้ว

๑.๒) หลังจากที่อธิบดีกรมสอบสวนคดีพิเศษอนุมัติแล้วให้ส่งสำเนาหนังสืออนุมัติพร้อมแบบขอให้ดำเนินการ ร้องขอให้ส่งผู้ร้ายข้ามแดน (สตท ๐๐๐) ให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศดำเนินการต่อไป

---

[๗]กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๓๕-๑๓๗

๑.๓) กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศตรวจสอบความครบถ้วนสมบูรณ์ของเอกสารประกอบการร้องขอให้ส่งผู้ร้ายข้ามแดน และประสานหน่วยงานหรือพนักงานสอบสวนเจ้าของคดีดำเนินการให้ได้เอกสารข้อมูลครบถ้วนสมบรูณ์ หลังจากนั้นกองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศจัดทำคำแปลสำนวนคดี และเอกสารที่เกี่ยวข้องรวมทั้งจัดทำคำร้องขอเป็นภาษาอังกฤษ

๑.๔) กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศมีบันทึกนำเรียนอธิบดีกรมสอบสวนคดีพิเศษ เพื่อมีหนังสือกราบเรียนอัยการสูงสุดในฐานะผู้ประสานงานกลางเพื่อดำเนินการร้องขอให้ส่งผู้ร้ายข้ามแดนต่อไป และให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศร่วมกับหน่วยงานหรือพนักงานสอบสวนเจ้าของคดี ประสานสำนักงานอัยการต่างประเทศ เพื่อดำเนินการจัดหาเอกสารข้อมูลเพิ่มเติมและปรับแก้เอกสารให้ครบถ้วน หรือจัดการประชุมร่วมระหว่างหน่วยงานหรือพนักงานสอบสวนเจ้าของคดี พนักงานอัยการที่เกี่ยวข้องและกองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ ในกรณีที่มีความจำเป็น

๑.๕) หลังจากอัยการสูงสุดพิจารณาเห็นชอบหรือไม่เห็นชอบให้ส่งคำร้องขอให้ส่งผู้ร้ายข้ามแดนให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศมีบันทึกนำเรียนอธิบดีกรมสอบสวนคดีพิเศษเพื่อทราบและแจ้งหน่วยงานเจ้าของคดีทราบเพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ในกรณีที่อัยการสูงสุดเห็นชอบให้ส่งคำร้องขอให้ส่งผู้ร้ายข้ามแดนให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศติดตามความคืบหน้าในการร้องขอให้ส่งผู้ร้ายข้ามแดนเป็นระยะ

๑.๖) เมื่อได้ผ่านกระบวนการภายในของประเทศผู้ถูกร้องขอและประเทศผู้ร้องขอได้มีคำสั่งหรือมีหนังสือ แจ้งความประสงค์ที่จะส่งตัวผู้ต้องหาที่ทางการไทยร้องขอเป็นผู้ร้ายข้ามแดนให้กับประเทศไทยแล้ว คณะผู้แทนไทยประกอบไปด้วยผู้แทนจากสำนักงานอัยการสูงสุดและกรมสอบสวนคดีพิเศษ เดินทางไปรับตัวผู้ต้องหากลับมาดำเนินคดีในประเทศไทยตามระเบียบขั้นตอนและวิธีปฏิบัติของพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. ๒๕๕๑ และสนธิสัญญาว่าด้วยการส่งผู้ร้ายข้ามแดนต่อไป

๒) ขั้นตอนการรับตัวผู้ต้องหาตามคำร้องขอให้ส่งผู้ร้ายข้ามแดน

๒.๑) กรมสอบสวนคดีพิเศษต้องประสานงานกับพนักงานอัยการต่างประเทศสำนักงานอัยการสูงสุด เพื่อประชุมหารือร่วมกันในการกำหนดวัน เวลา และรายละเอียดแนวทางการปฏิบัติในการรับตัวผู้ร้ายข้ามแดน และเมื่อกำหนดวันเวลาที่ชัดเจนแล้วสำนักงานอัยการสูงสุดจะมีหนังสือแจ้งไปยังทางการของประเทศที่จะส่งตัวผู้ร้ายข้ามแดนให้ทราบและส่งตัวให้กับประเทศไทย

๒.๒) มีหนังสือถึงกระทรวงการต่างประเทศเพื่อแจ้งให้ทราบถึงการเดินทางไปยังประเทศที่ส่งตัวผู้ร้าย ข้ามแดน ของคณะผู้แทนกรมสอบสวนคดีพิเศษและพนักงานอัยการและประสานงานเกี่ยวกับเอกสารหรือหนังสือเดินทางให้กับผู้ร้ายข้ามแดนในการนำตัวเข้ามาดำเนินคดีในประเทศไทย

๒.๓) ประสานงานกับสำนักงานตำรวจแห่งชาติ เพื่อขอความร่วมมือเรื่องพิธีการตรวจลงตรา การเข้าเมืองของผู้ร้ายข้ามแดน

๒.๔) ประสานงานกับบริษัทท่าอากาศไทย จำกัด (มหาชน) กรณีเดินทางโดยเครื่องบิน เพื่อขอใช้สถานที่ภายในสนามบินในการดำเนินการเกี่ยวกับกระบวนการส่งผู้ร้ายข้ามแดน เช่นสถานที่ในการส่งมอบตัวผู้ร้ายข้ามแดน เป็นต้น รวมทั้งขอให้อำนวยความสะดวกให้กับคณะผู้แทนฝ่ายไทยและเจ้าหน้าที่ในการนำตัวผู้ร้ายข้ามแดนเข้า - ออกจากสนามบิน เพื่อนำตัวผู้ร้ายข้ามแดนไปดำเนินการตามกฎหมายต่อไป

๒.๕) ติดต่อประสานงานกับผู้จัดการกองขายภาคราชการ บริษัทการบินไทย จำกัด (มหาชน) เพื่อขอให้อำนวยความสะดวกในการออกบัตรโดยสารเครื่องบินและกำหนดที่นั่งให้กับผู้ร้ายข้ามแดน, คณะผู้แทนฝ่ายไทยที่เดินทางไปรับตัวผู้ร้ายข้ามแดนและผู้ควบคุมตัวผู้ร้ายข้ามแดน (Escort) โดยขอให้ขึ้นเครื่องบินก่อนผู้โดยสารคนอื่น ๆ และให้นั่งในที่นั่งท้ายสุดของเครื่องบิน เพื่อง่ายต่อการควบคุมตัวผู้ร้ายข้ามแดน และไม่ทำให้ผู้โดยสารรายอื่นเกิดความวิตกกังวล และขอนำเครื่องพันธนาการขึ้นเครื่องบินเพื่อใช้ในการควบคุมตัวผู้ร้ายข้ามแดน รวมทั้งติดต่อแพทย์ถ้ามีความจำเป็นต้องทำการรักษาหรือใช้ยากรณีที่ผู้ร้ายข้ามแดนเจ็บป่วยหรืออาจก่อความวุ่นวายหรือไม่ยอมเดินทางกลับประเทศไทย อีกทั้งควรจัดทำแผนปฏิบัติการสำรองไว้ด้วยในกรณีที่มีเหตุไม่สามารถนำตัว ผู้ร้ายข้ามแดนกลับประเทศไทยตามแผนที่กำหนดไว้

๒.๖) เมื่อคณะผู้แทนฝ่ายไทยที่ไปรับตัวผู้ร้ายข้ามแดนเดินทางถึงประเทศที่ส่งตัวผู้ร้ายข้ามแดนแล้ว ต้องนัดประชุมหารือกับพนักงานอัยการและเจ้าหน้าที่ที่เกี่ยวข้องของประเทศที่ส่งตัวผู้ร้ายข้ามแดน เพื่อกำหนดรายละเอียดวิธีปฏิบัติและตรวจสอบเอกสารหลักฐานที่เกี่ยวข้องกับการส่งผู้ร้ายข้ามแดนให้ถูกต้องครบถ้วนและชัดเจน ก่อนที่จะทำการส่งตัวผู้ร้ายข้ามแดน

๒.๗) เมื่อรับตัวผู้ร้ายข้ามแดนเดินทางถึงประเทศไทยแล้ว คณะผู้แทนฝ่ายไทยต้องส่งมอบตัวผู้ร้ายข้ามแดน ให้กับพนักงานสอบสวนคดีพิเศษเจ้าของสำนวนเพื่อดำเนินการตามกฎหมายต่อไป

๓. แนวปฏิบัติในการขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา

๓.๑) เมื่อหน่วยงานมีความประสงค์จะขอให้ดำเนินการร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาในคดีพิเศษที่อยู่ในความรับผิดชอบ ให้หัวหน้าหน่วยงานดำเนินการขออนุมัติต่ออธิบดีกรมสอบสวนคดีพิเศษผ่านรองอธิบดีที่กำกับดูแล พร้อมแนบแบบขอให้ดำเนินการร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา (สตท ๐๐๒) พร้อมเอกสารหลักฐานตามที่กำหนด ซึ่งได้ลงลายมือชื่อรับรองความถูกต้องทุกแผ่นแล้ว

๓.๒) หลังจากได้รับการอนุมัติจากอธิบดี ให้จัดส่งสำเนาหนังสืออนุมัติพร้อมแบบขอให้ดำเนินการร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา (สตท ๐๐๒) ให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศดำเนินการต่อไป

๓.๓) กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศตรวจสอบความครบถ้วนสมบูรณ์ของเอกสารประกอบการร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา และประสานหน่วยงานหรือพนักงานสอบสวนเจ้าของคดีดำเนินการให้ได้เอกสารข้อมูลครบถ้วนสมบูรณ์ หลังจากนั้นกองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศจัดทำคำแปล และคำร้องขอเป็นภาษาอังกฤษ

