แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี

โดย

พลตำรวจตรี ฐายุฏฐ์ จันทร์ถาวร
รองผู้บัญชาการตำรวจสืบสวนสอบสวน
อาชญากรรมทางเทคโนโลยี
สำนักงานตำรวจแห่งชาติ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕
ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ - ๒๕๖๖

หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี” ลักษณะวิชาสังคมจิตวิทยา ของ พลตำรวจตรี ฐายุฏฐ์ จันทร์ เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๕ ประจำปีการศึกษา พุทธศักราช ๒๕๖๕ – ๒๕๖๖

พลโท

(ชาติชาย ชัยเกษม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

เรื่อง แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี
ลักษณะวิชา สังคมจิตวิทยา
ผู้วิจัย พลตำรวจตรี ฐายุฎฐ์ จันทร์ถาวร **หลักสูตร** วปอ. **รุ่นที่** ๖๕

อาชญากรรมทางเทคโนโลยีเป็นภัยคุกคามในโลกยุคใหม่ที่อยู่ใกล้ตัวเราทุกคน สำหรับประเทศไทยมีการรายงานเหตุและความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยีจำนวนมาก ส่งผลกระทบต่อสังคมเศรษฐกิจและความมั่นคงของชาติ แต่ทว่า ภัยอาชญากรรมทางเทคโนโลยีมิได้เกิดขึ้นเพียงเพราะมีกลุ่มคนร้ายที่อาศัยโอกาสประทุษร้ายต่อเหยื่อตามทฤษฎีสามเหลี่ยมอาชญากรรมเท่านั้น แต่เป็นเพราะโครงสร้างของรัฐและสังคม นโยบายและ เทคโนโลยีที่มีอยู่ในปัจจุบันยังมีช่องว่างมากมายที่เปิดโอกาสหรือเกื้อหนุนให้อาชญากรกระทำผิดได้โดยง่าย บทความนี้นำเสนอภัยคุกคามรูปแบบใหม่ที่เกิดจากช่องโหว่เหล่านี้ซึ่งอยู่ภายใต้การกำกับดูแลของหน่วยงานที่เกี่ยวข้องมากมาย ช่องโหว่เหล่านี้เกิดขึ้นจากความก้าวหน้าทางเทคโนโลยีและพัฒนาการเพื่อความสะดวกสบาย เช่น การเปิดบัญชีธนาคารออนไลน์จำนวนมากได้อย่างสะดวกรวดเร็ว การโอนและจ่ายเงินผ่านระบบธนาคารออนไลน์ที่สะดวกรวดเร็ว จนหลายครั้งไม่สามารถพิสูจน์อัตลักษณ์และสถานที่ของผู้ใช้บัญชีได้จริง หรือ ความก้าวหน้าของภาคการเงินดิจิทัลและคริปโตเคอเรนซี่อันเป็นช่องทางในการฟอกเงินของอาชญากรออกนอกประเทศ เป็นต้น สิ่งเหล่านี้ไม่เพียงแต่สร้างความสะดวกสบายและการพัฒนาในหลายมิติ แต่ยังเป็นภัยคุกคามรูปแบบใหม่ที่จะต้องปรับแก้โดยบูรณาการกันอย่างแท้จริง บทความนี้เสนอแนะข้อมูลและแนวทางเพื่อให้สังคมและประเทศชาติมีกลไกที่เหมาะสม ประชาชนมีความตระหนักรู้ และประเทศไทยมีศักยภาพมีความทนทาน Resilience ต่อภัยคุกคามรูปแบบใหม่ทุกรูปแบบที่จะมีเกิดขึ้นใหม่และเปลี่ยนแปลงไปโดยตลอด

Abstract

Title Guidelines for the integration of technological crime prevention
Field Social - Phychology
Name Pol.Gen.Maj. Thayut Chanthaworn **Course** NDC **Class** 65

Cybercrime is a contemporary threat attacking or coming close to all of us. In Thailand, an exponential number of cybercrime or cyber threat incidents with seriously financial damages have been reported. That affects our society, economy, and even national security. However, the threat of cybercrime occurred not only because the criminals can take advantage of the opportunity to attack the unaware victims as described by criminology theories, such as Crime Opportunity or Routine Activity Theory. But also, Thailand's governmental and social structures, existing policies and current technology provide some gaps or vulnerability that allow or even facilitate the criminals to commit crime conveniently. This article, therefore, provides an understanding of new threats posed by such vulnerabilities that are under the supervision of many relevant authorities and agencies. These vulnerabilities are accompanied with the advances in technology in public sectors or businesses, such as the convenience of opening online bank accounts quickly and easily in a large number without proper implementation of authentication and identity. That results in inefficient process to prove the identity and location of the bank account user, and money mules. In addition, the progress of the digital financial sector and cryptocurrencies, which is a channel for money laundering, to transfer assets overseas. These vulnerabilities not only create comfort and development in many dimensions, but also pose a new type of threats that must be addressed through practical integration and cooperation. By recognizing these difficulties, the society and the nation should have appropriate mechanisms, public awareness, and resilience against all new kinds of challenges and ever-changing threats.

คำนำ

การศึกษาวิจัยในหัวข้อนี้ มีสาเหตุสำคัญจากการที่กระผมสนใจในปัญหาอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นจำนวนมาก มีมูลค่าความเสียหายสูง ส่งผลกระทบต่อเศรษฐกิจสังคมของประชาชน จนอาจกลายเป็นภัยคุกคามต่อความมั่นคงของประเทศไทย โดยเฉพาะการแก้ไขปัญหาในมิติการป้องกันอาชญากรรมทางเทคโนโลยี ที่ปัจจุบันยังมิได้มีการบูรณาการแนวทางการแก้ไขปัญหาอย่างเหมาะสม กระผมมีความสนใจที่จะศึกษาหาแนวทางการบูรณาการร่วมกันกับทุกภาคส่วนในการป้องกันอาชญากรรมทางเทคโนโลยี ซึ่งกระผมมีประสบการณ์และความชำนาญจากการปฏิบัติงานในหน้าที่ สามารถเข้าถึงข้อมูลสำคัญเพียงพอที่จะทำการวิจัยในหัวข้อนี้ จึงได้ทำการศึกษาให้เข้าใจปัญหา อุปสรรค ข้อขัดข้อง เพื่อนำไปวิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี และแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม ตามแนวคิดภูมิคุ้มกันทางไซเบอร์ที่ทุกภาคส่วนร่วมแรงกันป้องกันภัยอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

กระผมหวังเป็นอย่างยิ่งว่างานวิจัยนี้จะเป็นประโยชน์ต่อผู้สนใจที่จะศึกษาด้านความมั่นคงของชาติ ในการประยุกต์ใช้การแก้ไขปัญหาการเข้าสู่ยุคดิจิทัลของประเทศที่ต้องเผชิญกับความท้าทายด้านเศรษฐกิจสังคม ที่อาจส่งผลกระทบต่อความมั่นคงของประเทศ ให้สามารถนำเอาแนวคิดและแนวทางในการศึกษาวิจัยนี้ไปใช้ในการบูรณาการพลังอำนาจของชาติทุกภาคส่วนมีความพร้อมในการเผชิญภัยคุกคามทางความมั่นคงรูปแบบใหม่ในปัจจุบันและในอนาคตต่อไป

พลตำรวจตรี

(ฐายุฏฐ์ จันทร์ถาวร)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๕
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

หน้า

แผนภาพที่

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

จากสถิติการรับแจ้งความออนไลน์รอบปีที่ผ่านมาพบว่าประเทศไทยมีภัยคุกคามด้านอาชญากรรมทางด้านเทคโนโลยีเพิ่มขึ้นเป็นจำนวนมาก โดยมีการสำรวจเป็นสถิติการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ ซึ่งในห้วงวันที่ ๑ มี.ค. ๒๕๖๕ - ๒๑ มี.ค. ๒๕๖๖ ได้มีแจ้งความออนไลน์จากประชาชน กว่า ๒๔๗,๗๕๓ เรื่อง โดยแบ่งเป็นคดีออนไลน์ ๒๒๔,๐๐๑ เรื่อง คดีอาญาอื่นๆ ๗,๖๘๔ เรื่อง จำหน่ายออกจากระบบ ๑๖,๐๖๘ เรื่อง ขณะที่ผลการอายัดบัญชีที่มีคำร้องทั้งหมด ๗๔,๑๒๙ บัญชี มีการขออายัด ๕๔,๐๑๗ บัญชี ยอดเงิน ๖,๙๔๑ ล้านบาท และอายัดได้ทัน ๔๔๙ ล้านบาท รวมมูลค่าความเสียหาย ๓๒,๐๘๓ ล้านบาท อีกทั้งยังมีการจัดอันดับ ๕ ประเภท ความเสียหายที่ประชาชนถูกมิจฉาชีพหลอกลวงมากที่สุด ได้แก่ ๑. หลอกลวงซื้อขายสินค้า จำนวน ๗๕,๓๐๗ ครั้ง คิดเป็นร้อยละ ๓๓.๖๒ ความเสียหาย ๑,๐๐๓ ล้านบาท ๒. หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม จำนวน ๓๐,๗๕๓ ครั้ง คิดเป็นร้อยละ ๑๓.๗๓ ความเสียหาย ๓,๔๑๕ ล้านบาท ๓.หลอกให้กู้เงินแต่ไม่ได้เงิน จำนวน ๒๕ ,๔๑๒ ครั้ง คิดเป็นร้อยละ ๑๑.๓๔ ความเสียหาย ๑,๐๕๘ ล้านบาท ๔.หลอกลวงทางโทรศัพท์เป็นขบวนการ (คอลเซ็นเตอร์) จำนวน ๒๐,๖๘๒ ครั้ง คิดเป็นร้อยละ ๙.๒๓ ความเสียหาย ๓,๖๐๑ ล้านบาท ๕.หลอกให้ลงทุน (ที่ไม่เข้าลักษณะฉ้อโกงประชาชน) จำนวน ๑๖,๗๔๒ ครั้ง คิดเป็นร้อยละ ๗.๔๗ ความเสียหาย ๗,๗๗๑ ล้านบาท ซึ่งคดีหลอกให้ลงทุนเป็นคดีที่มีมูลค่าความเสียหายมากที่สุดในทุกประเภทคดี (ออนไลน์, ๒๕๖๕)

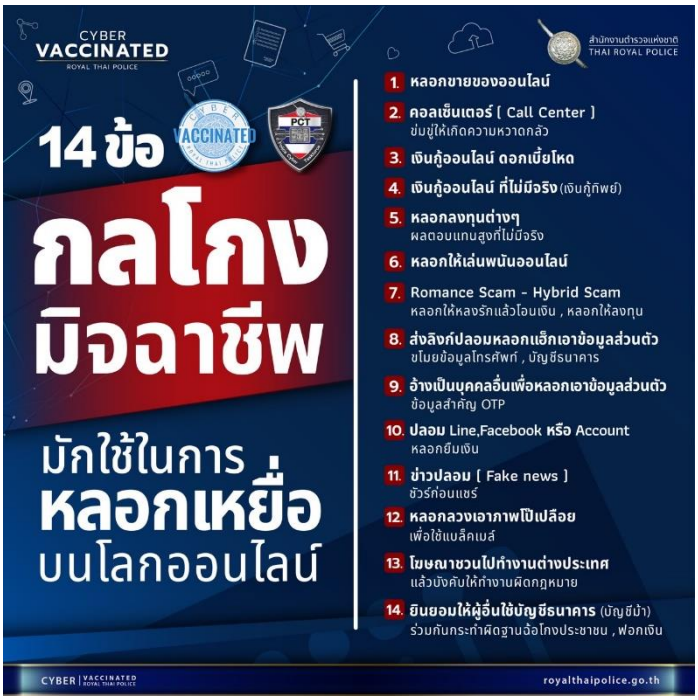
แผนภาพที่ ๑-๑ สถิติการรับแจ้งความออนไลน์

ที่มา : สำนักงานตำรวจแห่งชาติ, ๒๕๖๖

ปัญหาดังกล่าวเป็นปัญหาที่สำคัญและส่งผลกระทบเกี่ยวกับความมั่นคงของประชาชนและของประเทศชาติในทุกระดับ โดยเฉพาะในระดับนโยบายที่มีผลกระทบต่อสังคมโดยกว้างอย่างยิ่ง ในยุคปัจจุบัน การป้องกันเป็นแนวทางเชิงรุกที่สำคัญ ถึงแม้อาชญากรรมทางเทคโนโลยีจะเป็นความผิดตามประมวลกฎหมายอาญาเดิม (คนร้ายใช้กลอุบายแบบเดิมๆ หลอกโดยใช้กิเลสของเหยื่อเป็นตัวล่อ คือ ทางความโลภ ความกลัว ความน่าเชื่อถือ) แต่วิธีการที่คนร้ายใช้ในการเข้าถึงเหยื่อและวิธีการโอนเงิน (ได้ไปซึ่งทรัพย์สิน/เงินของเหยื่อ) เป็นวิธีใหม่ๆ ที่อาศัยเทคโนโลยี ซึ่งเรื่องนี้เป็นเรื่องใหม่ในสังคมไทยและสังคมโลก ซึ่งกฎหมายหรือกระบวนการป้องกันมิให้ประชาชนตกเป็นเหยื่ออาจยังตามไม่ทัน เช่น การเก็บหลักฐานในคดีซึ่งต้องใช้ความรู้ความชำนาญพิเศษเฉพาะการประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ผู้ให้บริการทางการสื่อสาร/Operator ผู้ให้บริการทางการเงินหน่วยงานควบคุมกำกับ ดูแลเทคโนโลยีการสื่อสารและการเงินต่างๆ ก็ยังขาดการประสานงานเพื่อต่อกรกับปัญหาดังกล่าว ตลอดจนกฎหมายที่ยังไม่เอื้อต่อการทำงานของหน่วยงานให้บริการหน่วยงานบังคับใช้กฎหมาย ทำให้คนร้ายใช้เป็นช่องโหว่ในการกระทำความผิด

การดำเนินคดีเพื่อติดตามจับกุมคนร้ายเป็นการแก้ปัญหาที่ปลายเหตุ ทั้งการยึดทรัพย์ที่คนร้ายได้ไปก็เป็นไปได้ยากและสามารยึดทรัพย์คืนมาได้จำนวนน้อยมาก ที่ผ่านมาสำนักงานตำรวจแห่งชาติได้พยายามประชาสัมพันธ์ให้ทราบถึง Vaccine Cyber ซึ่งเป็นแนวทางหนึ่งในการป้องกันอาชญากรรมทางเทคโนโลยี โดยการสร้างความตระหนักรู้ให้กับประชาชน แต่จากสถิติการตกเป็นเหยื่อของประชาชนที่ผ่านมาทำให้เห็นว่า การสร้างความตระหนักรู้แต่เพียงอย่างเดียวยังไม่สามารถลดปริมาณการตกเป็นเหยื่อได้

แผนภาพที่ ๑-๒ กลโกงของมิจฉาชีพใช้ในการลอกเหยื่อบนโลกออนไลน์



ที่มา : ออนไลน์, ๒๕๖๕

ดังนั้น การป้องกันอาชญากรรมทางเทคโนโลยีที่มีประสิทธิภาพควรต้องมีแนวทางอย่างไร มีผู้ใดที่มีส่วนเกี่ยวในการสร้างภูมิคุ้มกันภัยไซเบอร์ หรือ Cyber Immunity ให้กับสังคมและปรชาชนได้ดีกว่าที่เป็นอยู่ในปัจจุบัน ผู้วิจัยจึงมีความสนใจในการศึกษาแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี เพื่อหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีที่มีประสิทธิภาพ เพื่อให้สังคม ประชาชน เกิดความปลอดภัยอย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษา ปัญหา อุปสรรค ข้อขัดข้อง และแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี

๒. เพื่อศึกษาถึงผู้ที่มีส่วนเกี่ยวข้องในการบูรณาการ วิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี

๓. เพื่อศึกษาหาแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

ขอบเขตของการวิจัย

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยต้องการศึกษาแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี โดยมีขอบเขต ดังนี้

๑. ด้านเนื้อหา

ศึกษาแนวทางการป้องกัน อาชญากรรมทางเทคโนโลยี โดยพิจารณาจากสาเหตุและปัจจัยสำคัญที่ทำให้ประชากรในประเทศไทยโดยทั่วไปตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยี และไม่ศึกษาการป้องกันปราบปรามหรือการสืบสวนสอบสวนแผนประทุษกรรมใดเป็นพิเศษโดยเฉพาะ

๒. ด้านวิธีดำเนินการวิจัย

ใช้การวิจัยเชิงคุณภาพโดยการวิเคราะห์เอกสารที่เกี่ยวข้องและการสัมมนาอิงผู้เชี่ยวชาญ (connoisseurship) จำนวน ๑๐ ท่าน

๓. ด้านเวลา

ระเวลาในการศึกษา ๒๕๖๕-๒๕๖๖ โดยรวบรวมข้อมูลในคดีต่าง ๆ ที่เกิดขึ้นในกรอบระยะเวลาระหว่าง ๙ ก.ย. ๒๕๖๓ – ๒๑ มี.ค. ๒๕๖๖ ซึ่งเป็นห้วงที่เริ่มมีการจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี การแจ้งความออนไลน์ และความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องอย่างเป็นรูปธรรม

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์ วิธีการป้องกันอาชญากรรมทางเทคโนโลยีจาการวิจัยเอกสารและใช้เทคนิคการสัมมนาอิงผู้เชี่ยวชาญ (connoisseurship) ซึ่งเป็นเทคนิคที่เป็นรูปแบบการได้องค์ความรู้จากผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในศาสตร์และองค์ความรู้นั้น มาให้ข้อมูลเชิงลึกและทรรศนะต่อความรู้ที่ได้จากการวิเคราะห์เอกสารผู้ศึกษานำข้อมูลที่ได้จากวิธีวิจัยเอกสาร**ม**าทำการวิเคราะห์ข้อมูลเชิงคุณภาพโดยการนำข้อมูลที่ได้จากการค้นคว้าวิจัยมาจัดกระทำ (Data processing) ให้เป็นระบบโดยใช้กรอบการวิเคราะห์ข้อมูลตามทรรศนะของ Huberman & Miles (1994 : 12) ซึ่งมีองค์ประกอบสำคัญ ๓ ประการ ได้แก่ ๑. การลดทอนของข้อมูล (Data reduction) หมายถึง การปรับลด เพิ่มหาข้อมูลใหม่จนได้ผลหรือข้อสรุป ๒. การแสดงข้อมูล (Data display) หมายถึงการกระทำในรูปของการเล่าเรื่องว่าเกิดอะไรขึ้นก่อนหลัง อย่างไร ทำไม และ ๓. การสรุปและยืนยันข้อสรุป (Drawing and verifying conclusion) หมายถึง มีการสรุปข้อมูลในขั้นแรกเบื้องต้นก่อนแล้วหลังจากนั้นเก็บข้อมูลต่อแล้วทดสอบการสรุปเบื้องต้นไปเรื่อย ๆ จนยืนยันข้อสรุปดังกล่าวได้ชัดเจน นำเสนอผลการวิจัยโดยการบรรยายเชิงพรรณนาแบบความเรียง

ข้อจำกัดของการวิจัย

เนื่องจากอาชญากรรมทางเทคโนโลยีและภัยคุกคามทางไซเบอร์มีผลกระทบอย่างมากต่อประชาชน ทำให้เกิดการตอบสนองและแก้ไขปัญหาด้วยวิธีการต่าง ๆ อย่างรวดเร็ว ทั้งที่เกิดขึ้นแบบบูรณาการและแยกกันจัดการ ทำให้การขับเคลื่อนการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีโดยหน่วยงานทั้งภาครัฐและเอกชนที่เกี่ยวข้องอยู่โดยตลอด และก่อให้เกิดความเปลี่ยนแปลงของนโยบาย กฎหมาย กฎ คำสั่ง และมาตรการต่าง ๆ อย่างสม่ำเสมอ จึงทำให้ข้อมูลที่ได้จากการวิจัยอาจไม่ทันสมัยอยู่ตลอด แต่อย่างไรก็ตาม จะเป็นแนวทางในการพัฒนาแนวทางป้องกันในอนาคตได้ต่อไป

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบแนวทางแก้ไขปัญหา อุปสรรค ข้อขัดข้องในการแก้ไขปัญหาอาชญากรรมทาง เทคโนโลยี

๒. ทำให้ทราบผู้มีส่วนเกี่ยวข้องและโครงสร้างสามารถร่วมบูรณาการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

๓. ได้แนวทางในการบูรณาการเพื่อป้องกันเพื่อไม่ให้เกิดอาชญากรรมทาง เทคโนโลยีขึ้นกับประชาชนทั่วไป

คำจำกัดความ

อาชญากรรมทางเทคโนโลยี	หมายถึง	การกระทาการใด ๆ เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้เหยื่อได้รับ ความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน
ภัยไซเบอร์	หมายถึง	ภัยที่เกิดขึ้นบนโลกอินเตอร์เน็ต สามารถเกิดขึ้นได้กับบุคคลคอมพิวเตอร์ หรือระบบต่างๆ ทำให้เกิดความเสียหายต่างๆ เกิดขึ้น
คริปโตเคอร์เรนซี	หมายถึง	สกุลเงินดิจิทัลใช้ในการทำธุรกรรม ได้รับการตรวจสอบและบันทึกข้อมูลไว้บนระบบการกระจายศูนย์หรือ Decentralized ซึ่งใช้การเข้ารหัส
บัญชีม้า	หมายถึง	บัญชีเงินฝากธนาคารของบุคคลอื่นซึ่งถูกมิจฉาชีพผู้กระทำผิด นำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้
กระเป๋าเงินอิเล็กทรอนิกส์	หมายถึง	ที่รู้จักโดยทั่วไปว่า “E-Wallet” มักถูกเรียกว่า กระเป๋าเงินดิจิทัล หรือ กระเป๋าเงินออนไลน์ ที่อยู่ในรูปแบบของแอปพลิเคชั่น จะช่วยอำนวยความสะดวกในการทำ

		ธุรกรรมต่างๆ อาทิเช่น การช้อปปิ้งออนไลน์ การเลือกซื้อสินค้าตามห้างร้าน หรือแม้แต่รับประทานอาหารและบริการมากมาย ช่วยประหยัดเวลาและไม่ต้องกังวลเรื่องการพกพาเงินสด
Mobile banking	หมายถึง	ที่รู้จักโดยทั่วไปว่า "M-banking" การบริการธนาคารทางโทรศัพท์มือถือ เป็นบริการอิเล็กทรอนิกส์อีกช่องทางหนึ่งที่ลูกค้าสามารถทำธุรกรรมทางการเงินด้วยตนเองผ่านโทรศัพท์มือถือในลักษณะโต้ตอบกับระบบงานของธนาคารได้เองโดยอัตโนมัติ ซึ่งส่วนใหญ่จะใช้เพื่อการโอนเงินและชำระเงิน
E-Banking	หมายถึง	การทำธุรกรรมต่างๆ กับธนาคาร โดยผ่านเครือข่ายอินเตอร์เน็ต เช่น การฝากเงิน ถอนเงิน โอนเงิน หรือสอบถามยอดเงิน
Peer-to-Peer	หมายถึง	การซื้อ-ขายสินค้าต่างๆ ด้วยกันเองภายใน community นั้นๆ การซื้อ-ขายให้คนที่ต้องการสินค้านั้นๆ หรือต้องการขายสินค้านั้นๆ ด้วยกันเอง โดยทุกฝ่ายได้ประโยชน์
แอปพลิเคชัน	หมายถึง	โปรแกรม หรือ กลุ่มของโปรแกรม ที่ถูกออกแบบสำหรับอุปกรณ์ อิเล็กทรอนิกส์แบบพกพา เช่น โทรศัพท์มือถือ แท็บเล็ต เป็นต้น
เป๋าตัง	หมายถึง	แอปพลิเคชั่นกระเป๋าเงินออนไลน์ หรือ E-wallet ของธนาคารกรุงไทย ที่ทำขึ้นเพื่ออำนวยความสะดวกให้แก่ประชาชนในยุค ๔.๐ ทั้งยังเป็นแอปพลิเคลั่นที่เป็นตัวกลางในการรับเงินในโครงการ “เราเที่ยวด้วยกัน” และ “คนละครึ่ง”
Hack	หมายถึง	การเจาะระบบ โจรกรรมข้อมูล ก่ออาชญากรรม ก่อวินาศกรรม สร้างความเสียหาย ผ่านระบบคอมพิวเตอร์ โดยใช้เทคนิคที่ค่อนข้างซับซ้อน และมักทำโดยผู้ที่ความรู้ด้านคอมพิวเตอร์และเครือข่ายชั้นสูง
การตระหนักรู้ Vaccine Immunity		
	หมายถึง	เป็นการให้ความรู้และข้อมูลต่างๆ ที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีแก่ประชาชน เพื่อให้ประชาชนมีความรู้เกี่ยวกับอาชญากรรมทางเทคโนโลยี มีภูมิคุ้มกันที่ดีในการใช้เทคโนโลยี ช่วยป้องกันเหตุอาชญากรรมทางเทคโนโลยีที่จะเกิดขึ้นได้

บทที่ ๒
การทบทวนวรรณกรรม และงานวิจัยที่เกี่ยวข้อง

จากการศึกษาแนวคิดและทฤษฎีจากเอกสารงานวิจัยต่างๆ เพื่อนำมากำหนดเป็นกรอบแนวคิดในการวิจัย เรื่องปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ ผู้วิจัยขอนำเสนอผลการศึกษาค้นคว้า ดังนี้

๑. อาชญากรรมทางเทคโนโลยี
๒. ประเภทอาชญากรรมทางเทคโนโลยี
๓. สาเหตุของการเกิดอาชญากรรมเทคโนโลยี
๔. แนวภูมิคุ้มกันทางไซเบอร์และการป้องกันอาชญากรรมทางเทคโนโลยี
๕. งานวิจัยที่เกี่ยวข้อง
๗. กรอบแนวคิดของการวิจัย

อาชญากรรมทางเทคโนโลยี

อาชญากรรมทางเทคโนโลยี หมายถึง การกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์หรือเครื่องมือทางเทคโนโลยีต่างๆ ทำให้ผู้อื่นนั้นได้รับความเสียหาย เช่น การลักทรัพย์อุปกรณ์คอมพิวเตอร์ เป็นต้นนอกจากนี้ยังหมายรวมถึงการกระทำใดๆ ที่เป็นความผิดทางอาญา ซึ่งจะต้องใช้ความรู้เกี่ยวกับคอมพิวเตอร์ในการกระทำความผิดนั้น เช่น การบิดเบือนข้อมูล (Extortion) การเผยแพร่รูปอนาจารผู้เยาว์ (Child pornography) การฟอกเงิน (Money Laundering) ฉ้อโกง (Fraud) การถอดรหัสโปรแกรมคอมพิวเตอร์ โดยไม่รับอนุญาต แล้วเผยแพร่ให้ผู้อื่นดาวน์โหลดได้ บางครั้งเรียกว่า การโจรกรรมโปรแกรม (Software Pirating) และการขโมยข้อมูลความลับทางการค้าของบริษัท (Corporate Espionage) เป็นต้น (Shelly & Vermaat, 2010)

อาชญากรรมทางเทคโนโลยีเป็นความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มของปัจเจกบุคคลด้วยเหตุจูงใจทางอาญา ที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ ทั้งทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต (ห้องแช็ตอีเมล กระดานประกาศ และกลุ่มข่าว) และโทรศัพท์เคลื่อนที่ (เอสเอ็มเอส/เอ็มเอ็มเอส) (Halder,Jaishankar & Jaishankar, 2012) ปัจจุบันอาชญากรรมทางคอมพิวเตอร์ถือเป็นอาชญากรรมทางเศรษฐกิจ หรืออาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ เนื่องจากได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศจำนวนมหาศาล ซึ่งภัยจากอาชญากรรมทางเทคโนโลยี หรือ Cybercrime ที่คนร้ายอาศัยช่องโอกาสจากเทคโนโลยีในการเข้าถึงประชาชนได้อย่างกว้างขวางและรวดเร็ว โดยรูปแบบอาชญากรรมส่วนใหญ่เป็นการหลอกลวงให้เหยื่อหลงเชื่อไว้ใจ หรือหลงรัก หรือเกิดความกลัว แล้วชักจูงให้เข้าใจผิดว่าเรื่องที่หลอกนั้นเป็นเรื่องจริงและยินยอมส่งมอบเงินหรือทรัพย์สินให้ โดยช่องทางสมัยใหม่ที่คนร้ายอาศัยความก้าวหน้าทางเทคโนโลยีทำให้ง่ายต่อ

การโอนเงินหรือทรัพย์สินให้ไปคราวละมากๆ โดยขาดความยั้งคิดหรือขาดสติ ซึ่งกว่าจะรู้ตัวก็สูญเงินหรือทรัพย์สินไปเป็นจำนวนมากแล้ว ซึ่งในกรณีนี้คนร้ายจะให้เหยื่อโอนเงินหรือทรัพย์สินให้ผ่านบัญชีม้า (บัญชีธนาคารในชื่อของบุคคลอื่นเพื่อให้ยากต่อการติดตามคืน) โดยคนร้ายจะโอนต่อจากบัญชีม้าแถวหนึ่ง ไปยังบัญชีม้าแถวสองอีกหลายบัญชี และโอนต่อไปยังบัญชีม้าแถวสามในอีกหลายบัญชี ก่อนจะโอนออกไปให้คนร้ายระดับหัวหน้า หรือถอนออกไปในรูปแบบเงินดิจิทัล Crypto Currency ซึ่งทำให้การติดตามยึดคืนเป็นไปได้ยาก

ประเภทอาชญากรรมทางเทคโนโลยี

สำนักงานตำรวจแห่งชาติได้กำหนดลักษณะคดีอาชญากรรมทางเทคโนโลยีไว้ ตามข้อ ๔ ของคำสั่งสำนักงานตำรวจแห่งชาติ ที่ ๓๒๒/๒๕๖๕ และที่แก้ไขเพิ่มเติม ตามคำสั่ง ตร. ที่ ๔๐๐/๒๕๖๕ โดยแบ่งออกเป็น ๒๒ ประเภท และได้ปรับให้เหลือ ๑๔ ประเภท ดังนี้

๑. หลอกขายของออนไลน์ เป็น คดีหลอกลวงเกี่ยวกับสินค้า หรือบริการ หมายความถึง คดีที่มีการกระทำผิดโดยทุจริตหลอกลวงโฆษณาขายสินค้าหรือบริการผ่านสื่อสังคมออนไลน์ เชิญชวนให้ผู้เสียหายเข้าไป ซื้อสินค้าหรือใช้บริการและเมื่อผู้เสียหายสั่งซื้อและชำระเงินเรียบร้อยแล้ว กลับไม่ได้รับสินค้าหรือบริการนั้นๆ เช่น ผู้เสียหายติดต่อซื้อกระเป๋าแบรนด์เนมมือสองในราคาถูกกว่าปกติในร้านขายสินค้าออนไลน์ เมื่อชำระเงิน ค่าสินค้าแล้ว คนร้ายไม่ส่งสินค้าให้ตามที่ตกลงซื้อขายกัน จากนั้นได้ปิดร้านขายสินค้าออนไลน์ไป ไม่สามารถ ติดต่อได้ เป็นต้น และให้หมายความรวมถึง การหลอกซื้อสินค้าหรือบริการโดยมีเจตนาไม่จ่ายค่าสินค้าหรือบริการ เช่น สั่งซื้อสินค้า แล้วส่งเอกสารโอนเงิน (สลิป) ปลอมให้ผู้ขายดูทางออนไลน์เพื่อให้จัดส่งสินค้ามาให้ แต่ความจริงไม่ได้จ่ายเงินค่าสินค้าแต่อย่างใด เป็นต้น (๒๒,๘๓๗ เรื่อง) ตลอดจน คดีซื้อสินค้าหรือบริการ แต่มีเจตนาส่งสินค้าหรือให้บริการไม่ตรงตามที่โฆษณาไว้ อันอาจจะเป็นความผิดฐานฉ้อโกง หรือหลอกลวงให้ผู้เสียหายหลงเชื่อในแหล่งกำเนิด สภาพ คุณภาพ หรือปริมาณแห่งของนั้นอันเป็น เท็จ ตามประมวลกฎหมายอาญา มาตรา ๒๗๑ หรือพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.๒๕๒๒ อย่างใดอย่างหนึ่ง เช่น ผู้เสียหายสั่งซื้อโทรศัพท์มือถือ ที่โฆษณาว่าเป็นสินค้าใหม่จากศูนย์บริการ แต่กลับได้สินค้าที่ ผ่านการใช้งานมาแล้ว หรือหน่วยความจำน้อยกว่าที่โฆษณาไว้ หรือเปิดบริษัทรับต่อเติมบ้าน แต่เมื่อรับมัดจำแล้วไม่ดำเนินการตามที่ตามตกลงกับลูกค้าทุกราย เป็นต้น (๑,๑๔๖ เรื่อง) รวมถึงเชื่อมโยงของคนร้ายในลักษณะที่เป็นขบวนการ หรือมีผู้เสียหายเป็นจำนวนมากหลายพื้นที่ เช่น คนร้ายร่วมกัน หลอกลวงผู้เสียหายอันมีลักษณะเป็นการแบ่งหน้าที่กันทำงาน โดยคนหนึ่งมีหน้าที่ในการสร้างเพจขายโทรศัพท์มือถือราคาถูกในแอปพลิเคชั่น เฟซบุ๊ก อีกคนหนึ่งมีหน้าที่หาบัญชีม้า อีกคนหนึ่งมีหน้าที่ตอบข้อความที่ ลูกค้าส่งมา เมื่อผู้เสียหายโอนเงินไปแล้ว กลุ่มคนร้ายจะปิดบัญชีเฟซบุ๊ก และไม่สามารถติดต่อได้ (๑,๑๔๖ เรื่อง)

๒. คอลเซ็นเตอร์ (Call Center) ข่มขู่ให้เกิดความกลัว เป็นคดีข่มขู่ให้เกิดความกลัว (Call center) หมายความถึง คดีที่มีการกระทำผิดโดยใช้ โทรศัพท์ หรือโทรศัพท์ผ่านระบบอินเทอร์เน็ต (โดยเพื่อให้เกิดความกลัวใน รูปแบบต่างๆ เช่น ขู่ว่าจะส่งหมายเรียกหรือหมายจับ หรือจะดำเนินคดีเกี่ยวกับการฟอกเงิน หรือมีหมายจับคดี ฟอกเงิน จากนั้นคนร้ายจะเสนอความช่วยเหลือโดยให้ผู้เสียหายโอนเงินเข้าบัญชีคนร้ายหรือบัญชีม้าหรือโดยวิธีการอื่นใด โดยอ้างว่า

เพื่อตรวจสอบว่าเงินของผู้เสียหายเกี่ยวข้องกับการกระทำความผิดฐานฟอกเงินหรือไม่ หากไม่มีส่วนเกี่ยวข้องจะโอนคืนให้ แต่เมื่อโอนเงินไปแล้วกลับไม่ได้รับเงินคืนกลับมาอีก (๕,๐๙๖ เรื่อง) VoiceoverInternet Protocol หรือ VoIP) ติดต่อไปยังผู้เสียหาย สร้างเรื่องราวหลอกลวงหรืออ้างตนเป็นบุคคลอื่น เช่น การแอบอ้างเป็นเจ้าหน้าที่บริษัทไปรษณีย์ ไทย จำกัด หรือเจ้าหน้าที่บริษัทขนส่งต่างๆ แล้วโอนสายให้พูดคุยกับคนร้ายที่อ้างว่าเป็นเจ้าหน้าที่หน่วยงานของรัฐ ซึ่งคนร้ายจะอ้างว่าผู้เสียหายมีส่วนเกี่ยวข้องกับการกระทำผิดกฎหมายต่างๆ

๓. เงินกู้ออนไลน์ ดอกเบี้ยโหด เป็นคดีที่มีการกระทำผิดโดยการหลอกลวงผู้เสียหายด้วยวิธีการต่างๆ โดยคนร้ายอาจสร้างเรื่องราว หรือสร้างข้อมูลอันเป็นเท็จในระบบคอมพิวเตอร์แล้ว ส่งข้อความให้ผู้เสียหายทางโทรศัพท์ ทางสื่อสังคมออนไลน์ หรือโดยการประกาศหรือโฆษณาในสื่อสังคม ออนไลน์ เพื่อหลอกลวงผู้เสียหายให้โอนเงินให้คนร้าย โดยอ้างเป็นค่าสมัคร ค่าสมาชิก หรือค่าใช่จ่ายอื่นๆ เช่น หลอกลวงว่าจะให้ผู้เสียหายถ่ายแบบ โดยให้โอนเงินค่าสมัคร ค่าดำเนินการไปก่อน แต่สุดท้ายได้ปิดเฟซบุ๊คหนี ไป หรือหลอกว่าจะคืนเงินค่าซื้อสินค้า แล้วส่ง QR code ให้ผู้เสียหายตรวจสอบและยืนยันยอด แต่แท้จริงแล้ว เป็นการหลอกให้เหยื่อกดโอนเงินให้ เป็นต้น (ประมาณ ๑,๕๐๐ เรื่อง)

