Vol.3 No.1 (January-June 2021)

สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย

กรกัญญ์ญารัก บุญสุขเกิด[1]

วันได้รับบทความ: 11 ตุลาคม 2563 วันแก้ไข: 19 กุมภาพันธ์ 2564 วันยอมรับเผยแพร่: 23 กุมภาพันธ์ 2564

บทคัดย่อ

ภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์นั้นมีวิวัฒนาการหลากหลายรูปแบบ ซึ่งส่งผลกระทบได้อย่างรวดเร็วและเป็นวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำผิดจำนวนมาก ซึ่งในยุคปัจจุบันการกระทำความผิดนั้นมีการพัฒนารูปแบบใหม่ๆมากขึ้นเรื่อย ๆ ตามการพัฒนาของเทคโนโลยี ทำให้ระบบกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยเองต้องมีการพัฒนาให้ควบคุมกับการกระทำความผิด โดยพึ่งมีการปรับปรุงและบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สำหรับปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) เพื่อให้ประเทศไทยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับปกป้องความเป็นส่วนบุคคลของประชาชน เทียบเท่ากับ GDPR ที่บังคับใช้ในสหภาพยุโรป และมีการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 โดยสำนักงานสภาความมั่นคงแห่งชาติ ซึ่งประเด็นปัญหาแม้มีการพัฒนากฎหมายแต่ก็ยังมีช่องว่าง เนื่องจากอาชญากรรมทางคอมพิวเตอร์นั้นมีการพัฒนารูปแบบใหม่ๆ มากขึ้นเรื่อย ๆ ตามเทคโนโลยีที่มีการพัฒนาสมัยใหม่ตลอดเวลา ซึ่งก็ยังมีข้อจำกัดในองค์ความรู้ ทักษะในการดำเนินงานของเจ้าหน้าที่อยู่ ซึ่งแนวทางการแก้ไขนั้นควรจะมีการดำเนินงานทุกภาคส่วนทั้งองค์กรภาครัฐและภาคเอกชนเอง

คำสำคัญ: อาชญากรรมคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ การก่อการร้าย อาชญากรรมไซเบอร์

[1] นักศึกษาหลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาการบังคับใช้กฎหมาย คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ (ผู้ประพันธ์บรรณกิจ)

Vol.3 No.1 (January-June 2021)

Situations and Preventive Approaches of Cybercrime in Thailand

Kornkanyaruk Boonsukkerd[1]

Received: October 11, 2020 Revised: February 19, 2021 Accepted: February 23, 2021

Abstract

Cyber threats and cybercrime evolve in many forms that impact quickly and extensively even without a large number of offenders. Nowadays with the development of technology, more and more new forms of offenses are committed. The legal system for controlling computer crimes in Thailand has to be developed to control offenses by improving and enforcing Thailand's Cybersecurity Act 2019, which was enacted to protect Critical Information Infrastructure (CII) and to provide Thailand with measures to prevent, tackle and mitigate the risks from cyber threats affecting the state security and domestic order, as well as Thailand's Personal Data Protection Act 2019 for protecting the privacy of the people. These measures are equivalent to the General Data Protection Regulation (GDPRX applicable in the European Union) and part of Thailand's National Cybersecurity Strategy 2017 – 2021, which was issued by the Office of the National Security Council. Despite the development of laws, there are still gaps because computer crime has evolved in more and more new forms. As technology is constantly evolving, there are still limitations in the body of knowledge. The operational skills of staff provide solutions which should be implemented in every sector in both public and private organizations.

Keywords: Computer crime, Cyber threat, Terrorism, Cybercrime

[1] Graduate student in Master of Arts Program in Criminology and Law Enforcement, Social Sciences Faculty, Royal Police Cadet Academy (Corresponding author)

บทนำ (Introduction)

ปัจจุบันทุกประเทศทั่วโลกกำลังก้าวเข้าสู่ยุคสังคมดิจิทัล ซึ่งความก้าวหน้าของเทคโนโลยีสารสนเทศนั้นถือมีบทบาทสำคัญต่อวิถีชีวิตและสังคมของมนุษย์มากยิ่งขึ้น โดยสำหรับประเทศไทยเองก็มีการผลักดันนโยบายเศรษฐกิจดิจิลทัลตามยุทธศาสตร์ชาติ พ.ศ. 2561 - 2580 และภารกิจสำคัญในการขับเคลื่อนการปฏิรูปประเทศในด้างต่างๆ เพื่อปรับปรุง แก้ไข จัดวางระบบ ปรับทิศทาง และสร้างหนทางในการพัฒนาประเทศให้เจริญมากยิ่งขึ้น เพื่อสามารถรับมือกับโอกาสและภัยคุกคามรูปแบบใหม่ๆที่มีการเปลี่ยนแปลงอย่างรวดเร็ว รุนแรง และด้วยนโยบายไทยแลนด์ 4.0 ที่มีความมุ่งมั่นที่จะปรับเปลี่ยนประเทศเป็น “เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม” (Value-Based Economy) เน้นการบริหารจัดการและเทคโนโลยี (Smart Farming) ที่เปลี่ยนจาก Traditional Services ซึ่งมีการสร้างมูลค่าค่อนข้างต่ำไปสู่ High Value Services และเปลี่ยนจากแรงงานทักษะต่ำไปสู่แรงงานที่มีความรู้ ความเชี่ยวชาญ และทักษะสูง (สุรัชพงศ์ สิกขาบัณฑิต. 2561) ซึ่งในการส่งเสริมให้มีการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสารเทคโนโลยีดิจิทัล และนวัตกรรมในทุกภาคส่วนนั้น ซึ่งเทคโนโลยีดิจิทัลที่มีการใช้มากที่สุด คือการใช้งานอินเตอร์เน็ต ไม่ว่าจะเป็นการส่งเสริมการเรียน การศึกษา การสร้างธุรกิจใหม่ๆ การส่งเสริมด้านสุขภาพ และการขนส่งคมนาคมโลจิสติกส์ การใช้เทคโนโลยีในการขับเคลื่อนไปสู่เศรษฐกิจดิจิทัลนั้น

แต่การพัฒนาด้านเทคโนโลยีดิจิทัลก็ถือว่ายังมีช่องโหว่ในการใช้เป็นเครื่องมือในการก่อให้เกิดภัยคุกคามไซเบอร์ และการก่ออาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) ซึ่งผู้ทำไม่จำเป็นต้องมีจำนวนมาก เพียงคลิกเดียวก็อาจส่งผลกระทบในวงกว้างก็ได้ มีลักษณะข้ามพรมแดน และในหลายครั้งเป็นการข้ามเขตอำนาจศาลด้วย โดยหลายกรณีไม่ถือว่าเป็นอาชญากรรม เนื่องจากเป็นเรื่องของกฎหมายเทคนิค โดยผู้กระทำความผิดมีหลายกลุ่ม ทั้งพวก Hacker คือพวกกลุ่มนักศึกษาที่ศึกษาทางด้านนี้ที่ทำการเจาะระบบเพื่อทดสอบความสามารถของตัวเอง หรือทดสอบระบบว่ามีจุดอ่อนหรือไม่ พวก Hacktivism คือแฮกเพื่อประโยชน์ในทางการเมือง เช่น กลั่นแกล้งด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ เพื่อสร้างความเสียหายให้หน่วยงานราชการ และพวก Cyberterrorism คือเจาะระบบเพื่อทำลายระบบสาธารณูปโภคที่สำคัญ ซึ่งอาจก่อให้เกิดความกลัวหรือมีข้อเรียกร้องทางการเมือง ถือเป็นภัยคุกคามที่ไร้พรหมแดน และมีผลกระทบในทุกมิติไม่ว่าจะเป็นเศรษฐกิจ สังคม และความมั่งคงของประเทศ