๓.๔) กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ มีบันทึกนำเรียนอธิบดีกรมสอบสวนคดีพิเศษ เพื่อมีหนังสือกราบเรียนอัยการสูงสุดในฐานะผู้ประสานงานกลาง เพื่อดำเนินการร้องขอให้ความร่วมมือระหว่างประเทศในเรื่องทางอาญาต่อไป และให้กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศร่วมกับหน่วยงานหรือพนักงานสอบสวนเจ้าของคดี ประสานสำนักงานอัยการต่างประเทศ เพื่อดำเนินการจัดหาเอกสาร ข้อมูลเพิ่มเติม และปรับแก้เอกสารให้ครบถ้วน หรือจัดการประชุมร่วมระหว่างหน่วยงานเจ้าของคดี พนักงานอัยการที่เกี่ยวข้อง และกองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ ในกรณีที่มีความจำเป็น

๓.๕) หลังจากอัยการสูงสุดพิจารณาเห็นชอบหรือไม่เห็นชอบให้ส่งคำร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา ให้สำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศมีบันทึกนำเรียนอธิบดีกรมสอบสวนคดีพิเศษเพื่อทราบ และแจ้งหน่วยงานเจ้าของคดีทราบเพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป ซึ่งในกรณีที่อัยการสูงสุดเห็นชอบให้ส่งคำร้องขอความร่วมมือระหว่างประเทศในเรื่องทางอาญาแล้ว ให้สำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศติดตามความคืบหน้าในการร้องขอให้ส่งผู้ร้ายข้ามแดนเป็นระยะ

๓.๖) ในกรณีที่จำเป็นต้องเดินทางไปต่างประเทศ เพื่อขอความร่วมมือระหว่างประเทศในเรื่องทางอาญา ให้หน่วยงานเจ้าของเรื่องเป็นผู้ดำเนินการขออนุมัติการเดินทางและค่าใช้จ่ายต่ออธิบดีกรมสอบสวนคดีพิเศษผ่านรองอธิบดีที่กำกับดูแลและให้สำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศเป็นผู้ประสานงานกับอัยการและหน่วยงานต่างประเทศ

๔.๔ กรณีศึกษาและแนวทางแก้ไข

๔.๔.๑ กรณีศึกษาที่ ๑ Internet Fraud สภาพปัญหาที่พบในปัจจุบัน มีดังต่อไปนี้

๔.๔.๑.๑ Call Center สังเกตได้จากหลอกลวงโอนเงินจากคนประเทศไหนใช้คนประเทศนั้นเป็นคนหลอก ส่วนมากที่พบ คือ คนประเทศไต้หวัน โดยมีคนจีนเป็นลูกน้องและมีการย้ายถิ่นฐานในหลาย ๆ ประเทศ มีวิธีการโอนเงิน คือ การโอนเงินจาก Bitcoin และโอนเข้าบัญชีปลายทาง และใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยเพื่อเปลี่ยนวิธีการหลอกลวง และมีการแบ่งหน้าที่กันชัดเจน ซึ่งประกอบด้วย คนจัดหาบัญชี ม้าถอนเงิน คนจัดการทางการเงิน/โพยก๊วน Call Center และคนสั่งการ

<u>แนวทางการแก้ไขปัญหา</u>

๑) ความร่วมมือในการตรวจพิสูจน์หลักฐาน เช่น โทรศัพท์มือถือ คอมพิวเตอร์ เป็นต้น เนื่องจากบางครั้งตำรวจมีหลักฐานที่ต้องการตรวจพิสูจน์เป็นจำนวนมาก ถ้ากรณีเร่งด่วนไม่สามารถจัดการได้ทัน

๒) ความร่วมมือกับธนาคารเรื่องความรวดเร็วในการได้ข้อมูล เช่น ความต้องการรูปจากหน้ากล้องตู้เอทีเอ็ม ซึ่งบางครั้งเกิดความล่าช้าทำให้ไม่สามารถติดตามคนร้ายได้ทันท่วงที

๓) ความร่วมมือกับธนาคารในการแจ้งเตือน Awareness เกี่ยวกับการยืนยันตัวตนด้วย OTP

๔) สร้างความร่วมมือกับธนาคารต่างประเทศ/ศูนย์ Visa ประเทศไทย : ประเด็นเรื่อง ผู้ต้องหากดเงินในต่างประเทศใช้บัตร Visa ไทยถอนได้ทั่วโลก เสียค่าธรรมเนียม หรือใช้วิธี Skim ข้อมูลบัตรแล้วส่งไปยังต่างประเทศ เพื่อคัดลอกทำบัตรใช้ถอนเงินในต่างประเทศ

๕) ความร่วมมือกับต่างประเทศในการสืบสวน และเข้าตรวจค้นในต่างประเทศ ซึ่งแต่ละประเทศจะมีลักษณะและวิธีการที่แตกต่างกัน

๖) การให้ความรู้ผ่านทางสื่อต่าง ๆ การแถลงข่าวภายหลังการจับกุม

๔.๔.๑.๒ Romance Scam โดยใช้การติดต่อทาง Facebook เมื่อติดต่อกันในระยะเวลาหนึ่งพัฒนาจนถึงขั้นจะแต่งงานด้วย หรือจะมาหาที่เมืองไทย หลอกลวงโดยบอกว่ามีพัสดุส่งมาให้แต่ติดอยู่ที่สนามบิน ซึ่งจะมีเจ้าหน้าที่ติดต่อมาว่ามีของติดอยู่อาจเป็นสิ่งของมีค่าและมีค่าธรรมเนียม โดยเมื่อผู้เสียหายเกิดความหลงเชื่อจะมีการโอนเงินให้เป็นค่าธรรมเนียม ซึ่งมีผู้เสียหายได้รับความเสียหายหลายสิบล้าน หลักการของ Romance Scam คือ ความรัก ความเชื่อใจ และความโลภ โดยมากกลุ่มคนดำเป็นผู้กระทำความผิดเป็นส่วนใหญ่ ผู้เสียหายจำนวน ๙๐% เป็นผู้หญิงที่มีปัญหาทางครอบครัว หรือมีครอบครัวอยู่แล้วแต่ยังคุยกับผู้กระทำผิด ปัญหาที่สำคัญ คือ ผู้เสียหายไม่เชื่อว่าตนเองกำลังตกเป็นเหยื่อ

<u>แนวทางการแก้ไขปัญหา</u>

๑) หน่วยงานที่เกี่ยวข้องประชุมร่วมกัน เพื่อทำการรวบรวม และวิเคราะห์ข้อมูลที่เกี่ยวข้องในการกระทำความผิด เช่น บัญชีทางการเงิน ชื่อ Facebook เป็นต้น

๒) ความร่วมมือกับ Facebook กับธนาคาร Western Union

๓) การให้ความรู้ผ่านทางสื่อต่าง ๆ การแถลงข่าวภายหลังการจับกุม

๔.๔.๑.๓ E-mail Scam เป็นการหลอกลวงทางอีเมล ติดตามยาก คือ การแฮกอีเมล โดยมีการแฮกดูรายละเอียดของการค้า เมื่อถึงเวลานัดชำระสินค้ากลุ่มคนร้ายจะส่งเมล์และเลขที่บัญชีเพื่อให้โอนเงินเข้าบัญชีของตนแทน

<u>แนวทางการแก้ไขปัญหา</u>

๑) การตอบ ไม่ควรใช้ Reply all ให้พิมพ์ E-mail บุคคลที่ต้องการตอบเพื่อป้องกันบุคคลที่ต้องการดักระหว่างทางของ E-mail

๒) คู่ค้า : ถ้ามีการแจ้งเปลี่ยนบัญชีที่ใช้ในการโอนเงินระหว่างกัน ควรมีการยืนยันผ่านทางช่องทางอื่นก่อน

๓) ควรเปลี่ยน Password บ่อย ๆ

๔.๔.๑.๔ การให้คำแนะนำการลงทุนเถื่อน/Eaglegates การโฆษณาชักชวนให้มาลงทุนเกี่ยวกับประกอบธุรกิจหลักทรัพย์/ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

<u>แนวทางการแก้ไขปัญหา</u>

๑) การให้ความรู้เกี่ยวกับการลงทุนที่ถูกต้อง

๒) ก.ล.ต. แนะนำให้ตรวจสอบรายชื่อบริษัทที่ได้รับอนุญาต และรายชื่อบริษัทที่ไม่ได้รับอนุญาต (มีผู้แจ้งเบาะแส)

๓) การลงทุนต่างประเทศ ต้องตรวจสอบที่เว็บ ก.ล.ต. ต่างประเทศ

๔.๔.๑.๕ การแฮก Line/Facebook เพื่อติดต่อยืมเงินผู้อื่น โดยผู้กระทำผิดมักจะเลือกคนที่ค่อนข้างเปิดในสังคมออนไลน์ เช่น พ่อค้าออนไลน์ โดยกลุ่มผู้กระทำผิดจะนำอีเมลของบุคคลเหล่านี้มาใช้ Sign in เข้าระบบไลน์ เพื่อทำการหลอกลวงขอยืมเงิน