๔. เงินกู้ออนไลน์ ที่ไม่มีจริง (เงินกู้ทิพย์) คดีหลอกให้กู้เงินแต่ไม่ได้เงิน หมายความถึง คดีที่มีการกระทำผิดโดยหลอกลวง ประกาศ หรือโฆษณาในสื่อสังคมออนไลน์เชิญชวนให้ประชาชนกู้ยืมเงิน เมื่อผู้เสียหายหลงเชื่อเข้าทำรายการขอกู้ยืมเงิน คนร้ายจะหลอกว่าได้รับการอนุมัติแล้ว แต่ต้องมีเงินค้ำประกัน หรือต้องจ่ายเงินอย่างอื่นเพิ่มก่อนจึงจะได้รับ เงินกู้ สุดท้ายผู้เสียหายไม่ได้ทั้งเงินกู้และเงินที่โอนไปให้คนร้าย เช่น ผู้เสียหายเห็นข้อความ “ปล่อยกู้ โดยไม่ต้อง มีหลักทรัพย์ค้ำ” ในระบบอินเทอร์เน็ต เกิดความสนใจจึงกดลิงค์ของเว็บไซต์เงินกู้ปลอม เมื่อกรอกข้อมูลแล้ว คนร้ายจะติดต่อกลับมาแจ้งว่าได้รับการอนุมัติเงินแล้ว แต่เพื่อเป็นหลักประกันว่าผู้เสียหาย มีเงินพอที่จะชำระ เงินกู้ ต้องโอนเงินมาก่อน ๒๐% เมื่อผู้เสียหายโอนแล้ว คนร้ายก็จะอ้างเหตุต้องจ่ายเงินอื่นๆ เพิ่มขึ้นมา ได้แก่ ค่าธรรมเนียม,ค่าภาษี หรือค่าประกันภัย, ปลดล๊อกบัญชีฟอกเงิน หรือส่งเลขบัญชีผิดต้องโอนมาปลดล๊อก โดย คนร้ายหลอกว่าจะโอนคืนทั้งหมดเมื่อดำเนินการแล้ว ด้วยความเสียดายเงินที่โอนไปก่อนหน้านั้น ผู้เสียหายก็ จะโอนเงินไปให้คนร้ายเรื่อยๆ ตามที่คนร้ายหลอก สุดท้ายแล้วผู้เสียหายไม่ได้ทั้งเงินกู้และเงินที่โอนไปให้คนร้าย (๘,๒๒๐ เรื่อง)

๕. หลอกให้ลงทุนต่างๆ ได้แก่ คดีหลอกให้ลงทุน ที่ไม่เข้าลักษณะฉ้อโกงประชาชน หมายความถึง คดีที่มีการกระทำผิด โดยหลอกลวงให้ลงทุนทางธุรกิจ การเงิน หรือการค้า โดยเชิญชวนผ่านสื่อออนไลน์ให้ผู้เสียหายมาลงทุนคน เดียวเป็นรายบุคคล ไม่ได้ให้มีการสร้างเครือข่ายในการลงทุน อ้างว่าจะได้รับผลตอบแทนหรือกำไรในอัตราสูง แต่ความจริงแล้ว ไม่มีกิจการหรือได้รับผลตอบแทนสูงตามที่กล่าวอ้าง เมื่อผู้เสียหายโอนเงินลงทุนหรือ ค่าใช้จ่ายอื่นๆ ไปแล้ว กลับไม่ได้รับผลตอบแทนและเงินลงทุน หรือค่าใช้จ่ายอื่นๆ แต่อย่างใด เช่น คนร้าย หลอกว่าตนเองเป็นผู้ที่มีความเชี่ยวชาญในตลาดแลกเปลี่ยนเงินตรา(Forex), หุ้น, รับฝากเทรด(copy trade), เงินเหรียญดิจิทัล, เทรดทองคำ หรือน้ำมัน โดยทำเว็บไซต์ปลอมขึ้นมาหลอกลวงว่าได้กำไรต่อวันจำนวนมากแล้วให้ผู้เสียหายโอนเงินไปร่วมลงทุน หรือแนะนำให้ซื้อขายในเว็บเทรดที่สร้างขึ้น หรืออ้างว่าเป็นคนที่สามารถซื้อตั๋วเครื่องบิน, ซื้อสินค้าจากโรงงาน(Pre Order), ทำธุรกิจนำเข้าและส่งออกที่ซื้อสินค้า

เหล่านั้นมาในราคาถูกแล้วนำไปขายในราคาแพง หรืออ้างว่าทำโรงงานขุดเหรียญดิจิทัล แล้วให้ผู้สนใจมาร่วมลงทุน ซื้อ/เช่าเครื่องขุดเหรียญเพิ่มขึ้น ทั้งที่ไม่ได้มีเครื่องขุดอยู่จริง (ประมาณ ๓,๐๐๐ เรื่อง) รวมถึง ๒๐ คดี หลอกให้ลงทุน ที่เข้าลักษณะฉ้อโกงประชาชน หรือแชร์ลูกโซ่ หมายความถึง คดีที่มีการกระทำผิดในลักษณะเดียวกับข้อ ๑๙ ที่มีการประกาศหรือเชิญชวนให้ร่วมลงทุนผ่านสื่อสังคมออนไลน์ที่ปรากฏต่อประชาชนทั่วไป หรือระดมทุนโดยการหาสมาชิกใหม่ผ่านสื่อสังคมออนไลน์ในรูปแบบเครือข่าย ให้ ผลตอบแทนสูงกว่าที่สถาบันการเงินตามกฎหมายจะให้ได้ โดยจะมีผลตอบแทนในการหาสมาชิก ค่าบริหารทีม หรือไม่ก็ได้ ผลตอบแทนที่ผู้ลงทุนได้นั้นไม่ได้เกิดจากผลิตภัณฑ์สินค้าหรือธุรกิจตามที่คนร้ายแอบอ้างแต่ เกิดจากเงินที่สมาชิกใหม่จ่ายค่าสมัครสมาชิกหรือลงทุน เช่น เปิดบริษัทผลิตเครื่องกำเนิดไฟฟ้าพลังงาน แม่เหล็กขายให้ต่างประเทศได้กำไรจำนวนมาก แต่ต้องการช่วยเหลือประชาชนโดยให้เข้ามาซื้อหุ้นละ ๑๐๐ บาท ให้ปันผลเดือนละ ๒๐% พร้อมให้ค่าชักชวนสมาชิกใหม่และค่าบริหารทีม ๕% จนทำให้สมาชิกแต่ละคน ต้องการเป็นแม่ทีมที่มีรายได้สูงต่อเดือนเพราะการหาสมาชิกใหม่เข้ามาซื้อหุ้นบริษัท ด้วยการทำโฆษณาผ่านสื่อออนไลน์ต่างๆ แต่สุดท้ายเมื่อไม่สามารถหาสมาชิกเพิ่มได้ ก็จะไม่ได้เงินทั้งเงินต้นและดอกเบี้ยตามที่ตกลงไว้ หรือ เปิดบริษัทขุดเหรียญ Bitcoin แล้วให้คนมาระดมทุนผ่านสื่อออนไลน์ จากนั้นได้ปิดบริษัทหนีไป เป็นต้น และลักษณะคดีดังกล่าวนี้ให้รวมถึงกรณีการเปิดวงแชร์ออนไลน์เพื่อหลอกลวงสมาชิก หรือเปิดวงแชร์ออนไลน์ ที่ไม่มีลักษณะให้สมาชิกวงแชร์หมุนเวียนกันรับทุนกองกลางแต่ละงวด เช่น เปิดวงแชร์ ๑๐ วง โดยแอบอ้างชื่อ สมาชิกอื่นๆ ที่ไม่มีตัวตนจริงเพื่อหลอกลวงผู้เสียหาย หรือแชร์ออมเงินกินดอกให้ผลตอบแทนสูงกว่าธนาคาร ทั่วไป แล้วปิดเพจหนีไป เป็นต้น(ประมาณ ๕,๐๐๐ เรื่อง)

๖. หลอกให้เล่นพนันออนไลน์ เป็นการหลอกลวงหรือชักจูงให้ผู้อื่นเล่นพนันออนไลน์

๗. คดีหลอกให้รักแล้วโอนเงิน (Romance Scam) หมายความถึง คดีที่มีการกระทำผิดโดยปลอมโปรไฟล์เป็นบุคคลอื่น พูดคุยตีสนิท เพื่อให้เกิดความรัก ความน่าสนใจ หรือความน่าเชื่อถือ จากนั้นคนร้าย จะสร้างเรื่องราวหลอกให้ผู้เสียหายโอนเงินให้ เช่น

๗.๑ หลอกว่าคนร้ายได้ส่งของมีค่ามาให้ผู้เสียหาย โดยมีผู้ร่วมขบวนการอ้างตัวเป็นเจ้าหน้าที่กรมศุลกากร หรือเจ้าหน้าที่ของบริษัทขนส่งต่างๆ แจ้งผู้เสียหายว่ามีพัสดุจากต่างประเทศส่งมาถึงผู้เสียหายจะต้องเสียภาษีหรือค่าธรรมเนียมต่าง ๆ จึงจะสามารถรับพัสดุนั้นได้

๗.๒ คนร้ายสร้างเรื่องขึ้นมาว่าได้ขายทรัพย์สินในต่างประเทศแล้ว แต่มีปัญหาเกิดขึ้นไม่สามารถถอนเงินจากธนาคารได้ จะขอยืมเงินจากผู้เสียหาย โดยให้ผู้เสียหายโอนเงินไปให้บุคคลอื่นในประเทศไทยก่อน

๗.๓ คนร้ายอ้างว่าเจ็บป่วย มีปัญหาเกี่ยวกับบัตรเครดิต ขอยืมเงินจากผู้เสียหายก่อน (๖๖๓ เรื่อง) ตลอดจนรวมถึง คดีหลอกให้รักแล้วลงทุน (Hybrid scam) หมายความถึง คดีที่มีการกระทำผิดโดยปลอม โปรไฟล์เป็นบุคคลอื่น โดยใช้สื่อสังคมออนไลน์ในการพูดคุยเพื่อให้เกิดความน่าสนใจหรือน่าเชื่อถือ แล้วชักชวน หรือออกอุบายให้ร่วมลงทุน โดยให้ผู้เสียหายโอนเงินเข้าบัญชีคนร้าย(บัญชีม้า) หรือซื้อเหรียญดิจิทัลใน แอพพลิเคชั่นปลอม หรือใช้วิธีการอื่นๆ โดยไม่ได้รับผลตอบแทนจริง เช่น คนร้ายนำภาพนักธุรกิจที่มีชื่อเสียงมา สร้างโปรไฟล์ปลอมและส่งข้อความไปยังผู้เสียหาย โดยใช้แอพพลิเคชั่นอินตราแกรม (Instagram) จากนั้น คนร้ายจะชักชวนผู้เสียหาย

พูดคุยเป็นการส่วนตัวให้เกิดความรัก ส่งภาพผลกำไรจากการลงทุนและการใช้ชีวิตที่ สุขสบาย จากการลงทุนเพื่อให้เกิดความน่าเชื่อถือ และคนร้ายจะชักชวนให้ผู้เสียหายร่วมลงทุน โดยวิธีการส่งลิงค์เว็บไซต์การลงทุนปลอมมาให้เพื่อให้ผู้เสียหายเข้าร่วมลงทุน (๑,๗๕๖ เรื่อง)

๘. ส่งลิงก์ปลอมเพื่อหลอกแฮกเอาข้อมูลส่วนตัว เป็น ๙. คดีเข้าถึงระบบหรือข้อมูลคอมพิวเตอร์ผู้อื่นโดยมิชอบ(Hack) หมายความถึง คดีที่มีการกระทำความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ ทั้งการเข้าถึงระบบ แก้ไข ดัดแปลง ก่อกวน หรือจำหน่ายเผยแพร่ ชุดคำสั่งระบบของผู้อื่นโดยมิชอบ อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม เช่น เข้าถึงข้อมูลบุคคลอื่น แล้วนำข้อมูลบัตรประชาชนไปปลอมแปลง เปิดบัญชีและโอนเงินของผู้เสียหายเข้าบัญชีของคนร้าย รวมถึงการหลอกเอารหัสการใช้งานระบบ คอมพิวเตอร์ หรือหลอกเอารหัสเข้าบัญชีสื่อสังคมออนไลน์(Phishing) เพื่อนำไปใช้โดยมิชอบ เช่น การส่งลิงค์ หลอกให้กรอกข้อมูลหรือให้ติดตั้งแอปพลิเคชั่นปลอม เพื่อควบคุมคอมพิวเตอร์ทางไกล ขโมยข้อมูลของเหยื่อไป ใช้ในการถอนเงินจากบัญชี หรือเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ของผู้เสียหายโดยตรง เป็นต้น (ประมาณ ๒๐๐ เรื่อง)

๙. อ้างเป็นบุคคลอื่นเพื่อหลอกเอาข้อมูลส่วนตัว เป็นการอ้างตัวเป็นบุคคลอื่นเพื่อหลอกลวงเอาข้อมูลส่วนตัวมาเพื่อประโยชน์อันมิชอบ

๑๐. ปลอม Line, Facebook หรือ Account หลอกยืมเงิน เป็นการปลอมเพื่อหลอกยืมเงินผู้อื่น

๑๑. ข่าวปลอม (Fake news) - ชัวร์ก่อนแชร์ คดีข่าวปลอม (Fake News) หมายความถึงคดีที่มีการกระทำผิดอาญา โดยนำข้อมูลอันเป็น เท็จ บิดเบือน หรือปลอมทั้งหมดหรือบางส่วนเข้าสู่ระบบคอมพิวเตอร์ ที่ประชาชนโดยทั่วไปสามารถเข้าถึงได้ อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไข เพิ่มเติม มาตรา ๑๔ และมาตรา ๑๖ เช่น ลงข่าวในสื่อออนไลน์ว่าเกิดภัยธรรมชาติสึนามิ ทำให้เกิดความ ตระหนกตกใจกับประชาชนทั้งประเทศ หรือการตัดต่อภาพดารา ทำให้ถูกดูหมิ่น เกลียดชัง (๒๔๗ เรื่อง)

๑๒. หลอกลวงเอาภาพโป๊เปลือยเพื่อใช้แบล็กเมล์ เป็นคดีเกี่ยวกับเพศล่วงละเมิดทางเพศ หมายความถึง คดีที่มีการกระทำผิดทางอาญาเกี่ยวกับ เพศในลักษณะต่างๆ ซึ่งเป็นความผิดตามประมวลกฎหมายอาญา หรือความผิดตามกฎหมายอื่นๆ ที่มีโทษทาง อาญา โดยใช้ระบบคอมพิวเตอร์หรือระบบเทคโนโลยีเป็นเครื่องมือหรือช่องทางในการกระทำความผิด เช่น การเผยแพร่สื่อลามกอนาจาร, ภาพเคลื่อนไหวการมีเพศสัมพันธ์, ภาพถ่ายที่เห็นอวัยวะเพศตนเองหรือบุคคลอื่นหรือภาพเปลือย หรือหลอกลวงให้เหยื่อถ่ายภาพโป๊เปลือย เพื่อให้เกิดความอับอายหรือข่มขู่เรียกทรัพย์สิน หรือสิ่งอื่นใดจากเหยื่อ นำเข้าสู่ระบบคอมพิวเตอร์ โดยผู้กระทำความผิดจะได้มาซึ่งผลประโยชน์หรือไม่ก็ได้ (๒๑๙ เรื่อง)

๑๔. โฆษณาชวนไปทำงานต่างประเทศแล้วบังคับให้ทำงานผิดกฎหมาย เป็นคดีหลอกลวงให้ทำงานออนไลน์ หมายความถึง คดีที่มีการกระทำผิดโดยหลอกลวง ประกาศ หรือโฆษณาในสื่อสังคมออนไลน์เชิญชวนให้ผู้เสียหายทำงานพิเศษ ทำกิจกรรมใดๆ หรือซื้อสินค้าในระบบออนไลน์ เพื่อให้เกิดความน่าสนใจหรือน่าเชื่อถือว่างานดังกล่าวสามารถสร้างรายได้หรือค่าตอบแทนได้จริง โดยให้ผู้เสียหายโอนเงินค่าสมัครหรือค่าใช้จ่ายอื่นๆ ให้ก่อนเมื่อได้ทำงาน ทำกิจกรรม หรือ

โอนเงินค่าสินค้าไปแล้ว ผู้เสียหายกลับไม่ได้รับรายได้ สินค้า หรือค่าตอบแทนจริง เช่น คนร้ายได้ส่งข้อความชักชวนทำงาน หารายได้พิเศษหลังเลิกงานในระบบอินเทอร์เน็ต โดยทำเพียงกดไลค์ (Like) หรือแชร์ (Share) หรือเพิ่มยอด คนดู (View) ในแอพพลิเคชั่น YouTube, Instagram (IG), TIK TOK หรือเว็บไซต์ขายสินค้า โดยจะมีรายได้ ต่อวัน ตามจำนวนเงินที่ลงทุน ยิ่งลงทุนมากยิ่งได้ผลตอบแทนต่อวันมาก หรือให้ผู้เสียหายกดสั่งซื้อสินค้าเพื่อ เพิ่มยอดขายหรือทำสต๊อกสินค้า ๘ ขั้นตอน โดยลงทุนซื้อสินค้าครั้งที่ ๑ จะลงทุนหลัก ๑๐๐ บาท มีกำไร ๒๐% แต่ยังไม่สามารถถอนได้ ผู้เสียหายต้องลงทุนซื้อสินค้าในครั้งที่ ๒ ถึง ๘ เพิ่มอีก โดยราคาสินค้าจะแพงขึ้นเรื่อย ๆ ทำให้ผู้เสียหายต้องเพิ่มเงินลงทุนขึ้นเรื่อย ๆ โดยเห็นผลกำไรจำนวนมากขึ้นในระบบ แต่สุดท้ายผู้เสียหายไม่สามารถถอนเงินได้ (๑๐,๐๐๘ เรื่อง)

๑๔. ยินยอมให้ผู้อื่นใช้บัญชีธนาคาร (บัญชีม้า) ซึ่งเข้าข่ายเป็นความผิดฐานฉ้อโกงประชาชน เป็นการยินยอมให้ผู้อื่นใช้บัญชีของตนเพื่อฉ้อโกงประชาชน

ความผิดทั้งหมดแบ่งเป็นกลุ่มต่าง ๆ ได้ ดังนี้

กลุ่ม ๑ (ความผิดที่เกิดขึ้นกับข้อมูลและระบบคอมพิวเตอร์ หรือ Cyber Dependent Crime)

๑. เข้าถึงระบบหรือข้อมูลของผู้อื่นโดยไม่ชอบ หรือเปิดเผยมาตรการ (มาตรา ๕-๘) ในส่วนที่เกี่ยวข้องกับความลับในการเข้าถึงระบบ Confidentiality

หากเข้าไปเจาะระบบหรือเข้าถึงข้อมูลทางคอมพิวเตอร์ของคนอื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต หรือ การปล่อยไวรัสมัลแวร์เข้าคอมพิวเตอร์คนอื่น เพื่อเข้าถึงระบบหรือเจาะเอาข้อมูลบางอย่าง หรือพวกแฮคเกอร์ที่เข้า ไปขโมยข้อมูลของคนอื่น หรือล่วงรู้มาตรการป้องกันการเข้าถึงระบบแล้วนำไปเปิดเผยโดยมิชอบก็ผิดเช่นกัน

บทลงโทษ

๑. เข้าถึงระบบคอมพิวเตอร์ : จำคุกไม่เกิน ๖ เดือน ปรับไม่เกิน ๑ หมื่นบาท หรือทั้งจำทั้งปรับ (ผิดตาม ม.๕)

๒. ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย : จำคุกไม่เกิน ๑ ปี ปรับไม่เกิน ๒ หมื่นบาท หรือทั้งจาทั้งปรับ (ผิดตาม ม.๖)

๓. เข้าถึงข้อมูลคอมพิวเตอร์ : จำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ (ผิดตาม ม.๗)

๔. ดักรับข้อมูลคอมพิวเตอร์ : จำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๖ หมื่นบาท หรือทั้งจำทั้งปรับ (ผิดตาม ม.๘)

๒. การแก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่น เสียหาย เปลี่ยนแปลง (มาตรา ๙) ในส่วนที่เกี่ยวข้องกับความสมบูรณ์ของข้อมูลคอมพิวเตอร์ Integrity

ในข้อนี้จะรวมถึงการทำให้ข้อมูลเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติมข้อมูลของผู้อื่นโดยมิชอบ หรือจะเป็นในกรณี ที่ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ อย่างเช่น กรณีของกลุ่มคนที่ไม่ชอบใจกับการกระทำของอีกฝ่าย แล้วต่อต้านด้วยการเข้าไปขัดขวาง ทำร้ายระบบเว็บไซต์ของฝ่าย ตรงข้าม ให้บุคคลอื่นๆ ใช้งานไม่ได้ หรือกลุ่มแฮกเกอร์

ที่เข้าไปแฮกระบบและข้อมูล เพื่อมุ่งหวังประโยชน์โดยมิชอบ เช่นการเรียก ค่าไถ่ หรือกลุ่มที่อาจจะต้องการแสดงจุดยืนทางการเมือง ฯ เป็นต้น

บทลงโทษ ต้องระวางโทษ : จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ

๓. ทำให้ระบบคอมพิวเตอร์ระงับ ชะลอ ขัดขวาง รบกวนระบบคอมพิวเตอร์จนไม่สามารถทำงานตามปกติได้ (มาตรา ๑๐) ในส่วนที่เกี่ยวข้องกับการใช้ระบบและข้อมูลคอมพิวเตอร์ Availability

ข้อนี้เป็นการทำให้ระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติ บทลงโทษต้องระวางโทษ : จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ

๔. ส่งข้อมูลหรืออีเมล์โดยปกปิดหรือปลอมแปลมแหล่งที่มาอันรบกวนผู้อื่น หรือส่งอีเมล์สแปม (มาตรา ๑๑)

ประเด็นพ่อค้าแม่ค้าออนไลน์ หรือนักการตลาดที่ส่งอีเมล์ ขายของที่ลูกค้าไม่ยินดีจะรับ เช่น อีเมล์ สแปม หรือ แม้แต่การฝากร้านตาม Facebook กับ Instragram ก็เป็นสิ่งที่ไม่ควรทำ (แต่อาจมีประเด็นว่าแพลตฟอร์มเหล่านั้นยินยอมให้ทำหรือไม่) และยังรวมถึงคนที่ขโมย Database ลูกค้าจากคนอื่นแล้วส่ง อีเมล์ขายของตัวเอง โดยที่ปกปิดหรือปลอมแปลงแหล่งที่มา หรือไม่ให้บอกเลิกได้ เป็นต้น

บทลงโทษ

๑. ถ้าส่งโดยปกติหรือปลอมแปลงแหล่งที่มา:ปรับไม่เกิน ๑ แสนบาท

๒. ถ้าส่งโดยไม่เปิดโอกาสให้ปฏิเสธตอบรับได้โดยง่ายต้องได้รับโทษ : ปรับไม่เกิน ๒ แสนบาท

๕. บทฉกรรจ์ของการเข้าถึงระบบหรือข้อมูล availability ทำให้ข้อมูลไม่สมบูรณ์ Integrity หรือ ทำให้ระบบคอมพิวเตอร์ใช้การไม่ได้ availability ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (มาตรา ๑๒)

ความผิดมาตรา ๑๒ ได้บอกไว้ว่าการเข้าถึงระบบหรือข้อมูล หรือเปิดเผยมาตรการการป้องกัน รวมถึงการส่งข้อมูล รบกวนต่อระบบหรือข้อมูลคอมพิวเตอร์ทางด้านความมั่งคงโดยมิชอบ

บทลงโทษ

๑. กรณีไม่เกิดความเสียหาย : จำคุก ๑-๗ ปี และปรับ ๒ หมื่น – ๑.๔ แสนบาท

๒. กรณีเกิดความเสียหายต่อข้อมูลหรือระบบคอมพิวเตอร์ : จำคุก ๑-๑๐ ปี และปรับ ๒ หมื่น – ๒ แสนบาท

๓. กรณีเข้าไปความเปลี่ยนแปลง แก้ไข ต่อข้อมูลหรือกระทำต่อระบบ เพื่อให้การ ทางานของคอมพิวเตอร์ชะลอ ขัดขวาง หรือรกวนจนไม่ปกติ : จำคุก ๓-๑๕ ปี และ ปรับ ๖ หมื่น – ๓ แสนบาท

๔. กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย : จำคุก ๕-๒๐ ปี และปรับ ๑ แสน – ๔ แสนบาท

๖. จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด (มาตรา ๑๓)

๑. กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทาง คอมพิวเตอร์ตามมาตรา ๕-๑๑ (ทั่วไป) : ต้องจำคุกไม่เกิน ๑ ปี ปรับไม่เกิน ๒ หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

๒. กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทาง คอมพิวเตอร์ มาตรา ๑๒ (ความมั่นคง) : ต้องจำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

๗. ข่าวปลอม หรือ นำข้อมูลเท็จ, ปลอม, บิดเบือน, ผิดความมั่นคง, ลามกเข้าสู่ระบบหรือแชร์ (มาตรา ๑๔)

๑. โพสต์หรือส่งข้อมูล บิดเบือน หรือปลอม หรือเท็จ เจตนาทุจริตหรือหลอกลวง ยกเว้น เรื่องหมิ่น ประมาท (อย่างเช่น ข่าวปลอมโฆษณาธุรกิจลูกโซ่ที่หลอกลวงเอาเงินลูกค้า หรือส่งอีเมลล์ให้กรอกเพื่อหลอกลวงเอาข้อมูลทางการเงินการฉ้อโกงต่าง ๆ เป็นต้น)

๒. โพสต์ข้อมูลเท็จ น่าเสียหายต่อความมั่งคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงทางด้านเศรษฐกิจหรือโครงสร้างพื้นฐานสาธารณะหรือก่อให้เกิดความตื่นตระหนก แก่ประชาชน (เช่นโพสต์ข่าวปลอมเรื่องแผ่นดินจะไหวแต่ไม่เป็นความจริง เป็นต้น)

๓. โพสต์ข้อมูลความผิดเกี่ยวกับความมั่นคงก่อการร้าย

๔. โพสต์ข้อมูลลามก ที่ประชาชนเข้าถึงได้

๕. เผยแพร่ส่งต่อข้อมูลที่รู้แล้วว่าผิด (เช่น กดShareข้อมูลที่มีเนื้อหาเข้าข่ายตาม ๑ - ๔)

บทลงโทษ

๑. หากเป็นการกระทำที่ส่งผลถึงประชาชน : จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับตาม วรรคหนึ่ง (๑)

๒. หากเป็นกรณีที่เป็นการกระทำผลต่อบุคลใดบุคคลหนึ่ง :จำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๖ หมื่นบาท หรือทั้งจำทั้งปรับ (แต่ในกรณีอย่างหลังนี้สามารถยอมความกันได้)

๘. ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจ กับผู้ร่วมกระทำความผิด (มาตรา ๑๕)

กรณีนี้ถ้าเทียบให้เห็นภาพชัดๆ ก็เช่น เพจต่างๆ ที่เปิดให้มีการแสดงความคิดเห็น แล้วมีความคิดเห็นที่มีเนื้อหาผิดกฎหมายก็มีความผิด แต่ถ้าหากแอดมินเพจตรวจสอบแล้ว พบเจอและลบออก จะถือว่าเป็นผู้ที่พ้นความผิด

บทลงโทษ แต่ถ้าไม่ยอมลบออกต้องได้รับโทษ ถือว่าเป็นผู้กระทำความผิดตามมาตร ๑๔ ต้องได้รับโทษเช่นเดียวกันผู้โพสต์ หรือแสดง ความคิดเห็นทางออนไลน์ แต่ถ้าผู้ดูแลระบบพิสูจน์ได้ว่า ตนได้ปฏิบัติตามขั้นตอนการแจ้งเตือนแล้วก็ไม่ต้องรับโทษ

๙. ตัดต่อ เติม หรือดัดแปลงภาพ (มาตรา ๑๖)

ความผิด แบ่งออกเป็น ๒ ประเด็นหลักคือ

การโพสต์ภาพของผู้อื่นที่เกิดจากการสร้าง ตัดต่อ หรือดัดแปลงที่น่าจะทาให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง อย่างเช่นกรณีที่เอาภาพดาราไปตัดต่อ และตกแต่งเรื่องขึ้นมาจนทำให้บุคคลนั้นเกิดความเสียหาย ก็ถือว่ามีความผิดตาม พ.ร.บ. คอมพิวเตอร์ (โดยเฉพาะขณะนี้มีการใช้เทคโนโลยี DEEP FAKE ทำเป็นวีดีโอ เช่นใส่หน้าผู้นำประเทศ แล้วพูดในคอนเทนต์ที่เสียหาย)

การโพสต์ภาพผู้เสียชีวิต หากเป็นการโพสต์ที่ทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย

บทลงโทษ หากทาผิดตามนี้ ต้องได้รับโทษ : จำคุกไม่เกิน ๓ ปี และปรับไม่เกิน ๒ แสนบาท

๑๐. ผู้ให้บริการต้องเก็บข้อมูลฯ (มาตรา๒๖)

ความผิด แบ่งออกเป็น ๒ ประเด็นหลัก คือ

ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ (หากจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ เก็บไว้เกิน ๙๐ วัน แต่ไม่เกิน ๒ ปี) ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง

บทลงโทษ หากทำผิดตามนี้ ต้องได้รับโทษ : ปรับไม่เกิน ๕ แสนบาท

กลุ่ม ๒ (ฉ้อโกง หรือ หลอกลวง โดยการใช้ข้อมูลหรือระบบคอมพิวเตอร์มากระทำผิดหลอกลวง ปกปิดเท็จจริงที่ควรบอก แสดงตนเป็นบุคคลอื่น โดยอาศัยความเชื่อใจ ความโลภ ความหลง ความกลัว อาทิ)

๑. หลอกลวงซื้อขายสินค้า
๒. หลอกลวงซื้อขายบริการ
๓. หลอกลวงซื้อขายสินค้า(เป็นกระบวนการ)
๔. หลอกลวงเกี่ยวกับเงินดิจิทัล
๕. โอนเงินเพื่อรับรางวัลฯ
๖. หลอกลวงทางโทรศัพท์เป็นกระบวนการ(Call Center)
๗. หลอกเป็นบุคคลอื่นเพื่อยืมเงิน
๘. หลอกให้รักแล้วโอนเงิน

ข้อกฎหมาย : **ประมวลกฎหมายอาญา มาตรา ๓๔๑** “การทุจริตหลอกลวงผู้อื่นด้วยข้อความที่เป็นเท็จ หรือปกปิดข้อความจริง ซึ่งควรบอกและแจ้งให้ทราบ จะมีโทษจำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๖,๐๐๐ บาท หรือทั้งจำทั้งปรับ โดยจะมีอายุความ ๓ เดือน นับตั้งแต่วันที่รู้เรื่องกระทำผิดและรู้ตัวผู้กระทำผิด” หากมีการใช้ข้อความ รูปภาพสินค้าสู่ระบบคอมพิวเตอร์ที่เป็นข้อมูลปลอมหรือเท็จเพื่อหลอกลวงให้ได้รับความเสียหาย ถือเป็นความผิดตาม**พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ มาตรา ๑๔** ที่ว่า “การนำเข้าซึ่งข้อมูลอันเป็นเท็จ หลอกลวง ทำให้ผู้อื่นได้รับความเสียหาย มีโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท โดยมีอายุความ ๑๐ ปี”

กลุ่ม ๓ (ฉ้อโกงประชาชน หลอกลวงให้ทำการลงทุนหรือทำธุรกิจ โดยการใช้ข้อมูลหรือระบบคอมพิวเตอร์มากระทำผิด หลอกลวง ปกปิดเท็จจริงที่ควรบอก แสดงตนเป็นบุคคลอื่นอาทิ)

๑. หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม

๒. หลอกให้ลงทุน(ที่ไม่เข้าลักษณะฉ้อโกงประชาชน)

๓. หลอกให้ลงทุน(ที่เข้าข่ายฉ้อโกงประชาชน)

๔. หลอกให้ลงทุน(ที่เข้าลักษณะแชร์ลูกโซ่)

๕. หลอกให้รักแล้วลงทุน(Hybrid Scam)

ข้อกฎหมาย : **ประมวลกฎหมายอาญา มาตรา ๓๔๓** ฉ้อโกงประชาชน ต้องระวางโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ **พ.ร.บ.คอมพิวเตอร์ฯ มาตรา ๑๔(๑)** นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชนฯ ต้องระวางโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

ข้อกฎหมาย : ความผิดในเรื่องการฉ้อโกงประชาชนโดยแสดงตนเป็นคนอื่น **ตามประมวลกฎหมายอาญา มาตรา ๓๔๒ วรรคสอง** ที่มีอัตราโทษจำคุกตั้งแต่ ๖ เดือน ถึง ๗ ปี และปรับตั้งแต่ ๑๐,๐๐๐ บาท (หนึ่งหมื่นบาท) หรือ ๑๔๐,๐๐๐ บาท (หนึ่งแสนสี่หมื่นบาท) **พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ มาตรา ๑๔** ที่ว่า “การนำเข้าซึ่งข้อมูลอันเป็นเท็จ หลอกลวง ทำให้ผู้อื่นได้รับความเสียหาย มีโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท โดยมีอายุความ ๑๐ ปี” หรืออาจมีลักษณะของการกู้เงินออนไลน์ ดอกเบี้ยเกินอัตรา

๖. หลอกให้กู้แต่ไม่ได้เงิน

ข้อกฎหมาย : **พ.ร.ก. การกู้ยืมเงิน ที่เป็นการฉ้อโกงประชาชน มาตรา ๑๒** ผู้ใดกระทำความผิดตามมาตรา ๔ หรือมาตรา ๕ ต้องระวางโทษจำคุกตั้งแต่ ๕ ปีถึง ๑๐ ปี และปรับตั้งแต่ ๕๐๐,๐๐๐ บาท ถึง ๑,๐๐๐,๐๐๐ บาท และปรับอีกไม่เกินวันละ ๑๐,๐๐๐ บาทตลอดเวลาที่ยังฝ่าฝืนอยู่ **ประมวลกฎหมายอาญา มาตรา ๓๔๓** ฉ้อโกงประชาชน ต้องระวางโทษ จำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ **พ.ร.บ.คอมพิวเตอร์ฯ มาตรา ๑๔(๑)** นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชนฯ ต้องระวางโทษจำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

กลุ่ม ๔ ใช้เทคโนโลยีกระทำให้เกิดความเสียหายต่อเสรีภาพ ชื่อเสียง ความผิดทางเพศและต่อผู้เยาว์

๑. หมิ่นประมาท ดูหมิ่น

ข้อกฎหมาย : การนินทาคนอื่นลงในไลน์กลุ่ม อาจเข้าข่ายความผิดฐานหมิ่นประมาท เพราะเป็นการใส่ความผู้อื่นต่อบุคคลที่ ๓ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง ต้องระวางโทษจำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๒ หมื่นบาท หรือ

ทั้งจำทั้งปรับ **ตามประมวลกฎหมายอาญา มาตรา ๓๒๖** การโพสต์เฟสบุ๊คด่าคนอื่น, ประจานเมียน้อย,ประจานลูกหนี้,ทวงถามหนี้ลูกหนี้ผ่านทางเฟสบุ๊ค ระบุชื่อ-นามสกุล ลงรูป โดยมีลักษณะเป็นการเผยแพร่ข้อความอันเป็นการหมิ่นประมาทออกไปยังสาธารณชน หรือประชาชนทั่วเป็นความผิดอาญา ฐานหมิ่นประมาทผู้อื่นด้วยการโฆษณา **ตามประมวลกฎหมายอาญา มาตรา ๓๒๖ และมาตรา ๓๒๘** โทษจำคุกไม่เกิน ๒ ปี และปรับไม่เกิน ๒ แสนบาท

๒. ข่มขู่หรือคุกคามทางเพศ

ข้อกฎหมาย : **ประมวลกฎหมายอาญา มาตรา ๓๙๗** กำหนดให้การรังแก ข่มเหง คุกคาม หรือกระทำให้ได้รับความอับอายหรือ เดือดร้อนรำคาญ ต้องระวางโทษปรับไม่เกิน ๕,๐๐๐ บาท

๓. หลอกลวงไปทำงานต่างประเทศ

ข้อกฎหมาย : **ประมวลกฎหมายอาญา มาตรา ๓๔๔** “ผู้ใดโดยทุจริต หลอกลวงบุคคลตั้งแต่สิบคนขึ้นไปให้ประกอบการงานอย่างใด ๆ ให้แก่ตนหรือให้แก่บุคคลที่สาม โดยจะไม่ใช้ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้น หรือโดยจะใช้ค่าแรงงานหรือค่าจ้างแก่บุคคลเหล่านั้นต่ำกว่าที่ตกลงกัน ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ประมวลกฎหมายอาญา มาตรา ๒๘๗

๑. เพื่อความประสงค์แห่งการค้า หรือโดยการค้า เพื่อการแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออกหรือยังให้ส่งออกไปนอกราชอาณาจักร พาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใด ๆ ซึ่งเอกสาร ภาพเขียน ภาพพิมพ์ ภาพระบายสี สิ่งพิมพ์ รูปภาพ ภาพโฆษณา เครื่องหมาย รูปถ่าย ภาพยนตร์ แถบบันทึกเสียง แถบบันทึกภาพหรือสิ่งอื่นใดอันลามก

๒. ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับวัตถุหรือสิ่งของลามกดังกล่าวแล้ว จ่ายแจกหรือแสดงอวดแก่ประชาชน หรือให้เช่าวัตถุหรือสิ่งของเช่นว่านั้น

๓. เพื่อจะช่วยการทำให้แพร่หลาย หรือการค้าวัตถุหรือสิ่งของลามกดังกล่าวแล้ว โฆษณาหรือไขข่าวโดยประการใด ๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณาหรือไขข่าวว่าวัตถุ หรือสิ่งของลามกดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด

จำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๖๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

ประมวลกฎหมายอาญา มาตรา ๒๘๗/๑ วรรคหนึ่ง ครอบครองสื่อลามกอนาจารเด็กเพื่อแสวงหาประโยชน์ในทางเพศสำหรับตนเองหรือผู้อื่น จำคุกไม่เกิน ๕ ปี หรือปรับไม่เกิน ๑๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

ประมวลกฎหมายอาญา มาตรา ๒๘๗/๑ วรรคสอง กระทำความผิดตามวรรคหนึ่งส่งต่อซึ่งสื่อลามกอนาจารเด็กแก่ผู้อื่น จำคุกไม่เกิน ๗ ปี หรือปรับไม่เกิน ๑๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

ประมวลกฎหมายอาญา มาตรา ๒๘๗/๒

๑. เพื่อความประสงค์แห่งการค้า หรือโดยการค้า เพื่อการแจกจ่ายหรือเพื่อการแสดงอวดแก่ประชาชน ทำ ผลิต มีไว้ นำเข้าหรือยังให้นำเข้าในราชอาณาจักร ส่งออกหรือยังให้ส่งออกไป