จากรายงานล่าสุดของ Cybint และ Cybersecurity Ventures พบว่าร้อยละ 60 ขององค์กรเคยประสบกับการถูกโจมตีทางไซเบอร์ เช่น DDoS Attack, Phishing หรือ Social Engineering คาดว่าความเสียหายอันเนื่องมาจากอาชญากรรมไซเบอร์จะพุ่งขึ้นแตะ 6 ล้านล้านดอลลาร์ (ประมาณ 181 ล้านล้านบาท) ในปี 2021 นี้ สอดคล้องกับรายงาน The Global Risks Report ประจำปี 2019 ของ World Economic Forum ที่ระบุว่า ความเสี่ยงอันเนื่องมาจากการโจมตีไซเบอร์สูงเกินค่าเฉลี่ยเป็นที่เรียบร้อย โดยมี Impact เป็นอันดับ 7 และ Likelihood เป็นอันดับ 5 ท่ามกลางปัจจัยเสี่ยงรวม 30 รายการ (TechTalkThai. 2562) ค่าดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index : GCI) ปี 2561 ประเทศไทย ร้อยละ 0.796 อยู่อันดับ 35 จาก 194 ประเทศ จากข้อมูลศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยพบว่า ภัยคุกคามไซเบอร์ของประเทศไทย ปี 2562 ทั้งหมด 2,470 เรื่อง โดยประเภท

ภัยคุกคาม ปี พ.ศ. 2562 ที่พบมากที่สุด คือการฉ้อโกงหรือหลอกลวง (Fraud) คิดเป็นร้อยละ 40 ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) คิดเป็นร้อยละ 21 และโปรแกรมไม่พึ่งประสงค์ (Malicious code) คิดเป็นร้อยละ 19 จะเห็นว่าภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) ในการป้องกันนั้นต้องอาศัยความรวดเร็ว ทันเหตุการณ์ เทคโนโลยีที่ทันสมัย และการทำงานที่มีระบบและมีประสิทธิภาพ เพราะไม่อย่างนั้นอาจส่งผลกระทบได้อย่างรวดเร็ว และทำให้เกิดความเสียหายได้ในหลากหลายมิติ โดยข้อมูลสถิติจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ในปี 2561 มีมูลค่าความเสียหายจากอาชญากรรมดังกล่าว 527 ล้านบาท เฉพาะคดีที่มาแจ้งกับ บก.ปอท. โดยตรงมีราว 2,700 คดี ไม่รวมโรงพักอื่น ๆ และคดีที่ความเสียหายน้อยจนคนไม่มาแจ้งความ ส่วนในปี 2562 ระบุว่า มีมูลค่าความเสียหายจากอาชญากรรมดังกล่าวถึง 371 ล้านบาท จาก 2,871 คดี ประเภทคดี คือ scam หลอกเอาเงิน และการทำsocial engineering (กองบังคับการปราบปรามการกระทำความผิด เกี่ยวกับอาชญากรรมทางเทคโนโลยี. 2561) และรูปแบบการกระทำความผิดที่พบเป็นข่าวในปัจจุบัน เช่น การหลอกลวง ปลอมแปลก ที่ทำได้แนบเนียนมากยิ่งขึ้นกว่าเดิม แต่อาจส่งผลความเสียหายได้มากขึ้น รวมทั้งการหลอกลวงพวกแชร์หรือการลงทุนนั้นก็อาจเป็นรูปแบบแปลกๆ ไปเรื่อย ๆ จากอดีตในประเทศไทยที่มีต้นกำเนินของแชร์ในประเทศไทย อย่างแชร์แม่ชม้อยที่หลอกล่อให้ลงทุนน้ำมัน ปัจจุบันก็มีการพัฒนารูปแบบแปลกมาเรื่อย ๆ การชวนการลงทุน ที่ได้ทัวร์ไปต่างประเทศ แชร์แม่มณีที่หลอกลงทุนทองคำ ปัจจุบันที่เป็นเป็นข่าวไม่นานกับการสร้างสกุลเงินดิจิตอลอย่างบิทคอย โดยอนาคตในด้านพวกการค้าที่ผิดกฎหมายอาจมีการค้าที่ควบคุมได้ยากมากขึ้น เนื่องจากในปัจจุบันที่มีการค้าของเถื่อนใต้ดินที่เราเรียกกันว่าเว็บดำนั้น ที่ค้าของผิดกฎหมายทุกชนิด อนาคตอาจดูเสรีและควบคุมได้ยากมากยิ่งขึ้นเรื่อย ๆ และก่อความไม่สงบหรือทำร้ายบุคคล อย่างที่ต่างประเทศที่มีการใช้โดรนในการสั่งหารที่ประเทศสหรัฐใช้สั่งหารผู้บัญชาการกองทัพประเทศอิหร่าน เป็นต้น

สำหรับมาตรการในการป้องกันภัยคุกคามไซเบอร์ และการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ (Cybercrime) ของประเทศไทยนั้น ได้มีกฎหมายที่เกี่ยวข้องที่สำคัญ ได้แก่ พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติที่ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับปกป้องความเป็นส่วนบุคคลของประชาชน เทียบเท่ากับ GDPR ที่บังคับใช้ในสหภาพยุโรป และโดยล่าสุดมีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เมื่อวันที่ 28 พฤษภาคม 2562 เพื่อให้มีมาตรการหรือการดำเนินการเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ ที่มีผลกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางด้านเศรษฐกิจ ความมั่นคงทางด้านทหาร และความสงบเรียบร้อยภายในประเทศ เพื่อให้เข้ากับภัยอาชญากรรมไซเบอร์ในปัจจุบัน

ดังนั้นจะเห็นว่าภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) นั้นมีวิวัฒนาการหลากหลายรูปแบบ ซึ่งส่งผลกระทบได้อย่างรวดเร็วและเป็นวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำผิดจำนวนมาก ซึ่งในยุคปัจจุบันนั้นก็มีการกระทำผิดที่พัฒนารูปแบบมากขึ้นเรื่อย