<u>แนวทางการแก้ไขปัญหา</u>

๑) ควรเปลี่ยน Password บ่อย ๆ

๒) การตรวจสอบจากตัวจริงว่าเป็นผู้ที่มาขอยืมจริง

๓) การตั้ง Password ให้มีความซับซ้อนไม่ง่ายเกินไป

๔.๔.๒ กรณีศึกษาที่ ๒ Cryptocurrency

การป้องกันและแก้ไขปัญหาการหลอกลวงสินทรัพย์ดิจิทัล (Scam Coin) ปัจจุบันเทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันของคนทั่วไป การประกอบธุรกิจสามารถติดต่อข้ามถึงกันในลักษณะไร้พรมแดน เกิดการกำหนดมูลค่า (Value) ในการประกอบธุรกิจระหว่างความต้องการ (Demand) และการจัดหา (Supply) ที่มีลักษณะใช้เทคโนโลยีเข้ามาเป็นสื่อกลางและยอมรับมูลค่า (Value) ดังกล่าว ซึ่งมีความแตกต่างไปจากเดิมอย่างสิ้นเชิง ดังนั้นจึงเกิดวิวัฒนาการทางการเงินในรูปแบบเงินดิจิทัลหรือสกุลเงินที่ถูกเข้ารหัส (Cryptocurrency) ที่มีลักษณะไม่เป็นตัวกลางในการซื้อขายแลกเปลี่ยนและตัวเก็บมูลค่าที่ดี Decentralized Cryptocurrencies อาจกล่าวได้ว่าเป็นจุดเปลี่ยนของวิวัฒนาการของเงินที่ก่อให้เกิดเงินตราดิจิทัลในสกุลต่าง ๆ จำนวนมากมาย เช่น Litecoin, Ethereum, Zcash, Ripple, Monero, Bitcoin, Litecoin, Darkcoin และ Dodgecoin ซึ่งสกุลเงินแรกก็คือ Bitcoin

สถาบันการเงินทั่วโลกส่วนใหญ่ยังไม่รับชำระธุรกรรมในรูปแบบไม่เป็นตัวกลางในการซื้อขายแลกเปลี่ยน Decentralized Cryptocurrencies เช่น ในสาธารณรัฐประชาชนจีน สาธารณรัฐฟิลิปปินส์ ที่ยังไม่มีการออกกฎหมายรองรับสกุลเงินดิจิทัล (Cryptocurrency) ดังกล่าว และแม้กระทั่งสกุลเงิน Bitcoin เอง จะใช้เทคโนโลยี Blockchain ที่ยืนยันได้ว่า ยังไม่สามารถถูกเจาะได้ก็ตาม

Cryptocurrency คือ สกุลเงินดิจิทัล หรือ เงินดิจิทัล โดยออกแบบมาให้เข้ารหัสกระจายออกไปในส่วนอื่น ๆ ไม่มีศูนย์กลาง ไม่มีการควบคุมจากกลุ่มใดกลุ่มหนึ่ง ราคาของ Cryptocurrency ขึ้นอยู่กับความต้องการของคนไม่ได้เกิดจากสภาพเศรษฐกิจหรือในโลกภายนอก มีการซื้อขาย Cryptocurrency ในสกุลเงินต่าง ๆ ออนไลน์กันอยู่ตลอด ๒๔ ชั่วโมง หากความต้องการสกุลเงินไหนมากและเป็นที่นิยม สกุลเงินดังกล่าวก็จะสูงขึ้นเรื่อย ๆ

สภาพปัญหาที่พบในปัจจุบัน และแนวทางการแก้ไขปัญหา มีดังต่อไปนี้

๔.๔.๒.๑ Cryptocurrency การเงินและการธนาคารยังไม่ยอมรับว่าเงินดิจิทัลมีคุณสมบัติเป็นเงินตรา เพราะไม่สามารถชำระหนี้ได้ตามกฎหมาย เป็นสินทรัพย์ที่ควบคุมไม่ได้ ฉะนั้นจึงไม่อยู่ภายใต้การดูแลของธนาคารแห่งประเทศไทย แต่เป็นสินทรัพย์ดิจิทัลจึงอยู่ภายใต้การดูแลของ ก.ล.ต.

๔.๔.๒.๒ การนำไปใช้ระหว่างบุคคล (Peer to Peer) สามารถนำไปใช้ได้ขึ้นอยู่กับความยินยอมของสองฝ่าย กรณีเกิดปัญหาการฉ้อโกงจึงเป็นปัญหาที่ไม่มีกฎหมายเฉพาะเพื่อเยียวยาผู้เสียหาย แต่สามารถใช้หลักกฎหมายทั่วไปในเรื่องนิติกรรมสัญญามาใช้บังคับกับผู้กระทำผิดแทน

๔.๔.๒.๓ กรณีเกิดการฉ้อโกงในเรื่อง Cryptocurrency ระหว่างประเทศทาง ก.ล.ต. มีหน่วยงานในลักษณะเดียวกันในต่างประเทศ เพื่อประสานเรื่องพยานหลักฐานหรือมอบหมายให้ดำเนินการสอบปากคำเมื่อร้องขอ ภายใต้เงื่อนไขว่าจะต้องผิดกฎหมายในประเทศนั้น ๆ ด้วย

๔.๔.๒.๔ ปัญหาการยึดเงินดิจิทัลได้นั้นจะต้องเข้าไปยึดในขณะทำการ Log in ต้องมี Private key ก่อน ไม่เช่นนั้นจะไม่สามารถเข้าสู่ระบบการเงินได้ และเงินดิจิทัลของผู้กระทำผิดที่ถูกอายัดไว้นั้นผู้กระทำผิดสามารถโอนเงินไปไว้ Wallet อื่นได้

บทที่ ๕
บทสรุปและข้อเสนอแนะ

๕.๑ บทสรุป

การพัฒนาเทคโนโลยีใหม่ ๆ การกำกับดูแล และความต้องการทางนโยบายขององค์กรที่เปลี่ยนแปลงไป ทำให้องค์กรต้องมีการตื่นตัวและให้ความสำคัญในความมั่นคงปลอดภัยไซเบอร์เพิ่มมากขึ้น ภัยคุกคามที่อาจเกิดขึ้นได้ เช่น ภัยคุกคามที่เกิดกับระบบ Cloud Cryptocurrency สกุลเงินดิจิทัล รวมถึงความสะดวกสบายจากการใช้เทคโนโลยีในการทำธุรกรรมทางการเงินผ่านสมาร์ทโฟน สิ่งเหล่านี้เป็นภัยใกล้ตัวที่ไม่อาจคาดคิด ถ้าประชาชนขาดความรู้ความเข้าใจจากการใช้เทคโนโลยี ฉะนั้นแนวทางในการป้องกันอาชญากรรมคอมพิวเตอร์ ผู้เขียนเห็นว่า ควรให้ความรู้และความตระหนักรู้กับประชาชน หากจะดำเนินการในเชิงปราบปรามโดยการสืบสวนสอบสวนเพียงอย่างเดียว คงไม่เท่าทันกับการก้าวกระโดดของเทคโนโลยี การให้ความรู้ และความตระหนักรู้กับประชาชน หน่วยงานภาครัฐและหน่วยงานภาคเอกชนควรให้ความร่วมมือกันพัฒนาและพร้อมที่จะแก้ไขปัญหาที่อาจเกิดขึ้น ดังจะเห็นจากแนวทางการกำหนดยุทธศาสตร์ชาติ ๒๐ ปี ที่มีเรื่องการจัดการกับระบบฐานข้อมูลขนาดใหญ่ การนำนวัตกรรม เทคโนโลยีข้อมูลขนาดใหญ่ ระบบการทำงานที่เป็นดิจิทัล เข้ามาประยุกต์ใช้อย่างคุ้มค่าและปฏิบัติงานเทียบได้กับมาตรฐานสากล

ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑ - ๒๕๘๐) เป็นยุทธศาสตร์ชาติฉบับแรกของประเทศไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา ๖๕ ซึ่งจะต้องนำไปสู่การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” ภายในช่วงเวลาดังกล่าว เพื่อความสุขของคนไทยทุกคน

๕.๑.๑ ยุทธศาสตร์ชาติด้านความมั่นคง มีเป้าหมายการพัฒนาที่สำคัญ คือ ประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคงปลอดภัย เอกราชอธิปไตย และมีความสงบเรียบร้อยในทุกระดับ ตั้งแต่ระดับชาติ สังคม ชุมชน มุ่งเน้นการพัฒนาคน เครื่องมือ เทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบและทุกระดับความรุนแรง ควบคู่ไปกับการป้องกันและแก้ไขปัญหาด้านความมั่นคงที่มีอยู่ในปัจจุบันและที่อาจจะเกิดขึ้นในอนาคต ใช้กลไกการแก้ไขปัญหาแบบบูรณาการทั้งกับส่วนราชการ ภาคเอกชน ประชาสังคม และองค์กรที่ไม่ใช่รัฐ รวมถึงประเทศเพื่อนบ้านและมิตรประเทศทั่วโลกบนพื้นฐานของหลักธรรมาภิบาล เพื่อเอื้ออำนวยประโยชน์ต่อการดำเนินการของยุทธศาสตร์ชาติด้านอื่น ๆ ให้สามารถขับเคลื่อนไปได้ตามทิศทางและเป้าหมายที่กำหนด

๕.๑.๒ ยุทธศาสตร์ชาติด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ มีเป้าหมายการพัฒนาที่สำคัญเพื่อปรับเปลี่ยนภาครัฐที่ยึดหลัก “ภาครัฐของประชาชนเพื่อประชาชนและประโยชน์ส่วนรวม” โดยภาครัฐต้องมีขนาดที่เหมาะสมกับบทบาทภารกิจ แยกแยะบทบาทหน่วยงานของรัฐที่ทำหน้าที่ในการกำกับหรือในการให้บริการในระบบเศรษฐกิจที่มีการแข่งขันมีสมรรถนะสูง ยึดหลักธรรมาภิบาล ปรับวัฒนธรรมการทำงานให้มุ่งผลสัมฤทธิ์และผลประโยชน์ส่วนรวมมีความทันสมัย และพร้อมที่จะปรับตัวให้ทันต่อการเปลี่ยนแปลงของโลกอยู่ตลอดเวลา