นอกราชอาณาจักร พาไปหรือยังให้พาไปหรือทำให้แพร่หลายโดยประการใด ๆ ซึ่งสื่อลามกอนาจารเด็ก

๒. ประกอบการค้า หรือมีส่วนหรือเข้าเกี่ยวข้องในการค้าเกี่ยวกับสื่อลามกอนาจารเด็ก จ่ายแจกหรือแสดงอวดแก่ประชาชนหรือให้เช่าสื่อลามกอนาจารเด็ก

๓. เพื่อจะช่วยการทำให้แพร่หลาย หรือการค้าสื่อลามกอนาจารเด็กแล้ว โฆษณาหรือไขข่าวโดยประการใด ๆ ว่ามีบุคคลกระทำการอันเป็นความผิดตามมาตรานี้ หรือโฆษณาหรือไขข่าวว่าสื่อลามกอนาจารเด็กดังกล่าวแล้วจะหาได้จากบุคคลใด หรือโดยวิธีใด

จำคุกตั้งแต่ ๓ ถึง ๑๐ ปี และปรับตั้งแต่ ๖๐,๐๐๐ บาทถึง ๒๐๐,๐๐๐ บาท

สาเหตุของการเกิดอาชญากรรมเทคโนโลยี

จากการศึกษางานวิจัยในอดีตที่นำทฤษฎีแรงจูงใจเพื่อสร้างภูมิคุ้มกันทางไซเบอร์มาเป็นกรอบแนวคิดในการวิจัยแล้ว นอกจากนี้ยังมีงานวิจัยที่นำทฤษฎีอื่นๆ มาใช้ในการศึกษาปัจจัยที่ส่งผลต่อการแสดงพฤติกรรมการป้องกันหรือปฏิบัติตามคำแนะนำด้านการป้องกันอาชญากรรมทางเทคโนโลยี ซึ่งสิ่งเหล่านี้เป็นปัจจัยที่เป็นสาเหตุของการเกิดอาชญากรรมทางเทคโนโลยี สามารถแยกเป็น ๒ ประเภทคือ ปัจจัยส่วนบุคคลและปัจจัยด้านสภาพแวดล้อม ดังนี้

๑. ปัจจัยส่วนบุคคล (Personal Factors)

๑.๑ บุคลิกภาพ (Personality)

บุคลิกภาพ (Personality) หมายถึง ลักษณะเฉพาะของบุคคลซึ่งเป็นสิ่งบ่งชี้ความเป็นปัจเจกบุคคล และเป็นสิ่งกำหนดลักษณะการมีปฏิสัมพันธ์กับสิ่งแวดล้อมหรือสถานการณ์ของบุคคลนั้นๆ หนึ่งในทฤษฎีเกี่ยวกับบุคลิกภาพที่ยอมรับกันอย่างแพร่หลายมากที่สุดคือ Big Five Personality Theories โดย Costa และ McCrae (Robert R. McCrae & Paul T. Costa, 1987) ได้จำแนกลักษณะของบุคลิกภาพออกเป็น ๕ ประเภทใหญ่ ภายใต้เงื่อนไขว่าคนทุกคนล้วนมีบุคลิกทั้ง ๕ แบบในระดับที่ต่างกัน บุคลิกภาพทั้ง ๕ แบบคือ บุคลิกภาพแบบเปิดเผย (Extraversion) บุคลิกภาพแบบหวั่นไหว (Neuroticism) บุคลิกภาพแบบประนีประนอม (Agreeableness) บุคลิกภาพแบบมีจิตสานึก (Conscientiousness) และบุคลิกภาพแบบเปิดรับประสบการณ์ (Openness) รายละเอียดแสดงดังตารางที่ ๑

ตารางที่ ๒-๑ คำอธิบายลักษณะบุคลิกภาพ

ประเภท	ลักษณะบุคลิกภาพ
บุคลิกภาพแบบเปิดเผย (Extraversion)	ลักษณะของบุคคลที่ถูกปลุกปั่นได้ง่าย มีความเป็นกันเอง ชอบติดต่อสื่อสารกับผู้อื่น เป็นคนช่างพูดช่างเจรจา กล้าแสดงออกในความคิดของตนเอง และแสดงออกทางอารมณ์ความรู้สึกสูง
บุคลิกภาพแบบประนีประนอม (Agreeableness)	ลักษณะของบุคคลที่มีความสุภาพเอื้อเฟื้อเผื่อแผ่ ซื่อสัตย์สุจริต มีไหวพริบ เข้าใจและเห็นใจผู้อื่น
บุคลิกภาพแบบมีจิตสำนึก (Conscientiousness)	ลักษณะของบุคคลที่มีความตั้งใจในการทำกิจกรรมต่างๆ เป็นผู้ที่มีระเบียบวินัย มีความแม่นยำ มีความรับผิดชอบ สามารถทำตามคำสั่งให้สำเร็จไปได้ด้วยดี
บุคลิกภาพแบบหวั่นไหว (Neuroticism)	บุคลิกภาพแบบหวั่นไหว คือ องค์ประกอบของบุคลิกภาพด้านอารมณ์ในการตอบสนองต่อสิ่งเร้าต่างๆ
บุคลิกภาพแบบเปิดรับประสบการณ์ (Openness)	ลักษณะของบุคคลที่มีความรอบรู้ มีสติปัญญาในการปฏิบัติงาน มีจินตนาการ มีความคิดสร้างสรรค์ ยอมรับความคิดของคนอื่น ยึดหลักความจริง ชอบศึกษาหาความรู้ใหม่ๆ มีความสนใจในเรื่องของสังคมและวัฒนธรรม

หมายเหตุ จาก Validation of the five-factor model of personality across instruments and observers

ที่มา : McCrae and Costa, 1987

งานวิจัยในอดีตได้มีการนาทฤษฎี Big Five Personality มาใช้เพื่อหาความสัมพันธ์ระหว่างบุคลิกภาพกับพฤติกรรมการปฏิบัติตามแนวทางการรักษาความปลอดภัยในโลกไซเบอร์ต่อมาได้มีการนำมาใช้ในการหาความสัมพันธ์กับพฤติกรรมการป้องกันภัย งานวิจัยของ Shropshire และคณะ (๒๐๐๖) พบว่าบุคคลที่มีบุคลิกภาพแบบมีจิตสำนึก (Conscientiousness) และแบบประนีประนอม (Agreeableness) จะมีโอกาสถูกคุกคามน้อยกว่าบุคคลที่มีบุคลิกภาพแบบหวั่นไหว (Neuroticism) บุคลิกภาพจึงเป็นจุดเริ่มต้นที่ทำให้เกิดแรงจูงใจที่แตกต่างกันของแต่ละบุคคลในการแสดงพฤติกรรมหรือไม่แสดงพฤติกรรมการป้องกันภัย(Shropshire et al., 2006) สอดคล้องกับงานวิจัยของ Warkentin และคณะ (๒๐๑๑) ซึ่งกล่าวว่าลักษณะบุคลิกภาพที่แตกต่างกันจะส่งผลต่อการรับรู้ที่แตกต่างกันด้วย ดังนั้นรูปแบบการให้ความรู้ของกลุ่มคนแต่ละประเภทจึงต้องเหมาะสมกับลักษณะของคนประเภทนั้น

๑.๒ การรับรู้คุณค่าของข้อมูล (Perceived Value of data)

งานวิจัยในอดีตได้ให้คำนิยามข้อมูลที่มีคุณค่าว่าเป็นข้อมูลที่มีความสำคัญในการดำเนินธุรกิจที่สามารถส่งผลต่อความสำเร็จหรือล้มเหลวขององค์กรได้ เช่น ข้อมูลในด้านการลงทุน ข้อมูลลับทางการค้า เป็นต้น ซึ่งมีลักษณะเป็นข้อมูลที่ล้าสมัยเร็ว และคุณค่าลดลงตามเวลา

(Moody & Walsh, 1999) คุณค่าของข้อมูลที่บุคคลรับรู้นั้นเป็นไปได้ทั้งคุณค่าทางด้านตัวเงินและคุณค่าทางด้านความรู้สึก (Malimage & Warkentin, 2011) งานวิจัยในอดีตได้ทาการศึกษาอิทธิพลของการรับรู้คุณค่าของข้อมูลของบุคคลต่อพฤติกรรมการป้องกันเมื่อเครื่องคอมพิวเตอร์ถูกคุกคาม งานวิจัยของ Chai และคณะ (๒๐๐๙) พบว่าการรับรู้ถึงคุณค่าและความสำคัญของข้อมูลที่เป็นข้อมูลส่วนตัวเป็นแรงจูงใจในการดาเนินการเพื่อป้องกันข้อมูลเหล่านั้น เช่นเดียวกับ Malimage และ Warkentin (๒๐๑๑) ที่กล่าวว่าการรับรู้คุณค่าของข้อมูลมีอิทธิพลต่อความเชื่อของบุคคลที่ว่าการใช้เทคโนโลยีป้องกันเช่น โปรแกรมแอนติไวรัส เป็นต้น สามารถหยุดยั้งผลกระทบจากการโจมตีของไวรัสคอมพิวเตอร์ได้

๑.๓ ประสบการณ์ในอดีต (Prior experience)

ทฤษฎีพฤติกรรมนิยม (Behavioral View of Motivation) ให้ความสำคัญกับประสบการณ์ในอดีตว่ามีผลต่อแรงจูงใจของบุคคลเป็นอย่างมาก ส่วนใหญ่พฤติกรรมของมนุษย์จะได้รับอิทธิพลที่เป็นแรงจูงใจมาจากประสบการณ์ในอดีต โดยประสบการณ์ด้านบวกจะกลายเป็นแรงจูงใจทางบวกที่ส่งผลเร้าให้มนุษย์มีความต้องการแสดงพฤติกรรมในทิศทางนั้นมากยิ่งขึ้น ในขณะที่ประสบการณ์ด้านลบในอดีตจะกลายเป็นแรงจูงใจทางบวกที่ส่งผลเร้าให้มนุษย์มีความต้องการแสดงพฤติกรรมในทิศทางตรงกันข้ามมากยิ่งขึ้นเช่นกัน ประสบการณ์ในอดีตจึงมีผลกระทบต่อการตัดสินใจแสดงพฤติกรรมใดๆ ในปัจจุบัน ซึ่งสอดคล้องกับงานวิจัยของ Chai และคณะ (๒๐๐๙) กล่าวว่าประสบการณ์ในอดีตเช่นการที่เครื่องคอมพิวเตอร์โดนไวรัสหรือถูกขโมยข้อมูลส่วนตัว เป็นปัจจัยทีมีอิทธิพลต่อแรงจูงใจในการป้องกันภัยมากขึ้นเพราะมีความกังวลและไม่ต้องการถูกคุกคามอีกในอนาคต

๒. ปัจจัยด้านสภาพแวดล้อม (Environmental Factors)

๒.๑ การคล้อยตามกลุ่มอ้างอิง (Subjective Norm)

การคล้อยตามกลุ่มอ้างอิงหรือบุคคลรอบข้าง เป็นเสมือนแรงกดดันหรือแรงกระตุ้นทางสังคม (Bulgurcu, Cavusoglu, & Benbasat, 2010) การแสดงพฤติกรรมของกลุ่มอ้างอิงจะมีอิทธิพลหรือกระตุ้นให้บุคคลคล้อยตามและแสดงพฤติกรรมเช่นเดียวกันนั้นออกมา (Johnston & Warkentin, 2010) ซึ่งส่วนใหญ่เกิดจากการชักชวนด้วยวาจา (Pahnila et al., 2007) การให้คำปรึกษาหรือสังเกตจากพฤติกรรมของบุคคลอื่น (M. T. Siponen, Pahnila, & Mahmood, 2010) โดยกลุ่มอ้างอิงอาจเป็นคนใกล้ตัว เช่น เพื่อนร่วมงาน ผู้บังคับบัญชา เพื่อนสนิท หรือคนในครอบครัว เป็นต้น กลุ่มอ้างอิงจะมีอิทธิพลต่อการกระทำพฤติกรรมมากหรือน้อยขึ้นอยู่กับความสำคัญของบุคคลนั้นๆ (Ajzen, 1991)

๒.๒ ความรู้เกี่ยวกับการรักษาความปลอดภัย (Security Knowledge)

ปัญหาสำคัญที่ทำให้เกิดภัยคุกคามจากอาชญากรรมคอมพิวเตอร์ในประเทศกำลังพัฒนา คือการขาดความรู้ ขาดทักษะในการรักษาความปลอดภัย และขาดความชำนาญในการใช้ภาษาอังกฤษ เนื่องจากคำแนะนา คู่มือการใช้งานและเนื้อหาอื่นๆ สำหรับการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศส่วนใหญ่เป็นภาษาอังกฤษ ทำให้เกิดการละเลยและปฏิเสธที่จะเรียนรู้แนวทางการป้องกันภัยนั้นด้วยตนเอง (Kshetri, 2010) การให้ความรู้และความเข้าใจถึงภัยจากอาชญากรรมคอมพิวเตอร์และมาตรการป้องกันที่มีประสิทธิภาพ โดยเน้นให้เห็นโอกาส

เสี่ยงของการเกิดภัยคุกคามและความรุนแรงของการสูญเสียที่เกิดจากภัยคุกคาม (D'Arcy, Hovav, & Galletta, 2009; H. Liang & Y. Xue, 2010) เป็นปัจจัยสำคัญในการสร้างแรงจูงใจในการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ ซึ่งจะทาให้การจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ (Bulgurcu, Cavusoglu, & Benbasat, 2009) วิธีการให้ความรู้นั้นไม่ใช่เพียงการฝึกอบรมเท่านั้น แต่ยังรวมถึงการรณรงค์ การโฆษณา การพูดคุยอย่างเป็นทางการหรือไม่เป็นทางการ และการให้ความรู้ผ่านสื่อต่างๆ (M. Siponen, Pahnila, & Mahmood, 2006) นอกจากนี้การรายงานเหตุละเมิดจากภัยคุกคามที่เกิดขึ้นก็เป็นอีกวิธีที่ได้ผล (M. T. Siponen et al., 2010) เช่นเดียวกับที่ Boon-Yuen และคณะ (๒๐๐๙) ได้กล่าวไว้ว่า หลักสูตรการฝึกอบรมการให้ความรู้ผ่านสื่อหรือคำแนะนำจากผู้เชี่ยวชาญเป็นสิ่งกระตุ้นให้เกิดแรงจูงใจและแสดงพฤติกรรมการรักษาความปลอดภัยคอมพิวเตอร์

องค์กรต้องมีกลยุทธ์ในการฝึกอบรมและให้ความรู้ที่เหมาะสมกับพนักงานแต่ละกลุ่มไม่ว่าจะเป็นกลุ่มผู้บริหารระดับสูง กลุ่มผู้บริหารระดับกลาง และพนักงาน สำหรับพนักงานยังสามารถแบ่งได้เป็นพนักงานที่มีทักษะด้านเทคโนโลยีสารสนเทศ (IT People) กับพนักงานที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (Non-IT People) กลยุทธ์ในการจัดโปรแกรมฝึกอบรมแก่พนักงานแต่ละกลุ่มต้องแตกต่างกัน (M. T. Siponen et al., 2010) เนื่องจากจะมีพื้นฐานความรู้และความเชี่ยวชาญด้านคอมพิวเตอร์ที่แตกต่างกัน การฝึกอบรมนั้นไม่เพียงสอนให้ผู้ใช้คอมพิวเตอร์มีความเข้าใจถึงวิธีการใช้งานและวิธีป้องกันที่ถูกต้องเท่านั้น แต่ยังต้องเน้นในเรื่องของการสร้างจิตสำนึกและการตระหนักในการป้องกันภัยจากการใช้งานคอมพิวเตอร์ด้วย จึงจะสามารถจูงใจให้ผู้ใช้คอมพิวเตอร์แสดงพฤติกรรมการป้องกันได้ (Lu & Jen, 2010)

๒.๓ ค่าใช้จ่ายในการป้องกัน (Safeguard cost)

ความพยายามหรือค่าใช้จ่ายที่ต้องเสียไปเป็นข้อจำกัดต่อการแสดงพฤติกรรมและลดแรงจูงใจในการแสดงพฤติกรรม เนื่องจากโดยปกติบุคคลจะเปรียบเทียบค่าใช้จ่ายที่ต้องเสียไปกับผลประโยชน์ที่ได้รับก่อนที่จะตัดสินใจกระทำหรือไม่กระทำพฤติกรรมใด (H. Liang & Y. Xue, 2010) ถ้าประเมินแล้วว่าค่าใช้จ่ายที่ต้องเสียเพื่อดำเนินการป้องกันสูงเกินไปบุคคลนั้นก็เลือกที่จะยอมรับความเสี่ยง และไม่กระทำการป้องกันใดๆ ในทำนองเดียวกันถ้าค่าใช้จ่ายไม่สูงเกินไปแต่การป้องกันนั้นมีประสิทธิภาพ บุคคลนั้นก็จะตัดสินใจดำเนินการป้องกัน (LaRose, Rifon, Liu, & Lee, 2005; Woon et al., 2005)

๒.๔ การรับรู้ต่อสภาวะคุกคาม (Threat appraisal)

กระบวนการรับรู้ต่อสภาวะคุกคามเกิดจากการ ๒ องค์ประกอบสำคัญคือการรับรู้โอกาสเสี่ยงของการถูกคุกคาม (Perceived Vulnerability) และการรับรู้ความรุนแรงของภัยคุกคาม(Perceived Severity) ซึ่งการรับรู้ความรุนแรงของภัย (Perceived Severity) (R. W. Rogers, ๑๙๘๓) นั้นหมายถึงความเชื่อมั่นของบุคคลต่อความรุนแรงจากการที่ไม่มีการป้องกันความเสียหายที่จะเกิดขึ้น โดยเฉพาะอย่างยิ่งความเสียหายที่เกิดขึ้นกับข้อมูลเช่น การสูญเสียข้อมูลอันเป็นความลับข้อมูลขาดความสมบูรณ์และไม่พร้อมใช้งาน เป็นต้น ซึ่งส่งผลกระทบต่อองค์กรและพนักงานให้ไม่สามารถปฏิบัติงานได้อย่างต่อเนื่อง งานวิจัยของ Boon-Yuen และคณะ (๒๐๐๙) ได้ทำการศึกษาปัจจัยที่ส่งผลให้พนักงานแสดงพฤติกรรมการป้องกันภัย พบว่าพนักงานมีการรับรู้ความ

รุนแรงและความเสียหายที่จะเกิดจากการถูกคุกคามในระดับที่แตกต่างกัน ถ้ารับรู้ความรุนแรงมากก็จะรู้สึกกลัวและวิตกกังวลต่อความเสียหายที่จะเกิดขึ้นซึ่งเป็นเหตุให้บุคคลนั้นแสดงพฤติกรรมการป้องกันภัยมากยิ่งขึ้น ส่วนการรับรู้โอกาสเสี่ยงของการถูกคุกคามมาจากแบบแผนความเชื่อด้านสุขภาพ (Health Belief Model) หมายถึงความเชื่อของบุคคลที่มีผลโดยตรงต่อคาแนะนาในการป้องกันภัย บุคคลจะมีการรับรู้โอกาสเสี่ยงของการถูกคุกคามที่แตกต่างกันแม้ว่าจะได้รับข้อมูลที่เหมือนกันก็ตาม ซึ่งจะส่งผลต่อพฤติกรรมการป้องกันภัยที่แตกต่างกันตามไปด้วย (Ng et al., ๒๐๐๙) สามารถสรุปได้ว่าการให้ข้อมูลเกี่ยวกับความน่าจะเป็นของการถูกคุกคามส่งผลให้บางคนรับรู้ว่ามีความเสี่ยงสูงที่จะถูกคุกคามในขณะที่บางคนรับรู้ว่าโอกาสเสี่ยงนั้นจะไม่มีทางเกิดขึ้น บุคคลจะประเมินความเป็นไปได้ที่ตนเองจะถูกคุกคามประกอบกับประเมินว่าภัยนั้นมีความรุนแรงมากน้อยเพียงใดรวมทั้งคาดคะเนโอกาสที่จะเกิดซ้ำ ดังนั้นแต่ละบุคคลจะมีความเชื่อมั่นต่อภาวการณ์เกิดภัยคุกคามในระดับที่แตกต่างกัน

๒.๕ การรับรู้ความสามารถในการจัดการกับภัยคุกคาม (Coping appraisal)

กระบวนการรับรู้ความสามารถในการจัดการกับภัยคุกคามประกอบไปด้วยประสิทธิภาพในการตอบสนอง (Response Efficacy) และ การรับรู้ความสามารถของตนเอง (Self-Efficacy) (R. W. Rogers, 1983) การรับรู้ความสามารถในการจัดการกับภัยคุกคามเกิดขึ้นเมื่อบุคคลนั้นได้ประเมินประสิทธิภาพในการตอบสนองซึ่งเป็นความเชื่อมั่นของบุคคลต่อประสิทธิภาพของวิธีการหรือมาตรการในการป้องกันภัยที่ได้รับการแนะนำรวมกับการประเมินความความสามารถของตนเองที่จะกระทำตามมาตรการนั้น เช่น การติดตั้งโปรแกรม Antivirus หรือการปิดการใช้งาน cookie บนเว็บบราวเซอร์ เป็นต้น เมื่อรับรู้ความสามารถในการจัดการกับภัยคุกคามแล้ว ก็จะส่งผลต่อการแสดงพฤติกรรมการป้องกัน งานวิจัยหลายงานในอดีตได้ทาการพิสูจน์แล้วว่า บุคคลจะมีแรงจูงใจในการดำเนินการป้องกันภัยเพิ่มมากขึ้นถ้าระดับความเชื่อมั่นต่อประสิทธิภาพในการตอบสนองและความเชื่อมั่นในตนเองเพิ่มสูงขึ้น (H. Liang & Y. Xue, 2010; Ng et al., 2009; Woon et al., 2005; Workman et al., 2008)

๒.๖ แรงจูงในในการป้องกัน (Protection Motivation)

ทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory) กล่าวว่าแรงจูงใจเกิดจากการเรียนรู้ทางสังคมและเป็นปัจจัยสำคัญในการทำนายการแสดงพฤติกรรมของบุคคล (Ajzen, 1991) แรงจูงใจเป็นตัวพยากรณ์ที่ดีในการทำนายพฤติกรรมที่จะแสดงออกมาจริงๆ ของบุคคล (M.Siponen et al., 2006) กล่าวคือ เมื่อมีปัจจัยที่มีอิทธิพลให้บุคคลเกิดแรงจูงใจในการป้องกันภัยเพิ่มมากขึ้น พฤติกรรมการป้องกันภัยที่แสดงออกมาก็จะเพิ่มมากขึ้นเช่นเดียวกัน (Bulgurcu et al., 2009; H. Liang & Y. Xue, 2010; Ng et al., 2009)

๒.๗ พฤติกรรมการป้องกันภัย (Protection Behavior)

งานวิจัยของ Siponen และคณะ (๒๐๐๖) พบว่าการที่บุคคลจะแสดงพฤติกรรมการป้องกันภัยนั้น ต้องได้นั้นเกิดจากปัจจัยต่างๆ ทั้งส่วนบุคคลเองเช่น ทัศนคติ ทัศนวิสัย และปัจจัยจากภายนอกที่ส่งเสริมให้บุคคลนั้นเกิดกระบวนการเรียนรู้และวิเคราะห์ว่าจะแสดงพฤติกรรมใดออกมา เช่น แรงกระตุ้นจากหัวหน้างาน การให้การอบรม หรือคู่มือเกี่ยวกับการรักษาความปลอดภัยเป็นต้น

แนวภูมิคุ้มกันทางไซเบอร์และการป้องกันอาชญากรรมทางเทคโนโลยี

ภูมิคุ้มกันภัยไซเบอร์ (Cyber Immunity) ภูมิคุ้มกันภัยไซเบอร์ของประชาชนที่เข้มแข็งจะเป็นพลังสำคัญสำหรับการรักษาความมั่นคงของชาติในอนาคต ภูมิคุ้มกันภัยไซเบอร์ เป็นแนวคิดที่ประยุกต์มาจากภูมิคุ้มกันในร่างกายมนุษย์ เป็นกลไกตามธรรมชาติของร่างกายที่ทำหน้าที่ป้องกันหรือต่อต้านไม่ให้เชื้อโรคเข้าสู่ร่างกาย และพัฒนาร่างกายให้รับรู้ในการป้องกันและต่อสู้กับโรคร้ายที่มีลักษณะใกล้เคียงกัน โดยไม่จำเป็นต้องได้รับเชื้อโรคนั้นมาก่อนก็ได้ เช่นเดียวกันภัยคุกคามทางด้านไซเบอร์ที่เปลี่ยนแปลงรูปแบบและวิธีการโดยตลอด หากประชาชนมีภูมิคุ้มกันภัยไซเบอร์ที่ดีก็จะเป็นรากฐานความปลอดภัยของสังคมและประเทศชาติ

การสร้างภูมิคุ้มกันภัยไซเบอร์ที่สำคัญเริ่มจากความตระหนักรู้ของประชาชนถึงภัยคุกคามทางไซเบอร์ การมีกระบวนการทางกฎหมายที่เหมาะสม มีนโยบายและมาตรการที่ช่วยสร้างสภาพแวดล้อมที่ดีของประเทศในด้านความมั่นคงทางไซเบอร์ในทุกระดับ และการใช้เทคโนโลยีที่เหมาะสมกับประเทศ ในหัวข้อนี้จะทำการศึกษาถึงภูมิคุ้มภัยไซเบอร์ของประชาชนที่ได้จากการปฏิบัติงานของสำนักงานตำรวจแห่งชาติ และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ผู้วิจัยเล็งเห็นถึงความสำคัญที่ว่า ภูมิคุ้มกันภัยไซเบอร์ของประชาชนของชาติจะนำไปสู่การพัฒนาศักยภาพประเทศ เพื่อเตรียมความพร้อมเผชิญภัยคุกคามทางไซเบอร์ที่จะเป็นปัญหาความมั่นคงแห่งชาติที่สำคัญในอนาคตภูมิคุ้มกันทางไซเบอร์กับความมั่นคงของชาติจึงเป็นเรื่องที่สอดคล้องกับเหมาะสมกับสถานการณ์ปัจจุบัน และเป็นเรื่องที่จะมีความท้าทายมากขึ้นอย่างยิ่งในอนาคตอันใกล้ แต่ปัจจุบัน ยังไม่มีการศึกษาในเรื่องนี้อย่างเพียงพอ ความรู้ความเข้าใจเกี่ยวกับภูมิคุ้มกันทางไซเบอร์ และความสัมพันธ์กับความมั่นคงไซเบอร์ของประเทศชาตินี้ จะนำไปสู่การกำหนดแนวทาง และมาตรการที่เหมาะสมเพื่อป้องกันและพัฒนาความมั่นคงของชาติได้อย่างเหมาะสมกับสถานการณ์ในอนาคต

งานวิจัยที่เกี่ยวข้อง

ณรงค์ กุลนิเทศ (๒๕๕๘) ทำการวิจัยเรื่อง “รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์” โดยมีวัตถุประสงค์เพื่อ ๑. ศึกษาสภาพปัญหาอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย ๒. ศึกษากฎหมายที่เกี่ยวข้องกับ อาชญากรรมไซเบอร์ รวมทั้ง ระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ และ ๓. เพื่อสร้างรูปแบบและมาตรการในการแกปัญหาอาชญากรรมไซเบอร์ เป็นการวิจัยเชิงคุณภาพ (Qualitative Methodology) โดยใช้การประชุมกลุ่มย่อย (Focus Group) ผลการวิจัยพบว่า ๑. สภาพปัญหาของอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทย สามารถแบ่งประเด็นสำคัญออกได้เป็น ๑. ปัญหาด้านข้อกฎหมาย ฐานความผิด เขตอำนาจ ใครต้องเป็นผู้รับผิดชอบ ลักษณะพยาน ๒. ปัญหาด้านเทคนิค เทคนิคพัฒนาต่อเนื่อง การศึกษา เทคนิคในการเก็บหลักฐาน ๓. แนวทางการปฏิบัติ การประสานงานแนวทางปฏิบัติระหว่าง ตำรวจ อัยการ ศาล ๔. วัฒนธรรมที่แตกต่างกันในแต่ละประเทศ ๒. กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ที่สำคัญ เช่น พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชบัญญัติว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และกฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์

เป็นต้น และกำหนดกฎของระบบการพิสูจน์หลักฐานอาชญากรรมไซเบอร์ ๔ ข้อ ได้แก่ ๑. ความสมบูรณ์ของหลักฐาน ๒. ระบุที่มาของหลักฐานได้ ๓. บุคคลที่ดูแล หรือเก็บหลักฐานต้องเป็นผู้เชี่ยวชาญ และ ๔. หลักฐานต้องได้รับการตรวจสอบด้วยกระบวนการทางกฎหมาย ๓. รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์ที่สำคัญ คือ การนาส่งวัตถุพยานในการตรวจพิสูจน์ทางอาชญากรรมไซเบอร์ เช่น อย่าเปิดเครื่องอุปกรณ์ถ้า หากว่าเครื่องปิดอยู่ เป็นต้น ด้านมาตรการในการแก้ไขปัญหาอาชญากรรมไซเบอร์ เช่น ควรเร่งการออกกฎหมายให้ครอบคลุม การกระทำความผิดมากขึ้น เป็นต้น

ยุทธศักดิ์ เทียมทัศน์ (๒๕๕๘) ทำการวิจัยเรื่อง “การแบ่งปันความรู้งานสืบสวนอาชญากรรมทางเทคโนโลยี” โดยมีวัตถุประสงค์ ๑. เพื่อต้องการแบ่งปันและแลกเปลี่ยนความรู้ให้ทั่วถึงทั้งองค์กร ๒. เพื่อรวบรวมความรู้ในเรื่องการสืบสวนคดีอาชญากรรมทางเทคโนโลยี ไว้เป็นหมวดหมู่เพื่อสะดวกในการสืบค้น และการเข้าถึงข้อมูล ๓. เพื่อจัดทำและออกแบบระบบ แบ่งปันความรู้ในการสืบสวนคดีอาชญากรรมทางเทคโนโลยี ๔. เพื่อถ่ายทอดความรู้ในการสืบสวนคดีอาชญากรรมทางเทคโนโลยีในรูปแบบสื่อต่างๆ ที่ทำให้ผู้ใช้สามารถเข้าใจง่ายและสะดวกในการเข้ามาเรียนรู้เป็นการวิจัยเชิงคุณภาพ ใช้การจัดการเนื้อหาองค์ความรู้ที่จำเป็นและนำเทคโนโลยีสารสนเทศเข้ามาใช้โดยนาเสนอผ่านเว็บไซต์

ผลการวิจัยพบว่า ผลการทดลองใช้งานระบบแบ่งปันความรู้งานสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี มีสมาชิกของระบบได้เข้ามาใช้งาน ค้นคว้าหาข้อมูลในระบบ เป็นจานวนมากขึ้น ซึ่งจะส่งผลให้องค์ ความรู้ที่มีอยู่ในองค์กรนั้น ถูกเผยแพร่ออกไปและสมาชิกที่เข้ามาค้นคว้าหาความรู้ในระบบก็จะได้องค์ความรู้นั้นติดตัวไป เพื่อใช้ในการปฏิบัติหน้าที่ ให้เกิดประโยชน์ ต่องานที่ทาต่อไป

กองวิจัยสานกับงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ (๒๕๕๙, บทสรุปผู้บริหาร) ทำการวิจัยเรื่อง “การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์” โดยมีวัตถุประสงค์เพื่อ ๑. ศึกษาวิเคราะห์ขบวนการบริหารงาน สืบสวนและสอบสวนคดีอาญาที่เกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ ๒. จัดทำรายงานผลการศึกษา และข้อเสนอแนะเชิงยุทธศาสตร์การพัฒนากระบวนการบริหารสืบสวนสอบสวนเกี่ยวกับคดีอาชญากรรมคอมพิวเตอร์ เป็นการวิจัยแบบผสม (Mix Method) ระหว่างการวิจัยเชิงปริมาณ (Quantitative Research) และเชิงคุณภาพ (Qualitative Method)

ผลการวิจัย พบว่า ๑. ความรู้ด้านเทคนิคการสืบสวนของผู้ปฏิบัติงาน ๑.๑ ด้านการสอบสวน พบว่า โดยรวมอยู่ในระดับน้อย โดยในประเด็นที่เข้าใจในความหมายของสิ่งต่าง ๆ และสิ่งที่ควรรู้ เกี่ยวกับคอมพิวเตอร์ เช่น Hosting, ISP, Protocol, Log File, FTP มีค่าเฉลี่ยน้อยที่สุด ถือว่าเป็น ปัญหาสำคัญ ๑.๒ ด้านการสืบสวน พบว่า โดยรวมอยู่ในระดับน้อย โดยในประเด็นเข้าใจความหมาย ของสิ่งต่าง ๆ และสิ่งที่ควรรู้เกี่ยวกับคอมพิวเตอร์ มีค่าเฉลี่ยน้อยที่สุด ถือว่าเป็นปัญหาสำคัญ เช่นเดียวกับ การสอบสวน ๒. การรวบรวมพยานหลักฐาน ๒.๑ ด้านการสอบสวน พบว่า โดยรวมอยู่ ในระดับน้อย ๒.๒ ด้านการสืบสวน พบว่า โดยรวมอยู่ในระดับน้อย

Heinl (2013) ทำการศึกษาเรื่องความปลอดภัยทางไซเบอร์ของภูมิภาค กรณีศึกษาการจัดการเพื่อคงไว้ซึ่งความปลอดภัยไซเบอร์ของอาเซียน โดยงานวิจัยนี้ทำการศึกษาถึงความร่วมมือระดับภูมิภาคของประชาคมอาเซียน ในการจัดการกับภัยคุกคามไซเบอร์ร้ายแรงข้ามชาติ ซึ่งเป็นปัญหาที่จำเป็นแก่การจัดการและพิจารณาอย่างเร่งด่วนถึงความครอบคลุมของการคงไว้ซึ่งความปลอดภัยทางไซเบอร์ภายในภูมิภาคอาเซียน นอกจากนั้นยังทำการตรวจหาช่องโหว่ด้านการจัดการ เพื่อให้คำแนะนำที่เป็นประโยชน์ต่อการพัฒนาในอนาคต ผลจากการศึกษาผู้วิจัยได้ให้คำแนะนำไว้ ดังนี้ ๑. การจัดตั้งกลไกการประสานงานถาวรขึ้น เพื่อให้เกิดความร่วมมือและการแลกเปลี่ยนข้อมูลสารสนเทศ ๒. การจัดตั้งศูนย์ประสานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของอาเซียน (ASEANCERT) เพื่อเป็นการสนับสนุนและทำให้เกิดความร่วมมือกันระหว่างศูนย์ประสานความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ของแต่ละประเทศได้ดียิ่งขึ้น ๓. เพิ่มความเชื่อมั่นด้านความปลอดภัยของสำนัก เลขาธิการของอาเซียน ๔. การจัดตั้งศูนย์กลางผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ประจำภูมิภาค เพื่อการจัดการฝึกอบรมและการพัฒนาประสิทธิภาพให้เพิ่มขึ้น ๕. สร้างความมั่นคงทางความปลอดภัยของภูมิภาคตามมาตรฐานสากล เป็นการสร้างโซนปลอดภัยในการใช้งานทางไซเบอร์ ๖. เพิ่มการตระหนักให้กับประชาชนเรื่องการป้องกันภัยทางไซเบอร์ ๗. ผลักดันการประสานงานและการบังคับใช้กฎหมายของแต่ละประเทศให้มีความสอดคล้องและเชื่อมโยงกันกับภัยคุกคามทางไซเบอร์ ๘. ลงความเห็นร่วมกันในการรับผิดชอบต่อพฤติกรรมของแต่ละรัฐและยอมรับการใช้งาน กฎหมายระหว่างประเทศ ๙.ผลักดันสู่ความร่วมมือความปลอดภัยทางไซเบอร์ในระดับโลกต่อไปจากการศึกษาพบว่าการสร้างความร่วมมือด้านไซเบอร์จำเป็นต้องคำนึงถึงผลประโยชน์ของประเทศ สมาชิกแต่ละประเทศเป็นหลัก ซึ่งการสนับสนุนจุดมุ่งหมายของอาเซียนในการสร้างตลาดร่วมให้ประสบผลสำเร็จจะช่วยเพิ่มอำนาจในการต่อรองให้เกิดขึ้นภายในกลุ่มเอเชียแปซิฟิกได้อีกด้วย จาก การประชุมอาเซียนครั้งที่ ๒๒ ใน พ.ศ. ๒๕๕๗ ซึ่งมุ่งเน้นการเตรียมความพร้อมเข้าสู่ประชาคมเศรษฐกิจอาเซียนที่กำหนดไว้ใน พ.ศ. ๒๕๕๘ ซึ่งได้รวมเอายุทธศาสตร์ด้านการสนับสนุนความปลอดภัยทางไซเบอร์ของปัจจุบันและอนาคต โดยการสร้างความร่วมมือระหว่างประเทศร่วมกับการจัดการ ภายในประเทศ เพื่อให้สามารถจัดการกับปัญหาความปลอดภัยทางไซเบอร์ข้ามชาติได้อย่างมี ประสิทธิภาพ ซึ่งรัฐบาลและองค์กรต่างๆ ภายในประเทศจำเป็นอย่างยิ่งในการปรับตัวเพื่อรองรับ การร่วมมือกันที่จะเกิดขึ้นในอนาคต