ๆ ตามความก้าวหน้าของเทคโนโลยีที่มีความฉลาดมากขึ้นเป็น 2 เท่าจากเดิมในทุกๆ ปีและระบบกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยเองก็พึ่งมีการปรับและบังคับใช้ จนเป็นที่มาของการศึกษาวิวัฒนาการอาชญากรรมไซเบอร์ในประเทศไทย เพื่อการศึกษาหารูปแบบของการกระทำผิดทางคอมพิวเตอร์ในประเทศไทย เพื่อเป็นแนวทางในการนำไปปรับใช้พัฒนามาตรการการป้องกันต่อไป

วิวัฒนาการอาชญากรรมคอมพิวเตอร์

วิวัฒนาการอาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) เริ่มจากการกระทำความผิดต่อ สิทธิส่วนบุคคล หรือข้อมูลส่วนบุคคล เนื่องจากยุคแรกๆมีการใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลเข้าด้วยกัน เป็นเหตุให้ข้อมูลต่างๆถูกรวบรวมและเชื่อมโยงเข้าถึงกัน ซึ่งจะเป็นการจารกรรมข้อมูลข่าวสารที่เกี่ยวกับความปลอดภัยของรัฐ โดยมีการขโมยข้อมูลส่วนบุคคล เพื่อใช้ในการข่มขู่ หรือรีดไถจากเจ้าของข้อมูล รวมถึงอาชญากรรมเศรษฐกิจ ที่มีการใช้คอมพิวเตอร์ในการร่วมกระทำความผิด เช่น การปลอมแปลงเงินตรา การปั่นหุ้น เป็นต้น

ต่อมาจะเป็นการกระทำความผิดโดยใช้คอมพิวเตอร์ในการหลอกลวง โดยอาศัยการเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ สมัยก่อนจะเกี่ยวข้องกับการเงินซึ่งมีการปลอมแปลงบัญชีด้านการเงินของธนาคารของบริษัท และผู้ประกอบการต่างๆ ในการปลอมแปลงตัวเลขในบัญชีเพื่อการยักยอกเงินดังกล่าวไปใช้ และพัฒนากระทำความผิดในเครื่องเบิกเงินอัตโนมัติ หรือตู้เอทีเอ็ม รวมทั้งบัตรชำระเงินหรือบัตรเครดิตประเภทต่างๆ มีการขโมยบัตรชำระเงินโดยใช้เทคนิคในการสุ่มหลายเลขเพื่อเบิกเงิน ไปจนถึงการติดตั้งเครื่องมือดักรหัสสลับไว้ที่ตู้เบิกเงิน ต่อมาก็มีการพัฒนาในการกระทำความผิดเกี่ยวกับบริการโทรศัพท์ผ่านเครือข่ายอินเตอร์เน็ต โดยผู้กระทำความผิดอาจใช้วิธีเปลี่ยนแปลง ยักย้ายรายการ หรือบัญชีการใช้โทรศัพท์ของตนให้กลายเป็นของผู้ใช้บริการโทรศัพท์ทางอินเตอร์เน็ตคนอื่นๆ

มีการใช้คอมพิวเตอร์ในการก่อวินาศกรรมคอมพิวเตอร์ หรือการก่อวินาศกรรมอินเตอร์เน็ตและการข่มขู่ทางอินเตอร์เน็ต จากสถิติเริ่มจากกระทำผิดส่วนบุคคลด้วยวิธีการปล่อยโปรแกรมไวรัส หรือวอร์มทำลายระบบ หรือข้อมูลคอมพิวเตอร์ หลังจากนั้นเริ่มมีการขยายเกิดผลเสียต่อคนจำนวนมากหลังจากมีระบบเครือข่ายคอมพิวเตอร์ ซึ่งผู้กระทำความผิดสามารถเขียนโปรมแกรมครั้งเดียว แต่ส่งเผยแพร่ต่อเหยื่อได้จำนวนมาก ซึ่งไวรัสนั้นมีการทำลายล้างเพื่อก่อวินาศกรรมหลังจากนั้นเริ่มมีการเจาะระบบ หรือเข้าถึงระบบของผู้อื่นโดยปราศจากอำนาจ เริ่มแรกเป็นทดลองว่าสามารถเจาะเข้าระบบของคนบุคคลอื่นได้หรือป่าว แต่ปัจจุบันการเจาะเข้าระบบนั้นสร้างความเสียหายได้กว้างขวาง จนต่อมาเริ่มมีการจารกรรมทางคอมพิวเตอร์ แม้ไม่ได้เกิดขึ้นบ่อยแต่ก็พบว่ามีอันตรายและความเสียหายสูงกว่าอาชญากรรมเศรษฐกิจแบบเดิม ๆ โดยวิธีในการจารกรรมข้อมูลที่ใช้จะมีทั้งเจาะระบบเพื่อเข้าถึงฐานข้อมูลในคอมพิวเตอร์ ข้อมูลที่ตกเป็นเป้าหมาย เช่น โปรแกรมคอมพิวเตอร์ ข้อมูลการศึกษาการวิจัย ข้อมูลความลับทางทหารหรือราชการ เป็นต้น การเผยแพร่เนื้อหาข้อมูลที่ไม่ชอบด้วยกฎหมาย กับอาชญากรรมไซเบอร์ เช่น การเผยแพร่ภาพลามกอนาจารเด็ก การพนัน การจำหน่ายอาวุธ หรือแม้แต่การบิดเบือนข้อมูลอันเป็นเท็จที่ละเมิดต่อกฎหมายหรือผิดกฎหมาย เป็นต้น