โดยเฉพาะอย่างยิ่งการนำนวัตกรรม เทคโนโลยีข้อมูลขนาดใหญ่ ระบบการทำงานที่เป็นดิจิทัลเข้ามาประยุกต์ใช้อย่างคุ้มค่าและปฏิบัติงานเทียบได้กับมาตรฐานสากล รวมทั้งมีลักษณะเปิดกว้างเชื่อมโยงถึงกัน และเปิดโอกาสให้ทุกภาคส่วนเข้ามามีส่วนร่วมเพื่อตอบสนองความต้องการของประชาชนได้อย่างสะดวก รวดเร็ว และโปร่งใส โดยทุกภาคส่วนในสังคมต้องร่วมกันปลูกฝังค่านิยมความซื่อสัตย์สุจริต ความมัธยัสถ์ และสร้างจิตสำนึกในการปฏิเสธไม่ยอมรับการทุจริตประพฤติมิชอบอย่างสิ้นเชิง นอกจากนั้น กฎหมายต้องมีความชัดเจน มีเพียงเท่าที่จำเป็น มีความทันสมัย มีความเป็นสากล มีประสิทธิภาพและนำไปสู่การลดความเหลื่อมล้ำและเอื้อต่อการพัฒนา โดยกระบวนการยุติธรรมมีการบริหารที่มีประสิทธิภาพ เป็นธรรมไม่เลือกปฏิบัติ และการอำนวยความยุติธรรมตามหลักนิติธรรม

๕.๒ ข้อเสนอแนะ

๕.๒.๑ เชิงนโยบายระดับประเทศ

๕.๒.๑.๑ รัฐบาลของประเทศอาเซียนจำเป็นที่จะต้องเสริมสร้างความร่วมมือระหว่างกันในภูมิภาคและควรมียุทธศาสตร์ความร่วมมือของภูมิภาคอาเซียนในด้านกระบวนการยุติธรรมทางอาญา โดยสมควรพิจารณาประเด็นที่เกี่ยวข้องใน ๓ ด้าน ได้แก่ การพัฒนากลไกความร่วมมือของกระบวนการยุติธรรมทางอาญาให้เหมาะสม การพัฒนาความร่วมมือระหว่างประเทศด้านกฎหมายและการบริหารจัดการ และการพัฒนาและเสริมสร้างศักยภาพของบุคลากรในกระบวนการยุติธรรม

๑) การพัฒนากลไกความร่วมมือของกระบวนการยุติธรรมทางอาญาให้เหมาะสม ได้แก่ รัฐอาเซียนควรจัดตั้งทีมปฏิบัติการสืบสวนสอบสวนร่วมของภูมิภาคอาเซียนประกอบด้วย หน่วยงานในกระบวนการยุติธรรมหลักที่เกี่ยวข้อง เช่น กรมสอบสวนคดีพิเศษ สำนักงานตำรวจแห่งชาติ สำนักงานอัยการ สำนักงานศาลยุติธรรม กรมศุลกากร สำนักงานนิติวิทยาศาสตร์ เป็นต้น ให้มีอำนาจหน้าที่ในการสืบสวนสอบสวนคดีอาชญากรรมข้ามชาติที่ส่งผลกระทบต่อความมั่นคงของประเทศอาเซียนในวงกว้าง เช่น การก่อการร้ายข้ามชาติ การค้ามนุษย์ และอาชญากรรมคอมพิวเตอร์

๒) การพัฒนาความร่วมมือระหว่างประเทศด้านกฎหมาย และการบริหารจัดการ ได้แก่ รัฐอาเซียนควรส่งเสริมผลักดันให้ประเทศสมาชิกใช้เครื่องมือ และระบบการบริหารจัดการคดีระหว่างประเทศ เช่น ระบบฐานข้อมูลและการตรวจพิสูจน์ขององค์การตำรวจสากล ระบบฐานข้อมูลตำรวจอาเซียน ระบบการบริหารจัดการและการสืบสวนคดี ซึ่งที่เกี่ยวข้องกับฐานข้อมูลอาชญากรรมข้ามชาติหลายประเภท การค้ามนุษย์ การฉ้อโกงข้ามชาติ อาชญากรรมคอมพิวเตอร์ อาชญากรรมเศรษฐกิจและการเงิน มาใช้ในการปฏิบัติงานและให้สามารถยอมรับเป็นพยานหลักฐานชั้นศาลได้

รัฐอาเซียนควรส่งเสริมการพัฒนาความร่วมมือระหว่างประเทศในเรื่องทางอาญาของภูมิภาคอาเซียน ทั้งในรูปแบบที่เป็นทางการและไม่เป็นทางการ โดยให้ความสำคัญต่อความร่วมมือและการให้ความช่วยเหลือระหว่างประเทศในเรื่องทางอาญาเพิ่มมากขึ้น และแสดงให้เห็นถึงความจริงใจที่จะให้ความช่วยเหลือซึ่งกันและกันบนหลักปฏิบัติต่างตอบแทน ซึ่งสามารถกระทำได้ทั้งในระดับนโยบายและระดับปฏิบัติ เช่น การกำหนดให้เรื่องความร่วมมือระหว่างประเทศในเรื่องทางอาญาอยู่ในแผนแม่บทของรัฐบาลที่จะต้องดำเนินการ การแก้ไขกฎหมายอาญาและกฎหมายวิธีพิจารณาความอาญาให้ครอบคลุมถึงกิจกรรรมผิดกฎหมายต่าง ๆ ที่เกี่ยวข้องกับองค์กรอาชญากรรมข้ามชาติไม่ว่าจะกระทำภายในหรือภายนอกประเทศ การเพิ่มอำนาจให้เจ้าหน้าที่บังคับใช้กฎหมาย

ที่เกี่ยวข้องในการสืบสวนสอบสวนคดีที่มีลักษณะข้ามชาติ การจัดตั้งหน่วยงานเฉพาะขึ้นมาเพื่อรับผิดชอบในการสืบสวนปราบปรามอาชญากรรมข้ามชาติ นอกจากนี้ การใช้ช่องทางประสานงานเพื่อเพิ่มประสิทธิภาพความร่วมมือระหว่างภูมิภาคในเรื่องทางอาญาอื่น ๆ นอกเหนือจากกลไกทางกฎหมาย เช่น การประสานงานผ่านช่องทางตำรวจสากล ฐานข้อมูลตำรวจอาเซียน และการประสานงานผ่านเจ้าหน้าตำรวจประจำสถานทูต ควรได้รับการยอมรับเป็นส่วนหนึ่งของกระบวนการยุติธรรมทางอาญาอย่างเป็นทางการของประเทศอาเซียน

๓) การพัฒนาและเสริมสร้างศักยภาพของบุคลากรในกระบวนการยุติธรรม ได้แก่ รัฐอาเซียนควรจัดเตรียมบุคลากรหน่วยงานบังคับใช้กฎหมายโดยเฉพาะที่เกี่ยวข้องกับการสืบสวนสอบสวน และประสานงานทางคดีให้มีความรู้ในลักษณะสหวิทยาการ ประกอบด้วย กฎหมายระหว่างประเทศ กฎหมายสารบัญญัติและวิธีสบัญญัติทางอาญา และการสืบสวนสอบสวนคดี

๕.๒.๑.๒ หน่วยงาน IGCI เป็นส่วนงานหนึ่งขององค์การตำรวจสากล (INTERPOL) ที่ได้เปิดทำการอย่างเป็นทางการแล้วเมื่อเดือนเมษายน พ.ศ. ๒๕๕๘ ที่ผ่านมา โดยมีภารกิจหน้าที่เกี่ยวกับการวิจัยและพัฒนาอุปกรณ์และเครื่องมือต่าง ๆ ที่ใช้ในการระบุอาชญากรรมและตัวตนของผู้กระทำความผิด สนับสนุนงานด้านการตรวจพิสูจน์ทางคอมพิวเตอร์ มีห้อง Lab ที่ทันสมัยตลอดจนมีการจัดการฝึกอบรมเกี่ยวกับนวัตกรรมและเทคโนโลยีใหม่ที่ช่วยในการสืบสวนสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ มีเจ้าหน้าที่ประจำประมาณ ๑๕๐ คน โดยมีเจ้าหน้าที่ที่เป็น Seconded Officers จำนวน ๔๐ คน จาก ๒๔ ประเทศ ได้แก่ ประเทศออสเตรเลีย อาร์เจนตินา ออสเตรีย บราซิล แคนาดา จีน อินโดนีเซีย เนเธอร์แลนด์ อิตาลี อิหร่าน อิสราเอล เคนย่า นอร์เวย์ กาตาร์ รวันดา สิงคโปร์ สเปน ไนจีเรีย เกาหลี สหรัฐอเมริกา คูเวต ฝรั่งเศส อังกฤษ และญี่ปุ่น ซึ่งจะเห็นได้ว่าไม่มีเจ้าหน้าที่ของประเทศไทยอยู่ในกลุ่มหน่วยงานนี้ ทั้งที่ในภูมิภาคอาเซียนอย่างอินโดนีเซีย สิงคโปร์ ก็ได้มีการเข้าร่วมกับหน่วยงานนี้ ดังนั้น หน่วยงานที่มีหน้าที่เกี่ยวข้องควรจะผลักดันให้ประเทศไทยได้เข้าไปมีส่วนร่วมดังกล่าว เพื่อประโยชน์ในการป้องกันและปราบปราม Cyber Crime ในอนาคต