Adelson et al. (2014) ทำการศึกษาถึงความร่วมมือทางความปลอดภัยไซเบอร์ระหว่าง ประเทศจีนและสหรัฐอเมริกา เนื่องจากความมั่นคงทางไซเบอร์เป็นประเด็นปัญหาระหว่างประเทศจีน และสหรัฐอเมริกามาเป็นเวลานาน จึงทำให้เกิดการดำเนินงานในการร่วมกันวางยุทธศาสตร์ด้านความ มั่นคงปลอดภัยทางไซเบอร์เพื่อรักษาผลประโยชน์ของทั้งสองประเทศ ทั้งจีนและสหรัฐอเมริกาต่าง เป็นประเทศมหาอำนาจที่มีการลงทุนจำนวนมหาศาลไปกับระบบทางการค้าขายแลกเปลี่ยน และระบบการเงินทั้งของภายในประเทศ และระบบอื่นๆ ทั่วโลก ซึ่งระบบต่างๆ เหล่านี้ มีการใช้งานที่ต้อง เชื่อมต่อกับโครงข่ายไซเบอร์ และกลายเป็นโครงสร้างพื้นฐานวิกฤตที่แต่ละรัฐต้องให้ความสำคัญ การป้องกันความมั่งคงปลอดภัยทางไซเบอร์จึงจำเป็นต้องอาศัยการแลกเปลี่ยนข้อมูลด้านภัยคุกคาม และการพัฒนาศักยภาพในการจัดการรักษาความปลอดภัยทางไซเบอร์ร่วมกัน งานวิจัยนี้ได้กล่าวถึง การสร้างความร่วมมือโดย ทำการศึกษา

ถึงพื้นฐานของทั้งสองประเทศ โดยเริ่มจากการทำความเข้าใจ ถึงมุมมองด้านความปลอดภัยทางไซเบอร์ และสิ่งที่ประเทศให้ความสำคัญเป็นอันดับต้นๆ ไปจนถึงตัว แสดงหลักที่มีความสำคัญในการดูแลด้านความปลอดภัยทางไซเบอร์ อย่าง CNCERT ของประเทศจีน โดยโครงสร้างพื้นฐานวิกฤติของทั้งสองประเทศที่มีความจำเป็นต้องอาศัยความร่วมมือเป็นพิเศษ ประกอบด้วย ระบบสถาบันทางการเงิน การรักษาความปลอดภัยท่าเรือการค้า และระบบพลังงานนิวเคลียร์เพื่อประชาชน ซึ่งส่วนต่างๆเหล่านี้เองที่เป็นตัวกำหนดให้ทั้งประเทศจีน และสหรัฐอเมริกา ต้องร่วมมือกันทางด้านความปลอดภัยทางไซเบอร์โดยความร่วมมือนั้นจะตั้งอยู่บนพื้นฐานของ ผลประโยชน์ที่สองประเทศจะได้รับร่วมกัน กระบวนการสร้างความร่วมมือด้านความปลอดภัยทางไซ เบอร์ ผ่านการแลกเปลี่ยนข้อมูลเพื่อร่วมกันป้องกันภัยจากบุคคลหรือประเทศที่สาม การสร้างขอบเขตของความร่วมมือ การร่วมกันฝึกฝนการปฏิบัติงานจากหลายฝ่าย และการแลกเปลี่ยนความรู้เกี่ยวกับวิธีปฏิบัติที่ถูกต้องในการจัดการกับภัยคุกคามทางไซเบอร์

Olusola (2013) การศึกษาผลกระทบของอาชญากรรมทางไซเบอร์ ที่มีต่อเศรษฐกิจของประเทศไนจีเรีย โดยมีวัตถุประสงค์งานวิจัยเพื่อให้ทราบถึงการตระหนักรู้ของบุคคลถึงปรากฏการณ์ที่เกิดขึ้นในประเทศไนจีเรียและผลกระทบของอาชญากรรมนี้ต่อเศรษฐกิจ เพื่อสร้างการรับรู้ถึงอาชญากรรมสายพันธุ์ใหม่ชนิดนี้ให้กับชาวไนจีเรีย รัฐบาล และองค์กรต่างๆ จากการศึกษาสามารถ แยกประเภทของอาชญากรรมทางไซเบอร์ได้เป็น ๓ ประเภท คือ อาชญากรรมที่ส่งผลกระทบต่อบุคคลส่งผลกระทบต่อองค์กรทั้งทางธุรกิจและองค์กรอื่นๆ และผลกระทบต่อรัฐบาล โดยมีการใช้ข้อมูลการศึกษาผลกระทบของอาชญากรรมทางไซเบอร์ต่อเศรษฐกิจของประเทศเยอรมันมาเป็น ตัวอย่างเพื่อให้ทราบถึงความสูญเสียที่ตีค่าออกมาเป็นมูลค่าเงินดอลล่าห์ ผู้วิจัยได้ใช้การวิจัยโดย การตั้งคำถามกับกลุ่มตัวอย่าง เพื่อให้ทราบความคิดเห็นว่าอาชญากรรมทางไซเบอร์ส่งผลต่อเศรษฐกิจของประเทศหรือไม่ จากผลการวิจัยทำให้ทราบว่า อาชญากรรมทางไซเบอร์เป็นภัยคุกคามต่อเศรษฐกิจของประเทศ และนอกจากนั้นยังเป็นภัยต่อความสงบสุขและความมั่นคงของชาติ และได้ทำการเสนอแนะให้มีการจัดตั้งตำรวจไซเบอร์ cyber police ซึ่งเป็นพนักงานที่ได้รับการฝึกฝนมาเป็นพิเศษเพื่อการจัดการกับอาชญากรรมทางไซเบอร์ในประเทศ นอกจากนั้น เจ้าหน้าที่ตำรวจสมควรมีการจัดตั้งศูนย์กลางด้านอาชญากรรมคอมพิวเตอร์ เพื่อเป็นศูนย์กลางในการให้คำแนะนำกับรัฐและหน่วยงานอื่น เพื่อความร่วมมือด้านการสืบสวนอาชญากรรมคอมพิวเตอร์ นอกจากในส่วนของเจ้าหน้าที่ตำรวจแล้ว รัฐบาลสมควรมีการจัดตั้งศูนย์แหล่งข้อมูลอาชญากรรมคอมพิวเตอร์แห่งชาติ มีหน้าที่ในการออกนโยบาย กฎระเบียบข้อบังคับ และมาตรฐานให้กับประชาชนและองค์กรต่างๆ สุดท้ายคือการก่อตั้งหน่วยงานที่ทำหน้าที่ในการตรวจพิสูจน์หลักฐานพยานทางคอมพิวเตอร์ เพื่อรับหน้าที่ในการตรวจสอบและบังคับใช้กฎหมาย

Saini (2012) การศึกษาทบทวนประเภทของอาชญากรรมทางไซเบอร์และผลกระทบ มีวัตถุประสงค์เพื่อทำความเข้าใจอาชญากรรมทางไซเบอร์และผลกระทบต่อสังคมในด้านต่างๆ รวมถึง การคาดการณ์ถึงแนวทางของอาชญากรรมทางไซเบอร์ในอนาคต งานวิจัยนี้ได้แบ่งผลกระทบของอาชญากรรมทางไซเบอร์ออกเป็น ๔ ด้าน ดังนี้

๑. ผลกระทบทางเศรษฐกิจ ความเจริญก้าวหน้าทางเศรษฐกิจนำมาซึ่งการเพิ่มขึ้นของการใช้งานเครือข่ายอินเทอร์เน็ต อย่างเช่น การซื้อขายหุ้น การทำธุรกรรมของธนาคาร การซื้อสินค้าโดยใช้บัตรเครดิต เป็นต้น อาชญากรรมทางไซเบอร์ที่เกิดขึ้นจากการโจมตีธุรกรรมที่เกี่ยวข้องทางการเงินเหล่านี้ส่งผลกระทบต่อองค์กรและเศรษฐกิจ การทำงานที่ล่าช้าของระบบต่างๆ ที่เป็นผลมาจากการถูกโจมตีจนทำให้เกิดความล่าช้าในการปฏิบัติงาน ก็เป็นความสูญเสียขององค์กรในรูปแบบหนึ่ง ผู้ใช้งานที่ต้องการใช้งานผ่านระบบอย่างการซื้อของออนไลน์ เกิดความไม่มั่นใจในระบบการจ่ายเงิน e–commerce ก็เป็นอีกสาเหตุที่ทำให้องค์กรสูญเสียรายได้

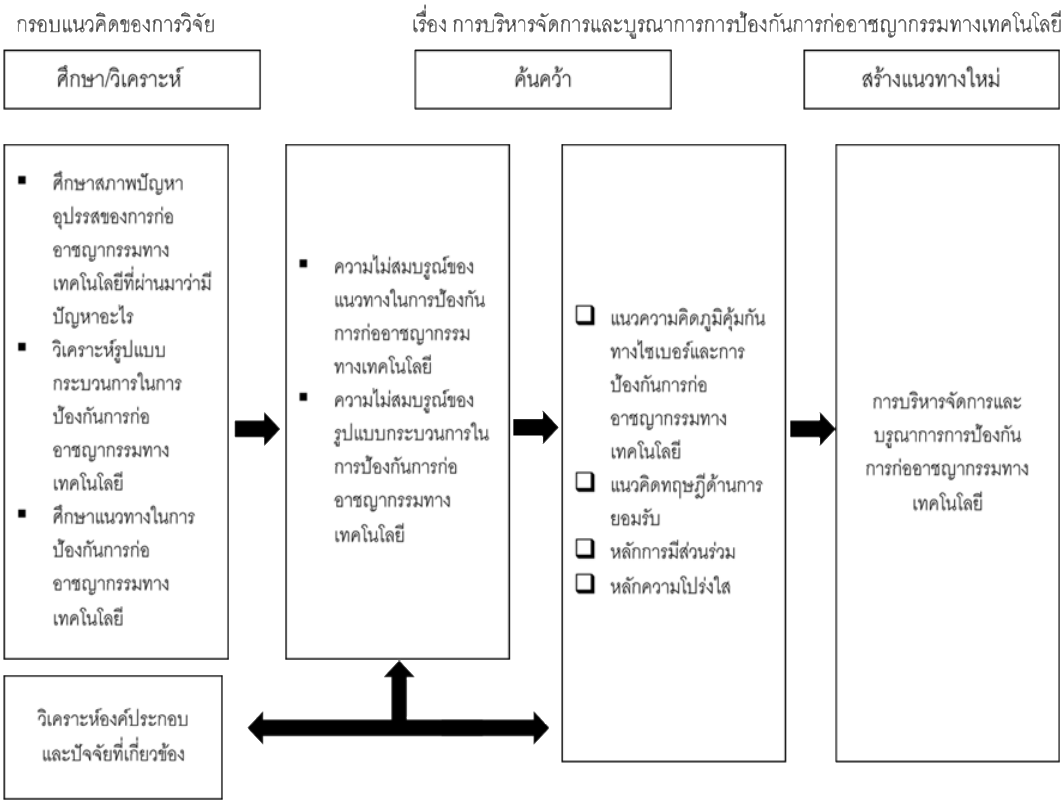
๒. ผลกระทบด้านการตลาด การจัดการระบบสารสนเทศขององค์กรที่มักมีช่องโหว่และถูกโจมตีได้ง่าย เนื่องจากไม่มีการจัดการรักษาความปลอดภัยระบบสารสนเทศได้ดีพอ บริษัทต่างๆ ประสบปัญหาด้านการเปิดเผยข้อมูลขององค์กร รวมถึงข้อมูลของการถูกโจมตี เพราะกลัวว่าข้อมูลที่ถูกเปิดเผยสู่สาธารณะจะส่งผลกระทบต่อภาพลักษณ์ของบริษัท ซึ่งภาพลักษณ์นี้เองที่เป็นตัวชี้วัดความน่าเชื่อถือ และจากหลายๆ กรณีพบว่า ข่าวในแง่ลบของบริษัทที่ออกไปส่งผลให้ราคาหุ้นของบริษัทตกลง

๓. ผลกระทบต่อความไว้วางใจของผู้บริโภค ความกังวลต่อการใช้จ่ายหรือการทำธุรกรรมทางอินเทอร์เน็ตของผู้บริโภคมีความสำคัญอย่างมากต่อภาคธุรกิจ

๔. ผลกระทบต่อความมั่นคงแห่งชาติ ทางกองทัพสมัยใหม่ของประเทศส่วนใหญ่มีการพึ่งพาเทคโนโลยีสารสนเทศที่ล้ำหน้า สงครามข้อมูลรวมถึงการโจมตีเครือข่าย ถูกใช้เป็นเครื่องมือทาง การทหารในการโจมตีและการแข่งขัน เนื่องจากเป็นเครื่องมือที่ใช้ต้นทุนต่ำแต่มีประสิทธิภาพมาก การแพร่กระจายของมัลแวร์เพื่อทำให้เครือข่ายล่ม หรือการกระจายข่าวข้อมูลผิดๆ เป็นตัวอย่างของการโจมตีทางการทหาร พวกผู้ก่อการร้ายและอาชญากรใช้เทคโนโลยีสารสนเทศในการวางแผนและประกอบอาชญากรรม โดยอาชญากรรมส่วนใหญ่จะเกิดขึ้นในประเทศที่กำลังพัฒนา เนื่องจากประเทศเหล่านี้เป็นประเทศที่มีการเข้าถึงและใช้งานอินเทอร์เน็ตได้ และมีช่องโหว่จากการขาดความรู้ ด้านความปลอดภัยสารสนเทศ ผลของงานวิจัยนี้ได้นำเสนอแนวทางของอาชญากรรมทางไซเบอร์ที่ คาดว่าจะเด่นชัดขึ้นและมีความสำคัญมากในอนาคต อย่างเช่น การโจมตีโดยการใช้ความรู้ทางด้าน วิศวกรรมขั้นสูง การโจมตีผ่าน social media เป็นต้น โดยผู้วิจัยได้ให้ข้อสรุปด้วยการเสนอแนะใน การจัดการกับปัญหา คือการกำหนดกฎหมายทางไซเบอร์ (cyber law) การให้การศึกษาเรียนรู้ เกี่ยวกับอาชญากรรมทางไซเบอร์และสุดท้ายคือการกำหนดนโยบายเพื่อการจัดการกับปัญหา

Mehrdad Sepehri Sharbaf (2014) ได้ทำการศึกษาเรื่อง A New Perspective to Information Security : Total Quality Information Security Management งานวิจัยนี้ ได้นำเสนอแนวคิดใหม่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยการออกแบบการพัฒนาและการสร้างแบบจำลอง TQISM เพื่อการรักษาความมั่นคงสารสนเทศ และสินทรัพย์ขององค์กร TQISM เป็นการรวมของการรักษาความมั่นคงปลอดภัยสารสนเทศ และการบริหารจัดการโดยที่ผู้บริหารและพนักงานมีส่วนร่วมในการพัฒนาอย่างต่อเนื่อง

กรอบแนวคิดของการวิจัย



สรุป

อาชญากรรมทางเทคโนโลยี เป็นการกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์หรือเครื่องมือทางเทคโนโลยีต่างๆ ทำให้ผู้อื่นนั้นได้รับความเสียหาย โดยที่สำนักงานตำรวจแห่งชาติได้กำหนดลักษณะคดีอาชญากรรมทางเทคโนโลยีไว้ ๑๔ ประเภท และ ๔ กลุ่ม ซึ่งแต่ละประเภทจะมีข้อหา และบทลงโทษที่ต่างกันออกไปตามพฤติการณ์ของอาชญากรรม โดยสาเหตุของการเกิดอาชญากรรมเทคโนโลยี นั้นเกิดจาก ปัจจัยส่วนบุคคลและปัจจัยด้านสภาพแวดล้อม จึงต้องมีแนวทางการป้องกันที่เรียกว่า “ภูมิคุ้มกันภัยไซเบอร์” เริ่มจากความตระหนักรู้ของประชาชน มีนโยบายและมาตรการ ที่ช่วยสร้างสภาพแวดล้อมที่ดีของประเทศในด้านความมั่นคงทางไซเบอร์ในทุกระดับ

บทที่ ๓
สถานการณ์การแก้ไขปัญหาทางอาชญากรรมทางเทคโนโลยีในปัจจุบัน

ในบทนี้ ผู้วิจัยนำเสนอแนวทางการป้องกันแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสมจากการวิเคราะห์เอกสารและการใช้เทคนิคการสัมมนาอิงผู้เชี่ยวชาญ (connoisseurship) โดยในที่นี้ อาชญากรรมทางเทคโนโลยีเน้นไปที่ การคุกคามทางไซเบอร์และความปลอดภัยทางไซเบอร์ โดยนำเสนอตามวัตถุประสงค์การวิจัย ดังนี้

ปัญหา/อุปสรรค และแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี

ผู้วิจัยขอนำเสนอเป็น ๒ ประเด็น ดังนี้

๑. สถานการณ์การใช้งานอินเทอร์เน็ต และภัยคุกคามจากอาชญากรรมทางเทคโนโลยี

จากการวิจัยเอกสารพบว่า สถานการณ์การใช้งานอินเทอร์เน็ต และภัยคุกคามจากอาชญากรรมทางเทคโนโลยีในประเทศไทย ในปัจจุบัน มีดังนี้

๑.๑ อาชญากรรมทางเทคโนโลยีอันเนื่องมาจากการผลักดันการใช้งานอินเทอร์เน็ตจากรัฐบาล และการพึ่งพาเทคโนโลยีสารสนเทศของภาครัฐ

รัฐบาลไทยมีการผลักดันการใช้งานอินเทอร์เน็ตผ่านกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. ๒๕๕๔ – ๒๕๖๓ ซึ่งเป็นฉบับที่ ๒ ที่มีการประกาศใช้งานต่อจาก ฉบับแรกที่เมื่อปี พ.ศ. ๒๕๓๙ หรือ IT๒๐๐๐ โดยการกำหนดภารกิจหลัก ๓ ประการ คือ ๑. การลงทุน ในโครงสร้างพื้นฐานสารสนเทศแห่งชาติ ๒. การลงทุนในด้านการศึกษาที่ดีของพลเมืองและบุคลากรด้านสารสนเทศ ๓. การปรับปรุงบทบาทภาครัฐ เพื่อให้บริการที่ดีขึ้น และสร้าง รากฐานให้กับอุตสาหกรรมสารสนเทศภายในประเทศให้มีความเข้มแข็ง ตัวอย่างการผลักดันการใช้งานอินเทอร์เน็ตของรัฐบาลไทย คือการพัฒนานวัตกรรม เพื่อสนับสนุนการใช้งาน IoT ที่เรียกว่า NETPIE แพลตฟอร์ม เป็นการตอบรับกระแสของการใช้งาน IoT ภายในประเทศ

ประเภทของข้อมูลที่รัฐจัดเก็บในระบบเทคโนโลยีสารสนเทศ สามารถแบ่งออกได้เป็น ๓ ประเภท ได้แก่

๑. ข้อมูลภายใน (Intrinsic Data) คือข้อมูลที่รัฐเป็นผู้สร้าง รวบรวม จัดเก็บภายในหน่วยงานรัฐ

๒. ข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมกับภาครัฐ (Commercial Data) คือข้อมูลที่เกิดจากการทำธุรกรรมและการสื่อสารต่างๆ ระหว่างภาครัฐ และภาคเอกชน

๓. ข้อมูลส่วนบุคคลของภาคประชาชน (Personal Data) คือข้อมูลที่ภาคประชาชน ส่งให้รัฐตามกฎระเบียบข้อบังคับที่มีอยู่ หรือเพื่อประโยชน์สาธารณะ

ข้อมูลทั้ง ๓ ประเภท จะถูกทำการประมวลผล และจัดเก็บโดยรัฐ โดยคำนึงถึงระดับชั้นความลับของข้อมูล (Information Classification) ซึ่งนอกเหนือจากการจัดเก็บแล้วยังมีการเผยแพร่ข้อมูลสู่สาธารณะให้ประชาชนสามารถเข้าถึงได้ในรูปแบบเอกสารของรัฐ การรวบรวม จัดเก็บ ประมวลผล ไปจนถึงการเผยแพร่ข้อมูล ทั้งระหว่างหน่วยงานรัฐ และการเผยแพร่สู่สาธารณะชน ทำให้เกิดความเสี่ยงต่อภัยคุกคามทางเทคโนโลยีสารสนเทศได้ ซึ่งข้อมูลสาธารณะที่อ่อนไหว ข้อมูล สาธารณะจำนวนมากที่รัฐเป็นผู้ดูแลเป็นเรื่องอ่อนไหว (Sensitive Public Data) ข้อมูลนี้อาจได้แก่ ชื่อ วันเกิด หมายเลขโทรศัพท์ หมายเลขประจำ ตัวผู้เสียภาษี หมายเลขประจ าตัวประชาชน หมายเลขหนังสือเดินทาง รายละเอียดสุขภาพ/การแพทย์ ระเบียนคนเข้าเมือง เป็นต้น ซึ่งตัวอย่าง บริการของรัฐซึ่งบริการจัดการข้อมูลดังกล่าว ได้แก่ ข้อมูลทะเบียนราษฎร ระบบชำระภาษีออนไลน์ ข้อมูลการเข้าเมืองใบขอวีซ่าและท่องเที่ยว และการขอใบอนุญาตประกอบธุรกิจ เป็นต้น

การผลักดันการใช้งานระบบสารสนเทศทั้งหมด ส่งผลให้ระบบสารสนเทศของภาครัฐที่เป็นแหล่งเก็บรวบรวมข้อมูลจำนวนมหาศาลไว้เกิดความเสี่ยงทางด้านภัยคุกคามสารสนเทศ

๑.๒ อาชญากรรมทางเทคโนโลยีอันเนื่องมาจากการพัฒนาเทคโนโลยีและธุรกรรมทางด้าน การเงินการธนาคารผ่านอินเทอร์เน็ต

การพัฒนาเทคโนโลยีและธุรกรรมทางด้านการเงินการธนาคารผ่านอินเทอร์เน็ตไม่ว่าจะเป็นการทำธุรกรรมกับธนาคารผ่านอินเทอร์เน็ต (Internet banking & Mobile banking) การใช้ฟินเทค (Fintech) การพาณิชย์อิเล็กทรอนิกส์ (E–Commerce) เหล่านี้ ล้วนมีภัยคุกคาม ได้แก่ ภัยประเภทการฉ้อโกงทางการ เงิน (Fraud) มากที่สุด ซึ่งส่วนใหญ่จะเกิดจากการใช้วิธีการฟิชชิ่ง (Phishing) เพื่อให้ได้มาซึ่งข้อมูล อย่างเช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่นๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดย ไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่นๆ ต่อไป การถูกโจรกรรมเงินจากบัญชีในรูปแบบส่งข้อความทางโทรศัพท์เคลื่อนที่ หรือ SMS โดยการปลอมเลขหมายให้เหมือนเบอร์ Call Center ของธนาคาร เพื่อหลอกให้ดาวน์โหลด หรือติดตั้งแอพพลิเคชั่น ซึ่งแอปพลิเคชั่นเหล่านี้จะมีโปรแกรมมัลแวร์ หรือ โปรแกรมโทรจัน แฝงมาเพื่อขโมยข้อมูลลับ หรือรหัสผ่านต่างๆ ในโทรศัพท์ แล้วจึงนำไปใช้ใน การถอนเงินจากบัญชีของผู้เสียหายออกไป สถานการณ์อาชญากรรมทางเทคโนโลยีที่พบในประเทศไทยได้มุ่งเป้าไป ยังหลายภาคส่วน โดยพบภัยคุกคามไซเบอร์ที่มีจุดประสงค์ทางการเงินในรูปแบบต่างๆ เช่น เว็บไซต์ ธนาคารปลอม เพื่อหลอกขโมยรหัสผ่านผู้ที่ใช้งานธนาคารอิเล็กทรอนิกส์

๑.๓ อาชญากรรมทางเทคโนโลยีอันเนื่องมาจากการพัฒนาเทคโนโลยีทางการแพทย์และ สุขภาพ (Health Care) ผ่านระบบเทคโนโลยีสารสนเทศ

ในประเทศไทยพบการประกาศเตือนเรื่องการระบาดของมัลแวร์ในโรงพยาบาลหลายแห่ง โดยจะมีเป้าหมายอยู่ที่ส่วนสำคัญ ๒ ส่วน ส่วนแรกคือ อุปกรณ์ทางการแพทย์ (Medical Device) อย่างเช่น อุปกรณ์ที่ใช้กับผู้ป่วยในห้องไอซียู อุปกรณ์ใช้ในการผ่าตัด เครื่องช่วยหายใจ อุปกรณ์วัดค่าต่างๆ ในร่างกาย หรือหุ่นยนต์ผ่าตัด เป็นต้น ส่วนที่สองคือ ข้อมูลการรักษาพยาบาล

(Information) ที่มีความอ่อนไหว อย่างเช่น ประวัติครอบครัวของคนไข้ ชื่อบิดามารดา ที่อยู่ ยาที่แพ้ ประวัติการเจ็บป่วย โรคประจำตัว อุบัติเหตุที่เคยเกิดขึ้น ซึ่งเป็นข้อมูลส่วนบุคคลที่หากมีการรั่วไหล จะสามารถถูกนำไปเป็นหลักฐานในการพิสูจน์ตัวตนเพื่อทำธุรกรรมทางการเงินต่างๆ ได้ หรืออาจนำเอาข้อมูลการเจ็บป่วยไปทำอันตรายกับผู้ป่วย เป็นต้น

๑.๔ อาชญากรรมทางเทคโนโลยีจากการใช้งานโทรศัพท์เคลื่อนที่

ภัยคุกคามการใช้งานโทรศัพท์มือถือสามารถแบ่งออกได้เป็น ๓ ประเภทคือ ภัยที่เกิด จากการใช้งานโปรแกรมบนโทรศัพท์มือถือ (Application-Based Threats) ภัยที่เกิดจากการใช้งาน เว็บไซต์บนโทรศัพท์มือถือ (Web-based Threats) จากการใช้งานโปรแกรมบนมือถือ (Application Based Threats) และภัยคุกคามจากการใช้งานเครือข่าย (Network Threats)

ภัยที่เกิดจากการใช้งานโปรแกรมบนโทรศัพท์มือถือ (Application-Based Threats) เกิดขึ้นเนื่องจากมีโปรแกรมแอปพลิเคชั่นจำนวนมากที่ไม่สามารถตรวจสอบความปลอดภัย ได้ทำให้ผู้ใช้งานไม่ทราบล่วงหน้าถึงปัญหาที่อาจจะตามมาในการใช้งานแอปพลิเคชั่น โดยตัวอย่างของภัยคุกคามที่เกิดขึ้นผ่านการใช้งานโปรแกรมบนโทรศัพท์มือถือ มีดังต่อไปนี้

๑. มัลแวร์ (Malware) หรือโปรแกรมไม่พึงประสงค์ที่ได้รับการออกแบบมาเพื่อแสดงพฤติกรรมที่เป็นอันตรายต่อข้อมูลต่างๆ ในโทรศัพท์มือถือ เช่น การสั่งให้เครื่องโทรศัพท์ส่งข้อความออกไปยังรายการผู้ติดต่อในเครื่อง โดยที่ผู้ใช้งานหรือเจ้าของเครื่องไม่รู้ตัว การขโมยข้อมูลสำคัญที่ถูกบันทึกอยู่ในเครื่อง อย่างเช่นข้อมูลทางบัญชี หมายเลขบัตรประชาชน และรหัสผ่านต่างๆ ซึ่งจะนำไปสู่การจารกรรมประเภทอื่นต่อไป

๒. สปายแวร์ (Spyware) คือ โปรแกรมที่ได้รับการออกแบบมาเพื่อเก็บรวบรวม ข้อมูลต่างๆ ของผู้ใช้งาน ถูกนำมาใช้งานเพื่อเก็บประวัติการใช้งานต่างๆ บนเครื่องโทรศัพท์ อย่างเช่น ข้อความ รายชื่อผู้ติดต่อ ที่อยู่ การใช้งานอีเมล์ และภาพถ่าย เป็นต้น โดยผู้ใช้งานจะถูกหลอกให้ดาวน์ โหลดโปรแกรมมาติดตั้งโดยไม่รู้ตัว เช่นการให้คลิกที่ลิงก์ที่ดูปลอดภัยและน่าเชื่อถือ และเมื่อคลิกเข้า ไปก็จะทำให้มีการติดตั้งโปรแกรมมัลแวร์ หรือสปายแวร์ โดยอัตโนมัติ

ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์บนโทรศัพท์มือถือ (Web-based Threats) ปัจจุบันผู้ใช้งานโทรศัพท์เคลื่อนที่นิยมที่จะเข้าหาข้อมูลหน้าเว็บผ่านทางโทรศัพท์มือถือเพิ่มมากขึ้น เนื่องจากมีความสะดวกและรวดเร็ว โดยภัยคุกคามที่เกิดขึ้นจะคล้ายกับภัยที่เกิดจากการเข้าหน้าเว็บ ผ่านเครื่องคอมพิวเตอร์ อย่างเช่น ฟิชชิ่ง (Phishing) หรือการหลอกลวงโดยใช้หน้าเว็บไซต์ที่ออกแบบ ให้มีลักษณะคล้ายคลึงกับของจริง เพื่อหลอกให้ผู้ใช้กรอกข้อมูลสำคัญส่วนบุคคล และภัยจากช่องโหว่ ของโปรแกรมประเภทเบราว์เซอร์ เป็นช่องโหว่ที่ถูกพบในโปรแกรมเบราว์เซอร์ หรือโปรแกรมปลั๊กอิน ที่สามารถติดตั้งเพิ่มเติมได้ในเบราว์เซอร์ ตัวอย่างเช่น โปรแกรม Flash player หรือ PDF Reader เป็นต้น ซึ่งเพียงแค่ให้ผู้ใช้งานเข้าชมหน้าเว็บไซต์ที่มีการใช้งานโปรแกรมเบราว์เซอร์ ก็จะทำให้ ผู้ใช้งานติดมัลแวร์หรือโปรแกรมอันตรายต่างๆ ได้

ภัยคุกคามจากการใช้งานเครือข่าย (Network Threats) เป็นภัยที่เกิดขึ้นจากการ ใช้โทรศัพท์เคลื่อนที่ในการเชื่อมต่ออินเทอร์เน็ตจากเครือข่ายไร้สาย (Wireless Network) ซึ่งปัจจุบัน พบว่ามีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก แต่ไม่สามารถระบุความปลอดภัยของเครือข่ายได้ ผู้ใช้บริการจึงอาจจะมีความเสี่ยงต่อภัยคุกคามได้โดยไม่รู้ตัว โดยภัยคุกคามที่สามารถ

เกิดขึ้นจากการใช้ งานเครือข่ายไร้สายบนโทรศัพท์มือถือ เป็นการเปลี่ยนสถานะจากผู้ใช้งานเป็นผู้โจมตี ผ่านข้อบกพร่อง ของระบบปฏิบัติการบนโทรศัพท์เคลื่อนที่ ส่งผลให้โทรศัพท์มือถือที่ใช้กลายเป็นเครื่องมือในการส่งต่อ หรือแพร่กระจายมัลแวร์ต่อไปอย่างอัตโนมัติ นอกจากนั้นยังมีการดักจับข้อมูลบนเครือข่ายไร้สาย (WiFi sniffing) ซึ่งเป็นลักษณะของการขโมยข้อมูลผ่านเครือข่ายไร้สายที่เครื่องโทรศัพท์นั้นเชื่อมต่อ เนื่องจากการใช้งานบนเครื่องโทรศัพท์ส่วนใหญ่จะไม่มีการเข้ารหัสความปลอดภัยข้อมูลไว้ ทำให้มี โอกาสถูกลักลอบขโมยข้อมูลได้ง่าย (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

๒. กฎหมายที่เกี่ยวข้องการป้องกันอาชญากรรมทางเทคโนโลยี

ประเทศไทยได้กำหนดนโยบายและดำเนินงานทางด้านความปลอดภัยทางไซเบอร์ภายในประเทศ ทั้งพระราชบัญญัติ พระราชกฤษฎีกา และกฎหมายที่มีผลบังคับใช้อยู่ในปัจจุบัน ดังนี้

๒.๑ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๕๖

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ ฉบับ พ.ศ. ๒๕๕๖ เป็นฉบับที่สอง หลังจากมีการกำหนดพระราชกฤษฎีกาฯนี้ขึ้นครั้งแรกใน พ.ศ. ๒๕๔๙ โดยพระราชกฤษฎีกาฉบับนี้มีเป้าหมายในการกำหนดให้หน่วยงานภาครัฐต้องจัดทำนโยบายเพื่อให้เกิดความมั่นคงปลอดภัยและความน่าเชื่อถือในการใช้งานระบบสารสนเทศภายใน หน่วยงานรัฐ ซึ่งเป็นระบบที่มีความเชื่อมโยงทั้งภายในและภายนอกหน่วยงาน

๒.๒ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕

เป็นกฎหมายที่กำหนดให้ธุรกรรมทางอิเล็กทรอนิกส์ใดๆ ที่ได้กระทำตามวิธีแบบปลอดภัย ที่กำหนดใช้ในพระราชกฤษฎีกาฯนี้ ให้สันนิษฐานไว้ว่าเป็นวิธีการที่เชื่อถือได้ พระราชกฤษฎีกาฯ ฉบับนี้เป็นการส่งเสริมการบริหารจัดการความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ โดยมี สาระสำคัญตามหัวข้อต่างๆ ดังนี้ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๙)

๒.๒.๑ การให้คำนิยามความมั่นคงปลอดภัยของระบบสารสนเทศ (information security) ความมั่นคงปลอดภัยด้านการบริหารจัดการ (administrative security) ความมั่นคง ปลอดภัยทางกายภาพ (physical security) รวมไปถึงโครงสร้างพื้นฐานสำคัญของประเทศ (critical infrastructure) เป็นต้น

๒.๒.๒ การแบ่งระดับความมั่นคงปลอดภัยตาม มาตรา ๔ ออกเป็น ๒ ระดับ คือ ระดับ เคร่งครัด ระดับกลาง และระดับพื้นฐาน

๒.๒.๓ การกำหนดประเภทธุรกรรมทางอิเล็กทรอนิกส์ แยกเป็นธุรกรรมที่กระทบต่อความมั่นคงหรือความสงบเรียบร้อยชองประเทศหรือสาธารณะกับธุรกรรมของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

๒.๒.๔ กำหนดการประเมินความเสี่ยงตามมาตรา ๕ โดยให้คำนึงถึงความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ และผลกระทบต่อเศรษฐกิจและสังคมของประเทศ

๒.๒.๕ ข้อกำหนดขั้นต่ำของความมั่นคงปลอดภัยสารสนเทศ บนพื้นฐานของมาตรฐานความปลอดภัยสารสนเทศสากล ISO/IEC 27001 : 2005

๒.๒.๖ การกำหนดแนวปฏิบัติตามหลักของ C.I.A. รวมทั้ง การปฏิบัติตามแนวนโยบายและการควบคุมความปลอดภัยสารสนเทศ

๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

เป็นพระราชบัญญัติเพื่อการกำหนดการกระทำที่เป็นความผิดทางการใช้งานคอมพิวเตอร์ เพื่อใช้เป็นกฎหมายในการดำเนินคดีกับผู้ที่กระทำความผิดดังกล่าว โดยเนื้อหาของพระราชบัญญัติฉบับนี้จะถูกแบ่งออกเป็น ๒ หมวด หมวดที่ ๑ จะระบุรายละเอียดถึงการกระทำที่ถือว่าเป็นการกระทำผิดทางคอมพิวเตอร์ และระบุการระวางโทษเอาไว้ด้วย และหมวดที่ ๒ จะระบุถึงอำนาจหน้าที่ของเจ้าพนักงานในการดำเนินงานเพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้

๓.๑ รูปแบบ เทคนิค วิธีการและช่องทางของอาชญากรรมที่กระทำผ่านทางเทคโนโลยีสารสนเทศ

จากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ พบว่า รูปแบบ เทคนิค และช่องทางของอาชญากรรมที่กระทาผ่านเทคโนโลยี แบ่งออกได้เป็นรูปแบบการกระทาความผิดของอาชญากรรมที่กระทาผ่านเทคโนโลยี ประกอบด้วย

๓.๑.๑ การฉ้อโกง โดยการหลอกลวงในการหลอกให้โอนเงินซื้อสินค้าแต่ไม่ยอม ส่งสินค้าไปให้

๓.๑.๒ การหลอกลวง การหลอกลวงให้โอนเงินด้วยความรัก โรแมนซ์สแกม (Romance Scam) การขายของที่ผิดศีลธรรม เช่น การขายยาเสพติด การขายบริการทางเพศของผู้เยาว์ที่มีอายุต่ำว่า ๑๕ ปี และ คอลเซ็นเตอร์ (Call Center) เป็นต้น

๓.๑.๓ การเผยแพร่ข้อมูลที่ไม่เหมาะสม ข้อมูลที่เป็นเท็จ เช่น ภาพโป๊ ภาพลามก อนาจาร เป็นต้น

๓.๑.๔ การจำหน่ายยาเสพติด การจำหน่ายยาเสพติดโดยการใช้อุปกรณ์เทคโนโลยี เช่น คอมพิวเตอร์ หรือโทรศัพท์มือถือเป็นเครื่องมือ เช่น การใช้อีเมล์หรือ LINE ในการติดต่อกับเครือข่ายการค้ายาเสพติด การค้าอาวุธเถื่อน ธุรกิจสินค้าหนีภาษี

๓.๑.๕ การพนันออนไลน์ การพนันออนไลน์ ถือเป็นการใช้เทคโนโลยีในการหลอกลวงเงินทางอิเล็กทรอนิกส์รูปแบบหนึ่ง ซึ่งทำให้ผู้ตกเป็นเหยื่อ มีหนี้สินล้นพ้นตัวได้

๓.๑.๖ การหมิ่นประมาทโดยใช้เทคโนโลยี ซึ่งถือว่า เป็นการกระทำผิดที่ส่งผลกระทบ ต่อสิทธิหรือเสรีภาพของบุคคลที่ถูกกระทำเป็นย่างงมาก โดยเทคนิคที่ใช้มักมีรูปแบบตั้งแต่

๓.๑.๖.๑ การใช้หน้าเพจเพื่อทาการค้าขาย และทำธุรกรรมการโฆษณาชวนเชื่อให้ร่วมลงทุน

๓.๑.๖.๒ การใช้เครื่องมือสื่อสาร โทรศัพท์เคลื่อนที่ในการหลอกลวง

๓.๑.๖.๓ การใช้คอมพิวเตอร์ช่องทางในการกระทาผิดมักจะใช้ โทรศัพท์ อีเมล การแชร์เนื้อหาผ่านทางสังคม ออนไลน์ เช่น Facebook, Line และโปรแกรมสื่อสังคมออนไลน์อื่น ๆ

รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี

๑. หน่วยงานภาครัฐที่เกี่ยวข้องกับการบริหารจัดการให้เกิดความปลอดภัยทางไซเบอร์

หน่วยงานราชการของประเทศไทยที่ดูแลด้านการรักษาความปลอดภัยไซเบอร์ แบ่งตาม หน้าที่รับผิดชอบของแต่ละหน่วยงาน ดังนี้

๑.๑ กระทรวงกลาโหม มีหน้าที่ในการดูแลความปลอดภัยทางไซเบอร์ ที่เกี่ยวพันถึงความมั่นคงของประเทศ เช่น การรักษาข้อมูลทางการทหาร เป็นต้น ซึ่งจากประสบการณ์ปัญหาด้านความปลอดภัยไซเบอร์ที่ทำให้เกิดความวิตกกังวลด้านความมั่นคงไปทั่วโลก ส่งผลให้หน่วยงานทหารให้ความสำคัญกับปัญหานี้มากยิ่งขึ้น ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ. ๒๕๕๔ ได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วนและการพร้อมใช้งานของระบบทรัพย์สิน และข้อมูลสารสนเทศ

๑.๒ สำนักงานตำรวจแห่งชาติ มีหน้าที่ในส่วนของการตามจับกุมผู้กระทำความผิดเพื่อนำมาดำเนินคดีตามที่กฎหมายได้ระบุไว้ โดยกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ซึ่งมีอำนาจหน้าที่ และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์

๑.๓ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีหน้าที่ดูแลความปลอดภัยทางไซเบอร์ในภาคสังคม อย่างเช่น สังคมออนไลน์ หรือสื่อออนไลน์ โดยเฉพาะในเรื่องของการละเมิดสิทธิของประชาชนมีหน่วยงานภายใต้กระทรวงที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์ ดังนี้

๑.๓.๑ สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ทำหน้าที่สอดส่อง ดูแล เก็บรวบรวมพยานหลักฐาน พิสูจน์หลักฐาน เพื่อดำเนินคดีกับผู้กระทำความผิดทางเทคโนโลยี นอกจากนี้ ยังมีหน้าที่ศึกษา พิจารณาร่างกฎหมายเกี่ยวกับไซเบอร์เพื่อให้เกิดความเหมาะสมและการบังคับใช้ที่มีประสิทธิภาพ เช่น (ธนิต ประภาตนันท์, ๒๕๕๙)

๑.๓.๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เป็นหน่วยงานภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ที่ได้รับภารกิจในการส่งเสริม และสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ การพัฒนาโครงสร้างพื้นฐานสารสนเทศที่เอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์และธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการสร้างมาตรฐานเทคโนโลยีสารสนเทศ และการสื่อสารที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ

๑.๔ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center : NECTEC หรือเนคเทค)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center : NECTEC หรือเนคเทค) มีภารกิจหลัก ได้แก่

๑.๔.๑ ดำเนินการวิจัย พัฒนาและวิศวกรรมจากระดับห้องปฏิบัติการถึงขั้นโรงงานต้นแบบทั้งในด้านการสร้างขีดความสามารถและศักยภาพในสาขาเทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์

๑.๔.๒ วิเคราะห์ สนับสนุน และติดตามประเมินผลโครงการวิจัย พัฒนาและวิศวกรรมของภาครัฐ ภาคเอกชน และสถาบันการศึกษาเพื่อสร้างความสามารถและศักยภาพในสาขาเทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์

๑.๔.๓ ร่วมให้บริการวิเคราะห์และทดสอบคุณภาพผลิตภัณฑ์ การสอบเทียบมาตรฐานและความถูกต้องของอุปกรณ์ การให้บริการข้อมูล และการให้คำปรึกษาทางวิทยาศาสตร์และเทคโนโลยี

๑.๔.๔ ร่วมจัดการฝึกอบรมและพัฒนาบุคลากร รวมทั้งให้คำปรึกษาทางวิชาการ

๑.๔.๕ ส่งเสริมและจัดให้มีความร่วมมือระหว่างนักวิจัยและนักวิชาการในสถาบันและหน่วยงานต่าง ๆ ทั้งภายในประเทศและต่างประเทศ

๑.๔.๖ สนับสนุน ประสานงาน และดำเนินการด้านความร่วมมือระหว่างภาครัฐ ภาคเอกชน เพื่อกระตุ้นการนำวิทยาศาสตร์และเทคโนโลยีไปใช้ในการพัฒนาอุตสาหกรรมภายในประเทศ (เนคเทค, ๒๕๕๙)

๑.๕ สำนักงานพัฒนารัฐบาลดิจิทัล มีบทบาทในกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยีดังนี้

๑.๕.๑ เสนอพระราชบัญญัติ (พ.ร.บ.) ว่าด้วยรัฐบาลดิจิทัล เป็นกลไกสำคัญการขับเคลื่อนนโยบายประเทศไทย ๔.๐ เนื่องจากการเปลี่ยนแปลงทางเทคโนโลยีทั้งการทำธุรกรรมต่าง ๆ ที่มีการนำระบบปัญญาประดิษฐ์ หรือเอไอ เข้ามาจัดการจัดทำและใช้ประโยชน์จากฐานข้อมูลขนาดใหญ่ (big data) ซึ่งมีความสำคัญต่อการพัฒนาเศรษฐกิจ และสังคมของประเทศโดยรัฐจัดให้มีมาตรการแนวทางข้อปฏิบัติการจัดการด้านความมั่นคงไซเบอร์ของภาครัฐที่มีข้อบังคับอย่างจริงจัง

๑.๕.๒ กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูงด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘-bits Encryption) เพื่อเข้ารหัสข้อมูล

ที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ต ในทุกครั้งที่มีการทำธุรกรรมทางการเงิน ผ่านเครือข่ายอินเทอร์เน็ต ของ สพร. ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล

๑.๖ กรมสอบสวนคดีพิเศษ (DSI) กำหนดให้กองคดี เทคโนโลยีและสารสนเทศในกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยีดังนี้

๑.๖.๑ ปฏิบัติงานด้าน การป้องกัน การปราบปราม การสืบสวน และการสอบสวนคดีพิเศษ เพื่อดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับเทคโนโลยีและสารสนเทศ

๑.๖.๒ ปฏิบัติงานวิเคราะห์และพิสูจน์ความผิดที่อยู่ในความรับผิดชอบ

๑.๖.๓ ดำเนินการ รวบรวม ศึกษา จัดระบบ และวิเคราะห์ข้อมูลการข่าว วางแผนงาน บริหารจัดการ และประสานงานเพื่อการป้องกัน การปราบปราม การสืบสวน และการสอบสวนคดีพิเศษที่อยู่ในความรับผิดชอบ

๑.๖.๔ ปฏิบัติงานด้านการป้องกัน การปราบปราม การสืบสวน และการสอบสวนผู้กระทำความผิดในคดีอื่นตามที่ได้รับมอบหมาย

๑.๖.๕ ดำเนินการเกี่ยวกับการเก็บรักษาพยานหลักฐานและของกลางในคดี

๑.๖.๖ ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

๒. การดำเนินงานของรัฐด้านความปลอดภัยทางไซเบอร์

จากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ พบว่า สิ่งที่จำเป็นสำหรับกระบวนการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ ประกอบด้วย ความรู้ความเข้าใจในเรื่องการดำเนินคดี ได้แก่ ความรู้ ความเข้าใจ ในเรื่องการร้องทุกข์ กล่าวโทษ สอบสวน ฟ้องคดี หรือการพิจารณา พิพากษาคดี ซึ่งเจ้าหน้าที่ตำรวจในระดับสถานีมองว่าการดำเนินคดีอาชญากรรมทางเทคโนโลยีสารสนเทศ เป็นเรื่องทำได้ยาก และต้องใช้เวลา เพราะความยากในการรวบรวมพยานหลักฐาน โดยเฉพาะพยานหลักฐานทางด้านอิเล็กทรอนิกส์ รวมทั้งเจ้าหน้าที่ตำรวจในระดับสถานีส่วนมากยังขาดความรู้ความเข้าใจในเรื่องการรวบรวมหลักฐาน การพิสูจน์หลักฐาน จนทำให้หลายคดีไม่สามารถนำสู่การพิจารณาของศาล เพื่อลงโทษผู้กระทาความผิดได้ ความรู้เรื่องข้อกฎหมาย เจ้าหน้าที่ตำรวจยังมีปัญหาในเรื่องของการตีความข้อกฎหมาย การส่งเสริมความร่วมมือกับต่างประเทศ กระบวนการดำเนินคดีเป็นการดำเนินคดีที่เกี่ยวข้องกับคดีทางเทคโนโลยีสารสนเทศ การดำเนินคดีของเจ้าหน้าที่ตำรวจมากเป็นคดีฉ้อโกงในเรื่องการหลอกซื้อของทางออนไลน์ การหมิ่นประมาท ซึ่งปัญหาและอุปสรรคในการดำเนินคดีที่เกี่ยวข้องกับกระทำความผิดทางเทคโนโลยีที่พบประกอบด้วย ความล่าช้าในการขอข้อมูลจากหน่วยงานต่าง ๆ ที่ เกี่ยวข้อง เช่น การขอข้อมูลจากธนาคาร เครือข่ายโทรศัพท์มือถือ เป็นต้น โดยมีข้อสนับสนุน ประกอบด้วยการจัดอบรมเพื่อเพิ่มพูนความรู้ทั้งทางด้านการป้องกันปราบปราม สืบสวนและสอบสวน การจัดให้มีผู้มีความรู้ ความเชี่ยวชาญความชำนาญด้านเทคโนโลยีสารสนเทศเข้าร่วมเป็นคณะทำงานเพื่อให้เกิดประสิทธิภาพในการดำเนินคดี รวมถึงจัดตั้งหน่วยงานที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีสารสนเทศโดยเฉพาะ เพื่อให้มีหน่วยงานที่มีความรู้ความชำนาญเฉพาะทางเกี่ยวกับเทคโนโลยีโดยเฉพาะการมีเจ้าหน้าที่ที่มีความรู้ความชำนาญเฉพาะในการป้องกัน ปราบปรามการดำเนินคดี

และการพิสูจน์หลักฐานอาชญากรรมทางเทคโนโลยีสอดคล้องกับแนวคิดการกระทาอาชญากรรมทางเทคโนโลยีที่สำนักงานตำรวจ แห่งชาติ (สตช.) ประเมินว่า สถานการณ์ของอาชญากรรมทางเทคโนโลยีนับวันทวีความรุนแรง และมีขยายวงกว้างขวางมากขึ้น ดังนั้น สำนักงานตำรวจแห่งชาติ (สตช.) ในฐานะที่มีภารกิจรับผิดชอบในการรักษาความสงบเรียบร้อยของสังคม จำเป็นต้องต้องสนับสนุนให้เจ้าหน้าที่ตำรวจในทุกระดับที่สังกัดในสถานีตำรวจทั้งหมดทั่วประเทศสามารถรู้เท่าทันและรับมือกับ อาชญากรรมทางเทคโนโลยีที่เกิดขึ้นได้

แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี

๑. การประสานความร่วมมือระหว่างรัฐบาลกับหน่วยงานอื่นที่ไม่ใช่รัฐ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เป็นหน่วยงานหลักในการสร้างเครือข่ายกับหน่วยงานภาครัฐ โดย สพธอ. ต้องการดูแลความปลอดภัยไซเบอร์เพื่อป้องกันอาชญากรรมทางเทคโนโลยีของหน่วยงานรัฐ เนื่องจากเล็งเห็นถึงข้อจำกัดของหน่วยงานรัฐหลายหน่วยงานที่ไม่สามารถดำเนินงานด้านความปลอดภัยไซเบอร์ได้เอง สพธอ. ตระหนักถึงความสำคัญของข้อมูลของหน่วยงานรัฐที่เป็นข้อมูลลับของประชาชนในประเทศและจัดทำโครงการรับดูแลความปลอดภัยทางไซเบอร์ให้กับภาครัฐที่สนใจ ซึ่งในปัจจุบันมีหน่วยงานที่เข้าร่วมกว่า ๒๐ กระทรวง นอกจากความร่วมมือกับหน่วยงานภาครัฐแล้ว สพธอ. ยังมีความร่วมมือกับสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association: TISA) และสมาคมอื่นๆ ที่เกี่ยวข้อง โดยความร่วมมือระหว่างหน่วยงานต่างๆ เป็นการร่วมมือตามประเภทของผลกระทบที่เกิดขึ้นจากภัยคุกคามจากอาชญากรรมทางเทคโนโลยี โดยหน่วยงานที่ได้รับเรื่องร้องเรียนหรือตรวจสอบพบปัญหาจะทำการประสานงานไปยังหน่วยงานที่เกี่ยวข้องอีกทอดหนึ่ง เพื่อช่วยกันดำเนินงานตามขอบเขตหน้าที่และความสามารถของแต่ละหน่วยงาน (สันต์ทัศน์ มูลสันเทียะ, ๒๕๕๙)

ในการประสานความร่วมมือ มีรายละเอียด ดังนี้

๑.๑ การเจรจา (Negotiation) เป็นสิ่งแรกที่จำเป็นในการที่จะประสานขอความร่วมมือในรูปแบบเครือข่าย การเจรจาหรือการมีปฏิสัมพันธ์ การต่อรองที่เป็นทางการและไม่เป็นทางการย่อมสร้างความเข้าใจและการรับรู้ให้ตรงกันได้ เป็นจุดเริ่มต้นที่ก่อให้เกิดการตกลงยินยอมร่วมกัน เพื่อผลประโยชน์ต่างตอบแทนด้วยกันทุกฝ่ายเท่าเทียม

๑.๒ การตกลงยอมรับ (Commitment) เป็นการสร้างการตกลงยอมรับร่วมกันเพื่อดำเนินการในอนาคตผ่านการสร้างปฏิสัมพันธ์ต่าง ๆ และสามารถก่อเป็นรูปแบบเครือข่ายความร่วมมือในการดำเนินงานต่าง ๆ ได้

๑.๓ การดำเนินการ (Implementation) เป็นการปฏิบัติการตามข้อตกลงที่เกิดขึ้นร่วมกันผ่านบทบาทขององค์การและปฏิสัมพันธ์ระหว่างบุคคล ซึ่งควรดำเนินงานที่ก่อให้เกิดผลกระทบที่ดีหรือผลประโยชน์แก่องค์การที่เข้ามาเป็นสมาชิกในเครือข่ายร่วมมือ

๑.๔ การประเมิน (Assessments) เป็นการประเมินเชิงองค์การว่าทั้ง ๓ ขั้นตอนที่กล่าวมาข้างต้นอยู่บนพื้นฐานการแลกเปลี่ยนผลประโยชน์ต่อกันหรือไม่ ซึ่งหากประเมินแล้วพบว่า ข้อตกลงยอมรับร่วมกันไม่ได้ ก็จะเริ่มการดำเนินการเจรจาใหม่หรือสร้างข้อตกลงใหม่ซึ่งต้องคำนึงถึงการรักษาความร่วมมือให้ยั่งยืนอีกด้วย

๒. การพัฒนาบุคลากรให้มีความรู้ด้านอาชญากรรมทางเทคโนโลยี

ประเทศไทยประสบปัญหาขาดแคลนบุคลากรที่มีความรู้ด้านอาชญากรรมทางเทคโนโลยีเช่นเดียวกับประเทศอื่นๆ ทั่วโลก ซึ่งการพัฒนาบุคลากรทางด้านนี้ให้เพียงพอต่อความต้องการที่เพิ่มขึ้นสูงในภาคธุรกิจเป็นเรื่องที่ท้าทายและต้องได้รับการใส่ใจจากรัฐบาล

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้มีการมอบทุนการศึกษาแก่บุคลากรเพื่อไปศึกษาต่อยังต่างประเทศเกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสารสนเทศ เพื่อให้บุคคลเหล่านั้นกลับมาพัฒนาและให้ความรู้แก่บุคลากรอื่น นอกจากทุนการศึกษาแล้ว กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมยังเปิดโอกาสให้บุคลากรได้ไปอบรมและสัมมนาเพื่อสร้างความรู้ความเข้าใจทางไซเบอร์ (ธนิต ประภาตนันท์, ๒๕๕๙) ในขณะที่หน่วยงาน สพธอ. ทำการพัฒนาบุคลากรโดยแบ่งระดับตามความเชี่ยวชาญทางเทคนิคอย่างระดับผู้ใช้งานทั่วไป ระดับผู้บริหาร หรือระดับผู้เชี่ยวชาญทางเทคนิค และจัดทำการอบรมแตกต่างกันตามความชำนาญของแต่ละกลุ่มขึ้นอยู่กับระดับความซับซ้อนทางเทคนิคที่สามารถรับได้

ในส่วนของสำนักงานตำรวจแห่งชาติ พบว่า แนวทางในการพัฒนาศักยภาพของเจ้าหน้าที่ตำรวจในระดับต่าง ๆ ประกอบด้วย ความรู้ด้านเทคนิคด้านการสืบสวนสอบสวนโดยการเพิ่มทักษะการเรียนรู้ในด้านการสืบสวนสอบสวนแก้เจ้าหน้าที่ในระดับสถานี ทักษะด้านการรวบรวมพยานหลักฐาน โดยเฉพาะปัญหาในการรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์และหาตัวผู้กระทำความผิดที่เกี่ยวกับอาชญากรรมทางเทคโนโลยีที่ทำได้ล่าช้า และมักไม่ได้รับความร่วมมือจากหน่วยงานที่เกี่ยวข้องซึ่งรูปแบบการกระทำความผิดทางเทคโนโลยีต่าง ๆ ที่เจ้าหน้าที่ตำรวจในระดับสถานีเคยรับแจ้งความร้องทุกข์เพื่อดำเนินคดี จะเป็นคดีฉ้อโกงโดยซื้อของทางออนไลน์แล้ว ไม่ได้สินค้าหรือสินค้าไม่ตรงตามที่ซื้อ การบังคับใช้กฎหมายนั้นเห็นควรปรับปรุงและแก้ไขกฎหมายให้ครอบคลุม และทันสมัย ควรเป็นกฎหมายเฉพาะที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีที่ครอบคลุมการกระทำความผิดเกี่ยวกับเทคโนโลยีทุกประเภท โดยเฉพาะในด้านของการตีความกฎหมาย

นอกจากนี้ ปัจจุบันบริษัทเอกชน โดยเฉพาะบริษัทผู้ให้บริการอินเทอร์เน็ตกำลังประสบปัญหาการขาดแคลนแรงงาน ทั้งทางด้านจำนวนและคุณภาพของแรงงาน ภาคธุรกิจจึงมีการร่วมมือกับสถาบันการศึกษา โดยการให้ข้อมูลว่าภาคธุรกิจต้องการบุคลากรที่มีความรู้เฉพาะทางในด้านใดบ้าง อย่างเช่น มีการทำข้อตกลงร่วมกัน (MOU) ระหว่างบริษัทเอกชนและมหาวิทยาลัย เพื่อเข้าอบรมความรู้ด้านอาชญากรรมทางเทคโนโลยีให้กับนักศึกษา ไปจนถึงการเปิดโอกาสให้นักศึกษาเข้ามาฝึกงานที่บริษัท เป็นต้น โดยบริษัทเอกชนที่มีความต้องการต่อดังกล่าวช่วยสนับสนุนการศึกษาโดยการให้บุคคลากรผู้เชี่ยวชาญมาช่วยสอนให้ความรู้ และนำเครื่องมืออุปกรณ์มาให้ฝึกฝนการใช้งานจริง ในขณะที่ทางสถาบันการศึกษาหรือมหาวิทยาลัยก็มีบทบาทในการออกแบบหลักสูตร หรือเนื้อหาการเรียนการสอนให้ตรงกับสิ่งที่ตลาดแรงงานต้องการ

ทำให้นักศึกษาที่จบมามีงานรองรับ ซึ่งหากภาครัฐมีการเข้ามาช่วยกระตุ้น สถาบันการศึกษาอย่างเดียวกันก็จะช่วยทำให้กระบวนการพัฒนาบุคลากรนี้มีประสิทธิภาพยิ่งขึ้น (ก้อง จันทร์เต็ม, ๒๕๕๙)

๓. การพัฒนาศักยภาพด้านการรักษาความปลอดภัยไซเบอร์ และการฝึกฝนตอบสนอง ต่อการโจมตีทางไซเบอร์ (Incident Drill)

การฝึกฝนตอบสนองต่อการโจมตีทางไซเบอร์มีอยู่หลายระดับ ทั้งระดับของผู้บริหาร ระดับปฏิบัติการ และทางด้านเทคนิค อย่างเช่น ในระดับผู้บริหาร จะเน้นหัวข้อการฝึกตอบสนองเพื่อรับมือของผู้บริหารกับเหตุการณ์โจมตีที่อาจเกิดขึ้น เป็นต้น โดยการจัดการฝึกฝนตอบสนองการโจมตีทางไซเบอร์ให้มีประสิทธิภาพขึ้นอยู่กับความสามารถของหน่วยงานที่เป็นผู้นำในการฝึกฝน และการเลือกโจทย์ให้เหมาะสมกับการฝึกฝน เพื่อให้เกิดประโยชน์ต่อองค์กรที่เข้าร่วมงาน (นฤดม รุ่งศิริวงศ์, ๒๕๕๙) ในช่วงที่ผ่านมา พบการร่วมกันระหว่างรัฐบาลและบริษัทเอกชนที่เกี่ยวข้องในการจัดงานด้านการฝึกฝน ตอบสนองต่อการโจมตีทางไซเบอร์ ซึ่งการฝึกซ้อมทำให้ผู้ปฏิบัติงานเห็นภาพชัดเจนว่าต้องปฏิบัติอย่างไรเวลาเกิดปัญหาขึ้น อย่างไรก็ตาม ความจำเป็นของการฝึกฝนจะแตกต่างกันไปในแต่ละองค์กร แม้ว่าจะมีความจำเป็นต้องรู้ถึงวิธีการปฏิบัติงานในขั้นต้น แต่หากเกิดปัญหายากๆ กับองค์กรขนาดกลางหรือขนาดเล็กที่ทรัพยากรไม่เอื้ออำนวยก็อาจจะไม่สามารถปฏิบัติงานตามวิธีการที่ได้รับการฝึกฝนมาได้ ดังนั้น จึงไม่มีความจำเป็นที่จะต้องฝึกทุกๆ เรื่องให้กับทุกองค์กร แต่ควรเลือกฝึกในเรื่องที่มีความจำเป็นเท่านั้น ส่วนในเรื่องที่มีความซับซ้อนหรือมีความยาก ก็นำไปฝึกให้กับองค์กรเฉพาะทางที่เกี่ยวข้องกับหน้าที่นี้โดยตรงแทน โดยอาจมีการกำหนดข้อตกลงร่วมกันในการปฏิบัติงานในกรณีที่เกิดปัญหา อย่างเช่น หากเกิดปัญหาในเบื้องต้น องค์กรอาจจะหาทางจัดการกับปัญหาด้วยตัวเองก่อน ซึ่งหากเกิดปัญหาลุกลามก็ให้ทำการแจ้งเหตุต่อไปยังองค์กรที่รับผิดชอบด้านนี้อีกทอดหนึ่ง เป็นต้น ดังนั้น การฝึกฝนการโจมตีด้านความปลอดภัยไซเบอร์จึงจำเป็นต้องแบ่งแยกประเภทหรือแยกหมวดหมู่กันไปตามกลุ่มของปัญหาหรือรูปแบบของปัญหาที่เกิดขึ้นจริงตามแต่ละองค์กร (ก้อง จันทร์เต็ม, ๒๕๕๙)

การจัดการฝึกฝนตอบสนองต่อการโจมตีทางไซเบอร์ของ สพธอ. ในช่วงเริ่มต้นเป็นการรวมเอาหลายๆ หน่วยงานมาฝึกร่วมกัน เนื่องจากในช่วงแรกยังไม่มีบุคลากรด้านความปลอดภัยไซเบอร์มากนัก ต่อมาเมื่อมีบุคลากรแบ่งตามหน่วยงานมากขึ้น จึงเริ่มแยกการฝึกฝนตอบสนองต่อการโจมตีทางไซเบอร์ออกเป็นกลุ่มๆ โดยศึกษาจากรูปแบบของประเทศญี่ปุ่นที่แยกออกเป็นหลายๆ ภาคส่วน (Sector) โดยในแต่ละภาคส่วนก็จะมือเครือข่ายกันในการแลกเปลี่ยนขอมูลซึ่งกันและกัน โดยรัฐบาลทำหน้าที่ในการส่งเสริมความร่วมมือผ่านเครือข่ายในแต่ละภาคส่วน ซึ่งต้องใช้เวลาในการปรับความเข้าใจเพื่อสร้างความเชื่อมั่นระหว่างหน่วยงานภายในภาคส่วนเดียวกัน โดยรัฐบาลเริ่มต้นผลักดันจากภาคส่วนที่มีความวิกฤติ หรือมีความสำคัญอย่างมากก่อน อย่างเช่น สถาบัน ทางการเงิน เป็นต้น แล้วจึงใช้เป็นแนวทางในการผลักดันความร่วมมือของภาคส่วนอื่น ๆ ต่อไป อย่างเช่น กลุ่มบริษัทประกัน กลุ่มพลังงาน กลุ่มโรงพยาบาล เป็นต้น สพธอ. จะทำหน้าที่เป็นผู้อำนวยความสะดวกให้กับหน่วยงานต่างๆ โดยเป็นผู้นำในการจัดตั้งการฝึกฝนตอบสนองต่อการโจมตีทางไซเบอร์ในช่วงเริ่มต้น โดยจะผลักดันให้แต่ละภาคส่วนสามารถจัดการฝึกฝนตอบสนองต่อการโจมตีทางไซเบอร์ได้เองในอนาคต (สันต์ทัศน์ มูลสันเทียะ, ๒๕๕๙)

๔. ความร่วมมือระหว่างประเทศในการจัดการกับปัญหาความปลอดภัยทางไซเบอร์

๔.๑ ความร่วมมือด้านความปลอดภัยไซเบอร์ในระดับภูมิภาค

การรวมกลุ่มของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภูมิภาคเอเชีย-แปซิฟิก

ความร่วมมือของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ นอกจากจะมีความร่วมมือในระดับรัฐต่อรัฐแล้ว ยังมีการรวมกลุ่มในระดับภูมิภาคและระดับนานาชาติด้วย โดยประเทศไทยได้มีความร่วมมือผ่านกลุ่มประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภูมิภาคเอเชีย-แปซิฟิก หรือ เอพีเซิร์ต (The Asia Pacific Computer Emergency Response Team : APCERT) ซึ่งเป็นการประสานความร่วมมือกับประเทศในภาคพื้นเอเชีย-แปซิฟิก โดยใน พ.ศ. ๒๕๕๘ มีการซ้อมรับมือภัยคุกคาม APCERT Drill ๒๐๑๕ ซึ่งเป็นการซ้อมระหว่างหน่วยงาน เซิร์ตของแต่ละประเทศซึ่งเป็นสมาชิกในกลุ่มประเทศภูมิภาคเอเชีย-แปซิฟิก หรือเอพีเซิร์ต โดยมีวัตถุ ปะสงค์ในการเตรียมความพร้อมรับมือ วิเคราะห์ และประสานงานแก้ไขภัยคุกคามที่เกิดขึ้น งานในครั้งนี้มีผู้เข้าร่วมงานทั้งหมด ๒๕ ทีม จากทั้งหมด ๑๙ ประเทศในภูมิภาคเอเชีย-แปซิฟิก และประเทศภูมิภาคอื่น อย่างเช่น อียิปต์ โมร็อกโก ตูนิเซีย ซึ่งเป็นสมาชิกในเครือข่ายองค์กรความร่วมมือชาวมุสลิมด้านการประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Organisation of The Islamic Cooperation – Computer Emergency Response Teams : OIC-CERT) (สำนักงาน พัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๘)

๔.๒ ความร่วมมือด้านความปลอดภัยไซเบอร์ของประชาคมอาเซียน

ความร่วมมือของประชาคมอาเซียนด้านความปลอดภัยไซเบอร์ และการต่อต้านอาชญากรรมไซเบอร์ เริ่มต้นจากการประชุมเรื่องอาชญากรรมข้ามชาติทั้งในระดับรัฐมนตรี (ASEAN Ministry Meeting on Transnational Crime : AMMTC) และของในระดับเจ้าหน้าที่อาวุโส (ASEAN Senior Officials Meeting on Transnational Crime : SOMTC) และการประชุมอาเซียนว่าด้วย ความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (ASEAN Regional Forum : ARF) โดยในการประชุมระดับรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ ครั้งที่ ๓ ที่จัดขึ้นใน พ.ศ. ๒๕๔๔ มีข้อตกลงร่วมกันในการรวมเอาอาชญากรรมทางไซเบอร์เป็นเรื่องที่ต้องดำเนินงานตามแผนงานของประชาคมอาเซียนในการต่อสู้กับอาชญากรรมข้ามชาติ ซึ่งต่อมาใน พ.ศ. ๒๕๕๖ ได้มีการจัดตั้งกลุ่มเจ้าหน้าที่อาวุโส (SOMTC) เพื่อประชุมหารือโดยเฉพาะด้านอาชญากรรมไซเบอร์ โดยความปลอดภัยไซเบอร์ ได้ถูกจัดอยู่ในกลุ่มของ ๕ ประเด็นหลักที่จำเป็นต้องได้รับความร่วมมืออย่างจริงจัง ซึ่งประกอบไปด้วยการแลกเปลี่ยนข้อมูล ความสำคัญของกฎหมาย การบังคับใช้กฎหมายการอบรมและเสริมสร้างทักษะ และการประสานงานเพิ่มขึ้นภายในภูมิภาค โดยมีการกำหนดกรอบร่วมกันเพื่อการสร้างความสามารถในการจัดการกับปัญหาอาชญากรรมทางไซเบอร์ ขึ้นใน พ.ศ. ๒๕๕๐ และก่อตั้งกลุ่มดำเนินงานเฉพาะด้านอาชญากรรมไซเบอร์ขึ้นใน พ.ศ. ๒๕๕๖ (สำนักเลขาธิการอาเซียน, ๒๕๕๖)

ในการประชุม ASEAN Japan Information Security Policy Workshop พ.ศ. ๒๕๕๖ เป็นการประชุมระดับนโยบายเพื่อพิจารณากิจกรรมความร่วมมือระหว่างอาเซียนและญี่ปุ่นเกี่ยวกับการตระหนักรู้เรื่องความมั่นคงปลอดภัยทางสารสนเทศ การขยายแนวทางความร่วมมือระหว่างอาเซียนและญี่ปุ่น และการประชุมเชิงปฏิบัติการที่จะเป็นการให้ความรู้เชิงเทคนิคสำหรับปฏิบัติการด้านความมั่นคงปลอดภัยทางสารสนเทศ และการพัฒนาศักยภาพของศูนย์ประสานงานการรักษาความมันคงปลอดภัยทางคอมพิวเตอร์หน่วยงานไทยเซิร์ต ของ สพธอ. ได้รับมอบหมายจากกระทรวงดีอี ให้เป็นผู้เข้าร่วมประชุม โดยมีการลงนามบันทึกข้อตกลงความร่วมมือระหว่าง สพธอ. และหน่วยงาน Information and Communication Bureau (ICB) ภายใต้หน่วยงานกระทรวงกิจการภายในและการสื่อสารของรัฐบาลญี่ปุ่น (Ministry of Internal Affairs and Communications of Japan : MIC) ซึ่งการลงนามในครั้งนี้เป็นผลสืบเนื่องมาจากการการประชุมหารือทวิภาคีระหว่างรัฐมนตรีว่าการกระทรวงดีอี กับรัฐมนตรีว่าการกระทรวงกิจการภายในและการสื่อสารของประเทศญี่ปุ่น ในระหว่างการประชุมรัฐมนตรีเอเปก ด้านโทรคมนาคมและอุตสาหกรรมสารสนเทศ ครั้งที่ ๙ ณ นครเซนต์ปีเตอร์สเบิร์ก สหพันธรัฐรัสเซีย โครงการ Proactive Response Against Cyberattacks Through International Collaborative Exchange (PRACTICE) แบ่งออกเป็นสองส่วน คือ ส่วนงานวิจัย (Darknet) คือการติดตังซอฟต์แวร์และฮาร์ดแวร์ เพื่อเก็บข้อมูลสำหรับวิเคราะห์ หารูปแบบภัยคุกคามด้านสารสนเทศจากเครือข่ายคอมพิวเตอร์ และส่วนที่สองเป็นการดำเนินการ (Honeypot) ซึ่งนำตัวอย่างซอฟต์แวร์ไม่พึงประสงค์มาวิเคราะห์เพื่อนำไปกำหนดแนวทางการกำจัดซอฟต์แวร์ไม่พึงประสงค์ออกจากระบบ ซึ่งการลงนามข้อตกลงในครั้งนี้ มีจุดประสงค์เพื่อการแจ้งเตือน เมื่อมีเหตุต้องสงสัยว่าจะมีภัยคุกคาม การแลกเปลี่ยนข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยระหว่างประเทศไทยกับประเทศญี่ปุ่น และการสร้างความเข้าใจรูปแบบการโจมตีระบบหรือเครือข่ายสารสนเทศจากซอฟต์แวร์ไม่พึงประสงค์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

ประชาคมอาเซียนมีการดำเนินความร่วมมือด้านความปลอดภัยไซเบอร์เริ่มตั้งแต่ ปี พ.ศ. ๒๕๔๔ โดยการผลักดันการดำเนินงานผ่านการประชุมทั้งระดับรัฐมนตรีและระดับเจ้าหน้าที่อาวุโสในการพัฒนากรอบความร่วมมือในการแลกเปลี่ยนข้อมูล การกำหนดมาตรฐานและประสานความร่วมมือระหน่วยงานที่เกี่ยวข้องการกำหนดยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ร่วมกันในการสนับสนุนการดำเนินงานภายในประชาคมอาเซียน การร่วมมือด้านความปลอดภัยของประชาคมอาเซียนมีบทบาทสำคัญที่จะช่วยในการพัฒนามาตรฐานความปลอดภัยไซเบอร์ร่วมกันได้ โดยเป็นการเริ่มต้นการพัฒนาที่ระดับภูมิภาค เนื่องจากมีการประชุมในระดับรัฐมนตรีซึ่งมีอำนาจในการผลักดันนโยบายระดับประเทศ บวกกับพื้นฐานความใกล้เคียงของประเทศภายในภูมิภาคและความต้องการในการพัฒนาโครงสร้างพื้นฐานร่วมกัน จึงทำให้สามารถดำเนินความร่วมมือทางด้านความปลอดภัยไซเบอร์ได้ง่ายขึ้น ซึ่งการกำหนดนโยบายและมาตรฐานร่วมกัน ไปจนถึงการดำเนินงานที่สอดคล้องไปในทิศทางเดียวกันของกลุ่มประเทศอาเซียน จะช่วยเสริมสร้างความแข็งแกร่งให้กับประเทศสมาชิกซึ่งจะเป็นรากฐานในการพัฒนาทางด้านเศรษฐกิจต่อไป

๔.๓ ความร่วมมือกับบรรษัทข้ามชาติ

ใน พ.ศ. ๒๕๕๖ ได้มีการลงนามบันทึกความเข้าใจ (MOU) ระหว่าง ไทยเซิร์ต กับสถาบัน SANS ซึ่งเป็นสถาบันฝึกอบรม ออกใบรับรอง และวิจัยด้านความปลอดภัยระบบคอมพิวเตอร์ระดับสูงที่ได้รับความเชื่อถือระดับนานาชาติ มีหลักสูตรมากกว่า ๕๐ หลักสูตร และมีใบรับรองด้านความปลอดภัยสารสนเทศ (Information Security) มากถึง ๒๕ ประเภท การลงนามครั้งนี้มีจุดประสงค์ในการเพิ่มจำนวนผู้เชี่ยวชาญเฉพาะทางด้านความปลอดภัยระบบคอมพิวเตอร์ของประเทศ โดยกำหนดปัจจัยในการดำเนินการไว้ ๕ ข้อคือ การค้นหาผู้ที่มีพื้นฐานและศักยภาพสามารถรับการอบรมได้ การอบรมด้วยเนื้อหาที่ทันสมัยผ่านการรับรองและเอถือได้การคัดเลือกผู้ฝึกอบรมที่มีความสามารถ และทักษะในการสอนที่ดี ให้การรับรองผู้เข้าอบรมว่าเป็นผู้ที่เข้าใจในเนื้อหาอย่างแท้จริง โดยใช้การประเมินจากการปฏิบัติจริง และสุดท้ายคือการตั้งกลุ่มผู้มีความสามารถในการจัดโปรแกรมฝึกอบรมได้ด้วยตัวเอง เพื่อพัฒนาบุคลากรให้มีความสามารถต่อไป (สพธอ., ๒๕๕๖) และใน พ.ศ. ๒๕๕๗ ได้จัดสัมมนา เรื่อง “Client-side Attacks : Use-after-Free Exploitation” เพื่อแลกเปลี่ยนความรู้ และเผยแพร่ข้อมูลรูปแบบของภัยคุกคาม ที่สามารถหลบหลีกจากการตรวจจับหรือป้องกันจากอุปกรณ์และระบบการรักษาความมั่นคงปลอดภัยที่มีอยู่ในปัจจุบัน โดยผู้เชี่ยวชาญจาก SANS เป็นผู้ให้ความรู้ในเรื่องของภัยคุกคามประเภท Client-side attack โดยใช้เทคนิค Use-after-Free Exploitation (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๘)

ความร่วมมือกับสถาบัน EC-Council (The International Council of Electronic Commerce Consultants) ที่มีชื่อเสียงในการพัฒนาผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยระดับโลก (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