จะเห็นว่าวิวัฒนาการอาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ถือเป็นภัยคุกคามหนึ่งของประเทศ เช่นกัน โดยการกระทำความผิดก็จะมีวิวัฒนาการคล้ายกันตามการพัฒนาของระบบคอมพิวเตอร์ เริ่มจากการขโมยข้อมูลส่วนบุคคล การขโมยข้อมูลทางการเงินบัญชีเพื่อการปลอมแปลงตัวเลขและยักยอกเงิน การเจาะระบบของหน่วยงานราชการ หรือภาคธุรกิจ การโจมตีระบบ และปัจจุบันที่พบตามข่าว เช่น การพนันออนไลน์ การหลอกขายของออนไลน์ การขโมยข้อมูลบัตรกดเงินหรือข้อมูลการเงินการบัญชี การเผยแพร่ข้อมูลทางระบบคอมพิวเตอร์ที่ผิดกฎหมาย แก๊ง call center และการหลอกลวงทางสังคมออนไลน์ที่มีคนตกเป็นเหยื่อโดยเฉพาะสุภาพสตรี ที่มีการใช้โปรแกรมแชทโดยมีการสร้างโปรไฟล์ที่น่าเชื่อถือมาหลอกเหยื่อให้หลงรักและหลอกเงินไปเป็นจำนวนมาก การใช้สื่อโซเชียลในการโพสทำให้เกิดความเสียหายแก่ผู้ถูกกล่าวหา หรือการใช้สื่อในการบูลลี่ในสังคม ซึ่งจะเห็นว่า ปัญหาอาชญากรรมทางคอมพิวเตอร์นั้นอาจเป็นเครื่องในการกระทำผิดของอาชญากรรมอื่นที่ใช้จำนวนคนน้อย ใช้แรง เวลา ในการกระทำความผิดน้อย แต่ส่งผลกระทบที่รวดเร็วและวงกว้างได้ ซึ่งวัตถุประสงค์ก็จะคล้ายอาชญากรรมอื่นๆ อย่างการที่ส่งผลให้เกิดความเสียหายต่อร่างกาย จิตใจ เช่น การเจาะข้อมูลเพื่อเผยแพร่ข้อมูลลับส่วนบุคคล การโพสโดยให้ร้ายผู้อื่น หรือแม้แต่การบูลลี่โดยใช้ช่องทางสื่อออนไลน์ ซึ่งส่งผลทำให้เกิดผลกระทบที่รวดเร็ว ทำให้บุคคลนั้นเกิดความอับอาย ในวงกว้างอาจทำให้บุคคลนั้นเกิดคิดสั้นทำร้ายร่างกายตนเองเพื่อหนีปัญหา หรือส่งผลเป็นที่รังเกียดในสังคมและปัญหาอื่นๆที่ตามมา เช่นการใช้ความรุนแรงในสังคมนั้น ในส่วนที่ส่งผลวงกว้างที่ก่อให้เกิดความหวาดกลัวเช่นการโพสข่มขู่การวางระเบิดในพื้นที่ต่างๆ ก่อให้เกิดความหวาดกลัวความจลาจล หรือในปัจจุบันนี้ที่มีการระบาดของเชื้อไวรัสโคโรนาสายพันธุ์ใหม่ หรือโควิด 2019 (COVID-19) ที่ต่างมีการแชร์ข้อมูลมากมายทางสื่ออินเตอร์เน็ตทั้งจริงบางหรือทั้งเท็จบางที่ส่งผลต่อสังคมในวงกว้างที่ก่อให้เกิดความหวาดกลัวในสังคมไทยปัจจุบัน โดยบางคนที่มีอาการป่วยก็กังวลในการติดเชื้อมีการฆ่าตัวตายก็มี เป็นต้น นอกจากหวังผลที่ส่งผลต่อร่างกายหรือชีวิตแล้ว ก็คือหวังผลทางด้านทรัพย์ สิ่งของหรือผลประโยชน์ ซึ่งอดีตนั้นก็เป็นการวิ่ง ชิง ปล้น โดยใช้บุคคลในการกระทำโดยตรง แต่ปัจจุบันด้วยการพัฒนาของโลกเทคโนโลยีนั้นทำให้มีส่วนช่วยในการกระทำความผิดนั้นได้ผลตอบแทนได้มากขึ้นและเสียหายวงกว้างมากขึ้น เช่น แต่ก่อนก็เป็นการเจาะข้อมูลเพื่อเรียกค่าไถ่ข้อมูลนั้นหรือขายความลับจากการเจาะข้อมูล แก๊ง call center พัฒนามาเรื่อยการขโมยข้อมูลทางการเงินบัญชีเพื่อการปลอมแปลงตัวเลขและยักยอกเงิน อีกอย่างที่เห็นได้อีกอย่างคือปัญหาการพนันที่เมื่อก่อนต้องเป็นเปิดโดยบ่อนการพนันโดยที่ต้องอาศัยสถานที่ ปัจจุบันเราสามารถอยู่ส่วนไหนก็ได้ก็สามารถเข้าสู่การพนันได้หมด โดยเป็นการพนันออนไลน์ซึ่งการปราบปราม การตรวจสอบ การจับกุมนั้นทำได้ยาก เพราะการตรวจสอบแหล่งกระทำความผิดบางทีก็ไม่ได้อยู่ภายในประเทศไทย ปัญหาการหลอกลวงนั้นในปัจจุบันก็พบมากในทางอาชญากรรมทางคอมพิวเตอร์ ที่เห็นได้ชัดและยังคงส่งผลเรื่อยมาตั้งแต่อดีตจนถึงปัจจุบันทำให้เกิดผู้ที่รับผลกระทบวงกว้างและจำนวนเงินที่จำนวนมหาศาล อย่างการที่ชักชวนการลงทุนออนไลน์ หรือแชร์ออนไลน์ต่างๆที่ล่าสุดที่โด่งดัง อย่างแชร์แม่มณีที่มีมูลค่าเสียหายจำนวนมากที่เกิดจาการสร้างโปรไฟล์ของผู้ก่อเหตุที่ให้เกิดความน่าเชื่อถือ มีการอวดความร่ำรวย และหลอกล่อให้มีคนมาลงทุนโดยแชร์แม่มณีนั้นเป็นลงทุนทองคำโดยที่ผู้ก่อเหตุนั้นสร้างโปรไฟล์ว่าเป็นเจ้าของร้านทอง เป็นต้น และอีกอันที่ก่อให้เกิดความเสียหายต่อทรัพย์สิน

อีกอย่างคือการการใช้โปรแกรมแชทโดยมีการสร้างโปรไฟล์ที่น่าเชื่อถือมาหลอกเหยื่อให้หลงรักและหลอกเงินและติดตามตัวผู้กระทำความผิดได้ยากและน้อยที่จะสามารถติดตามเงินกลับคืนมาได้

ดังนั้น สำหรับประเทศไทยนั้นวิวัฒนาการอาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ นั้นถือเป็นภัยคุกคามหนึ่งของประเทศ เช่นกัน การกระทำความผิดก็จะมีวิวัฒนาการคล้ายกันตามการพัฒนาของระบบคอมพิวเตอร์ เริ่มจากการขโมยข้อมูลส่วนบุคคล การขโมยข้อมูลทางการเงินบัญชีเพื่อการปลอมแปลงตัวเลขและยักยอกเงิน การเจาะระบบของหน่วยงานราชการ หรือภาคธุรกิจ การโจมตีระบบ และปัจจุบันที่พบตามข่าว เช่น การพนันออนไลน์ การหลอกขายของออนไลน์ การขโมยข้อมูลบัตรกดเงินหรือข้อมูลการเงินการบัญชี การเผยแพร่ข้อมูลทางระบบคอมพิวเตอร์ที่ผิดกฎหมาย แก๊ง call center และการหลอกลวงทางสังคมออนไลน์ที่มีคนตกเป็นเหยื่อโดยเฉพาะสุภาพสตรี ที่มีการใช้โปรแกรมแชทโดยมีการสร้างโปรไฟล์ที่น่าเชื่อถือมาหลอกเหยื่อให้หลงรักและหลอกเงินไปเป็นจำนวนมาก เป็นต้น

ภัยคุกคามการก่ออาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime)

อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำผิดทางระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ประเภทของภัยคุกคามการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ (Cybercrime) (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์. 2555) โดยประเภทภัยคุกคามการก่ออาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ (Cybercrime) ดังนี้

1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) คือ ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)