๕.๒.๑.๓ กรมสอบสวนคดีพิเศษ ควรอยู่ในกลุ่มของ International Police เช่นเดียวกับสำนักงานตำรวจแห่งชาติ เพื่อความคล่องตัวในการประสานงานด้านการสืบสวนด้าน Cyber ที่ต้องอาศัยความรวดเร็วในการประสานงานและในการทำงาน

๕.๒.๑.๔ มีหน่วยงานที่เฝ้าระวังและพร้อมสนับสนุนข้อมูลให้กับเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมาย เพื่อดำเนินการตามแนวทางป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์อย่างจริงจัง

๕.๒.๑.๕ ให้ความรู้แก่ประชาชนทั่วไป ในเรื่องของอาชญากรรมคอมพิวเตอร์ใหม่ ๆ อยู่เสมอ โดยให้ความรู้เกี่ยวกับรูปแบบของอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น แต่จำต้องระวังผลกระทบอีกด้านหนึ่งที่รูปแบบอาชญากรรมคอมพิวเตอร์เหล่านี้ กลับกลายเป็นแนวทางที่ผู้ไม่หวังดีจะนำมาเป็นแบบอย่างในการก่ออาชญากรรมคอมพิวเตอร์ต่อไป

การให้ความรู้ด้านอาชญากรรมคอมพิวเตอร์ สามารถทำในรูปแบบของคู่มือความรู้ผ่านโซเชียลมีเดีย เช่น Line Facebook Instagram ออกอากาศผ่านจอทีวี แผ่นผับ รวมถึงจัดกิจกรรมให้ความรู้แก่ประชาชนตามสถานที่ต่าง ๆ เป็นต้น

๕.๒.๒ เชิงนโยบายระดับองค์กร

๕.๒.๒.๑ การเพิ่มประสิทธิภาพในการสืบสวน และสอบสวน มีการจัดการอบรมในเรื่องสืบสวน สอบสวน โดยการแลกเปลี่ยนความรู้ระหว่างหน่วยงานบังคับใช้กฎหมายในประเทศไทยและหน่วยงานบังคับใช้กฎหมายในกลุ่มประเทศอาเซียนที่มีความเสี่ยงต่ออาชญากรรมไซเบอร์ เช่น การแลกเปลี่ยนบุคลากรในการอบรมต่าง ๆ ปีละ ๑ - ๒ ครั้ง เพื่อเพิ่มพูนความรู้ด้านอาชญากรรมไซเบอร์ใหม่ ๆ และเป็นการสร้างความสัมพันธ์ระหว่างผู้ร่วมงานและหน่วยงานให้มากขึ้น จนเกิดการบูรณาการร่วมกัน เช่น เทคนิคการสืบสวน Cryptocurrency เป็นต้น

กองคดีเทคโนโลยีและสารสนเทศ ได้จัดสัมมนาภายในประเทศซึ่งเป็นกิจกรรมที่ ๒ ต่อเนื่องภายหลังจากการไปศึกษาดูงานในต่างประเทศ โดยภายหลังจากการศึกษาดูงานที่ประเทศมาเลเซียและสาธารณรัฐสิงคโปร์ ก็ได้มีการจัดสัมมนาเล็ก ๆ เพียงครึ่งวัน และได้เชิญหน่วยบังคับใช้กฎหมายที่เกี่ยวข้องร่วมประชุมหารือส่วนภายหลังจากการศึกษาดูงานที่สาธารณรัฐฟิลิปปินส์ ได้มีการจัดสัมมนา เรื่อง ความร่วมมือในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ในอาเซียน ซึ่งได้เชิญเจ้าหน้าที่สถานทูตประจำประเทศไทย เจ้าหน้าที่ UNODC เข้าร่วมประชุมเชิงปฏิบัติการ นอกจากนี้ยังได้จัดฝึกอบรมเจ้าหน้าที่ภายในหน่วยงาน เรื่อง เทคนิคการสืบสวน Cryptocurrency

๕.๒.๒.๒ มีกิจกรรมเพื่อพัฒนาความสัมพันธ์ของผู้ปฏิบัติงาน สร้างกิจกรรมให้ผู้ปฏิบัติงานระหว่างหน่วยงาน เช่น การจัดประชุมสัมมนา จัดกิจกรรมดูงานทั้งในและต่างประเทศ เข้าร่วมกิจกรรมละลายพฤติกรรม เป็นต้น เพื่อความสนิทสนมไว้เนื้อเชื่อใจกันได้มากขึ้น เพราะการติดต่อประสานงาน เพื่อขอข้อมูลด้านการสืบสวนอย่างไม่เป็นทางการมักจะยินดีช่วยเหลือให้ความร่วมมือกัน เพราะความสนิทสนมไว้เนื้อเชื่อใจกัน

๕.๒.๒.๓ จากแผนยุทธศาสตร์ชาติ ผู้เขียนได้นำแนวทางดังกล่าวมาวิเคราะห์กับงานที่อยู่ในความรับผิดชอบของกองคดีเทคโนโลยีและสารสนเทศ และหน่วยงานอื่น ๆ ภายในกรมสอบสวนคดีพิเศษ ซึ่งจะเห็นได้ว่า เรื่องการเตรียมความพร้อมด้านเทคโนโลยีและฐานข้อมูลขนาดใหญ่ให้มีความพร้อมสามารถรับมือกับภัยคุกคาม และภัยพิบัติได้ทุกรูปแบบนั้นเป็นสิ่งที่จำเป็นอย่างยิ่งบุคคลต้องปรับตัวให้ทันกับเทคโนโลยีและมีการติดตามข่าวสาร พัฒนาตอนเองอยู่เสมอ หน่วยงานก็ต้องให้การสนับสนุนในเรื่องอุปกรณ์ เครื่องมือ ซึ่งสอดคล้องกับยุทธศาสตร์ที่ ในข้อ ๑ ฐานข้อมูลจะต้องมีเพียงพอเพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์ที่เกิดขึ้น แต่การพัฒนาเพียงแค่นี้ยังไม่เพียงพอต่อการตอบสนองต่อสิ่งที่เปลี่ยนแปลงและภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เราจะต้องมีการบูรณาการร่วมกันระหว่างบุคลากรหน่วยงานภาครัฐและหน่วยงานภาคเอกชน ตามที่ได้ระบุไว้ในยุทธศาสตร์ข้อ ๖ ว่า “ภาครัฐของประชาชนเพื่อประชาชนและประโยชน์ส่วนรวม” พร้อมที่จะปรับตัวให้ทันต่อการเปลี่ยนแปลงของโลกอยู่ตลอดเวลา โดยเฉพาะอย่างยิ่งการนำนวัตกรรมเทคโนโลยีข้อมูลขนาดใหญ่ ระบบการทำงานที่เป็นดิจิทัลเข้ามาประยุกต์ใช้อย่างคุ้มค่าและปฏิบัติงานเทียบได้กับมาตรฐานสากล รวมทั้งมีลักษณะเปิดกว้าง เชื่อมโยงถึงกัน และเปิดโอกาสให้ทุกภาคส่วนเข้ามามีส่วนร่วมเพื่อตอบสนองความต้องการของประชาชนได้อย่างสะดวก รวดเร็ว และโปร่งใส กระบวนการยุติธรรมมีการบริหารที่มีประสิทธิภาพ เป็นธรรมไม่เลือกปฏิบัติ และการอำนวยความยุติธรรมตามหลักนิติธรรม

๕.๒.๓ เชิงการนำหลักการบริหารมาประยุกต์ใช้[๑]

๕.๒.๓.๑ การบริหารและพัฒนาบุคลากร ด้านการบังคับใช้กฎหมายในการสืบสวนสอบสวน กรมสอบสวนคดีพิเศษจะต้องมีบุคลากรที่มีลักษณะพิเศษ ดังนั้นการบริหารทรัพยากรมนุษย์ (Man) เช่น การวางแผนกำลังคนเพื่อให้ทันต่อการพัฒนาเทคโนโลยี การแสวงหาและการพัฒนาบุคลากรอย่างต่อเนื่อง การบรรจุแต่งตั้ง การเข้าสู่ตำแหน่ง การโยกย้ายให้ตรงกับสายงานและมีความก้าวหน้าในสายงาน เพื่อสร้างแรงจูงใจ เป็นต้น ในขณะเดียวกันการสอบสวนเกี่ยวข้องกับผู้มีอิทธิพล และมีผลประโยชน์ตอบแทนจากการกระทำผิดมหาศาล ดังนั้นต้องมีการบริหารคุณธรรม (Morality) ของบุคลากร ร่วมด้วย โดยการนำหลักธรรมในการบริหาร การสร้างบุคลากรให้มีมีจิตสำนึกดีงามในการปฏิบัติราชการหรือการปฏิบัติงาน การวางตนที่เหมาะสม เป็นต้น

๕.๒.๓.๒ สร้างความร่วมมือเพื่อเป็นการบูรณาการหน่วยงานภาครัฐ (Joint Force) เน้นบูรณาการทั้งภายในประเทศ และระหว่างประเทศ โดยที่จะต้องมีวิธีการ ระเบียบ แบบแผน หรือเทคนิค (Method) หมายถึง มีการเตรียมข้อมูลและการวางแผนงานอย่างเป็นระบบด้วยวิธีการที่ทันสมัย รวมทั้งมีการประสานงาน หรือการประนีประนอม (Mediation) ซึ่งหมายถึงความสัมพันธ์ระหว่างหน่วยงานกับบุคลากร ความสัมพันธ์ระหว่างหน่วยงานต่อหน่วยงาน และความสัมพันธ์ระหว่างหน่วยงานต่อประชาชน เช่น ประสานด้านนโยบายและวัตถุประสงค์ ประสานเจ้าหน้าที่ผู้ปฏิบัติงานร่วมกัน ประสานการเงินและวัสดุอุปกรณ์ และประสานความขัดแย้งของบุคลากร เป็นต้น