๔.๔ ความร่วมมือผ่านองค์กรระหว่างประเทศ

ความร่วมมือของ สมาพันธ์นานาชาติประสานความร่วมมือระหว่างหน่วยงานเซิร์ต ทั่วโลก หรือ เฟิร์ส (Forum of Incident Response and Security Teams: FIRST) ใน พ.ศ. ๒๕๕๖ ไทยเซิร์ต ได้เป็นตัวแทนประเทศไทยในการเป็นเจ้าภาพจัดประชุมระดับนานาชาติของ Forum of Incident Response and Security Teams (FIRST) ซึ่งเป็นการประชุมประจำปีที่ ๒๕ ในหัวข้อ “Incident Response : Sharing To Win” เป็นการส่งเสริมความร่วมมือของผู้เชี่ยวชาญจากทั่วโลก วัตถุประสงค์ของการประชุมคือการสร้างความร่วมมือ ประสานงานระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ การแลกเปลี่ยนแนวคิด แบ่งปันประสบการณ์ ไปจนถึงข้อมูลด้านความปลอดภัย (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

ใน พ.ศ. ๒๕๕๕ มีการจัดฝึกอบรม เรื่องการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย (Securing Networks) โดย สพธอ. ร่วมกับ ITU-IMPACT (International Telecom - munication Union - International Multilateral Partnership Against Cyber Threats) ซึ่งเป็นหน่วยงานด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภายใต้การกำกับดูแลของ UN (United Nation) ทำการอบรมให้กับผู้เชี่ยวชาญด้านเครือข่ายในภูมิภาคอาเซียน ประกอบด้วย กัมพูชา เมียนมาร์ ลาว เวียดนาม และ ไทย จำนวนทั้งหมด ๒๕ คน (สพธอ., ๒๕๕๕)

ใน พ.ศ. ๒๕๕๖ ไทยเซิร์ต ได้เข้าร่วมเป็นเครือข่ายกับ Team Cymru ซึ่งเป็นหน่วยงาน ประเภทไม่แสวงหาผลกำไรในประเทศสหรัฐอเมริกาที่ทำการวิจัยและพัฒนาเทคโนโลยีด้านความปลอดภัยสารสนเทศ โดยไทยเซิร์ตจะได้รับข้อมูลสถานการณ์ด้านความปลอดภัย (Incident) ที่เกิดขึ้นกับระบบคอมพิวเตอร์ภายในเครือข่ายอินเทอร์เน็ตของประเทศไทยจาก Team Cymru ที่ได้ตรวจจับจากระบบเฝ้าระวังที่ติดตั้งไว้ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖) นอกจากนั้น ไทยเซิร์ต ยังได้ร่วมมือกับกลุ่ม Anti-Phishing Working Group หรือ APWG ซึ่งเป็นกลุ่มศูนย์กลางที่รวบรวมข้อมูลและสถิติ ปัญหา และวิธีการแก้ปัญหาฟิชชิ่ง (Phishing) เพื่อเป็นกลไกสำคัญที่ช่วยยกระดับการทำงานเชิงรุกให้แก่ไทยเซิร์ตในการแก้ไขปัญหาภัยคุกคามฟิชชิ่ง (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

สำหรับความร่วมมือกับ OWASP ซึ่งเป็นองค์กรไม่แสวงหาผลกำไรที่มุ่งเน้นการพัฒนาความรู้ด้านความปลอดภัยให้แก่ผู้พัฒนาซอฟต์แวร์ ได้ร่วมกันจัดการอบรมเชิงปฏิบัติการในการพัฒนา Secure Web Application โดยวิทยากรที่เป็นผู้บริหารสูงสุดของบริษัท Thames Stanley และกรรมการผู้บริหารของ OWASP London Chapter มาให้ความรู้แก่ผู้พัฒนาเว็บไซต์และผู้ดูแล เว็บไซต์ไทย มีผู้สนใจเข้าร่วมงานทั้งจากภาครัฐและรัฐวิสาหกิจทั้งหมด ๑๘ หน่วยงาน โดยได้เรียนรู้เคล็ดลับที่ช่วยให้แอปพลิเคชั่นมีความปลอดภัยและเทคนิคการวิเคราะห์ช่องโหว่ในเว็บแอปพลิเคชั่นด้วย (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, ๒๕๕๖)

ในปีเดียวกัน สพธอ. ได้ร่วมมือกับ Business and Application Working Group ภายใต้ Asia PKI Consortium จัดงานสัมมนาเพื่อความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีต่างๆ ในหัวข้อ “The Common Denominators – Collaboration of Cross-Region on e–Government Application, Cloud Computing and Security” โดยประเทศไทยได้รับเกียรติให้เป็นเจ้าภาพในการจัดงานสัมมนา มีสมาชิก Asia PKI Consortium จากต่างประเทศเข้าร่วม อาทิ จีน ฮ่องกง ไต้หวัน มาเก๊า รวมทั้งประเทศอื่นๆ อย่างเช่น ประเทศมาเลเซีย บังคลาเทศ เป็นต้น การจัดสัมมนาครั้งนี้ เกิดขึ้นจากการตระหนักถึงความปลอดภัยในการใช้งานเทคโนโลยีอย่าง Social Media และการใช้งาน Cloud Computing ที่รวมเอาข้อมูลจำนวนมากของผู้บริโภคไว้ และมีแนวโน้มเพิ่มสูงขึ้นอย่างมาก ทำให้จำเป็นต้องคำนึงถึงความปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล โดยการวิเคราะห์ถึงรูปแบบของภัยคุกคามที่เกิดขึ้น การสนับสนุนให้ความรู้กับประชาชนถึงวิธีการในการใช้งานเทคโนโลยีอย่างถูกต้องและมีมาตรฐาน รวมไปถึงการร่วมมือกันในการลดผลกระทบจากการใช้งานที่ไม่เหมาะสม (สพธอ., ๒๕๕๖)

๕. มาตรการในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมไซเบอร์

๕.๑ มาตรการในเชิงบริหาร

๕.๑.๑ เร่งออกกฎหมาย อาชญากรรมทางคอมพิวเตอร์ รวมทั้ง ระเบียบปฏิบัติที่เกี่ยวข้อง

๕.๑.๒ กำหนดกลุ่มผู้พิพากษา หรือจัดตั้งศาล IT ขึ้นมา เพื่อให้พิจารณาคดีความด้าน IT เป็นการเฉพาะ เช่นเดียวกับศาลทรัพย์สินทางปัญญา

๕.๑.๓ กำหนดกลุ่มพนักงานอัยการ หรือจัดตั้งอัยการกองพิเศษ ขึ้นมาเพื่อให้พิจารณาคดีความด้าน IT เป็นการเฉพาะ

๕.๑.๔ จัดตั้งกองบังคับการสืบสวนอาชญากรรมไซเบอร์ ในสังกัดสำนักงานตำรวจแห่งชาติ เพื่อให้เป็นหน่วยงานที่คอยตรวจตรา เฝ้าระวัง ค้นหาการกระทำผิดบนอินเทอร์เน็ตตลอดเวลา ๒๔ ชั่วโมง รวมทั้งการสืบสวนเฉพาะทางด้านเทคนิค เพื่อได้ทราบถึงแหล่งที่มาหรือผู้กระทำผิดแล้วส่งข้อมูลให้หน่วยที่เกี่ยวข้อง สืบสวน สอบสวนต่อไป อีกทั้ง ควรทำหน้าที่ตรวจพิสูจน์เครื่องคอมพิวเตอร์ของกลางค้นหาหลักฐาน เป็นการช่วยเหลือหน่วยปฏิบัติ และมีหน้าที่รับแจ้งเหตุเบื้องต้นจากผู้เสียหาย เพื่อประสานงานกับผู้ที่เกี่ยวข้อง เพื่อจำกัดความเสียหายให้ห้อยลงโดยเร็ว และเพื่อเก็บรวบรวมหลักฐานในทันทีก่อนที่จะถูกเปลี่ยนแปลง หรือสูญหายไป

๕.๑.๕ จัดตั้งศูนย์รักษาความปลอดภัยข้อมูลในเครือข่าย (Thai CERT) ในสังกัดของ NECTEC เพื่อเป็นศูนย์กลางในการประสานงานกับหน่วยงานและผู้เกี่ยวข้องทั้งในและต่างประเทศ และเป็นศูนย์รวมความรู้ แนวทางปฏิบัติ เพื่อการป้องกันภัยของข้อมูล ในเครือข่าย

๕.๑.๖ กสท. กำชับให้ผู้บริการอินเทอร์เน็ต (ISP) ปฏิบัติตามสัญญาอย่างเคร่งครัด รวมทั้ง ต้องกำชับให้ ISP กวดขัน และกำชับให้ผู้ให้บริการต่อช่วงของตน ปฏิบัติตามสัญญาอย่างเคร่งครัด

๕.๑.๗ กำหนดให้มีช่องทางติดต่อสื่อสารพิเศษ ระหว่าง NECTEC (Thai CERT), ตำรวจ, กสท. ISP และสถาบันการศึกษาที่ต่อเชื่อมอินเทอร์เน็ตโดยไม่ผ่าน ISP ในประเทศการสื่อสารดังกล่าวเป็นคล้าย Hot Line ในระดับของผู้ปฏิบัติทางเทคนิค โดยให้แต่ละฝ่ายแจ้ง ชื่อ-นามสกุล, ตำแหน่ง, โทรศัพท์ที่ทำงาน, โทรศัพท์ที่บ้าน, โทรศัพท์มือถือ, เพจเจอร์ และอีเมล์ เพื่อใช้ในการติดต่อประสานงานได้โดยตรง

๕.๑.๘ กำหนดให้ ISP ทุกแห่ง ตั้งเวลาเครื่องให้ตรงตามมาตรฐาน

๕.๑.๙ สร้างแนวร่วมในหมู่ของผู้ใช้อินเทอร์เน็ต ให้ช่วยกันสอดส่องดูแลและแจ้งเบาะแส หากพบเห็นการกระทำผิดบนอินเทอร์เน็ต ไปยังหน่วยงานที่เกี่ยวข้อง รวมทั้งอาจใช้แนวร่วมนี้เป็นพลังในการต่อต้านสิ่งที่ไม่เหมาะสมบนอินเทอร์เน็ต

๕.๒ มาตรการในทางปฏิบัติกรณีเว็บไซต์ผิดกฎหมาย จาบจ้วง เป็นภัยต่อความมั่นคงของชาติ และที่ไม่เหมาะสม

๕.๒.๑ ในส่วนของเว็บไซต์ผิดกฎหมาย เว็บไซต์จาบจ้วง เว็บไซต์เป็นภัยต่อความมั่นคงของชาติ และเว็บไซต์ที่ไม่เหมาะสมนั้น ควรกำหนดให้ฝ่ายตำรวจเป็นศูนย์กลาง แจ้งเวียนไปยัง ISP และผู้ดูแลระบบของสถาบันการศึกษา (ที่ไม่ผ่าน ISP ในประเทศ) ทำการปิดกั้นเว็บไซต์ดังกล่าว ไม่ให้สามารถเรียกได้จากในประเทศ รวมทั้งแจ้งไปยัง NECTEC (Thai CERT) และ กสท. เพื่อทราบ การแจ้งเวียนดังกล่าวควรใช้อีเมล์ที่ได้ ตกลงกันไว้เป็นหลัก โดยจะส่งถึงระดับผู้บริหารของ ISP และระดับผู้ปฏิบัติ (admin) ของ ISP นั้นด้วย เว้นแต่เป็นกรณีเร่งด่วน อาจใช้โทรศัพท์แจ้งไปก่อน แล้วจึงส่งอีเมล์ ตามไปภายหลัง

๕.๒.๒ การใช้อีเมล์ในการติดต่อนั้น ควรเป็นอีเมล์ที่มีการเข้ารหัสรักษาความปลอดภัยไว้ด้วย หากผู้รับเกิดความสงสัย ให้โทรศัพท์สอบถามกลับไปตามหมายเลข โทรศัพท์ที่กำหนดไว้ เพื่อเป็นการยืนยันความถูกต้อง

๕.๒.๓ เมื่อผู้ปฏิบัติ (admin) ของ ISP แต่ละรายรวมทั้งผู้ดูแลระบบของสถาบันการศึกษาฯ ได้รับแจ้งทางอีเมล์ดังกล่าวแล้ว และอาจตรวจสอบแล้วว่าเว็บไซต์ดังกล่าวเข้าข่ายอยู่ในประเภทข้างต้นจริง ก็ให้ดำเนินการปิดกั้นเว็บไซต์นั้นในทันที โดยไม่จำเป็นต้องรอขออนุมัติจากผู้บริหารของ ISP นั้นก่อน อนึ่ง เมื่อได้ดำเนินการปิดกั้นแล้ว ให้ส่งอีเมล์แจ้งให้ฝ่ายตำรวจทราบด้วย

๕.๒.๔ ภายใน ๓ วันทำการ นับจากได้มีการแจ้งให้ปิดกั้นเว็บไซต์นั้นแล้ว แต่ ISP นั้นยังไม่ดำเนินการ ให้ฝ่ายตำรวจทำเป็นหนังสือราชการ และส่งอีเมล์แจ้งไปยังผู้บริหาร ISP นั้น ทราบอีกครั้ง และสำเนาแจ้งให้ กสท. และ NECTEC ทราบ หากภายใน ๑๕ วัน (นับแต่การแจ้งให้ทราบครั้งแรก) ISP นั้น ยังไม่ดำเนินการ โดยไม่มีเหตุผลชี้แจงให้ กสท. ดำเนินการตามที่สัญญาได้กำหนดไว้ และให้ NECTEC ดำเนินการปลดสายสัญญาณของ ISP นั้น ออกจาก PIE หรือระบบอื่น ๆ

๕.๒.๕ หากเว็บไซต์ดังกล่าว ใช้ Server ในประเทศที่อยู่ในความรับผิดชอบของ ISP ใด หรือของผู้ให้บริการเช่าช่วงต่อจาก ISP ใด ให้ ISP นั้น ยุติการให้บริการในทันทีแล้วให้ส่งข้อมูลของผู้เช่าพื้นที่ใน Server นั้น ให้ฝ่ายตำรวจทราบ มิฉะนั้นอาจถือได้ว่าเป็นผู้ร่วมกระทำความผิดด้วย

๕.๒.๖ ในกรณีของเว็บไซต์จาบจ้วง เว็บไซต์เป็นภัยต่อความมั่นคงของชาติ และเว็บไซต์ที่ไม่เหมาะสม ลบหลู่ศาสนา อาจขอความร่วมมือไปยังกลุ่มแนวร่วมผู้ใช้อินเทอร์เน็ตผู้รักชาติให้ช่วยกันต่อต้านและประณามเว็บไซต์ดังกล่าวได้อีกทางหนึ่ง

สรุป

ปัญหา/อุปสรรค และแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี แบ่งเป็น สถานการณ์การใช้งานอินเทอร์เน็ต และภัยคุกคามจากอาชญากรรมทางเทคโนโลยี ซึ่งมีภัยคุกคามต่างๆ ได้แก่ ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์บนโทรศัพท์มือถือ ภัยคุกคามจากการใช้งานเครือข่าย รวมถึงและกฎหมายต่างๆ ที่เกี่ยวข้องกับการป้องกันอาชญากรรมทางเทคโนโลยี โดยจำเป็นต้องมี การประสานความร่วมมือระหว่างรัฐบาลกับหน่วยงานอื่นที่ไม่ใช่รัฐที่สามารถช่วยในการพัฒนาบุคลากรให้มีความรู้ด้านอาชญากรรมทางเทคโนโลยีและการพัฒนาศักยภาพด้านการรักษาความปลอดภัยไซเบอร์ และการฝึกฝนตอบสนอง ต่อการโจมตีทางไซเบอร์ได้

บทที่ ๔
อภิปรายผล

ในบทนี้ ผู้วิจัยขอเสนอการอภิปรายผล ในประเด็นต่าง ๆ ดังนี้

ลักษณะเด่นของนโยบายเกี่ยวกับการป้องกันอาชญากรรมทางเทคโนโลยี

๑. ลักษณะเด่นของนโยบายด้านความปลอดภัยไซเบอร์ของรัฐบาลไทย

รัฐบาลมีการกำหนดกรอบข้อบังคับและกฎหมายในการปฏิบัติเพื่อให้เกิดความปลอดภัยในการใช้งานอินเทอร์เน็ตที่เป็นจุดเริ่มต้นที่กระตุ้นทั้งภาครัฐ เอกชน และประชาชน ในการจัดทำแผนงานด้านการรักษาความปลอดภัยในการใช้งานคอมพิวเตอร์ โดยการดำเนินงานภายในประเทศด้านความปลอดภัยไซเบอร์ของ สพธอ. พบว่า สพธอ. มีการดำเนินงาน ครบทุกด้าน ทั้งการสร้างเครือข่ายของหน่วยงานรัฐ และการประสานความร่วมมือกับองค์กรอื่นๆ ที่ เกี่ยวข้อง การผลักดันให้เกิดการก่อตั้งกลุ่มเซิร์ต ของแต่ละภาคส่วน (Sector Base CERT) เพื่อให้เกิดความร่วมมือกันด้านความปลอดภัยไซเบอร์ภายในกลุ่มการดำเนินงานจัดทำสถิติภัยคุกคาม รวมถึงการพัฒนาระบบเฝ้าระวังและวิเคราะห์ช่องโหว่ภัยคุกคามให้กับหน่วยงานภาครัฐ การดำเนินงานเพื่อพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์ ทั้งการจัดฝึกอบรม การมอบทุนการศึกษา และการพัฒนามาตรฐานใบรับรองด้านความปลอดภัยไซเบอร์ การจัดฝึกซ้อมการตอบสนองต่อภัยคุกคามให้กับหน่วยงานต่างๆ การยกระดับมาตรฐานความปลอดภัยไซเบอร์ โดยเริ่มจากการสร้างความเข้มแข็งให้กับหน่วยงานภาครัฐ การกำหนดมาตรฐานความปลอดภัยไซเบอร์ของไทย และการเผยแพร่ข้อมูลข่าวสารภัยคุกคามไซเบอร์เพื่อสร้างความตระหนักด้านความปลอดภัยไซเบอร์ในสังคมไทย

๒. ลักษณะเด่นของความร่วมมือระหว่างประเทศด้านความปลอดภัยไซเบอร์

รัฐบาลไทยใช้ความร่วมมือระหว่างประเทศเป็นเครื่องมือเพื่อให้บรรลุเป้าหมายในการสร้างความปลอดภัยทางไซเบอร์ให้กับประเทศ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ภายใต้การกำกับดูแลของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้รับหน้าที่ให้เป็นตัวแสดงหลักที่สำคัญในการประสานความร่วมมือกับต่างประเทศ ประเด็นด้านความปลอดภัยทางไซเบอร์กลายเป็นหัวข้อที่เชื่อมโยงความสัมพันธ์ในรูปแบบของการพึ่งพาอาศัยซึ่งกันและกันในการจัดการแก้ไขปัญหา และยังพบความร่วมมือในหลายรูปแบบ เป็นการประสานงานจากทั้งความร่วมมือเดิมที่มีอยู่ก่อนแล้ว อย่างเช่น ความร่วมมือของประชาคมอาเซียนที่มีการเพิ่มหัวข้อด้านการรักษาความปลอดภัยไซเบอร์ไว้เป็นประเด็นหนึ่งในเรื่องของอาชญากรรมข้ามชาติ เป็นต้น และการดำเนินความสัมพันธ์ใหม่ๆ ที่เกิดขึ้นเฉพาะเพื่อการจัดการปัญหาความปลอดภัยไซเบอร์ อย่างเช่น การประสานความร่วมมือผ่านหน่วยงานเซิร์ตของแต่ละประเทศ และการร่วมมือกับสถาบัน

อบรมและออกใบรับรองที่มีชื่อเสียงจากต่างประเทศ เป็นต้น โดยจากการศึกษาการดำเนินงานความร่วมมือระหว่างประเทศของ สพธอ. สามารถแบ่งรูปแบบของความร่วมมือทางด้านความปลอดภัยไซเบอร์หลักๆ ได้ดังนี้

๒.๑ การแลกเปลี่ยนข้อมูลการถูกโจมตี ความรู้ด้านนวัตกรรมทางเทคโนโลยีและวิธีปฏิบัติในการรักษาความปลอดภัยไซเบอร์ที่ทันสมัย สพธอ. มีการดำเนินงานโดยหน่วยงานไทยเซิร์ต เป็นตัวแทนของรัฐบาลในการดำเนินความร่วมมือผ่านกลุ่มเซิร์ต ทั้งในระดับภูมิภาค เอพี เซิร์ต ระดับนานาชาติ เฟิร์ส และความร่วมมือระหว่างรัฐ ในการแลกเปลี่ยนแนวคิด แบ่งปันประสบการณ์ไปจนถึงข้อมูลด้านความปลอดภัย ซึ่งความสำคัญของการแลกเปลี่ยนข้อมูลคือการเพิ่มความสามารถในการจัดการกับปัญหาความปลอดภัยทางไซเบอร์ การรู้เท่าทันภัยคุกคามทางไซเบอร์ที่มีการวิวัฒนาการไปอย่างรวดเร็ว

๒.๒ การแลกเปลี่ยนบุคลากรผู้เชี่ยวชาญ การจัดสัมมนา และฝึกอบรม เพื่อให้ความรู้ ทักษะ แลกเปลี่ยนประสบการณ์ และพัฒนาบุคลากรด้านความปลอดภัยทางไซเบอร์ร่วมกัน สพธอ. มีการซ้อมรับมือภัยคุกคามผ่านความร่วมมือของกลุ่มเซิร์ต ในการเตรียมความพร้อมรับมือวิเคราะห์ และประสานงานแก้ไขภัยคุกคามที่เกิดขึ้น การจัดอบรมความรู้ในการพัฒนาซอร์ฟแวร์แบบมั่นคงปลอดภัยในขณะที่ความร่วมมือกับสถาบันอบรมและออกใบรับรองด้านความปลอดภัยไซเบอร์จากต่างประเทศ ซึ่งช่วยในการพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์ให้มีคุณภาพตามมาตรฐานสากล

๒.๓ การกำหนดมาตรฐานความปลอดภัยทางไซเบอร์ร่วมกัน ประเทศไทยมีการร่วมมือผ่านประชาคมอาเซียนในการจัดประชุมเชิงนโยบายด้านความปลอดภัยไซเบอร์ การลงมติในการพัฒนาศักยภาพในการดำเนินงานของหน่วยงานเซิร์ต (CERTs) ของแต่ละประเทศให้ผ่านตามมาตรฐานขั้นต่ำ ซึ่งกลายเป็นจุดเริ่มต้นของการประชุมอาเซียนด้านความปลอดภัยไซเบอร์ การพัฒนากฎหมายความปลอดภัยไซเบอร์ของแต่ละประเทศ

๒.๔ การส่งเสริมการวิจัยและการพัฒนาร่วมกัน สพธอ. มีการร่วมมือด้านการวิจัยและพัฒนานวัตกรรมระหว่างประเทศผ่านเครือข่ายเซิร์ต และความร่วมมือระหว่างอาเซียนกับประเทศญี่ปุ่นอย่างการวิเคราะห์หารูปแบบภัยคุกคามด้านสารสนเทศจากเครือข่ายคอมพิวเตอร์ และการร่วมทุน เพื่อสนับสนุนงานวิจัยทางด้านความปลอดภัยไซเบอร์ เป็นต้น

จากการศึกษาการดำเนินงานของรัฐบาลไทยที่ผ่านมา พบว่า การดำเนินความร่วมมือระหว่างประเทศของรัฐบาลไทยที่มีความหลากหลาย ทั้งแบบรัฐต่อรัฐความร่วมมือระดับภูมิภาค ความร่วมมือกับบริษัทข้ามชาติและองค์กรระหว่างประเทศ รัฐบาลไทยใช้ช่องทางที่หลากหลายเหล่านี้เป็นเครื่องมือในการดำเนินความร่วมมือเพื่อให้ได้มาซึ่งผลประโยชน์ด้านการพัฒนาศักยภาพด้านความปลอดภัยไซเบอร์ของประเทศ โดยในช่วงที่ผ่านมา รัฐบาลไทยเน้นในเรื่องของการพัฒนาศักยภาพทั้งของบุคคลากรและองค์กรเป็นหลัก เนื่องจากความสามารถในการจัดการกับปัญหาความปลอดภัยไซเบอร์ ต้องอาศัยประสบการณ์ และความชำนาญ ความร่วมมือระหว่างประเทศในการแลกเปลี่ยนข้อมูลการถูกโจมตี ความรู้ด้านนวัตกรรม และการแลกเปลี่ยนบุคลากรผู้เชี่ยวชาญ การจัดสัมมนาและฝึกอบรมเป็นความร่วมมือที่จะช่วยในการพัฒนาศักยภาพทั้งของบุคลากรและองค์กรได้ดีและรวดเร็วกว่าการพัฒนาศักยภาพด้วยตนเองภายในประเทศ

ปัญหาและอุปสรรคของนโยบายด้านความปลอดภัยไซเบอร์ของรัฐบาลไทย

๑. ปัญหาของการกำหนดนโยบายและกฎหมายด้านความปลอดภัยไซเบอร์

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และการกำหนดแต่งตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) ซึ่งมีการกำหนดยุทธศาสตร์ และระยะเวลาในการดำเนินงานของรัฐ เป็นความพยายามของรัฐบาลไทยในการกำหนดนโยบายด้านความปลอดภัยไซเบอร์ระดับชาติที่มีขึ้นตั้งแต่ พ.ศ. ๒๕๕๖ แต่ไม่ได้มีการดำเนินงานอย่างต่อเนื่องจากการเปลี่ยนแปลงรัฐบาล ทำให้พระราชบัญญัติฉบับนี้ได้รับการปรับปรุงและผลักดันการดำเนินงานของคณะกรรมการ กปช. ขึ้นใหม่อีกครั้งใน พ.ศ. ๒๕๕๘ ซึ่งรวมเป็นส่วนหนึ่งของการปรับปรุงโครงสร้างกระทรวงไอซีที เปลี่ยนเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงดีอี) โดยคณะกรรมการ กปช. และสำนักงานคณะกรรมการ กปช. จะอยู่ภายใต้กระทรวงดีอี โดยกำหนดให้รัฐมนตรีว่าการของกระทรวงดีอีเป็นประธาน และกำหนดให้มีการถ่ายโอนหน่วยงานด้านความปลอดภัยทางไซเบอร์ที่อยู่ในความดูแลของ สพธอ. อย่างหน่วยงานไทยเซิร์ต และหน่วยงานพิสูจน์หลักฐานทางดิจิทัล ย้ายไปดำเนินงานภายใต้สำนักงาน กปช. อย่างไรก็ตามยังไม่มีการผ่านร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และการกำหนดแต่งตั้ง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) ในปีดังกล่าว ทำให้ประเทศไทย ยังคงขาดนโยบายด้านความปลอดภัยไซเบอร์ระดับชาติ

จากการศึกษาประเทศออสเตรเลีย สิงคโปร์ และประเทศญี่ปุ่น พบว่าแต่ละประเทศมีการจัดตั้งคณะกรรมการและหน่วยงานแห่งชาติ เพื่อทำหน้าที่กำหนดนโยบายและยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ โดยทั้งสามประเทศมุ่งเน้นในการสร้างสภาพแวดล้อมทางธุรกิจที่ปลอดภัย โดยการหาจุดสมดุลระหว่างการรักษาความปลอดภัยกับการผลักดันภาคธุรกิจเพื่อการพัฒนาทางเศรษฐกิจของประเทศ ในขณะที่ประเทศไทยยังไม่มีการจัดตั้งหน่วยงานแห่งชาติ รวมถึง ไม่มีการกำหนดนโยบายและยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ระดับชาติ ทำให้แต่ละหน่วยงานต้องกำหนดนโยบายในการดำเนินงานด้านการรักษาความปลอดภัยไซเบอร์เอง ส่งผลให้การดำเนินงานของรัฐบาลในช่วงที่ผ่านมา แม้ว่าจะมีการพัฒนาที่ดีขึ้นแต่ก็ยังไม่ครอบคลุมปัญหาทั้งหมด เช่น ปัญหาที่เกี่ยวข้องกับโครงสร้างพื้นฐานวิกฤติ ซึ่งมีความเกี่ยวข้องและส่งผลกระทบกับการดำเนินของหลายหน่วยงาน เป็นต้น เนื่องจากปัญหาความปลอดภัยไซเบอร์เป็นปัญหาที่ต้องอาศัยความร่วมมือในการจัดการจากทุกหน่วยงานที่เกี่ยวข้องหรือมีส่วนได้เสียจากผลกระทบที่เกิดขึ้น ตัวอย่างเช่น การใช้งานโครงสร้างพื้นฐานสารสนเทศที่มีการใช้งานทั้งในภาคพลเรือนและทางการทหาร เป็นต้น ซึ่งปัญหาความทับซ้อนของอำนาจหน้าที่ในการจัดการกับปัญหาความปลอดภัยไซเบอร์เป็นประเด็นที่เกิดขึ้นทั่วโลกไม่เฉพาะในประเทศไทยเท่านั้น การกำหนดนโยบายความปลอดภัยไซเบอร์แห่งชาติ และการจัดตั้งหน่วยงานกลางเพื่อถกเถียงถึงผลลัพธ์ระหว่างความมั่นคงของประเทศกับผลประโยชน์ด้านเศรษฐกิจจะช่วยทำให้รัฐบาลสามารถหาข้อสรุปในการดำเนินนโยบายที่สามารถขับเคลื่อนการทำงานของทั้งประเทศให้ดำเนินไปในทิศทางเดียวกันได้ (วิสิฐ อติพญากุล, ๒๕๕๙)

ในส่วนของการปฏิบัติตามกฎหมายด้านความปลอดภัยไซเบอร์ พบปัญหาและอุปสรรค ในการปฏิบัติตาม ดังนี้

๑. การปฏิบัติตามข้อกำหนดที่ไม่ครบถ้วน หรือการเลือกปฏิบัติตามแค่บางส่วน ซึ่งเกิดจากขาดความเข้าใจในเนื้อหาของข้อบังคับ เนื่องจากมาตรฐานในการปฏิบัติงานไม่ได้ถูกบัญญัติไว้อย่างชัดเจน ทำให้เกิดการตีความไปตามแบบที่ตนเข้าใจ อย่างเช่น พรบ. คอมพิวเตอร์ ๒๕๕๐ ที่มีการใช้งานนานเกือบ ๑๐ ปี แต่ยังคงมีคำถามเรื่องความเข้าใจที่ไม่ตรงกันอยู่ในแง่ของผู้ปฏิบัติที่มักมีการถกเถียงถึงขอบเขตของการปฏิบัติงานและคำถามเกี่ยวกับการกระทำประเภทใดที่จัดว่าเป็นการละเมิดกฎหมาย เป็นต้น อย่างไรก็ตาม พบว่ารัฐบาลมีข้อจำกัดที่ไม่สามารถกำหนดมาตรฐานอย่างละเอียดไว้ในข้อบังคับได้ เนื่องจากมาตรฐานมีการพัฒนาอยู่ตลอดเวลา ซึ่งหากมีการกำหนดมาตรฐาน ความปลอดภัยแบบเจาะจงเกินไป ก็อาจกลายเป็นเหมือนการบีบบังคับได้ (ก้อง จันทร์เต็ม, ๒๕๕๙)

๒. นโยบายของภาครัฐที่ใช้งานในปัจจุบัน ถูกมองจากภาคเอกชนว่าเป็นการกำหนดเพื่อการควบคุมการใช้งานอินเทอร์เน็ต มากกว่าเป็นความตั้งใจที่จะกำหนดกลไกเพื่อจัดการความปลอดภัยไซเบอร์ หรือการป้องกันภัยคุกคามทางไซเบอร์ เช่น ร่างพระราชบัญญัติความปลอดภัยคอมพิวเตอร์ฉบับปรับปรุง พ.ศ. ๒๕๕๘ ที่กำลังอยู่ในช่วงพิจารณาร่าง ก็มีเนื้อหาที่บ่งชี้ถึงความต้องการที่จะควบคุมการใช้งานอินเตอร์เน็ตให้เป็นไปตามกลไกของรัฐ มากกว่าการตั้งใจเอากฎหมายมาเพื่อควบคุมการเกิดอาชญากรรมทางอินเทอร์เน็ต เป็นต้น (นฤดม รุ่งศิริวงศ์, ๒๕๕๙)

๓. การระบุข้อบังคับโดยไม่ได้กำหนดแบ่งแยกประเภทของหน่วยงานไว้อย่างชัดเจน ส่งผลให้เกิดความยุ่งยากในขั้นตอนของการปฏิบัติงาน และสร้างความยากลำบากในการดำเนินให้กับภาคธุรกิจภายในประเทศ เช่น ในส่วนของสถาบันการเงิน กฎหมายที่เกี่ยวข้องที่สถาบันทางการเงินต้องปฏิบัติตาม จะพบว่าข้อกำหนดหรือหลักปฏิบัติที่ออกโดยธนาคารแห่งประเทศไทยจะมีความครอบคลุม และตรงกับการดำเนินงานเฉพาะด้านของสถาบันการเงินมากกว่าข้อกำหนดที่ออกโดยกระทรวงไอซีที เป็นต้น (นฤดม รุ่งศิริวงศ์, ๒๕๕๙)

๒. ปัญหาจากการดำเนินงานด้านความปลอดภัยไซเบอร์

๒.๑ ปัญหาด้านการประสานความร่วมมือระหว่างหน่วยงานรัฐบาลและหน่วยงานอื่นที่ไม่ใช่ของรัฐบาล

ปัญหาของการประสานความร่วมมือระหว่างรัฐบาลกับหน่วยงานเอกชน รัฐบาลยังมีการประสานความร่วมมือกับภาคเอกชนน้อยอยู่ โดยการร่วมมือกับเอกชนจะอยู่ในรูปแบบของการให้เอกชนปฏิบัติตามกฎหมายและกฎระเบียบที่รัฐจัดทำไว้ รัฐบาลยังไม่มีการวางแผนที่ชัดเจนถึง รูปแบบความร่วมมือที่ต้องการจากภาคเอกชน โดยการสร้างความร่วมมือระหว่างรัฐและเอกชนให้เกิดขึ้นได้ รัฐบาลต้องพัฒนาหน่วยงานเพื่อสร้างความเชื่อมั่นให้กับภาคเอกชนว่ารัฐบาลมีการรักษาความปลอดภัยทางไซเบอร์ที่เข้มแข็ง ภาคเอกชนจึงจะมีความมั่นใจมากพอที่จะทำการแลกเปลี่ยนข้อมูลสำคัญขององค์กรกับทางภาครัฐได้ (ชาลี วรกุลพิพัฒน์, ๒๕๕๙)

ปัญหาการขาดหน่วยงานกลางในการประสานความร่วมมือด้านความปลอดภัยไซเบอร์ จึงทำให้ความร่วมมือที่เกิดขึ้นเป็นการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง หรือเป็นการประสานงานภายในกลุ่มองค์กรเท่านั้น ทำให้การดำเนินงานเป็นไปได้ช้าและการแก้ปัญหาก็ขึ้นกับความสามารถในแต่ละองค์กร ไม่มีการร่วมกันเพื่อบูรณาการความรู้ในการแก้ไขปัญหา โดยแม้ว่ากระแสความปลอดภัยทางไซเบอร์ในไทยจะถูกกระตุ้นด้วยมาตรฐานความปลอดภัยจากทั่วโลก แต่ก็ไม่สามารถทำให้เกิดขึ้นได้โดยเร็ว (ก้อง จันทร์เต็ม, ๒๕๕๙)

ปัญหาของการตั้งหน่วยงานกลางด้านความปลอดภัยไซเบอร์ เพื่อเป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานต่างๆ พบข้อจำกัดจากการความแตกต่างของปัญหาที่เกิดขึ้นในแต่ละภาคธุรกิจ เนื่องจากความต้องการในการแก้ไขปัญหาที่ต่างกัน ทำให้เกิดการแตกออกเป็นวาระที่หลากหลาย อย่างเช่น รูปแบบภัยคุกคามที่เกิดขึ้นกับธนาคาร จะไม่เกิดขึ้นกับสถาบันอื่น เป็นต้น เมื่อหัวข้อที่แต่ละภาคส่วนสนใจแตกต่าง ความสนใจในการร่วมมือจึงมีน้อยลง นอกจากนั้น จากปัญหาการโจมตีทางไซเบอร์ที่แตกต่างกันส่งผลให้แต่ละหน่วยงานมีความชำนาญ หรือประสบการณ์แตกต่างกันออกไปตามประเภทภัยคุกคามที่เคยเกิดขึ้นกับหน่วยงานของตน และอาจไม่สามารถช่วยเหลือหน่วยงานอื่นได้มากนัก (นฤดม รุ่งศิริวงศ์, ๒๕๕๙)

๒.๒ ปัญหาด้านการพัฒนาบุคลากรผู้เชี่ยวชาญทางด้านความปลอดภัยไซเบอร์

การพัฒนาบุคลากรภายในประเทศไทยยังไม่รวดเร็วพอเมื่อเทียบกับภัยคุกคามที่เพิ่มขึ้น จากการที่ประเทศไทยไม่เคยมีการสร้างบุคคลากรทางด้านนี้มาก่อน แต่เกิดปรากฏการที่ต้องการการใช้งานขึ้นมาอย่างมากในขณะที่สถาบันการศึกษาไม่ได้มีการเรียนการสอนที่มุ่งเน้นในการสร้างบุคลากรทางด้านนี้ แค่มีเพียงการสอนในลักษณะหัวข้อวิชาหนึ่งเท่านั้น รัฐบาลไทยดำเนินงานโดยการพัฒนาผู้เชี่ยวชาญขึ้นมาจากบุคคลที่ทำงานด้านสารสนเทศเดิมให้มาดูแลด้านความปลอดภัยเพิ่มเติม โดยบุคลากรด้านความปลอดภัยไซเบอร์จำเป็นต้องมีความรู้และเข้าใจถึงพื้นฐานการทำงานขององค์กรเป็นอย่างดี อย่างไรก็ตาม การส่งคนไปอบรมอาจช่วยสร้างความรู้ แต่ก็ไม่ได้เป็นเครื่องยืนยันว่าคนที่ผ่านการอบรมจะสามารถทำงานหรือแก้ปัญหาได้จริง ซึ่งสิ่งเหล่านี้จำเป็นต้องอาศัยประสบการณ์ทำงานจริงมาก่อน ต้องผ่านการฝึกฝนให้เกิดความชำนาญ (ก้อง จันทร์เต็ม, ๒๕๕๙) โดยในประเทศออสเตรเลีย รัฐบาลอาศัยการพัฒนาบุคลากรผ่านความร่วมมือกับภาคธุรกิจในการจัดตั้งภาควิชาด้านความปลอดภัยไซเบอร์ขึ้นในมหาลัยเพื่อผลิตบุคลากรทางด้านนี้โดยตรง