2. โปรแกรมไม่พึงประสงค์ (Malicious Code) คือ ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ

3. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) คือ ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)

4. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) คือ ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักใน

สาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)

5. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) คือ ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) คือ ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

7. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) คือ ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

8. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) คือ ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ

9. ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) คือ ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุก คามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

สถิติภัยคุกคามการก่ออาชญากรรมทางคอมพิวเตอร์ หรืออาชญากรรมไซเบอร์ (Cybercrime) ที่พบในประเทศไทย (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2563) ดังนี้ จำแนกตามประเภทภัยคุกคาม ปี พ.ศ. 2562 พบว่า การจำแนกตามประเภทภัยคุกคามจากมากสุดไปน้อยตามลำดับ 3 อันดับแรกได้แก่ การฉ้อโกงหรือหลอกลวง (Fraud) ร้อยละ 40 ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) ร้อยละ 21 และ โปรแกรมไม่พึงประสงค์ (Malicious code) และในปี พ.ศ. 2563 พบว่า โปรแกรมไม่พึงประสงค์ (Malicious code) มากที่สุด คิดเป็นร้อยละ 36.85 รองลงมา การฉ้อโกงหรือหลอกลวง (Fraud) คิดเป็นร้อยละ 20.32 และการบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) คิดเป็นร้อยละ 12.15

สถิติจำแนกตามประเภทภัยคุกคาม 5 ปี ย้อนหลัง ตั้งแต่ พ.ศ. 2558 -2562 พบว่ามีแนวโน้มที่ลดลง โดย ปี พ.ศ. 2558 มีภัยคุกคาม ทั้งหมด 4,371 เรื่อง เรียงการจำแนกตามประเภทภัยคุกคามจากมากสุดไป

น้อยตามลำดับ 3 อันดับแรกได้แก่ โปรแกรมไม่พึ่งประสงค์ (Malicious code) การฉ้อโกงหรือหลอกลวง (Fraud) และ การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) และในปี พ.ศ. 2562 มีภัยคุกคามที่ลดลงกว่าทุกปี ทั้งหมด 2,470 เรื่อง เรียงการจำแนกตามประเภทภัยคุกคามจากมากสุดไปน้อยตามลำดับ 3 อันดับแรก ได้แก่ การฉ้อโกงหรือหลอกลวง (Fraud) ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) และโปรแกรมไม่พึ่งประสงค์ (Malicious code)

จำแนกตามอันดับประเทศที่แจ้งเหตุภัยคุกคาม ย้อนหลัง 5 ปี ตั้งแต่ ปี พ.ศ. 2558 – 2562 พบว่า ที่มีการแจ้งเหตุภัยคุกคามมากที่สุดระบบของไทยเซิร์ต รองลงมา คือ เยอรมัน และอังกฤษ และในปี พ.ศ. 2562 อันดับประเทศที่แจ้งเหตุภัยคุกคามมากที่สุด ได้แก่ ระบบของไทยเซิร์ต รองลงมา คือ เยอรมัน และอังกฤษ โดยประเทศไทยอยู่ลำดับที่ 4

ข้อควรระวังป้องกันภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันแนวโน้มภัยคุกคามด้านไซเบอร์นั้นถือว่ามีวิวัฒนาการในการพัฒนามากขึ้น เรื่อย ๆตามความก้าวหน้าของเทคโนโลยีโดยมีความฉลาดมากขึ้นเป็น 2 เท่าจากเดิม ซึ่งการป้องกันนั้นก็เพียงเป็นการวางระบบเพื่อป้องกันการถูกโจมตีที่มีมาหลายรูปแบบ ดังนั้นข้อควรที่ต้องระวังภัยคุกคาม และความมั่นคงปลอดภัยทางไซเบอร์ ในปี พ.ศ. 2563 ดังนี้ (ELEADER. 2562)

1. การหลอกหลวงได้อย่างเนียบเนียนด้วยเทคโนโลยี (Deepfake) คือ การใช้เทคโนโลยีปัญญาประดิษฐ์(artificial intelligence) หรือ AI ในการสร้าง Content ปลอมอย่างแนบเนียน ซึ่งอาจแปลงได้ทั้งภาพ เสียง หรือวิดีโอ เช่น ตัดต่อใบหน้าของผู้มีชื่อเสียงเข้าไปแทนหน้าตัวเองในวิดีโอ ทำให้ผู้ไม่ประสงค์ดีสามารถนำผู้มีชื่อเสียงคนดังกล่าวไปพูดหลอกลวงหรือแสดงบทละครเท็จตามต้องการได้ เนื่องจากความฉลาดของ AI ที่สามารถเก็บข้อมูลมาประมวลผล วิเคราะห์ และเรียนรู้สิ่งต่าง ๆ

2. ขบวนการสร้างความเชื่อ (Beyond Fake News) คือ การสร้างข่าวโดยใช้ส่วนหนึ่งของความจริง ไม่ใช่ข่าวโดยธรรมชาติ เพื่อเปลี่ยนแปลงความคิดของคน เช่น การ์ตูนล้อเลียนเสียดสีทางการเมืองจากเพจต่างๆ ซึ่งข่าวเหล่านี้จะดูน่าเชื่อถือเพราะมีฐานมาจากความจริง แต่ส่งผลลบต่อเป้าหมายบุคคลหรือองค์กร มักมีเป้าหมายเพื่อการดิสเครดิต เพื่อตอกย้ำด้านลบของบุคคลหรือสถาบันนั้น มีเป้าหมายซึมซับความเชื่อจนกระทั่งเชื่ออย่างถาวร Beyond Fake News มุ่งเป้าโจมตีเป้าหมายโดยอ้อม และอาจไม่สามารถเอาผิดทางกฎหมายจากผู้กระทำได้ โดยเฉพาะในกรณีที่ผู้กระทำอยู่ในต่างประเทศ

3. อธิปไตยไซเบอร์ และระบบรักษาความปลอดภัยแห่งชาติ (Cyber Sovereignty and National Security) คือ อธิปไตยไซเบอร์ (Cyber Sovereignty) เกิดขึ้นจากข้อมูลส่วนบุคคลที่แชร์บนโลกออนไลน์ไม่ว่าจะเป็นแพลตฟอร์มใดก็ตาม เจ้าของแพลตฟอร์มอาจจะนำไปศึกษาวิเคราะห์ เพื่อใช้ประโยชน์เชิงวิเคราะห์ ศึกษาพฤติกรรมของผู้ใช้แต่ละรายเพื่อนำเสนอสินค้าและบริการเข้าถึงผู้ใช้โดยตรง นับเป็นการรุกล้ำความเป็นส่วนตัว เรียกว่า อธิปไตยไซเบอร์ (Cyber Sovereignty) ยกตัวอย่างเช่น เมื่อเสิร์ชหาข้อมูลโรงแรม คนแต่ละคนจะได้ข้อมูลที่แตกต่างกันไป บางคนอาจได้ข้อมูลโรงแรมระดับ 5 ดาวในขณะที่อีกคนหนึ่งจะได้ข้อมูลโรงแรมระดับ 3 ดาว เป็นต้น สาเหตุมาจากสื่อที่เรารับชมนั้นถูกคัดสรรค์และกลั่นกรอง (Filter