๕.๒.๓.๓ การบริหารจัดการองค์กรสู่ความเป็นเลิศ วางเป้าหมายเป็นผู้นำด้านเทคโนโลยีและสารสนเทศ เพื่อรับมือกับเทคโนโลยีที่เปลี่ยนแปลงในอนาคต โดยบริหารงบประมาณให้สอดคล้องกับภารกิจ (Money) การบริหารวัสดุอุปกรณ์ให้มีเครื่องมือที่ทันสมัยรองรับอาชญากรรมในอนาคต (Material) การบริหารงานทั่วไปเพื่อสนับสนุนการพัฒนาทางเทคโนโลยี (Management) และจำเป็นอย่างยิ่งต้องมีการวัดผล หรือการประเมินผลการปฏิบัติงาน (Measurement) อย่างต่อเนื่อง

๕.๒.๓.๔ การสร้างทักษะความเข้าใจด้านเทคโนโลยีดิจิทัล การปรับความคิด (Mindset) สร้างความตระหนักรู้ในการใช้เทคโนโลยีที่ถูกต้องแก่ประชาชน พัฒนาการศึกษาซึ่งเป็นการสร้างภูมิคุ้นกันทางดิจิทัล หรือทางไซเบอร์ให้กับประชาชน

๕.๒.๓.๕ การบริหารจัดการโดยมุ่งเน้นให้ประชาชนเป็นศูนย์กลาง และการสร้างเครือข่ายเด็กและเยาวชน เน้นการให้บริการประชาชน (Market) ที่รวดเร็วเพื่อลดความเสียหายจากอาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือ การบริหารข่าวสารหรือข้อมูลข่าวสาร (Message) เพื่อส่งต่อสื่อสารให้กับประชาชนได้รับรู้เพื่อป้องกันตนเองและมีส่วนสนับสนุนการดำเนินงานด้านข้อมูลข่าวสารของเจ้าหน้าที่ และมุ่งเน้นการสร้างเครือข่ายกับกลุ่มเด็กและเยาวชนเนื่องจากเป็นกลุ่มเสี่ยงในการกระทำความผิด

---

[๑]กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๖๓). *การจัดการความรู้ เรื่องการใช้เทคโนโลยีและสารสนเทศในการสืบสวนสอบสวน กรณีศึกษา การลักลอบถ่ายทอดสัญญาณฟุตบอลพรีเมียร์ลีก อังกฤษ*, หน้า ๔๘-๕๐

๕.๒.๓.๖ ส่งเสริม สนับสนุน สร้าง Leapfrog Digital Innovation Platform ของประเทศไทย ให้ประชาชนได้ใช้ระบบงานที่เหมาะสม

๕.๒.๓.๗ กระบวนการสร้างการรับรู้ด้วยการตักเตือน หรือการประชาสัมพันธ์ปัญหาภัยคุกคามทางไซเบอร์ ผ่านช่องทางอินเทอร์เน็ต หรือช่องทางทีวี วิทยุ ฯลฯ

ด้วยความก้าวหน้าทางเทคโนโลยี ทำให้เราไม่สามารถป้องกันปัญหาเกี่ยวกับเทคโนโลยีและสารสนเทศได้อย่างมีประสิทธิภาพครบถ้วนสมบูรณ์ เพราะฉะนั้นแนวคิดที่สำคัญ คือ กรมสอบสวนคดีพิเศษต้องเตรียมความพร้อมบุคลากรและการบริหารจัดการเพื่อให้เกิดการเรียนรู้และพัฒนาองค์กรให้ทันต่อความเปลี่ยนแปลงก้าวหน้าของเทคโนโลยีและสารสนเทศ เพื่อเป็นการเตรียมความพร้อมและปรับตัวในการที่จะรับมือกับภัยไซเบอร์ต่าง ๆ ที่จะเกิดขึ้นในอนาคต ได้อย่างมีประสิทธิภาพ

กรมสอบสวนคดีพิเศษควรนำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Framework) ในการบริหารจัดการหลักการบริหารความเสี่ยงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๑๓ วรรคหนึ่ง (๔)[๒] ที่อ้างอิงมาจาก NIST Cybersecurity Framework[๓] ซึ่งมี ๕ ขั้นตอน ดังนี้[๔]

๑) Identify คือการระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

๒) Protect คือมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

๓) Detect คือมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๔) Respond คือมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

๕) Recover คือมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

ในการนี้กรมสอบสวนคดีพิเศษควรเตรียมความพร้อมสำหรับปฏิบัติการในส่วน Detect และ Respond เมื่อเกิดเหตุอาชญากรรมทางไซเบอร์ขึ้นแล้ว กรมสอบสวนคดีพิเศษสามารถเข้าไปตรวจสอบที่เกิดเหตุได้อย่างทันท่วงที สามารถนำหลักฐานจากที่เกิดเหตุมาทำ Digital Forensic เพื่อใช้ในการสืบหาตัวผู้กระทำความผิดต่อไป พร้อมกันนี้กรมสอบสวนคดีพิเศษควรที่จะเพิ่มเติมในส่วนของการทำ Big Data ข้อมูล Cyber Threat Intelligence ที่จะดึงข้อมูลต่าง ๆ ที่ปรากฏอยู่ใน Dark Web เช่น การค้าอาวุธเถื่อน การซื้อขายยาเสพติด การซื้อขายภาพลามกเด็ก และข้อมูลส่วนบุคคลหรือข้อมูลของบริษัทต่าง ๆ

---

[๒]กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๒). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๒๐.PDF

[๓]National Institute of Standards and Technology U.S. Department of Commerce. (๒๕๖๔). *CYBERSECURITY FRAMEWORK* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: http https://www.nist.gov/cyberframework

[๔]ปริญญา หอมเอนก. (๒๕๖๓). *การประชุมเพื่อเพิ่มประสิทธิภาพการสืบสวนสอบสวนและการเตรียมความพร้อมรับมือภัยคุกคามด้านเทคโนโลยีและสารสนเทศ กรณีศึกษา การโจมตีระบบคอมพิวเตอร์และสารสนเทศของโรงพยาบาลสระบุรี* ณ ห้องประชุม ๑ ชั้น ๑ อาคารกรมสอบสวนคดีพิเศษ , ๒ ตุลาคม ๒๕๖๓

รายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community) กรณีศึกษา ประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์

ที่รั่วไหล เป็นต้น ซึ่งในปัจจุบันยังไม่มีหน่วยงานใดเป็นผู้รับผิดชอบ ที่จะทำให้กรมสอบสวนคดีพิเศษสามารถรู้ข้อมูลที่รั่วไหลได้อย่างทันท่วงที สามารถนำไปต่อยอดในการป้องกันเชิงรุก โดยการแจ้งเตือนข้อมูลดังกล่าวให้แก่ประชาชนหรือบริษัทที่เป็นเป้าหมาย ทำให้สามารถเตรียมการในการรับมือหรือหยุดอาชญากรรมไซเบอร์ที่จะเกิดขึ้นได้ล่วงหน้า ซึ่งในการปฏิบัติงานดังกล่าวกรมสอบสวนคดีพิเศษจะต้องคำนึงถึง ๓ ส่วนสำคัญ คือ ๑) บุคลากร (People) การพัฒนาบุคลากรให้มีทักษะทางด้านไซเบอร์พร้อมรับมือภัยไซเบอร์ที่จะเกิดขึ้นทุกประเภท ทั้งนี้ หากภารกิจใดที่บุคคลากรของกรมสอบสวนคดีพิเศษไม่มีความเชี่ยวชาญก็ควรที่จะจัดจ้างบุคคลากรจากภายนอก (Outsource) มาร่วมปฏิบัติงานดังกล่าว ๒) กระบวนการ (Process) การปรับเปลี่ยนกระบวนการทำงานขององค์กร ให้มีความยืดหยุ่น พร้อมรับความเปลี่ยนแปลง และ ๓) เทคโนโลยี (Technology) การนำเทคโนโลยีที่ทันสมัยเข้ามาใช้ในการปฏิบัติงาน เมื่อนำทั้ง ๓ ส่วนมาประยุกต์ใช้ร่วมกัน จะทำให้สามารถปฏิบัติงานดังกล่าวอย่างมีประสิทธิภาพ และใช้งานเครื่องมือพิเศษที่ใช้สนับสนุนงานอย่างคุ้มค่า ทำให้กรมสอบสวนคดีพิเศษสามารถนำข้อมูลที่ได้ไปสนับสนุนหรือแลกเปลี่ยนข้อมูลกับหน่วยงานภาครัฐต่าง ๆ เสริมการทำงานร่วมกันให้มีประสิทธิภาพมากยิ่งขึ้น ที่จะทำให้กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษมีหน้าที่ความรับผิดชอบที่แตกต่างจาก สำนักงานตำรวจแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือหน่วยงานอื่น ๆ ที่จะเป็นที่พึ่งพิงในการแก้ไขปัญหาอาชญากรรมไซเบอร์ให้แก่ประชาชนและประเทศชาติต่อไป


กรมสอบสวนคดีพิเศษ
DEPARTMENT OF SPECIAL INVESTIGATION
กระทรวงยุติธรรม
D S I
เกียรติศักดิ์ เที่ยวชาญ ซื่อสัตย์

บรรณานุกรม

บรรณานุกรม

กรุงเทพธุรกิจ. (๒๕๖๒). *อาเซียน๑๐+๕ ถกกฎระเบียบเพิ่มขีดแข่งขันการค้า*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: www.bangkokbiznews.com/news/detail/๘๔๕๕๖๓