ระบบการศึกษาของประเทศไทยมีความสำคัญอย่างมากต่อการพัฒนาศักยภาพบุคลากรทางด้านต่างๆ ประเทศไทยมีบุคลากรที่จบการศึกษาทางด้านเทคโนโลยีสารสนเทศเป็นจำนวนมากแต่คนที่มีพื้นฐานดีพอที่จะพัฒนาต่อทางด้านความปลอดภัยไซเบอร์กลับมีอยู่น้อยมาก จากการที่ประเทศไทยยังไม่มีการจัดตั้งสาขาเฉพาะทางด้านความปลอดภัยไซเบอร์ในระดับปริญญาตรี ทำให้หน่วยงานและองค์กรต่างๆ ต้องรับบัณฑิตจบใหม่มาทำการฝึกฝนและพัฒนาทักษะต่อยอดพื้นฐานด้านความปลอดภัยสารสนเทศจึงมีความสำคัญอย่างมากที่จะทำให้การพัฒนาไปได้อย่างมีประสิทธิภาพ (นฤดม รุ่งศิริวงศ์, ๒๕๕๙)

ปัญหาด้านการพัฒนาศักยภาพด้านการรักษาความปลอดภัยไซเบอร์ และการฝึกฝน ตอบสนองต่อการโจมตีทางไซเบอร์

ปัญหาเรื่องการจัดการฝึกตอบสนองต่อการโจมตีทางไซเบอร์ภายในประเทศไทยยังมีไม่มากนัก เนื่องจากหน่วยงานจำนวนมากยังขาดแคลนบุคลากรเฉพาะทางด้านความปลอดภัยไซเบอร์ที่มีความรู้ความเข้าใจมากพอที่จะเข้าร่วมรับการฝึกดังกล่าวได้ (ชาลี วรกุลพิพัฒน์, ๒๕๕๙)

๑. ปัญหาด้านการยกระดับมาตรฐานความปลอดภัยไซเบอร์

การช่วยเหลือหน่วยงานรัฐโดยรวมการจัดการด้านความปลอดภัยไซเบอร์ไว้ที่ศูนย์กลางไม่ใช่หนทางการพัฒนาความสามารถด้านความปลอดภัยไซเบอร์ที่ยั่งยืน เนื่องจากหน่วยงานรัฐบาลต่างๆ ไม่ได้มีการดำเนินนโยบายที่จะช่วยพัฒนาศักยภาพภายในองค์กรของตนเอง ต้องอาศัยการพึ่งพาหน่วยงานกลางเพียงอย่างเดียว ดังนั้น โครงการของ สพธอ. ในการช่วยเหลือหน่วยงานรัฐดูแลด้านการรักษาความปลอดภัยไซเบอร์ จึงเป็นเพียงการส่งเสริมความเข้มแข็งของหน่วยงานรัฐในช่วงเริ่มต้นเท่านั้น ซึ่งจำเป็นต้องมีการผลักดันให้เกิดการพัฒนาศักยภาพของแต่ละหน่วยงานให้สามารถดำเนินงานได้เองต่อไปในอนาคต

ปัญหาของการเผยแพร่ข้อมูลข่าวสารผ่านสื่อต่างๆ ในการให้ความรู้กับประชาชนทั่วไป พบว่า ช่องทางที่รัฐใช้ในการกระจายข้อมูลอาจไม่เป็นที่นิยมและไม่ตรงจุด จึงทำให้การให้ความรู้ด้านความปลอดภัยไซเบอร์กับประชาชน ไม่ปรากฏว่าได้เผยแพร่ออกไปในวงกว้างมากนัก ยังมีขอบเขตจำกัดอยู่แค่ในกลุ่มคนเล็กๆ เท่านั้น การเผยแพร่ความรู้ด้านความปลอดภัยไซเบอร์แค่ในเว็บไซต์ของหน่วยงานรัฐที่ดูแลด้านนี้ อย่างเช่น เว็บไซต์ของไทยเซิร์ต หรือของ สพธอ. เป็นต้น ไม่สามารถเสริมสร้างความตระหนักให้กับประชาชนทั่วไป เนื่องจากความสนใจของประชาชนทั่วไปที่จะเข้าไปดูยังหน้าเว็บของสำนักงานเฉพาะด้านนั้นเป็นไปได้ยาก (นฤดม รุ่งศิริวงศ์, ๒๕๕๙)

๒. ปัญหาและอุปสรรคของความร่วมมือระหว่างประเทศด้านความปลอดภัยไซเบอร์การดำเนินความร่วมมือระหว่างประเทศของรัฐบาลไทยในช่วงที่ผ่านมา พบว่าเกิดปัญหาและข้อจำกัดในการดำเนินงานในแต่ละด้าน ดังต่อไปนี้

๒.๑ การกำหนดมาตรฐานหรือหลักเกณฑ์การปฏิบัติร่วมกันมีความสำคัญอย่างมาก เนื่องจากเป็นการตั้งเป้าหมายของความปลอดภัยทางไซเบอร์ร่วมกัน โดยมาตรฐานนี้จะเป็นตัวกำหนดการดำเนินนโยบายและกฎหมายของแต่ละรัฐให้เป็นไปตามข้อตกลงนั้น ซึ่งจะเป็นการผลักดันให้เกิดการสร้างสภาวะแวดล้อมทางไซเบอร์ที่ปลอดภัยได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม จากข้อจำกัดทางพื้นฐานเศรษฐกิจของประเทศสมาชิกที่มีความแตกต่างกัน ทำให้แต่ละประเทศมีความพร้อมในการดำเนินงานที่แตกต่างกันไปด้วย การผลักดันความร่วมมือทางด้านนี้จึงต้องอาศัยระยะเวลาเพื่อให้เกิดการใช้งานตามมาตรฐานร่วมกันได้อย่างสมบูรณ์ ซึ่งรัฐบาลไทยควรให้ความสำคัญกับการกำหนดนโยบายร่วมกันโดยเริ่มต้นส่งเสริมความร่วมมือภายในกลุ่มประชาคมอาเซียนก่อน แล้วจึงผลักดันต่อเนื่องสู่ความร่วมมือระหว่างอาเซียนกับประเทศอื่นๆ ต่อไป

๒.๒ การส่งเสริมการวิจัยและการพัฒนาร่วมกัน จากการศึกษายังไม่พบ ประโยชน์ที่ได้รับจากความร่วมมือด้านงานวิจัยที่เด่นชัด สาเหตุหนึ่งอาจเกิดจากการดำเนินงานด้าน วิจัยและพัฒนานวัตกรรมเป็นหน้าที่ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (เนคเทค) มากกว่า ดังนั้น การศึกษาด้านงานวิจัยและพัฒนาร่วมกันระหว่างประเทศจึงจำเป็นต้อง ศึกษาการดำเนินงานของหน่วยงานเนคเทคเพิ่มเติมเพื่อให้สามารถระบุถึงการดำเนินงานของรัฐบาลทางด้านนี้ได้อย่างชัดเจน อย่าไรก็ตาม จากข้อมูลการสัมภาษณ์พบว่าประเทศไทยยังไม่ปรากฏว่ามีการใช้งานเทคโนโลยีทางด้านความปลอดภัยไซเบอร์ที่เป็นนวัตกรรมจากการคิดค้นและพัฒนาภายในประเทศ โดยเทคโนโลยีที่ใช้งานอยู่ในปัจจุบันเป็นการนำเข้าจากต่างประเทศทั้งสิ้น จึงอาจสรุปเบื้องต้นได้ว่า การพัฒนาทางด้านงานวิจัยของประเทศไทยในการผลิตผลงานทางด้านการรักษาความปลอดภัยไซเบอร์ออกสู่ตลาดนั้นยังไม่เป็นที่ประจักษ์ และสมควรได้รับการสนับสนุนความร่วมมือทางด้านนี้เพิ่มขึ้นต่อไป

๒.๓ การให้คำแนะนำและสนับสนุนด้านการกำหนดนโยบาย จากการศึกษาไม่ปรากฏว่ามีการขอคำแนะนำในการช่วยเหลือด้านการกำหนดนโยบายด้านความปลอดภัยทางไซเบอร์จากต่างประเทศ ซึ่งรัฐบาลสามารถขอรับคำแนะนำด้านการกำหนดนโยบายและการดำเนินงานหน่วยงานด้านความปลอดภัยไซเบอร์จากประเทศที่มีการพัฒนาด้านการจัดการความปลอดภัยไซเบอร์ในระดับสูงอย่างประเทศเกาหลี และ ญี่ปุ่น เป็นต้น หรือการขอความร่วมมือในการศึกษาเรียนรู้การดำเนินงานจากประเทศที่มีสภาพสังคมใกล้เคียงกับประเทศไทย อย่างเช่น ประเทศมาเลเซีย เป็นต้น นอกจากนั้น รัฐบาลยังสามารถประสานความร่วมมือในการขอคำปรึกษาด้านนโยบายจากองค์กรระหว่างประเทศ อย่างเช่น องค์กร ITU-IMPACT จากการที่รัฐบาลมีความร่วมมือกับ ITU ทางด้านเทคโนโลยีสารสนเทศและการสื่อสารอยู่ก่อนแล้ว ประกอบกับการที่ ITU มีการจัดตั้งสำนักงานประจำภูมิภาคเอเชีย-แปซิฟิกขึ้นที่ประเทศไทย จึงทำให้โอกาสในการประสานความร่วมมือกับ ITU-IMPACT น่าจะเป็นไปได้ง่ายกว่าการขอความร่วมมือจากองค์กรอื่น

การสร้างความร่วมมือในกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี

การสร้างความร่วมมือในกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี อภิปรายได้ว่า ใช้ทฤษฎีเครือข่ายความร่วมมือ (Collaborative Networks) เป็นกรอบในการออกแบบกระบวนการสร้างเครือข่าย และนำมาใช้เป็นหลักในการ วิเคราะห์เพื่อนำไปสู่การออกแบบเครือข่ายดังกล่าว ซึ่งเครือข่ายความร่วมมือ คือ แนวคิดการทำงานแบบมีส่วนร่วมในระนาบเดียวกันมีความเท่าเทียมกัน ปราศจากการสั่งการตามสายการบังคับบัญชาและเป็นอิสระต่อกัน ระหว่างกลุ่มบุคลากรองค์การหน่วยงานที่มีบทบาทและมีความสัมพันธ์ร่วมกันในการขับเคลื่อนแบบองค์รวมเป็นรูปของเครือข่าย เพื่อแลกเปลี่ยนข้อมูลข่าวสารที่เป็นประโยชน์ร่วมกันตัดสินใจ และดำเนินการตามเป้าหมาย เพื่อให้บรรลุวัตถุประสงค์ร่วมกันอย่างมีศักยภาพและประสิทธิภาพ

แนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

แนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม มี ๒ ประการ ดังนี้ ประการแรก คือ มาตรการ เชิงบริหารหรือเชิงนโยบาย ต้องมีกฎหมายเฉพาะอาชญากรรมทางคอมพิวเตอร์ รวมทั้ง ระเบียบปฏิบัติที่เกี่ยวข้องให้สอดคล้องกับภัยคุกคามที่เกิดขึ้น สอดคล้องกับงานวิจัยของ Mariam and Florian (2019) ได้ศึกษาการเมืองกับความปลอดภัยทางไซเบอร์ การสร้างสมดุลในบทบาทหน้าที่ของรัฐในแต่ละด้านที่เกี่ยวข้อง ได้อธิบายไว้ว่า บทบาทหน้าที่ ของรัฐมีหกส่วน ซึ่งได้แก่ ๑. ผู้ค้ำประกันความปลอดภัย (security guarantor) ๒. ผู้ออกกฎหมายและผู้บังคับใช้กฎหมาย ๓. ตัวแทนของประชาชน ๔. พันธมิตรด้านความปลอดภัย (security partner) ๕. ผู้สร้างและให้ความรู้แก่ประชาชน และ ๖. ผู้คุกคาม (threat actor) ผู้ที่รับผิดชอบทางด้าน Cyber Security ในองค์กร ต้องมีความเข้าใจในระบบไอทีของ องค์กรและมีการตรวจสอบระบบอยู่เสมอ อัพเดทซอฟต์แวร์ให้เป็นปัจจุบันเสมอ เพราะ บางครั้งความผิดพลาดอาจเกิดขึ้นจากบุคคลภายในองค์กรเอง หรือเกิดจากคนในองค์กร ที่ทำการก่อการโจรกรรมทางไซเบอร์เพื่อหาผลประโยชน์จากช่องโหว่ที่เกิดขึ้นในระบบได้ และประการที่สอง มาตรการเชิงปฏิบัติ ได้แก่ กรณีเว็บไซต์ผิดกฎหมาย จาบจ้วง เป็นภัย ต่อความมั่นคงของชาติ และที่ไม่เหมาะสม ลบหลู่ศาสนา อาจขอความร่วมมือไปยัง กลุ่มแนวร่วมผู้ใช้อินเทอร์เน็ตให้ช่วยกันต่อต้านและประณามเว็บไซต์ดังกล่าว รวมถึง การสร้างความตระหนักรู้ให้แก่ประชาชน ด้วยการรู้เท่าทันกับภัยอันตรายที่มาจากสังคมไซเบอร์ อันจะทำให้การป้องกันและการรับมือภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

สรุป

ลักษณะเด่นของนโยบายเกี่ยวกับการป้องกันอาชญากรรมทางเทคโนโลยี ได้แก่ ด้านความปลอดภัยไซเบอร์ของรัฐบาลไทย ด้านความร่วมมือระหว่างประเทศด้านความปลอดภัยไซเบอร์ โดยมี ปัญหาและอุปสรรคของนโยบายด้านความปลอดภัยไซเบอร์ของรัฐบาลไทย คือ การกำหนดนโยบายและกฎหมายด้านความปลอดภัยไซเบอร์ การประสานความร่วมมือระหว่างหน่วยงานรัฐบาลและหน่วยงานอื่นที่ไม่ใช่ของรัฐบาล และการพัฒนาบุคลากรผู้เชี่ยวชาญทางด้านความปลอดภัยไซเบอร์ ซึ่งกระบวนการต่างๆ นี้จะต้องมีการสร้างความร่วมมือในกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี ทำให้เกิดแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

บทที่ ๕
สรุปและข้อเสนอแนะ

การวิจัยเรื่อง “แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี” ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ มีวัตถุประสงค์เพื่อศึกษา ปัญหา อุปสรรค ข้อขัดข้องของแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี เพื่อทราบถึงผู้มีส่วนเกี่ยวข้องในการบูรณาการวิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี และเพื่อศึกษาหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม ผู้วิจัย ได้สรุปและมีข้อเสนอแนะ ดังนี้

สรุป

กล่าวโดยสรุปตามวัตถุประสงค์การวิจัย ได้ ดังนี้

วัตถุประสงค์ข้อที่ ๑ เพื่อศึกษา ปัญหา อุปสรรค ข้อขัดข้องของแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี

จากการวิจัยนี้พบว่า ประเทศไทยยังคงมีปัญหา อุปสรรค ในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีของไทยมากมายหลายด้าน แต่หากต้องการจะขับเคลื่อนการแก้ไขปัญหาอย่างบูรณาการ ควรจะต้องกำหนดกรอบแนวคิดที่สามารถสร้างการบูรณาการได้จริงอย่างเป็นรูปธรรม ซึ่งในที่นี้ได้กำหนดปัญหาสำคัญ 3 ประการ คือ คน, กฎหมาย/นโยบาย/คำสั่ง/มาตรการ และเทคโนโลยีจากนั้นจึงเอาหลักการสร้างภูมิคุ้มกันเพื่อให้สามารถต้านทานและต่อสู้กับภัยทางเทคโนโลยี ที่เปลี่ยนแปลงสภาพและความรุนแรงได้อย่างรวดเร็วไม่มีสิ้นสุด

จากการศึกษาจึงได้ค้นพบปัญหาความไม่สมบูรณ์ของแนวทางในการป้องกันการก่ออาชญากรรมทางเทคโนโลยี ความไม่สมบูรณ์ของรูปแบบกระบวนการในการป้องกันการก่ออาชญากรรมทางเทคโนโลยี เนื่องจากอาชญากรรมทางเทคโนโลยีและภัยคุกคามทางไซเบอร์มีผลกระทบอย่างมากต่อประชาชน ทำให้เกิดการตอบสนองและแก้ไขปัญหาด้วยวิธีการต่าง ๆ อย่างรวดเร็ว ทั้งที่เกิดขึ้นแบบบูรณาการและแยกกันจัดการ ทำให้เกิดการขับเคลื่อนการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีโดยหน่วยงานทั้งภาครัฐและเอกชนที่เกี่ยวข้องอยู่ตลอดเวลา และก่อให้เกิดความเปลี่ยนแปลงของกฎหมาย กฎ คำสั่ง นโยบายและมาตรการต่าง ๆ อย่างสม่ำเสมอ จึงทำให้ข้อมูลที่ได้จากการวิจัยอาจไม่ทันสมัยอยู่ตลอด จนทำให้เกิดอุปสรรคระหว่างหน่วยงานที่เกี่ยวข้องอันเนื่องมาจากกฎหมาย กฎ นโยบาย คำสั่ง และมาตรการที่ไม่สอดประสานไปในทิศทางเดียวกันแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี ที่เหมาะสมที่สุด คือ การสร้างภูมิคุ้มกันทางไซเบอร์ ซึ่งภูมิคุ้มกันทางไซเบอร์จะเกิดขึ้นได้อย่างมีประสิทธิภาพ หากมีการบริหารจัดการและบูรณาการป้องกันการก่ออาชญากรรมทางเทคโนโลยีใน ๓ ด้าน อย่างเหมาะสม อันประกอบ ไปด้วย คน, กฎหมาย/นโยบาย/มาตรการ และเทคโนโลยี

เหตุผลความจำเป็นที่จะต้องคำนึงถึงองค์ประกอบทั้ง ๓ ด้าน เนื่องมาจากการศึกษาที่พบว่าประเทศไทยในปัจจุบัน คนในประเทศยังคงขาดความรู้ขาดความตระหนักรู้ขาดความเข้าใจในเรื่องการใช้เทคโนโลยีได้อย่างปลอดภัย หรือยังไม่มีความรับผิดชอบต่อผู้อื่นในสิ่งที่ตนเองอาจมีส่วนสนับสนุนให้เกิดขึ้น ต่อมาคือเรื่องกฎหมาย นโยบาย และกระบวนการที่ยังคงเป็นอุปสรรคต่อการป้องกันอาชญากรรมทางเทคโนโลยี ระบบกฎหมายและนโยบายที่ไม่สนับสนุนเกื้อกูลกันระหว่าง ภาครัฐและเอกชน แต่เน้นการจับผิดจะทำให้ต่างฝ่ายต่างสร้างกำแพงมากกว่าช่วยเหลือแลกเปลี่ยน ข้อมูลกัน และสุดท้ายคือ การที่ยังคงมีเทคโนโลยีที่มีไม่สนับสนุนการป้องกันภัยหรือแม้แต่เป็นอุปสรรค ต่อการป้องกันอาชญากรรมทางเทคโนโลยี ยกตัวอย่างในกรณีของแอพพลิเคชั่นการทาธุรกรรมทาง การเงินออนไลน์ควรมีระบบคัดกรองและช่วยเหลือมิให้ผู้ใช้บัญชีโอนเงินไปยังบุคคลที่ไม่รู้จักและเข้าข่าย เป็นบัญชีม้าจากการตรวจจับของระบบ เป็นต้น

วัตถุประสงค์ข้อที่ ๒ เพื่อศึกษาถึงผู้มีส่วนเกี่ยวข้องในการบูรณาการ วิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี

รูปแบบกระบวนการในการป้องกันอาชญากรรมทางเทคโนโลยีโดยอาศัยผู้เกี่ยวข้องทุกภาคส่วนที่เกี่ยวข้อง มีดังนี้

๑. การปรับปรุงแก้ไขกฎหมาย ให้ทุกภาคส่วนมีความรับผิดชอบเชิงรุกที่จะป้องกันและยับยั้งภัยอาชญากรรมทางเทคโนโลยี เช่น การกำหนดหน้าที่ความรับผิดชอบในการคุ้มครองบุคคลที่ตนเองมีหน้าที่ให้บริการ หน่วยงานราชการที่อนุญาตให้มีการติดต่อสื่อสารทางเทคโนโลยีควรมีช่องทางกลางในการประชาสัมพันธ์ให้ความรู้และช่วยเหลือประชาชนที่อาจถูกฉ้อโกงหรือหลอกลวง แอบอ้างภาครัฐ ภาคธนาคารควรจะต้องมีความรับผิดชอบในการคุ้มครองลูกค้าที่โอนเงินไปบัญชีม้า โดยไม่จำเป็นต้องได้รับคำสั่งหรือร้องขอจากเจ้าหน้าที่บังคับใช้กฎหมาย เป็นต้น

๒. การพัฒนาปรับรูปแบบการบริหารจัดการการให้บริการทางด้านเทคโนโลยีสารสนเทศ ที่ทำให้เกิดการใช้ทรัพยากรได้อย่างเหมาะสม สะดวก ใช้งานง่ายและปลอดภัย สามารถคุ้มครองป้องกัน ผู้ใช้งานได้อย่างมีประสิทธิภาพ เช่น แอพพลิเคชั่นธนาคารควรมีการเตือนบัญชีต้องสงสัย และมีช่องทางในการแจ้งและรายงานบัญชีม้า จากนั้นนำข้อมูลไปแบ่งปันกับเจ้าหน้าที่ภาครัฐที่มีหน้าที่รับผิดชอบ รวมถึงมีการพัฒนาการสร้างการรับรู้และรับผิดชอบให้กับประชาชนที่มีส่วนเกี่ยวข้องกับการใช้บัญชีม้า เป็นต้น

๓. การพัฒนาบุคลากร และการประชาสัมพันธ์ให้ความรู้กับประชาชนทุกระดับอย่างเหมาะสมโดยไม่มีข้อจำกัดในเรื่องเวลา สถานที่และโอกาส

๔. การพัฒนาปรับปรุงเทคโนโลยีในการป้องกันอาชญากรรมทางเทคโนโลยี

วัตถุประสงค์ข้อที่ ๓ เพื่อศึกษาหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

ภูมิคุ้มกันภัยไซเบอร์ (Cyber Immunity) ที่เข้มแข็ง จะเป็นพลังสำคัญสาหรับการรักษาความมั่นคงของชาติในอนาคต ภูมิคุ้มกันภัยไซเบอร์ เป็นแนวคิด ที่ประยุกต์มาจากภูมิคุ้มกันในร่างกายมนุษย์ เป็นกลไกตามธรรมชาติของร่างกายที่ทาหน้าที่ป้องกัน หรือต่อต้านไม่ให้เชื้อโรคเข้าสู่ร่างกาย และพัฒนาร่างกายให้รับรู้ในการป้องกันและต่อสู้กับโรคร้าย ที่มีลักษณะใกล้เคียงกันโดยไม่จำเป็นต้องได้รับเชื้อโรคนั้นมาก่อนก็ได้ เช่นเดียวกันภัยคุกคาม ทางด้านไซเบอร์ที่เปลี่ยนแปลง

รูปแบบ และวิธีการโดยตลอด หากประชาชนมีภูมิคุ้มกันภัยไซเบอร์ที่ดี ก็จะเป็นรากฐานความปลอดภัยของสังคม และประเทศชาติ

การสร้างภูมิคุ้มกันภัยไซเบอร์ที่สำคัญเริ่มจากความตระหนักรู้ของประชาชนถึงภัยคุกคามทางไซเบอร์ การมีกระบวนการทางกฎหมายที่เหมาะสม มีนโยบายและมาตรการที่ช่วยสร้างภาพแวดล้อมที่ดีของประเทศในด้านความมั่นคงทางไซเบอร์ในทุกระดับ และการมีและใช้เทคโนโลยีที่เหมาะสมกันประเทศ ในหัวข้อนี้จะทำการศึกษาถึงภูมิคุ้มภัยไซเบอร์ของประชาชนที่ได้จากการปฏิบัติงานของสานักงานตำรวจแห่งชาติ และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีผู้วิจัยเล็งเห็นถึงความสำคัญทีว่า ภูมิคุ้มกันภัยไซเบอร์ของประชาชนของชาติจะนำไปสู่การพัฒนาศักยภาพประเทศ เพื่อเตรียมความพร้อมเผชิญภัยคุกคามทางไซเบอร์ที่จะเป็นปัญหาความมั่นคงแห่งชาติที่สำคัญในอนาคตภูมิคุ้มกันทางไซเบอร์กับความมั่นคงของชาติจึงเป็นเรื่องที่สอดคล้องกับเหมาะสมกับสถานการณ์ปัจจุบัน และเป็นเรื่องที่จะมีความท้าทายมากขึ้นอย่างยิ่งในอนาคตอันใกล้แต่ปัจจุบัน ยังไม่มีการศึกษาในเรื่องนี้อย่างเพียงพอ ความรู้ความเข้าใจเกี่ยวกับภูมิคุ้มกันทางไซเบอร์และความสัมพันธ์กับความมั่นคงไซเบอร์ของประเทศชาตินี้ จะนาไปสู่การกำหนดแนวทางและมาตรการ ที่เหมาะสมเพื่อป้องกันและพัฒนาความมั่นคงของชาติได้อย่างเหมาะสมกับสถานการณ์ในอนาคต

การสร้างภูมิคุ้มกันทางไซเบอร์ที่เหมาะสม จะช่วยเกิดการบูรณาการความร่วมมือเพื่อให้เกิดการป้องกันอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ และมีสอดคล้องกันอย่างเข้าใจถี่ถ้วน รอบด้าน (Comprehensive) ส่งผลให้ประเทศไทยมีความแข็งแกร่งทนทานและสามารถปรับตัวกับอาชญากรรมประเภทใหม่ได้โดยตลอด (Resilience) ซึ่งในการศึกษาวิจัยนี้มีกรอบแนวคิดที่นำเอาหลัก คิดทางวิชาการในการสร้างแนวคิดการบริหารจัดการและบูรณาการการป้องกันการก่ออาชญากรรมทาง เทคโนโลยีให้ได้ในทุกมิติ

หน่วยงานที่มีหน้าที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศประเภทต่าง ๆ ทั้งภาครัฐและเอกชนจะต้องคำนึงถึงการดำเนินกิจการหรือธุรกิจที่มุ่งสร้างภูมิคุ้มกันทางไซเบอร์ในแนวทางของการสร้างภูมิคุ้มกันภัยทางไซเบอร์ให้กับประชาชน หากทุกภาคส่วนดำเนินการในส่วนนี้อย่างครบถ้วนแล้ว ก็จะเกิดการบูรณาการความร่วมมือได้จริงอย่างเป็นรูปธรรม ยกตัวอย่าง ในกรณีของธนาคารที่มีการให้บริการแอพพลิเคชั่นทำธุรกรรมธนาคารออนไลน์ ควรมีระบบเทคโนโลยีที่สนับสนุนการป้องกันภัยจากบัญชีม้า สามารถพัฒนาความตระหนักรู้ให้กับประชาชนผู้ใช้แอพพลิเคชั่น ดังกล่าว และทั้งภาครัฐและเอกชนก็มีกฎหมายหรือนโยบายที่สนับสนุนให้เกิดการสร้างภูมิคุ้มกัน ดังกล่าวให้กับผู้ใช้บริการทุกราย เป็นต้น

ข้อเสนอแนะ

ข้อเสนอแนะแบ่งให้สอดคล้องกับการบริหารจัดการและบูรณาการป้องกันอาชญากรรมทางเทคโนโลยีให้อย่างเหมาะสม แบ่งเป็น 2 ส่วน ประกอบด้วยข้อเสนอแนะเชิงนโยบาย และข้อเสนอแนะในการวิจัยครั้งต่อไป

๑. ข้อเสนอแนะเชิงนโยบาย

ผู้วิจัยมีข้อเสนอแนะ ดังนี้

๑.๑ การกำหนดนโยบายความปลอดภัยไซเบอร์แห่งชาติ

รัฐบาลควรเร่งผลักดันการจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) และสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเดินหน้าในการกำหนดนโยบายและยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ของประเทศไทย อย่างไรก็ตาม การจัดตั้งคณะกรรมการรวมถึงการกำหนดอำนาจหน้าที่ผ่านพระราชบัญญัติว่าด้วยการรักษาความ มั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นเรื่องที่รัฐบาลควรเอาใจใส่ในรายละเอียดและรับฟังความคิดเห็นจากทุกภาคส่วนที่เกี่ยวข้อง เนื่องจากเป็นเรื่องที่ละเอียดอ่อนและส่งผลกระทบอย่างมากต่อการพัฒนาธุรกิจของประเทศ

๑.๒ กฎระเบียบและกฎหมายที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์

รัฐบาลควรทบทวนกฎระเบียบและกฎหมายทั้งหมดที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์ ซึ่งได้มีการใช้งานมาเป็นระยะเวลาหนึ่งแล้ว โดยปรับปรุงข้อจำกัดและช่องโหว่ของกฎหมายให้มี ความทันสมัยและสามารถนำ ไปปฏิบัติตามได้อย่างมีประสิทธิภาพ โดยข้อบังคับทั้งหมดที่ออกมาต้องเป็นในทิศทางเดียวกัน และต้องคำนึงถึงความเป็นไปได้ในการประยุกต์ใช้งานในแต่ละองค์ โดยอาศัยรับฟังความคิดเห็นและประสบการณ์จากทุกภาคส่วนที่เกี่ยวข้อง

๑.๓ การสร้างความร่วมมือเพื่อให้เกิดเป็นเครือข่ายรูปธรรมที่ชัดเจน

๑.๓.๑ มีการรับรู้และมุมมองที่เหมือนกัน (common perception) แสดงให้เห็นถึงความเกี่ยวข้องและเชื่อมโยงในด้านของการป้องกันและปราบปรามปัญหาอาชญากรรมทางไซเบอร์ เพราะหน่วยงานต่าง ๆ มีภาระหน้าที่รับผิดชอบและมีความรู้ที่เกิดจากการศึกษาและอยากจะแก้ไขปัญหาดังกล่าว เพราะมีการรับรู้ปัญหาร่วมกันและต้องการเพื่อที่จะนำความตั้งใจหรือแนวทางของตนเองที่มีเกี่ยวกับด้านปัญหาอาชญากรรมเข้ามาร่วมกันแลกเปลี่ยนประสบการณ์ปัญหาร่วมกัน

๑.๓.๒ การมีวิสัยทัศน์ร่วมกัน (common vision) มีการมองปัญหาและเห็นภาพของจุดมุ่งหมายในอนาคตร่วมกันระหว่างสมาชิกตัวแสดงในกลุ่ม ด้านการป้องกันและปราบปรามปัญหาอาชญากรรมทางไซเบอร์ ส่งผลให้เกิดเป้าหมายร่วมกัน ซึ่งจะเป็นพลังในการขับเคลื่อนมุมมองเหล่านั้นให้ประสบความสำเร็จ และยังช่วยลดการขัดแย้งอันเกิดจากมุมมองความคิดที่แตกต่างลงได้

๑.๓.๓ มีความสนใจหรือมีผลประโยชน์ร่วมกัน (mutualinterests/benefits) นอกจากจะมีจุดเป้าหมายร่วมกันแล้ว ในการสร้างแรงจูงใจให้เข้าร่วมเครือข่าย ต้องมีเรื่องของผลประโยชน์ตอบแทนกัน ทั้งในรูปแบบที่เป็นเงินตราและไม่เป็นเงินตรา ชื่อเสียง ความก้าวหน้าและประสิทธิภาพในการทำงานร่วมกัน รวมถึงทางด้านจิตใจ ความสุข ความพึงพอใจในการร่วมกันทำงาน

๑.๓.๔ การมีส่วนร่วมของสมาชิกทุกคนในเครือข่าย (stakeholders participation) จะเห็นได้จาก ในแต่ละหน่วยงานที่เกี่ยวข้องนั้น จะหน่วยหรือองค์กรขนาดเล็กหรือกลุ่มคนที่เป็นที่ปรึกษา หรือให้การสนับสนุนในเรื่องต่าง ๆ ถือได้ว่าเป็นกระบวนการร่วมมือจากทุกฝ่าย ซึ่งจะทำให้เกิดกระบวนการในรูปแบบ Deliberation ในการร่วมรับรู้ ร่วมคิด ร่วมกันวางแผน และตัดสินใจก่อเกิดเป็นเครือข่ายที่เข็มแข็งให้ความสำคัญกับทุกตัวแสดงทุกระดับ

๑.๓.๕ มีการเสริมสร้างซึ่งกันและกัน (complementary relationship) เมื่อเกิดความร่วมมือที่ได้จากเครือข่ายที่หลากหลายมาดำเนินการร่วมกัน แต่ละหน่วยงานย่อมมีจุดแข็งและจุดที่ต้องแก้ไข จึงจำเป็นต้องให้เครือข่ายแต่ละภาคส่วนนั้นเรียนรู้ศักยภาพของตนเองและเรียนรู้ศักยภาพของหน่วยงานที่เข้ามาร่วมกัน เพื่อเป็นการเสริมสร้างเครือข่ายให้แข็งแรงมีศักยภาพและประสิทธิภาพมากยิ่งขึ้น

๑.๓.๖. มีการเกื้อหนุนพึ่งพากัน (interdependent) เป็นสิ่งสำคัญที่จะดำรงให้เครือข่ายคงอยู่อย่างสมบูรณ์ สมาชิก หรือตัวแสดงแทนจากทุกภาคส่วนต้องอาศัยการพึ่งพาแลกเปลี่ยนข้อมูลซึ่งกันและกัน เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายทั้งในระยะสั้นและระยะยาวร่วมกัน ทั้งในด้านความคิดและทรัพยากรที่มีอยู่ของแต่ละองค์การ โดยทุกภาคส่วนต้องมีส่วนร่วมในการดำเนินการ

๑.๓.๗ มีปฏิสัมพันธ์กันในเชิงแลกเปลี่ยน (interaction) เป็นหัวใจสำคัญที่จะต้องทำให้สมาชิก หรือตัวแสดงแทนในเครือข่ายที่เข้ามาร่วมกันทำกิจกรรมร่วมกัน ก่อเกิดเป็นการพบปะพูดคุย ประชุมเป็นวาระ มีความแลกเปลี่ยนความคิดเห็นเพื่อนำไปสู่การแก้ไขต่าง ๆ และการสร้างช่องทางแลกเปลี่ยนความคิดเห็นผ่านสื่อสังคมออนไลน์โดยใช้เทคโนโลยีสมัยใหม่เป็นเครื่องมือ ให้ทันสมัย สะดวกกับทุกคน โดยนำมาออกแบบรูปแบบช่องทางการสื่อสารเพื่อให้เกิดปฏิสัมพันธ์ระหว่างสมาชิกด้วยกัน และจะส่งผลให้การดำเนินงานต่าง ๆ ราบรื่น และไปในทิศทางเดียวกันมากที่สุด เช่น การสร้างกลุ่มไลน์ เฟซบุ๊ก เว็บไซต์ กระดานถาม - ตอบ เป็นต้น

๑.๓.๘ มีการระดมความคิดของสมาชิก (brain storming) การสร้างเครือข่ายขึ้นมาเพื่อการระดมความคิดของสมาชิก หรือ ตัวแสดงแทนเพื่อให้เกิดการแสวงหาความรู้ใหม่ ๆ ร่วมกัน เพื่อใช้ในการวิเคราะห์สภาพปัญหา ประสานการใช้ทรัพยากรบุคคล อุปกรณ์ จัดสรรงบประมาณได้ตรงตามเป้าหมายของเครือข่ายและสามารถส่งผลให้การดำเนินการร่วมกันได้อย่างสำเร็จ

๑.๔ การสร้างวัฒนธรรมความปลอดภัยไซเบอร์ในสังคมไทย

รัฐบาลควรร่วมมือกับสถาบันการศึกษาในการปลูกฝังความรู้ด้านความปลอดภัยไซเบอร์ให้กับเยาวชน นอกจากนั้น ควรเพิ่มช่องทางในการเผยแพร่ความรู้ด้านความปลอดภัยทางไซเบอร์ให้กับประชาชนมากขึ้น โดยอาศัยช่องทางที่ประชาชนนิยมใช้งานเป็นการสอดแทรกความรู้ในการใช้งานอินเทอร์เน็ตในชีวิตประจำวันให้เกิดความปลอดภัย เพื่อให้เกิดวินัยและกลายเป็นวัฒนธรรมด้าน ความปลอดภัยไซเบอร์ต่อไป

๑.๕ การผลักดันความร่วมมือระหว่างประเทศ

รัฐบาลควรเพิ่มความร่วมมือระหว่างประเทศทางด้านงานวิจัยและพัฒนาด้านความปลอดภัยไซเบอร์ให้มากขึ้น และผลักดันความร่วมมือในระดับนโยบายของประชาคมอาเซียน เพื่อกำหนดนโยบายและการดำเนินงานภายในภูมิภาคให้มีความสอดคล้องและดำเนินไปในทิศทางเดียวกัน ซึ่งนอกจากการผลักดันการกำหนดนโยบายด้านความปลอดภัยไซเบอร์ร่วมกันภายในภูมิภาค แล้ว รัฐบาลยังสามารถรับคำแนะนำในการกำหนดนโยบายด้านความปลอดภัยไซเบอร์ได้จากองค์กร ระหว่างประเทศที่มีหน้าที่ในการให้คำปรึกษาและสนับสนุนการกำหนดนโยบายด้านความปลอดภัย ไซเบอร์ได้อีกด้วย

๒. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

๒.๑ ควรทำงานวิจัยที่หลากหลายด้านความปลอดภัยไซเบอร์ ทั้งงานวิจัยเชิงสำรวจโดยวิธีวิจัยปริมาณและวิธีวิจัยคุณภาพ และการวิจัยที่มีความเฉพาะเจาะจงในประเด็นต่างๆ เพื่อสามารถเผยแพร่ให้ประชาชนรับรู้และเข้าใจเรื่องความปลอดภัยทางไซเบอร์มากขึ้น

๒.๒ ควรทำวิจัยเปรียบเทียบการดำเนินงานของประเทศอื่นในประชาคมอาเซียนด้านความปลอดภัยทางไซเบอร์

๒.๓ เนื่องจากการวิจัยครั้งนี้เริ่มทำก่อนที่จะมีการประกาศใช้ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ จึงเห็นควรว่า หลังจากที่การบังคับใช้แล้วและมีหน่วยงานต่างๆที่เกี่ยวข้องแล้ว ควรที่จะมีการวิจัยเพื่อที่จะประเมินผลการบูรณาการร่วมกันว่ามีส่วนใดจะต้องมีการพัฒนาปรับปรุงต่อไปอีกหรือไม่

บรรณานุกรม

ภาษาไทย

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

ชนินทร เฉลิมทรัพย์, น.อ. “แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ”. เอกสารวิจัยส่วนบุคคล, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๖๐.