Bubble Effect) มาจากผู้ให้บริการ และเป็นตัวเราเองที่ยินยอมส่งมอบข้อมูลของตนให้ผู้ให้บริการเหล่านั้นโดยไม่รู้สึกรู้สาอะไรเสียด้วย เหล่านี้อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของชาติในระยะยาวได้ อย่างไรก็ตาม ยังคงมีประเทศที่เรียกได้ว่าสามารถเอาชนะการคุกคามอธิปไตยทางไซเบอร์ได้ นั่นก็คือประเทศจีน เนื่องมาจากความพยายามปิดกั้นการเข้าถึงบริการต่างๆ จากภายนอกและสนับสนุนให้ประชาชนใช้บริการภายในประเทศนั่นเอง

4. ความปกติแบบใหม่ (The New Normal in Cybersecurity) คือ ความปกติแบบใหม่ (The New Normal in Cybersecurity) ที่เกิดขึ้นบนโลกไซเบอร์ ที่ทุกคนต้องพร้อมรับมือกับภัยไซเบอร์จู่โจม เพราะจะเป็นเรื่องปกติที่จะต้องเกิดขึ้น จึงต้องวางแผนว่าจะทำอย่างไรเมื่อโดนจู่โจม ไม่ว่าจะเป็นหน่วยงาน องค์กร บริษัท หรือแม้แต่บุคคลทั่วไป ซึ่งอีกไม่นานสิ่งเหล่านี้จะกลายเป็นเรื่องธรรมดาสามัญ ผู้บริหารจึงจำเป็นต้องปรับเปลี่ยนแนวคิดในการรับมือกับภัยคุกคามไซเบอร์เสียใหม่ จาก “ถ้า” ถูกโจมตีจะป้องกันอย่างไร ไปเป็น “เมื่อไหร่ก็ตาม” ที่ถูกโจมตีจะรับมืออย่างไร เพื่อให้ธุรกิจยังคงดำเนินต่อไปได้ หรือก็คือเปลี่ยนจาก Cybersecurity ไปเป็น นั่นคือการก้าวเข้าสู่ยุค Cyber Resiliency

แนวทางการป้องกันและกฎหมายที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

สำหรับประเทศไทยนั้น ด้านความมั่นคงปลอดภัยไซเบอร์ที่เห็นชัดที่สุด คือ การออกกฎหมาย 2 ฉบับ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล สำหรับปกป้องความเป็นส่วนบุคคลของประชาชน เทียบเท่ากับ GDPR ที่บังคับใช้ในสหภาพยุโรป โดยกฎหมายฉบับแรกนั้นเริ่มบังคับใช้เป็นที่เรียบร้อยตั้งแต่เดือนพฤษภาคม 2562 ในขณะที่กฎหมายฉบับหลังจะเริ่มบังคับใช้เดือนพฤษภาคม 2563 โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ กฎหมายที่ตราขึ้นเพื่อให้ประเทศไทยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยพระราชบัญญัตินี้ มีผลบังคับใช้แล้ว ตั้งแต่วันที่ 28 พฤษภาคม พ.ศ. 2562 โดยมีสาระสำคัญคือแนวทางในการจัดการ การป้องกัน การรับมือ และการลดความเสี่ยงทางไซเบอร์ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ความสามารถของบุคคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์อีกด้วย และได้มีประกาศจัดตั้งคณะกรรมการ 3 คณะได้แก่ (Thai-PDPA. 2563)

1. คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. (National Cyber Security Committee : NCSC) โดยมีนายกรัฐมนตรีเป็นประธาน มีหน้าที่เสนอนโยบาย จัดทำแผนแม่บท กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนา ยกระดับทักษะความรู้ของเจ้าหน้าที่ ประสานงานความร่วมมือกับหน่วยงานต่างๆ รวมไปถึงการติดตามและประเมินผลการปฏิบัติตามนโยบายที่ได้ถูกกำหนดแล้ว

2. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน มีหน้าที่ดูแลและดำเนินการ เพื่อรับมือกับภัยคุกคามไซ

เบอร์ ในระดับร้ายแรง กำหนดแนวทางปฏิบัติสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ รวมทั้งกำหนดมาตรการ ในการประเมินความเสี่ยง การตอบสนอง และรับมือกับภัยคุกคามที่เกิดขึ้น

3. คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ กบส. โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน ทำหน้าที่ดูแลงานด้านการบริหารงานทั่วไป

การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นเรื่องสำคัญของทุกองค์กร ฉะนั้น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ให้อำนาจเจ้าหน้าที่รัฐในการตรวจสอบข้อมูลคอมพิวเตอร์ของผู้ที่อาจมีข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้วย พร้อมทั้งมีการกำหนดบทลงโทษผู้ที่ฝ่าฝืนหรือไม่ให้ความร่วมมือ โดยมีทั้งโทษปรับและจำคุก ในขณะเดียวกัน ก็มีบทลงโทษหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ย่อหย่อนในการปฏิบัติหน้าที่ด้วย เช่น หากหน่วยงานฯ ละเลยไม่รายงานเหตุภัยคุกคาม โดยไม่มีเหตุอันควร มีโทษปรับไม่เกิน 200,000 บาท เป็นต้น

โดยมีคณะทำงานมีหน้าที่ดูแลโครงสร้างบริการพื้นฐานสำคัญทางสารสนเทศ 8 ด้านสำคัญ ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติก ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม (ACINFOTEC, 2562)

การรับมือภัยคุกคามทางไซเบอร์ มีการแบ่งระดับของภัยคุกคาม ไว้ดังนี้

1. ระดับไม่ร้ายแรง หมายถึงภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงทำให้ระบบคอมพิวเตอร์หรือการให้บริการด้อยประสิทธิภาพลง

2. ระดับร้ายแรง หมายถึงภัย คุกคามทางไซเบอร์ที่มีจุดมุ่งหมายในการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศให้เสียหาย จนไม่สามารถทำงานหรือให้บริการได้

3. ระดับวิกฤต หมายถึงภัยคุกคามที่มีระดับสูงกว่าระดับร้ายแรง ทำให้โครงสร้างพื้นฐานล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ และอาจส่งผลกระทบต่อสวัสดิภาพของประชาชน กระทบต่อความสงบเรียบร้อย ทำให้ประเทศตกอยู่ในภาวะคับขัน มีการก่อการร้าย มีการทำสงคราม