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (๒๕๖๒). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: http://www.ratchakitcha.soc.go.th/DATA/PDF/๒๕๖๒/A/๐๖๙/T_๐๐๒๐.PDF

กองกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๕๙). *คู่มือการสืบสวนสอบสวนในกรอบประชาคมอาเซียน: การปฏิบัติเกี่ยวกับประชาคมอาเซียน*, หน้า ๑๓๓, ๑๒๑-๑๒๘, ๑๓๐-๑๓๓, ๑๓๕-๑๓๗

กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม. (๒๕๖๓). *การจัดการความรู้เรื่องการใช้เทคโนโลยีและสารสนเทศในการสืบสวนสอบสวน กรณีศึกษา การลักลอบถ่ายทอดสัญญาณฟุตบอลพรีเมียร์ลีก อังกฤษ*, หน้า ๔๘-๕๐

กองบรรณาธิการจุลสาร “จับตาอาเซียน”. (๒๕๕๙). *อาเซียนกับความร่วมมือด้านความมั่นคงไซเบอร์*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: https://aseanwatch.org/๒๐๑๖/๐๖/๓๐/current-issue-๐๒๕๙

ชิตพล กาญจนกิจ. (๒๕๕๙). *ความร่วมมือระหว่างประเทศว่าด้วยกระบวนการยุติธรรมทางอาญาอาเซียน: ข้อเสนอเชิงยุทธศาสตร์เพื่อการเตรียมความพร้อมเข้าสู่ประชาคมอาเซียน,* หน้า ๕

ทรงพจน์ สุภาผล. (๒๕๖๐). *'อาชญากรรมไซเบอร์ส' ภัยคุกคามใหม่ของประเทศในแถบเอเชียแปซิฟิก*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔ จาก: https://www.voathai.com/a/asia-cybercrime/๓๙๐๐๘๖๑.html

ปริญญา หอมเอนก. (๒๕๖๓). *การประชุมเพื่อเพิ่มประสิทธิภาพการสืบสวนสอบสวนและการเตรียมความพร้อมรับมือภัยคุกคามด้านเทคโนโลยีและสารสนเทศ กรณีศึกษา การโจมตีระบบคอมพิวเตอร์และสารสนเทศของโรงพยาบาลสระบุรี* ณ ห้องประชุม ๑ ชั้น ๑ อาคารกรมสอบสวนคดีพิเศษ , ๒ ตุลาคม ๒๕๖๓

CAT cyfence. (๒๕๖๒). *๑๐ เทรนด์ความปลอดภัยในโลกไซเบอร์ที่ต้องจับตามองในปี ๒๐๑๙*. ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: https://www.catcyfence.com/it-security/it-๓๖๐/๑๐-cyber-security-trend-๒๐๑๙

Josh Fruhlinger. (๒๕๖๓). *Top cybersecurity facts, figures and statistics.* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: www.csoonline.com/article/๓๑๕๓๗๐๗/security/top-๕-cybersecurity-facts-figures-and-statistics-for-๒๐๑๗.html

National Institute of Standards and Technology U.S. Department of Commerce. (๒๕๖๔). *CYBERSECURITY FRAMEWORK* ค้นเมื่อ ๕ กรกฎาคม ๒๕๖๔, จาก: https://www.nist.gov/cyberframework


กรมสอบสวนคดีพิเศษ
DEPARTMENT OF SPECIAL INVESTIGATION
กระทรวงยุติธรรม
DSI
เกียรติศักดิ์ เชี่ยวชาญ ซื่อสัตย์

ภาคผนวก

คำสั่งกองคดีเทคโนโลยีและสารสนเทศ
ที่ ๑๘/๒๕๖๑
เรื่อง แต่งตั้งคณะทำงานและคณะจัดทำรายงานการวิจัยโครงการแลกเปลี่ยนองค์ความรู้
แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC)
ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์

อนุสนธิกฎกระทรวงแบ่งส่วนราชการกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ.๒๕๖๐ ประกอบกับคำสั่งกรมสอบสวนคดีพิเศษ ที่ ๘๑๒/๒๕๖๐ ลงวันที่ ๑๘ สิงหาคม พ.ศ.๒๕๖๐ เรื่อง กำหนดหน่วยงานภายในของส่วนราชการตามกฎกระทรวงแบ่งส่วนราชการกรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม พ.ศ.๒๕๖๐ กำหนดอำนาจหน้าที่ให้กองคดีเทคโนโลยีและสารสนเทศรับผิดชอบด้านการป้องกัน การปราบปราม การสืบสวนสอบสวนคดีพิเศษคดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ คดีความผิดเกี่ยวกับทางอาญาที่เกี่ยวกับเทคโนโลยีและสารสนเทศหรือความผิดทางอาญาอื่นที่กระทำลงบนระบบคอมพิวเตอร์ ระบบอินเตอร์เน็ตหรือระบบเทคโนโลยีสารสนเทศ

ประกอบกับกระทรวงยุติธรรม ได้มอบหมายภารกิจให้กองคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ จัดโครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการ แนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม โดยในปีงบประมาณ พ.ศ.๒๕๕๙ จัดโครงการสร้างเครือข่ายกับหน่วยงานบังคับใช้กฎหมายในประเทศมาเลเซีย ณ กรุงกัวลาลัมเปอร์ ปีงบประมาณ พ.ศ.๒๕๖๐ ณ ประเทศสาธารณรัฐสิงคโปร์ และในปีงบประมาณ พ.ศ.๒๕๖๑ จัดโครงการต่อเนื่องปีที่ ๓ จัดทำโครงการเพื่อศึกษาดูงานและประชุมหารือหน่วยงานที่เกี่ยวข้องทางด้านการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม ณ สาธารณรัฐฟิลิปปินส์

เพื่อให้การปฏิบัติงานในการดำเนินคดีมีประสิทธิภาพ ประสิทธิผล และสอดคล้องกับยุทธศาสตร์ของกรมสอบสวนคดีพิเศษ และสนับสนุนให้การปฏิบัติงานเชิงรุกในด้านการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในกลุ่มประเทศอาเซี่ยนสัมฤทธิ์ผล อีกทั้งสามารถพัฒนาบุคคลากรและกระบวนการทำงานได้ดียิ่งขึ้นจากการมีเครือข่ายความร่วมมือระหว่างประเทศในระดับภูมิภาคในการร่วมพัฒนาประสิทธิภาพ เสริมสร้างกลไกการป้องกันภัยอาชญากรรมทางคอมพิวเตอร์ เพื่อรองรับเศรษฐกิจดิจิทัลของภูมิภาคกลุ่มประเทศในอาเซี่ยน จึงขอแต่งตั้งคณะทำงานเพื่อทำหน้าที่ในการดำเนินการโครงการดังกล่าว ดังนี้

๑. คณะทำงานดำเนินโครงการ

<u>องค์ประกอบ</u>

๑.๑ พันตำรวจโทวิชัย สุวรรณประเสริฐ เป็นประธานคณะทำงาน
ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

๑.๒ พันตำรวจโทสุกิจ จ้อยสำเภา เป็นรองประธานคณะทำงาน
รองผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

๑.๓ พันตำรวจโทเฉลิมชนม์ อุณหเสรี เป็นรองประธานคณะทำงาน
รองผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

/๑.๔ นายวสวัต...

๑.๔ นายวสวัต ชวลิตธำรง เป็นที่ปรึกษา
พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ

๑.๕ พันตำรวจตรีจตุพร อรุณฤกษ์ถวิล เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๑

๑.๖ พันตำรวจโทธวัชชัย ศรีวรกุล เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๒

๑.๗ นายสิทธิวิชญ์ อินทร์น้อย เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๓

๑.๘ นายรัชพร วรอินทร์ เป็นคณะทำงาน
หัวหน้าศูนย์ปฏิบัติการข่ายและสืบสวนคดีทางเทคโนโลยีและสารสนเทศ

๑.๙ พันโทสุรพันธ์ โชคปมิตต์กุล เป็นคณะทำงานและเลขานุการ
ผู้อำนวยการส่วนอำนวยการคดีเทคโนโลยีและสารสนเทศ

๑.๑๐ นางสาวปัทมาภรณ์ กฤษณายุทธ เป็นคณะทำงานและผู้ช่วยเลขานุการ
พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ

๑.๑๑ นางอรพิมพ์ แข่งขันดี เป็นคณะทำงานและผู้ช่วยเลขานุการ
เจ้าหน้าที่คดีพิเศษชำนาญการ

๑.๑๒ นางสาวชญาน์ณันท์ ฉิมกิตินันท์ เป็นคณะทำงานและผู้ช่วยเลขานุการ
เจ้าพนักงานธุรการปฏิบัติงาน

๑.๑๓ นางสาวภัทรา กาญจนวรางกูร เป็นคณะทำงานและผู้ช่วยเลขานุการ
นิติกร

<u>หน้าที่ความรับผิดชอบ</u>

๑. ดำเนินการจัดทำแผนงาน เสนอโครงการ เสนอขออนุมัติจัดทำโครงการแลกเปลี่ยนองค์ความรู้ แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์

๒. ติดต่อประสานงานกับหน่วยงานภายในกรมสอบสวนคดีพิเศษ

๓. ติดต่อประสานงานพร้อมทั้งจัดทำหนังสือเชิญหน่วยงานบังคับใช้กฎหมาย และหน่วยงานภายนอกผู้เข้าร่วมการสัมมนา

๔. ให้แต่ละส่วนแบ่งกลุ่มพร้อมทั้งจัดทำหัวข้อที่กำหนดในการประชุมเชิงปฏิบัติการ และสรุปรายงานผลการดำเนินการจนแล้วเสร็จเพื่อจัดส่งให้กับคณะทำงานในการทำรายงานการวิจัย

๕. ดำเนินการเรื่องการใช้จ่ายงบประมาณ การจัดซื้อจัดจ้างตามระเบียบพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐

๒. คณะทำงานศึกษาวิจัย

<u>องค์ประกอบ</u>

๒.๑ พันตำรวจโทวิชัย สุวรรณประเสริฐ เป็นประธานคณะทำงาน
ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

๒.๒ พันตำรวจโทเฉลิมชนม์ อุณหเสรี เป็นรองประธานคณะทำงาน
รองผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

๒.๓ พันตำรวจตรีจตุพร อรุณฤกษ์ถวิล เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๑

/๒.๔ พันตำรวจโท...