ตำรวจแห่งชาติ, สำนักงาน. “การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์” สำนักงานตำรวจแห่งชาติ กรุงเทพมหานคร, ๒๕๕๙.

ยุทธศักดิ์ เทียมทัศน์. “การแบ่งปันความรู้งานสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีโดยระบบการใช้ระบบการจัดการเนื้อหา” สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร, ๒๕๕๘.

ศิริรัตน์ ศรีสว่าง. “ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์”. วิทยานิพนธ์ วิทยาศาสตร์มหาบัณฑิตสาขาวิชาระบบสารสนเทศเพื่อการจัดการ, คณะพาณิชยศาสตร์และการบัญชีมหาวิทยาลัยธรรมศาสตร์, ๒๕๕๘.

กฎหมาย

“พระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ.๒๕๒๗”, ราชกิจจานุเบกษา. เล่มที่ ๑๐๑ ตอนที่ ๑๖๔ ก, ๑๒ พ.ย.๒๕๒๗, หน้า ๑

“พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.๒๕๒๒”, ราชกิจจานุเบกษา. เล่มที่ ๙๖ ตอนที่ ๗๒ ก, ๔ พ.ค. ๒๕๒๒, หน้า ๒๐

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐”, ราชกิจจานุเบกษา. เล่มที่ ๑๒๔ ตอนที่ ๒๗ ก, ๑๘ มิ.ย.๒๕๕๐, หน้า ๔

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่ ๒) พ.ศ.๒๕๖๐”, ราชกิจจานุเบกษา. เล่มที่ ๑๓๔ ตอนที่ ๑๐ ก, ๒๔ ม.ค.๒๕๖๐, หน้า ๒๔

“พระราชบัญญัติให้ใช้ประมวลกฎหมายอาญา พ.ศ.๒๔๙๙”, ราชกิจจานุเบกษา. เล่มที่ ๗๓ ตอนที่ ๙๕ ก, ๑๕ พ.ย. ๒๔๙๙, หน้า ๑

บทความ

ณรงค์ กุลนิเทศ. “รูปแบบและมาตรการแก้ปัญหา อาชญากรรมไซเบอร์” การประชุมวิชาการและนำเสนอผลงานวิจัย ระดับชาติและนานาชาติ ครั้งที่ ๖ มหาวิทยาลัยราชภัฏสวนสุนันทา. หน้า ๒๒๔-๒๓๗, ๒๕๕๘.

Books

Shelly, G., & Vermaat, M. “Discovering Computers 2011 : Complete : Cengage Learning”, 2010.

Journals and Newspapers

Ajzen, Icek. “The theory of planned behavior”. Organizational Behavior and Human Decision Processes. 50(2), 179-211. doi : 10.1016/0749- 5978 (91) 90020-T, 1991.

Bulgurcu, Burcu, Cavusoglu, Hasan, & Benbasat, Izak. “Information Security Policy Compliance : An Empirical Study of Rationality-Based Beliefs and Information Security Awareness”. MIS Quarterly. 34(3), 523-548, 2010.

Chai, Sangmi, Sharmistha, Bagchi-Sen, Claudia, Morrell, R., Rao H., & J., Upadhyaya Shambhu. “Internet and Online Information Privacy : An Exploratory Study of Preteens and Early Teens”. IEEE Transactions on Professional Communication, 52(2), 167-182, 2009.

Halder, Debarati, Jaishankar, Karuppannan, & Jaishankar, K. “Cyber crime and the victimization of women : laws, rights and regulations : Information Science Reference, 2012.

Heinl, Caitríona H. “Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime”. Asia Policy. 18, 131–160, 2014.

D'Arcy, John, Hovav, Anat, & Galletta, Dennis F. “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse : A Deterrence Approach”. Information Systems Research, 20(1), 79-98. doi: 10.1287/isre.1070.0160, 2009.

Kshetri, Nir. “Diffusion and Effects of Cyber-Crime in Developing Economies”. Third World Quarterly. 31(7), 1057-1079. doi: 10.1080/01436597.2010. 518752, 2010.

LaRose, Robert, Rifon, Nora, Liu, Sunny, & Lee, Doohwang. (2005). Understanding online safety behavior : A multivariate model. The 55th Annual Conference of the International Communication Association, New York City.

Liang, Huigang, & Xue, Yajiong (Lucky). “Understanding Security Behaviors in Personal Computer Usage : A Threat Avoidance Perspective”. Journal of the Association for Information Systems, 11(7), 394-413. (2010).

Lu, Chi-Chao, & Jen, Wen-Yuan. “A Historical Review of Computer User's Illegal Behavior Based on Containment Theory”. JSW, 5(6), 593-599. doi: 10.4304 /jsw.5.6.593-599, 2010.

Malimage, Kalana, & Warkentin, Merrill. “Influence of Perceived Value of Data on Anti-Virus Software Usage : An Empirical Study of Protection Motivation”. IFIP Dewald Roode Workshop on Information Security. 2011.

McCrae, R., & Costa, P. “A contemplated revision of the NEO Five-Factor Inventory”. Personality and Individual Differences. 36(3), 587-596. doi:citeulike-article-id:2485386 doi: 10.1016/s0191-8869(03)00118-1, 2004.

McCrae, Robert R., & Costa, Paul T. “Validation of the five-factor model of personality across instruments and observers”. Journal of Personality and Social Psychology. 52(1), 81-90. doi: 10.1037//0022-3514.52.1.81, 1987.

Mehrdad Sepehri Sharbaf. “A New Perspective to Information Security: .Total Quality Information Security Management”. In Ron Poet, Muttukrishnan Rajarajan, editors, Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, Scotland, UK, September 9-11, 2014. pages 56, 2014.

Ng, Boon-Yuen, Kankanhalli, Atreyi, & Xu, Yunjie Calvin. “Studying users' computer security behavior : A health belief perspective”. Decision Support Systems. 46(4), 815-825. doi: 10.1016/j.dss.2008.11.010, 2009.

Olusola, M., Samson, O., Semiu, A., & Yinka, A. “Cyber Crimes and Cyber Laws in Nigeria. The International Journal Of Engineering And Science. 2(4), 19- 25, 2013.

Pahnila, Seppo, Siponen, Mikko T., & Mahmood, M. Adam. (2007). Employees'

Electronic Data Base

Bulgurcu, Burcu, Cavusoglu, Hasan, & Benbasat, Izak. “Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance”. (Online). Available : http://www.aisel.aisnet.org/amcis2009 /419, 2009.

Moody, Daniel L., & Walsh, Peter. “Measuring the Value Of Information – An Asset Valuation Approach”. (Online). Available : http://www.is2.lse.ac.uk/asp/ aspecis/19990068. pdf, 1999).

ประวัติย่อผู้วิจัย

ชื่อ : พลตำรวจตรี ฐายุฏฐ์ จันทร์ถาวร

วัน เดือน ปี เกิด : ๑๒ พฤษภาคม ๒๕๑๒

ประวัติการศึกษา
: ปริญญาตรี รัฐประศาสนศาสตร์บัณฑิต รุ่นที่ ๔๔ : รร.นายร้อยตำรวจ กรมตำรวจ (พ.ศ.๒๕๓๔)
: ปริญญาโท สังคมศาสตรมหาบัณฑิต (อาชญาวิทยาและงานยุติธรรม) มหาวิทยาลัยมหิดล (พ.ศ.๒๕๔๐)
: ปริญญาเอก Pubic Administration : University of northem Philippines (พ.ศ.2552)

การศึกษางบรมเพิ่มเติม
: หลักสูตรวิทยาการตำรวจของตำรวจภูธรภาค ๑ : สำนักงานวิทยาการตำรวจ, กรมตำรวจ (พ.ศ.๒๕๓๘)
: หลักสูตรการสืบสวนประจำหน่วย : กองบัญชาการตำรวจภูธรภาค ๑ กรมตำรวจ (พ.ศ.๒๕๓๙)
: หลักสูตรเทคนิคการสืบสวนคดียาเสพติดให้โทษ ระดับผู้นำหน่วย(สัญญาบัตร) รุ่นที่ ๒
: สำนักงาน คณะกรรมการป้องกันและปราบปรามยาเสพติด (ปปส.), สำนักนายกรัฐมนตรี (พ.ศ.๒๕๓๙)
: หลักสูตรสารวัตร รุ่นที่ ๔๗ : สถาบันพัฒนาข้าราชการตำรวจ, กรมตำรวจ (พ.ศ.๒๕๔๐)
: หลักสูตร Road Safety Audi จะช่วยป้องกันอุบัติเหตุได้อย่างไร : สถาบัน เอ ไอ ที (พ.ศ.๒๕๔๓)
: หลักสูตรผู้กำกับการ รุ่นที่ ๕๔ : สถาบันพัฒนาข้าราชการตำรวจ สำนักงานตำรวจแห่งชาติ (พ.ศ.๒๕๔๘)
: Narcotics Unit Commanders Course : ILEA Bangkok (พ.ศ.2553)
: FBI Pacifc Training Initiative (PTI) Bangkok (พ.ศ.2553)
: Tactical Safety and Planning Course, ILEA Bangkok (พ.ศ.2554)
: Practical Applications in Leadership for Supervisors Course, ILEA Bangkok (พ.ศ.2555)
: Legal Aspects of Combating Terrorism (LCT) Course, Rhode Island, USA (พ.ศ.2555)

: FBINA : Quantico, USA (พ.ศ.2556)
: หลักสูตรการบริหารงานยุติธรรมระดับสูง รุ่นที่ ๕,
สำนักกิจการยุติธรรมกระทรวงยุติธรรม (พ.ศ.๒๕๕๘)
: หลักสูตรบริหารงานตำรวจชั้นสูง (บตส.) รุ่นที่ ๓๙
กองบัญชาการศึกษา (พ.ศ.๒๕๕๘)

ประวัติการทำงานโดยย่อ : รองสารวัตรสอบสวน สถานีตำรวจภูธรอำเภอบ้านโพธิ์
จังหวัดฉะเชิงเทรา (พ.ศ.๒๕๓๔-๒๕๓๖)
: รองสารวัตรสืบสวน สถานีตำรวจภูธรตำบลสำโรงใต้
จังหวัดสมุทรปราการ (พ.ศ.๒๕๓๖-๒๕๔๑)
: สารวัตร จราจร สถานีตำรวจภูธรอำเภอคลองหลวง
จังหวัดปทุมธานี (พ.ศ.๒๕๔๑-๒๕๔๕)
: นายเวร (สบ.๒) ผู้บัญชาการตำรวจภูธรภาค ๑ (พ.ศ.๒๕๔๕-๒๕๔๖)
: รองผู้กำกับการป้องกันปราบปราม สถานีตำรวจภูธรตำบลโพธิ์แก้ว
จังหวัดนครปฐม (พ.ศ.๒๕๔๖-๒๕๕๓)
: ผู้กำกับการฝ่ายอำนวยการ กองบังคับการสืบสวนสอบสวน
ตำรวจภูธรภาค ๗ (พ.ศ.๒๕๕๓-๒๕๕๕)
: ผู้กำกับการสถานีตำรวจภูธรกำแพงแสน
จังหวัดนครปฐม (พ.ศ.๒๕๕๕-๒๕๕๖)
: นายเวร (สบ ๕) รองผู้บัญชาการตำรวจแห่งชาติ (พ.ศ.๒๕๕๖-๒๕๕๘)
: รองผู้บังคับการตำรวจภูธรจังหวัดสมุทรสงคราม (พ.ศ.๒๕๕๘-๒๕๖๐)
: ผู้บังคับการภูธรจังหวัดสมุทรสงคราม (พ.ศ.๒๕๖๑-๒๕๖๒)
: ผู้บังคับการอำนวยการ ตำรวจภูธรภาค ๑ (พ.ศ.๒๕๖๓-๒๕๖๔)
: รองผู้บัญชาการสำนักงานคณะกรรมการข้าราชการตำรวจ
(พ.ศ.๒๕๖๔-๒๕๖๕)
: รองผู้บัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
(พ.ศ.๒๕๖๕-ปัจจุบัน)

ตำแหน่งปัจจุบัน : รองผู้บัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

สรุปย่อ

ลักษณะวิชา สังคมจิตวิทยา

เรื่อง แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี
ผู้วิจัย พล.ต.ต. ฐายุฎฐ์ จันทร์ถาวร **หลักสูตร** วปอ. **รุ่นที่** ๖๕
ตำแหน่ง รองผู้บัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

ความเป็นมาและความสำคัญของปัญหา

จากสถิติการรับแจ้งความออนไลน์รอบปีที่ผ่านมาพบว่าประเทศไทยมีภัยคุกคามด้านอาชญากรรมทางด้านเทคโนโลยีเพิ่มขึ้นเป็นจำนวนมาก โดยมีการสำรวจเป็นสถิติการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ ซึ่งในห้วงวันที่ 1 มี.ค. 2565 - 31 มี.ค. 2566 ได้มีแจ้งความออนไลน์จากประชาชน กว่า 253,951 เรื่อง โดยแบ่งเป็นคดีออนไลน์ 229,923 เรื่อง คดีอาญาอื่นๆ 7,848 เรื่อง รวมมูลค่าความเสียหาย 34,510 ล้านบาท แบ่งเป็นกลโกงตามแผนประทุษกรรมของคนร้าย ได้ 14 รูปแบบ มีการขออายัด 55,776 บัญชี ยอดเงิน 7,059 ล้านบาท และอายัดได้ทัน 449 ล้านบาท

ปัญหาดังกล่าวเป็นปัญหาที่สำคัญและส่งผลกระทบเกี่ยวกับความมั่นคงของประชาชนและของประเทศชาติในทุกระดับ โดยเฉพาะในระดับนโยบายที่มีผลกระทบต่อสังคมโดยกว้างอย่างยิ่งในยุคปัจจุบัน การป้องกันเป็นแนวทางเชิงรุกที่สำคัญ ถึงแม้อาชญากรรมทางเทคโนโลยีจะเป็นความผิดตามประมวลกฎหมายอาญาเดิม (คนร้ายใช้กลอุบายแบบเดิมๆ หลอกโดยใช้กิเลสของเหยื่อเป็นตัวล่อ คือ ทางความโลภ ความกลัว ความน่าเชื่อถือ) แต่วิธีการที่คนร้ายใช้ในการเข้าถึงเหยื่อและวิธีการโอนเงิน (ได้ไปซึ่งทรัพย์สิน/เงินของเหยื่อ) เป็นวิธีใหม่ๆ ที่อาศัยเทคโนโลยี ซึ่งเรื่องนี้เป็นเรื่องใหม่ในสังคมไทยและสังคมโลก ซึ่งกฎหมายหรือกระบวนการป้องกันมิให้ประชาชนตกเป็นเหยื่ออาจยังตามไม่ทัน เช่น การเก็บหลักฐานในคดีซึ่งต้องใช้ความรู้ความชำนาญพิเศษเฉพาะ การประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ผู้ให้บริการทางการสื่อสาร/Operator ผู้ให้บริการทางการเงินหน่วยงานควบคุมกำกับ ดูแลเทคโนโลยีการสื่อสารและการเงินต่างๆ ก็ยังขาดการประสานงานเพื่อต่อกรกับปัญหาดังกล่าว ตลอดจนกฎหมายที่ยังไม่เอื้อต่อการทำงานของหน่วยงานให้บริการ หน่วยงานบังคับใช้กฎหมาย ทำให้คนร้ายใช้เป็นช่องโหว่ในการกระทำความผิด

การดำเนินคดีเพื่อติดตามจับกุมคนร้ายเป็นการแก้ปัญหาที่ปลายเหตุ ทั้งการยึดทรัพย์ที่คนร้ายได้ไปก็เป็นไปได้ยากและสามารยึดทรัพย์คืนมาได้จำนวนน้อยมาก ที่ผ่านมาสำนักงานตำรวจแห่งชาติได้พยายามประชาสัมพันธ์ให้ทราบถึง Vaccine Cyber ซึ่งเป็นแนวทางหนึ่งในการป้องกันอาชญากรรมทางเทคโนโลยี โดยการสร้างความตระหนักรู้ให้กับประชาชน แต่จากสถิติการตกเป็นเหยื่อของประชาชนที่ผ่านมาทำให้เห็นว่า การสร้างความตระหนักรู้แต่เพียงอย่างเดียวยังไม่สามารถลดปริมาณการตกเป็นเหยื่อได้

ดังนั้น การป้องกันอาชญากรรมทางเทคโนโลยีที่มีประสิทธิภาพควรต้องมีแนวทางอย่างไร มีผู้ใดที่มีส่วนเกี่ยวในการสร้างภูมิคุ้มกันภัยไซเบอร์ หรือ Cyber Immunity ให้กับสังคมและประชาชนได้ดีกว่าที่เป็นอยู่ในปัจจุบัน ผู้วิจัยจึงมีความสนใจในการศึกษาแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี เพื่อหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีที่มีประสิทธิภาพ เพื่อให้สังคม ประชาชน เกิดความปลอดภัยอย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษา ปัญหา อุปสรรค ข้อขัดข้อง แนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี
2. เพื่อศึกษาถึงผู้มีส่วนเกี่ยวข้องในการบูรณาการ วิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี
3. เพื่อศึกษาหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

ขอบเขตของการวิจัย

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยต้องการศึกษาแนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี โดยมีขอบเขต ดังนี้

1. ด้านเนื้อหา

ศึกษาแนวทางการป้องกัน อาชญากรรมทางเทคโนโลยี โดยพิจารณาจากสาเหตุและปัจจัยสำคัญที่ทำให้ประชากรในประเทศไทยโดยทั่วไปตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยี และไม่ศึกษาการป้องกันปราบปรามหรือการสืบสวนสอบสวนแผนประทุษกรรมใดเป็นพิเศษโดยเฉพาะ

2. ด้านวิธีดำเนินการวิจัย

ใช้การวิจัยเชิงคุณภาพโดยการวิเคราะห์เอกสารที่เกี่ยวข้องและการสัมมนาอิงผู้เชี่ยวชาญ (connoisseurship) จำนวน 10 ท่าน

3. ด้านเวลา

ศึกษาในกรอบระยะเวลาระหว่าง 9 ก.ย. 2563 – 31 มี.ค. 2566 ซึ่งเป็นห้วงที่เริ่มมีการจัดตั้งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี การแจ้งความออนไลน์และความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องอย่างเป็นรูปธรรม

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์ วิธีการป้องกันอาชญากรรมทางเทคโนโลยีจากการวิจัยเอกสารและใช้เทคนิคการสัมมนาอิงผู้เชี่ยวชาญ (connoisseurship) ซึ่งเป็นเทคนิคที่เป็นรูปแบบการได้องค์ความรู้จากผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในศาสตร์และองค์ความรู้นั้นมาให้ข้อมูลเชิงลึกและทรรศนะต่อความรู้ที่ได้จากการวิเคราะห์เอกสารผู้ศึกษานำข้อมูลที่ได้จากวิธีวิจัยเอกสารมาทำการวิเคราะห์ข้อมูลเชิงคุณภาพโดยการนำข้อมูลที่ได้จากการค้นคว้าวิจัยมาจัดกระทำ

(Data processing) ให้เป็นระบบโดยใช้กรอบการวิเคราะห์ข้อมูลตามทรรศนะของ Huberman & Miles (1994 : 12) ซึ่งมีองค์ประกอบสำคัญ 3 ประการ ได้แก่ 1. การลดทอนของข้อมูล (Data reduction) หมายถึง การปรับลด เพิ่มหาข้อมูลใหม่จนได้ผลหรือข้อสรุป 2. การแสดงข้อมูล (Data display) หมายถึงการกระทำในรูปของการเล่าเรื่องว่าเกิดอะไรขึ้นก่อนหลัง อย่างไร ทำไม และ 3. การสรุปและยืนยันข้อสรุป (Drawing and verifying conclusion) หมายถึง มีการสรุปข้อมูลในขั้นแรกเบื้องต้นก่อนแล้วหลังจากนั้นเก็บข้อมูลต่อแล้วทดสอบการสรุปเบื้องต้นไปเรื่อย ๆ จนยืนยันข้อสรุปดังกล่าวได้ชัดเจน นำเสนอผลการวิจัยโดยการบรรยายเชิงพรรณนาแบบความเรียง

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบแนวทางแก้ไขปัญหา อุปสรรค ข้อขัดข้องในการแก้ไขปัญหาอาชญากรรมทาง เทคโนโลยี

2. ทำให้ทราบว่ามีผู้ใดที่มีส่วนเกี่ยวข้องและสามารถร่วมบูรณาการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี

3. เพื่อได้แนวทางในการบูรณาการเพื่อป้องกันไม่ให้เกิดอาชญากรรมทางเทคโนโลยีขึ้นกับประชาชนโดยทั่วไป

ผลการวิจัย

จากผลการวิจัยเรื่อง แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี สรุปผลการวิจัยตามวัตถุประสงค์ได้ ดังนี้

วัตถุประสงค์ข้อที่ 1 เพื่อศึกษา ปัญหา อุปสรรค ข้อขัดข้องของแนวทางการแก้ไขในการบูรณาการป้องกันอาชญากรรมทางเทคโนโลยี

จากการวิจัยนี้พบว่า ประเทศไทยยังคงมีปัญหา อุปสรรค ในการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีของไทยมากมายหลายด้าน แต่หากต้องการจะขับเคลื่อนการแก้ไขปัญหาอย่างบูรณาการ ควรจะต้องกำหนดกรอบแนวคิดที่สามารถสร้างการบูรณาการได้จริงอย่างเป็นรูปธรรม ซึ่งในที่นี้ได้กำหนดปัญหาสำคัญ 3 ประการ คือ คน, กฎหมาย/นโยบาย/คำสั่ง/มาตรการ และเทคโนโลยีจากนั้นจึงเอาหลักการสร้างภูมิคุ้มกันเพื่อให้สามารถต้านทานและต่อสู้กับภัยทางเทคโนโลยีที่เปลี่ยนแปลงสภาพและความรุนแรงได้อย่างรวดเร็วไม่มีสิ้นสุด

จากการศึกษาจึงได้ค้นพบปัญหาความไม่สมบูรณ์ของแนวทางในการป้องกันการก่ออาชญากรรมทางเทคโนโลยี ความไม่สมบูรณ์ของรูปแบบกระบวนการในการป้องกันการก่ออาชญากรรมทางเทคโนโลยี เนื่องจากอาชญากรรมทางเทคโนโลยีและภัยคุกคามทางไซเบอร์มีผลกระทบอย่างมากต่อประชาชน ทำให้เกิดการตอบสนองและแก้ไขปัญหาด้วยวิธีการต่าง ๆ อย่างรวดเร็ว ทั้งที่เกิดขึ้นแบบบูรณาการและแยกกันจัดการ ทำให้เกิดการขับเคลื่อนการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีโดยหน่วยงานทั้งภาครัฐและเอกชนที่เกี่ยวข้องอยู่ตลอดเวลา และก่อให้เกิดความเปลี่ยนแปลงของ กฎหมาย กฎ คำสั่ง นโยบายและมาตรการต่าง ๆ อย่างสม่ำเสมอ จึงทำให้ข้อมูลที่ได้จากการวิจัยอาจไม่ทันสมัยอยู่ตลอด จนทำให้เกิดอุปสรรคระหว่างหน่วยงาน

ที่เกี่ยวข้องอันเนื่องมาจากกฎหมาย กฎ นโยบาย คำสั่ง และมาตรการที่ไม่สอดประสานไปในทิศทางเดียวกัน

แนวทางการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี ที่เหมาะสมที่สุดคือการสร้างภูมิคุ้มกันทางไซเบอร์ ซึ่งภูมิคุ้มกันทางไซเบอร์จะเกิดขึ้นได้อย่างมีประสิทธิภาพหากมีการบริหารจัดการและบูรณาการป้องกันการก่ออาชญากรรมทางเทคโนโลยีใน 3 ด้านอย่างเหมาะสม อันประกอบไปด้วย คน, กฎหมาย/นโยบาย/มาตรการ, และเทคโนโลยี

เหตุผลความจำเป็นที่จะต้องคำนึงถึงองค์ประกอบทั้ง 3 ด้าน เนื่องมาจากการศึกษาที่พบว่าประเทศไทยในปัจจุบัน คนในประเทศยังคงขาดความรู้ขาดความตระหนักรู้ขาดความเข้าใจในเรื่องการใช้เทคโนโลยีได้อย่างปลอดภัย หรือยังไม่มีความรับผิดชอบต่อผู้อื่นในสิ่งที่ตนเองอาจมีส่วนสนับสนุนให้เกิดขึ้น ต่อมาคือเรื่องกฎหมาย นโยบาย และกระบวนการที่ยังคงเป็นอุปสรรคต่อการป้องกันอาชญากรรมทางเทคโนโลยี ระบบกฎหมายและนโยบายที่ไม่สนับสนุนเกื้อกูลกันระหว่างภาครัฐและเอกชน แต่เน้นการจับผิดจะทำให้ต่างฝ่ายต่างสร้างกำแพงมากกว่าช่วยเหลือแลกเปลี่ยนข้อมูลกัน และสุดท้ายคือ การที่ยังคงมีเทคโนโลยีที่มีไม่สนับสนุนการป้องกันภัยหรือแม้แต่เป็นอุปสรรคต่อการป้องกันอาชญากรรมทางเทคโนโลยี ยกตัวอย่างในกรณีของแอพพลิเคชั่นการทำธุรกรรมทางการเงินออนไลน์ควรมีระบบคัดกรองและช่วยเหลือมิให้ผู้ใช้บัญชีโอนเงินไปยังบุคคลที่ไม่รู้จักและเข้าข่ายเป็นบัญชีม้าจากการตรวจจับของระบบ เป็นต้น

วัตถุประสงค์ข้อที่ 2 เพื่อศึกษาถึงผู้มีส่วนเกี่ยวข้องในการบูรณาการ วิเคราะห์รูปแบบกระบวนการการป้องกันอาชญากรรมทางเทคโนโลยี

รูปแบบกระบวนการในการป้องกันอาชญากรรมทางเทคโนโลยีโดยอาศัยผู้เกี่ยวข้องทุกภาคส่วนที่เกี่ยวข้อง มีดังนี้

1. การปรับปรุงแก้ไขกฎหมาย ให้ทุกภาคส่วนมีความรับผิดชอบเชิงรุกที่จะป้องกันและยับยั้งภัยอาชญากรรมทางเทคโนโลยี เช่น การกำหนดหน้าที่ความรับผิดชอบในการคุ้มครองบุคคลที่ตนเองมีหน้าที่ให้บริการ หน่วยงานราชการที่อนุญาตให้มีการติดต่อสื่อสารทางเทคโนโลยีควรมีช่องทางกลางในการประชาสัมพันธ์ให้ความรู้และช่วยเหลือประชาชนที่อาจถูกฉ้อโกงหรือหลอกลวงแอบอ้างภาครัฐ ภาคธนาคารควรจะต้องมีความรับผิดชอบในการคุ้มครองลูกค้าที่โอนเงินไปบัญชีม้าโดยไม่จำเป็นต้องได้รับคำสั่งหรือร้องขอจากเจ้าหน้าที่บังคับใช้กฎหมาย เป็นต้น

2. การพัฒนาปรับรูปแบบการบริหารจัดการการให้บริการทางด้านเทคโนโลยีสารสนเทศที่ทำให้เกิดการใช้ทรัพยากรได้อย่างเหมาะสม สะดวก ใช้งานง่ายและปลอดภัย สามารถคุ้มครองป้องกันผู้ใช้งานได้อย่างมีประสิทธิภาพ เช่น แอพพลิเคชั่นธนาคารควรมีการเตือนบัญชีต้องสงสัย และมีช่องทางในการแจ้งและรายงานบัญชีม้า จากนั้นนำข้อมูลไปแบ่งปันกับเจ้าหน้าที่ภาครัฐที่มีหน้าที่รับผิดชอบ รวมถึงมีการพัฒนาการสร้างการรับรู้และรับผิดชอบให้กับประชาชนที่มีส่วนเกี่ยวข้องกับการใช้บัญชีม้า เป็นต้น

3. การพัฒนาบุคลากร และการประชาสัมพันธ์ให้ความรู้กับประชาชนทุกระดับอย่างเหมาะสมโดยไม่มีข้อจำกัดในเรื่องเวลา สถานที่และโอกาส

4. การพัฒนาปรับปรุงเทคโนโลยีในการป้องกันอาชญากรรมทางเทคโนโลยี

วัตถุประสงค์ข้อที่ 3 เพื่อศึกษาหาแนวทางการป้องกันอาชญากรรมทางเทคโนโลยีแบบบูรณาการที่เหมาะสม

ภูมิคุ้มกันภัยไซเบอร์ (Cyber Immunity) ที่เข้มแข็ง จะเป็นพลังสำคัญสาหรับการรักษาความมั่นคงของชาติในอนาคต ภูมิคุ้มกันภัยไซเบอร์ เป็นแนวคิด ที่ประยุกต์มาจากภูมิคุ้มกันในร่างกายมนุษย์ เป็นกลไกตามธรรมชาติของร่างกายที่ทาหน้าที่ป้องกัน หรือต่อต้านไม่ให้เชื้อโรคเข้าสู่ร่างกาย และพัฒนาร่างกายให้รับรู้ในการป้องกันและต่อสู้กับโรคร้าย ที่มีลักษณะใกล้เคียงกัน โดยไม่จำเป็นต้องได้รับเชื้อโรคนั้นมาก่อนก็ได้ เช่นเดียวกันภัยคุกคาม ทางด้านไซเบอร์ที่เปลี่ยนแปลงรูปแบบและวิธีการโดยตลอด หากประชาชนมีภูมิคุ้มกันภัยไซเบอร์ที่ดี ก็จะเป็นรากฐานความปลอดภัยของสังคมและประเทศชาติ

การสร้างภูมิคุ้มกันภัยไซเบอร์ที่สำคัญเริ่มจากความตระหนักรู้ของประชาชนถึงภัยคุกคามทางไซเบอร์ การมีกระบวนการทางกฎหมายที่เหมาะสม มีนโยบายและมาตรการที่ช่วยสร้างภาพแวดล้อมที่ดีของประเทศในด้านความมั่นคงทางไซเบอร์ในทุกระดับ และการมีและใช้เทคโนโลยีที่เหมาะสมกันประเทศ ในหัวข้อนี้จะทาการศึกษาถึงภูมิคุ้มภัยไซเบอร์ของประชาชนที่ได้จากการปฏิบัติงานของสานักงานตำรวจแห่งชาติ และกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีผู้วิจัยเล็งเห็นถึงความสำคัญทีว่า ภูมิคุ้มกันภัยไซเบอร์ของประชาชนของชาติจะนาไปสู่การพัฒนาศักยภาพประเทศ เพื่อเตรียมความพร้อมเผชิญภัยคุกคามทางไซเบอร์ที่จะเป็นปัญหาความมั่นคงแห่งชาติที่สำคัญในอนาคตภูมิคุ้มกันทางไซเบอร์กับความมั่นคงของชาติจึงเป็นเรื่องที่สอดคล้องกับเหมาะสมกับ สถานการณ์ปัจจุบัน และ เป็นเรื่องที่จะมีความท้าทายมากขึ้นอย่างยิ่งในอนาคตอันใกล้แต่ปัจจุบัน ยังไม่มีการศึกษาในเรื่องนี้อย่างเพียงพอ ความรู้ความเข้าใจเกี่ยวกับภูมิคุ้มกันทางไซเบอร์และ ความสัมพันธ์กับความมั่นคงไซเบอร์ของประเทศชาตินี้ จะนาไปสู่การกำหนดแนวทางและมาตรการ ที่เหมาะสมเพื่อป้องกันและพัฒนาความมั่นคงของชาติได้อย่างเหมาะสมกับสถานการณ์ในอนาคต

การสร้างภูมิคุ้มกันทางไซเบอร์ที่เหมาะสม จะช่วยเกิดการบูรณาการความร่วมมือเพื่อให้เกิดการป้องกันอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ และมีสอดคล้องกันอย่างเข้าใจถี่ถ้วนรอบด้าน (Comprehensive) ส่งผลให้ประเทศไทยมีความแข็งแกร่งทนทานและสามารถปรับตัวกับอาชญากรรมประเภทใหม่ได้โดยตลอด (Resilience) ซึ่งในการศึกษาวิจัยนี้มีกรอบแนวคิดที่นำเอาหลักคิดทางวิชาการในการสร้างแนวคิดการบริหารจัดการและบูรณาการการป้องกันการก่ออาชญากรรมทางเทคโนโลยีให้ได้ในทุกมิติ

หน่วยงานที่มีหน้าที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศประเภทต่าง ๆ ทั้งภาครัฐและเอกชนจะต้องคำนึงถึงการดำเนินกิจการหรือธุรกิจที่มุ่งสร้างภูมิคุ้มกันทางไซเบอร์ในแนวทางของการสร้างภูมิคุ้มกันภัยทางไซเบอร์ให้กับประชาชน หากทุกภาคส่วนดำเนินการในส่วนนี้อย่างครบถ้วนแล้ว ก็จะเกิดการบูรณาการความร่วมมือได้จริงอย่างเป็นรูปธรรม ยกตัวอย่าง ในกรณีของธนาคารที่มีการให้บริการแอพพลิเคชั่นทำธุรกรรมธนาคารออนไลน์ ควรมีระบบเทคโนโลยีที่สนับสนุนการป้องกันภัยจากบัญชีม้า สามารถพัฒนาความตระหนักรู้ให้กับประชาชนผู้ใช้แอพพลิเคชั่นดังกล่าว และทั้งภาครัฐและเอกชนก็มีกฎหมายหรือนโยบายที่สนับสนุนให้เกิดการสร้างภูมิคุ้มกันดังกล่าวให้กับผู้ใช้บริการทุกราย เป็นต้น

ข้อเสนอแนะ

ข้อเสนอแนะแบ่งให้สอดคล้องกับการบริหารจัดการและบูรณาการป้องกันการก่ออาชญากรรมทางเทคโนโลยีในอย่างเหมาะสม แบ่งเป็น 2 ส่วน ประกอบด้วยข้อเสนอแนะเชิงนโยบาย และข้อเสนอแนะในการวิจัยครั้งต่อไป

1. ข้อเสนอแนะเชิงนโยบาย

ผู้วิจัยมีข้อเสนอแนะ ดังนี้

1.1 การกำหนดนโยบายความปลอดภัยไซเบอร์แห่งชาติ รัฐบาลควรเร่งกำหนดนโยบายและยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ของประเทศไทย และรับฟังคามคิดเห็นจากทุกภาคส่วนที่เกี่ยวข้อง เนื่องจากเป็นเรื่องที่ละเอียดอ่อนและส่งผลกระทบอย่างมากต่อการพัฒนาธุรกิจของประเทศ

1.2 รัฐบาลควรทบทวนกฎหมายและระเบียบ ที่เกี่ยวข้องด้านความปลอดภัยไซเบอร์ของทุกภาคส่วนให้มีความทันสมัยและสามารถนำไปปฏิบัติตามได้อย่างมีประสิทธิภาพ โดยมีแนวทางไปในทิศทางเดียวกัน

1.3 รัฐบาลควรร่วมมือกับสถาบันการศึกษาในการปลูกฝังความรู้ด้านความปลอดภัยไซเบอร์ให้กับเยาวชน และควรเพิ่มช่องทางในการเผยแพร่ความรู้ด้านความปลอดภัยทางไซเบอร์ให้กับประชาชนมากขึ้น สอดแทรกความรู้ในการใช้งานอินเทอร์เน็ตในชีวิตประจำวันให้เกิดความปลอดภัย เพื่อให้เกิดวินัยและกลายเป็นวัฒนธรรมด้านความปลอดภัยไซเบอร์ต่อไป รวมถึงมีมาตรการในการประชาสัมพันธ์ถึงภัยของอาชญากรรมทางเทคโนโลยีไปในแนวทางเดียวกัน

2. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

2.1 ควรทำงานวิจัยที่หลากหลายด้านความปลอดภัยไซเบอร์ ทั้งงานวิจัยเชิงสำรวจโดยวิธีวิจัยปริมาณและวิธีวิจัยคุณภาพ และการวิจัยที่มีความเฉพาะเจาะจงในประเด็นต่างๆ เพื่อสามารถ เผยแพร่ให้ประชาชนรับรู้และเข้าใจเรื่องความปลอดภัยทางไซเบอร์มากขึ้น

2.2 ควรทำวิจัยถึงการดำเนินงานของประชาคมอาเซียนด้านความปลอดภัยทางไซเบอร์

2.3 เนื่องจากการวิจัยครั้งนี้เริ่มทำก่อนที่จะมีการประกาศใช้ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 จึงเห็นควรว่า หลังจากที่มีการบังคับใช้แล้ว และมีหน่วยงานต่างๆที่เกี่ยวข้องแล้ว ควรที่จะมีการวิจัยเพื่อที่จะประเมินผลการบูรณาการร่วมกันว่ามีส่วนใดจะต้องมีการพัฒนาปรับปรุงอีกหรือไม่