ในเชิงปฏิบัติ สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ไม่เพียงแต่เฉพาะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเท่านั้นที่จะต้องตระหนักและปฏิบัติตามแนวทางที่คณะกรรมการกำหนด แต่เป็นหน้าที่ของทุกคนที่ต้องช่วยกันเฝ้าระวังภัย ให้ข้อมูลที่เป็นประโยชน์ ช่วยอำนวยความสะดวกต่อการทำงานของรัฐ รวมถึงให้เบาะแสเพื่อการป้องกันแก้ไขอย่างทันท่วงที เป็นการปิดช่องโหว่ที่อาจส่งผลกระทบให้เกิดความเสียหายต่อประเทศชาติบ้านเมือง

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้อำนาจเจ้าหน้าที่รัฐในการตรวจสอบข้อมูลคอมพิวเตอร์ของผู้ที่อาจมีข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้วย พร้อมทั้งมีการกำหนดบทลงโทษผู้ที่ฝ่าฝืนหรือไม่ให้ความร่วมมือ โดยมีทั้งโทษปรับและจำคุก ในขณะเดียวกัน ก็มีบทลงโทษหน่วยงานโครงสร้างพื้นฐาน

สำคัญทางสารสนเทศที่ย่อหย่อนในการปฏิบัติหน้าที่ด้วย เช่น หากหน่วยงานฯ ละเลยไม่รายงานเหตุภัยคุกคามโดยไม่มีเหตุอันควร มีโทษปรับไม่เกิน 200,000 บาท เป็นต้น ซึ่งการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องสำคัญของทุกองค์กร

สรุปแนวทางในการรับมือหรือแนวทางการป้องกันกับอาชญากรรมทางคอมพิวเตอร์

1. ด้านบุคคล

1.1. มีการเพิ่มความระมัดระวังในการใช้บริการอินเตอร์เน็ต เว็บไซต์ หรือโซเชียลมีเดียต่างๆ ไม่ควรเข้าเว็บไซต์แปลกๆ หรือมีความเสี่ยงที่จะมีการขโมยข้อมูลส่วนบุคคลของเราได้ รวมตั้งควรตั้งค่าโปรไฟล์ให้มีความส่วนตัวไม่ควรโชว์ข้อมูลส่วนบุคคลมากเกินไป เช่น เฟสบุ๊คไม่ควรมีการลงข้อมูลส่วนบุคคล เช่น เลขบัญชี หรืออะไรที่สำคัญมากเกินไป

1.2. ควรตั้งรหัสความปลอดภัยในอุปกรณ์ทางคอมพิวเตอร์ หรือที่ต้องเชื่อมโยงอินเตอร์เน็ตต่างๆ รวมทั้งโทรศัพท์มือถือ ควรตั้งรหัสที่มีความยาก คาดเดายาก และซับซ้อนยากต่อการคาดเดา และไม่ควรใช้รหัสเหมือนๆกันๆ เพราะจะง่ายต่อการถูกเจาะข้อมูล

1.3. ควรมีการติดตามข่าวสารที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ หรือแม้แต่การแชร์ข้อมูลควรมีการตรวจสอบข้อเท็จจริงก่อนแชร์ต่อสาธารณะ หรือส่งต่อให้ผู้อื่น

2. ด้านภาครัฐและหน่วยงานที่เกี่ยวข้อง

2.1 การเสริมสร้างความรู้ให้แก่ประชาชน เช่น การรู้จักปัญหาอาชญากรรมทางคอมพิวเตอร์ ทิศทางแนวโน้มอาชญากรรมทางคอมพิวเตอร์ รวมถึงการป้องกันพื้นฐานแก่ประชาชน

2.2 มีการประชาสัมพันธ์ข้อมูลข่าวสารแก่ประชาชนให้สามารถเข้าถึงได้ง่าย อย่างข่าวเกี่ยวกับอาชญากรรมภายในประเทศและต่างประเทศ

2.3 มีการตั้งศูนย์หรือหน่วยงานเฉพาะในการตรวจสอบดูแลเรื่องปัญหาอาชญากรรมทางคอมพิวเตอร์ รวมถึงข้อมูลข่าวสารเกี่ยวกับความมั่งคงปลอดภัยทางคอมพิวเตอร์

2.4 เสริมความรู้หรือทักษะแก่เจ้าหน้าที่ในเรื่องเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ความรู้ด้านเกี่ยวกับระบบคอมพิวเตอร์ และอื่นที่เกี่ยวข้อง โดยควรมีการเสริมสร้างความรู้ทักษะในทุกๆปี เพื่อได้ศึกษาการพัฒนาอาชญากรรมทางคอมพิวเตอร์ และการพัฒนาของเทคโนโลยี

2.5 การวางระบบป้องกันเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ภายในประเทศ เช่น ระบบการตรวจสอบ หรือแม้ระบบการป้องให้กับหน่วยงานทั้งภาครัฐและส่งเสริมภาคเอกชน

2.6 การพัฒนาระบบด้วยขบวนการดำเนินคดีที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ที่มีหน่วยงานที่ตรวจสอบได้รวดเร็ว เฉพาะ และขบวนการในการดำเนินคดีที่รวดเร็วในการจับกุม การดำเนินคดีการฟ้อง ระบบศาลที่รวดเร็ว หรือขบวนการด้านยุติธรรมที่เกี่ยวกับคดีอาชญากรรมทางคอมพิวเตอร์ที่รวดเร็วมีประสิทธิภาพ

2.7 ด้านกฎหมายมีการพัฒนากฎหมายให้มีความคลุมตามทันการพัฒนาของอาชญากรรมทางคอมพิวเตอร์ และมีการกำหนดโทษที่เด็ดขาดเหมาะสมกับความผิด

2.8 ด้านการร่วมมือกับหน่วยงานที่เกี่ยวข้อง หรือหน่วยงานระหว่างประเทศ ในการบริหารจัดการอาชญากรรมทางคอมพิวเตอร์ เพราะอาชญากรรมบางอย่างผู้กระทำความผิดอาจไม่ได้บ่งการในประเทศก็จำเป็นที่ต้องมีการประสานหน่วยงานของประเทศนั้นๆ

สรุป (Conclusion)