๒.๔ พันตำรวจโทธวัชชัย ศรีวรกุล เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๒

๒.๕ นายสิทธิวิชญ์ อินทร์น้อย เป็นคณะทำงาน
ผู้อำนวยการส่วนคดีเทคโนโลยีและสารสนเทศ ๓

๒.๖ นายรัชพร วรอินทร์ เป็นคณะทำงาน
หัวหน้าศูนย์ปฏิบัติการข่ายและสืบสวนคดีทางเทคโนโลยีและสารสนเทศ

๒.๗ พันโทสุรพันธ์ โชคปมิตต์กุล เป็นคณะทำงาน
ผู้อำนวยการส่วนอำนวยการคดีเทคโนโลยีและสารสนเทศ

๒.๘ นางอรพิมพ์ แข่งขันดี เป็นคณะทำงาน
เจ้าหน้าที่คดีพิเศษชำนาญการ

๒.๙ นางปรียาภรณ์ ไชยภักดี เป็นคณะทำงาน
เจ้าหน้าที่คดีพิเศษชำนาญการ

๒.๑๐ นางสาวปัทมาภรณ์ กฤษณายุทธ เป็นคณะทำงานและเลขานุการ
พนักงานสอบสวนคดีพิเศษชำนาญการพิเศษ

๒.๑๑ นางสาวจุฑารัตน์ โม้วงษ์ เป็นคณะทำงานและผู้ช่วยเลขานุการ
เจ้าหน้าที่ธุรการ

<u>หน้าที่ความรับผิดชอบ</u>

๑.ศึกษาวิจัยการบังคับใช้กฎหมายเพื่อเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยีและสารสนเทศในกลุ่ม ASEAN Economic Community (AEC) โดยให้ดำเนินการตามระเบียบวิธีการวิจัย

๒. นำผลการศึกษาดูงานโครงการแลกเปลี่ยนองค์ความรู้ และกำหนดมาตรการแนวทางการบังคับใช้กฎหมายในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์เพื่อพัฒนากฎหมายและกระบวนการยุติธรรม ในช่วงปีงบประมาณ พ.ศ.๒๕๕๙ จนถึงปีงบประมาณปัจจุบัน พร้อมข้อเสนอมาวิเคราะห์

๓. นำผลสรุปการจัดประชุมสัมมนาและการศึกษาค้นคว้าเพิ่มเติมมาวิเคราะห์เปรียบเทียบหรือดำเนินการอื่นใดเพื่อให้การศึกษาวิจัยเกิดประสิทธิภาพสูงสุด

๔. จัดทำรายงานทั้งหมดเป็นงานวิจัยรูปเล่มเพื่อนำไปใช้ประโยชน์ในการปฏิบัติงานและรายงานผู้บังคับบัญชา

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓๐ เมษายน พ.ศ. ๒๕๖๑

พันตำรวจโท
(วิชัย สุวรรณประเสริฐ)
ผู้อำนวยการเฉพาะด้าน (พนักงานสอบสวนคดีพิเศษ) สูง รักษาราชการแทน
ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

คำสั่งกองคดีเทคโนโลยีและสารสนเทศ
ที่ ๒๘ /๒๕๖๔
เรื่อง แต่งตั้งคณะทำงานและคณะจัดทำรายงานการวิจัยโครงการแลกเปลี่ยนองค์ความรู้
แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC)
ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพิ่มเติม

.....

ตามคำสั่งกองคดีเทคโนโลยีและสารสนเทศที่ ๑๘/๒๕๖๑ ลงวันที่ ๓๐ เมษายน ๒๕๖๑ ได้แต่งตั้งคณะทำงานและคณะจัดทำรายงานการวิจัยโครงการแลกเปลี่ยนองค์ความรู้ แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพื่อดำเนินการจัดทำรายงานการวิจัยโครงการแลกเปลี่ยนองค์ความรู้ แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ นั้น

เนื่องจากคณะทำงานตามคำสั่งดังกล่าวข้างต้น บางส่วนได้เกษียณอายุราชการ และบางส่วนได้มีการโอนย้ายไปปฏิบัติราชการในหน่วยงานอื่น ดังนั้น เพื่อให้การดำเนินการจัดทำรายงานการวิจัยโครงการดังกล่าว เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ จึงแต่งตั้งคณะทำงานและคณะจัดทำรายงานการวิจัยโครงการแลกเปลี่ยนองค์ความรู้ แนวทางการบังคับใช้กฎหมาย ในกลุ่ม ASEAN Economic Community (AEC) ในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เพิ่มเติม ดังต่อไปนี้

๒. คณะทำงานศึกษาวิจัย

<u>องค์ประกอบ</u>

๑. นายนทีธร มีชัย รองผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ	เป็นรองประธานคณะทำงาน
๒. นายราชพฤกษ์ ชูดำ ผู้อำนวยการส่วนอำนวยการคดี	เป็นคณะทำงาน
๓. นายภัทรดนัย รุจิชัยกุล เจ้าหน้าที่คดีพิเศษปฏิบัติการ	เป็นคณะทำงาน
๔. นายภูวนัย แสงพล เจ้าหน้าที่คดีพิเศษปฏิบัติการ	เป็นคณะทำงาน
๕. นายเกริกเกียรติ สุขเนาว์ เจ้าหน้าที่คดีพิเศษปฏิบัติการ	เป็นคณะทำงาน
๖. นายนิภัทร์ สุวรรณ เจ้าหน้าที่คดีพิเศษปฏิบัติการ	เป็นคณะทำงาน
๗. นายธนวัฒน์ องอาจอิทธิชัย เจ้าหน้าที่คดีพิเศษปฏิบัติการ	เป็นคณะทำงาน

/๘. นางปุณยนุช...

๘. นางปุณยนุช รักญาติ เป็นคณะทำงาน/ผู้ช่วยเลขานุการ
เจ้าพนักงานธุรการปฏิบัติงาน

โดยให้มีหน้าที่ความรับผิดชอบตามที่กำหนดไว้ในคำสั่งกองคดีเทคโนโลยีและสารสนเทศที่ ๑๘/๒๕๖๑ ลงวันที่ ๓๐ เมษายน ๒๕๖๑

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๔

พันตำรวจโท
(วิชัย สุวรรณประเสริฐ)
ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ

คณะทำงานศึกษาวิจัย

๑. พันตำรวจโท วิชัย สุวรรณประเสริฐ	ประธานคณะทำงาน
๒. พันตำรวจโท เฉลิมชนม์ อุณหเสรี	รองประธานคณะทำงาน
๓. นายนทีธร มีชัย	รองประธานคณะทำงาน
๔. พันโท สรพันธ์ โชคปมิตต์กุล	คณะทำงาน
๕. นายราชพฤกษ์ ชูดำ	คณะทำงาน
๖. พันตำรวจตรี จตุพร อรุณฤกษ์ถวิล	คณะทำงาน
๗. พันตำรวจโท ธวัชชัย ศรีวรกุล	คณะทำงาน
๘. นายสิทธิวิชญ์ อินทร์น้อย	คณะทำงาน
๙. นางสาวปัทมาภรณ์ กฤษณายุทธ	คณะทำงาน
๑๐. นายรัชพร วรอินทร์	คณะทำงาน
๑๑. นางอรพิมพ์ แข่งขันดี	คณะทำงาน
๑๒. นางปรียาภรณ์ ไชยภัคดี	คณะทำงาน
๑๓. นายภัทรดนัย รุจิชัยกุล	คณะทำงาน
๑๔. นายเกริกเกียรติ สุขเนาว์	คณะทำงาน
๑๕. นายภูวนัย แสงพล	คณะทำงาน
๑๖. นายนิภัทร์ สุวรรณ	คณะทำงาน
๑๗. นายธนวัฒน์ องอาจอิทธิชัย	คณะทำงาน
๑๘. นางปุณยนุช รักญาติ	คณะทำงาน
๑๙. นางสาวจุฑารัตน์ โม้วงษ์	คณะทำงาน

รายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมาย
เกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community)
กรณีศึกษา ประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์

ISBN : 978-616-8108-35-2
พิมพ์ครั้งที่ : ๑
จำนวนพิมพ์ : ๒๐๐ เล่ม
พิมพ์ที่ : บริษัท รำไทยเพรส จำกัด
๑๑๑/๙๓-๙๖ ซอยสามเสน ๒๘ ถนนสามเสน เขตดุสิต กรุงเทพฯ ๑๐๓๐๐
โทร. ๐ ๒๖๖๙ ๐๓๐๐
E-mail : rum_thai@yahoo.com

รายงานการศึกษาวิจัยเพิ่มประสิทธิภาพการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในกลุ่มประชาคมอาเซียน (ASEAN Economic Community) กรณีศึกษา ประเทศมาเลเซีย สาธารณรัฐสิงคโปร์ และสาธารณรัฐฟิลิปปินส์