ปัญหาด้านภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ (Cybercrime) นั้นมีวิวัฒนาการหลากหลายรูปแบบ ซึ่งส่งผลกระทบได้อย่างรวดเร็วและวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำผิดจำนวนมาก และในยุคปัจจุบันนั้นก็มีการกระทำผิดที่พัฒนามากขึ้นเรื่อย ๆ และระบบกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์ในประเทศไทยก็พึ่งมีการปรับและบังคับใช้ ซึ่งโดยประเทศไทยก็มีการออกกฎหมาย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล สำหรับปกป้องความเป็นส่วนบุคคลของประชาชน เทียบเท่ากับ GDPR ที่บังคับใช้ในสหภาพยุโรป และมีการกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 โดยสำนักงานสภาความมั่นคงแห่งชาติ ซึ่งประเด็นปัญหาแม้มีการพัฒนากฎหมายแต่ก็ยังมีช่องว่างเนื่องจากอาชญากรรมทางคอมพิวเตอร์นั้นมีการพัฒนารูปแบบใหม่ๆมากขึ้นเรื่อย ๆ ตามเทคโนโลยีที่มีการพัฒนาสมัยใหม่ตลอดเวลา ซึ่งก็ยังมีข้อจำกัดในองค์ความรู้ ทักษะในการดำเนินงานของเจ้าหน้าที่อยู่ ซึ่งแนวทางการแก้ไขนั้นควรจะมีการดำเนินงานทุกภาคส่วนทั้งองค์กรภาครัฐและภาคเอกชนเอง ที่ต้องมีการเตรียมพร้อมและบริหารจัดการความเสี่ยงที่จะเกิดขึ้น การวางแผนสำรองข้อมูลเมื่อถูกจู่โจม และความเข้มงวดของกฎหมาย ปัญหาที่เกิดขึ้นจากข้อมูลรั่วไหลอยู่บ่อยครั้ง องค์กรจึงจำเป็นต้องพร้อมรับต่อการจู่โจมทางไซเบอร์ ทั้งมาตรการทำระบบให้รองรับต่อกฎหมายคุ้มครองข้อมูลส่วนบุคคล ทำระบบรักษาความปลอดภัยเพื่อให้การบริการดิจิทัลขององค์กรมีเสถียรภาพ สร้างกลไกในการพัฒนาและควบคุมระบบกฎหมายและเจ้าหน้าที่ให้ดำเนินการได้อย่างเหมายสม และที่สำคัญคือประชาชนเองควรมีการเผยแพร่องค์ความรู้ในการป้องกันตนเองให้กับประชาชนได้อย่างถูกต้องและเหมาะสม ได้แก่ การไม่เปิดเผยข้อมูลส่วนบุคคล การป้องกันตนเองทุกครั้งเมื่อมีการเข้าสู่ระบบอินเตอร์เน็ต ในการป้อนรหัสที่มีความปลอดภัย การสำรองข้อมูลโดยไม่เก็บข้อมูลทุกอย่างไว้รวมกัน เป็นต้น

เอกสารอ้างอิง (References)

กองบังคับการปราบปรามการกระทำความผิด เกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2561). *TCSD ร่วมกับ MFEC แข่งความปลอดภัยไซเบอร์ เพื่อให้สังคมตระหนักภัยออนไลน์*. สืบค้นจาก https://tcsd.go.th/tcsd%E0%B8%A3%E0%B9%88%E0%B8%A7%E0%B8%A1%E0%B8%81%E0%B8%B1%E0%B8%9Amfec/.

กองบังคับการปราบปรามการกระทำความผิด เกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2562). *แนวทางการป้องกันอาชญากรรมทางคอมพิวเตอร์*. สืบค้นจาก https://tcsd.go.th/แนวทางการป้องกันอาชญากรรมทางคอมพิวเตอร์/.

ข่าวสาร. (2558). *อาชญากรรมไซเบอร์พุ่ง ไทยเสี่ยงสูงเป็นฐานโจมตีที่อื่น ชี้ทุกฝ่ายต้องร่วมรับมือ*. สืบค้นจาก https://ictlawcenter.etda.or.th/news/detail/news-cyber-crime-and-international-cooperation.

โครงงานคอมพิวเตอร์. (2561). *เทคโนโลยีโลกปัจจุบันและอนาคต*. สืบค้นจาก http://jsmicky.blogspot.com/2018/11/blog-post.html.

โครงงานคอมพิวเตอร์. (2563). *สถิติภัยคุกคาม 2563*. สืบค้นจาก https://www.thaicert.or.th/statistics/statistics.html.

ณรงค์ กุลนิเทศ. (2561). รูปแบบและมาตรการแก้ปัญหาอาชญากรรมไซเบอร์. ใน *การประชุมวิชาการและนำเสนอผลงานวิจัยระดับชาติและนานาชาติ ครั้งที่ 6* (น. 224). กรุงเทพฯ.

สุธี จันทรพันธุ์. (2559). *รายงานการวิเคราะห์ "โครงการศึกษาความเป็นไปได้ในการพัฒนาระบบเตือนภัยการโจมตีและแนวทางการบริหารจัดการของประเทศไทย". สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง*. สืบค้นจาก http://lib.nbtc.go.th:8080/aion-streaming/access.do?p=Y29udGVudCUyRl9jb250ZW50U291cmNlXzIwMTYwNTI0XzAzMjI1MV8xNDY0MDc4MTcxMTgxLnBkZg==&m=stream.

สุรัชพงศ์ สิกขาบัณฑิต. (2561). *นโยบายประเทศไทย ๔.๐ : โอกาส อุปสรรค และผลประโยชน์ของไทยในภูมิภาคอาเซียน.กลุ่มงานสหภาพสมาชิกรัฐสภาเอเชียและแปซิฟิก*. สำนักองค์การรัฐสภาระหว่างประเทศ.บทความ.เอกสาร.

สำนักงานสภาความมั่นคงแห่งชาติ. (2560). *ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 -2564*. กรุงเทพมหานคร: สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา.

สรณันท์ จิวะสุรัตน์ และ ชัยชนะ มิตรพันธ์. (2555). *ความเป็นมาของไทยเซิร์ต จากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที*. สืบค้นจาก https://www.thaicert.or.th/papers/general/2012/pa2012ge001.html.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). (2562). *รายงานประจำปีไทยเซิร์ต 2560-2561*. กรุงเทพฯ: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต).

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). (2561). *2017-2018 ThaiCERT Annual Report. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อ*

เศรษฐกิจและสังคม.ครั้งที่ 1. กรุงเทพฯ: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต).

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). (2562). *สถิติภัยคุกคาม.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์*. สืบค้นจาก https://www.thaicert.or.th/statistics/statistics.html.

ACINFOTEC. (2562). *องค์กรต้องปรับตัวอย่างไร เมื่อ พ.ร.บ. ไซเบอร์ 2562 ประกาศใช้แล้ว*. สืบค้นจาก https://www.acinfotec.com/2019/07/23/thai-cyber-law-2562/.

ELEADER. (2562). *5 แนวโน้ม Cyber Security และ Privacy ที่ต้องระวัง ในปี 2563*. สืบค้นจาก https://www.theeleader.com/cyber-security/5-trends-in-cyber-security-and-privacy-to-look-out-for-in-2020/.

Tech Talk THAI. (2562). *[CDIC 2019] สรุปแนวโน้มภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์ในปี 2020 โดย อ.ปริญญา หอมอเนก*. สืบค้นจาก https://www.techtalkthai.com/cdic-2019-threat-landscape-and-cybersecurity-trends-in-2020/.

Thai-PDPA. (2563). *พรบ.คุ้มครองฯ มีผลอย่างไรกับองค์กร หรือ หน่วยงาน*. สืบค้นจาก https://thai-pdpa.com/%E0%B8%9E%E0%B8%A3%E0%B8%9A-%E0%B8%84%E0%B8%B8%E0%B9%89%E0%B8%A1%E0%B8%84%E0%B8%A3%E0%B8%AD%E0%B8%87%E0%B8AF.