เศรษฐศาสตร์และบริหารธุรกิจปริทัศน์
BUSINESS ADMINISTRATION AND ECONOMICS REVIEW

เศรษฐศาสตร์อาชญากรรมไซเบอร์: สถานะองค์ความรู้และการวิจัยในอนาคต

The Economics of Cybercrime: State of Knowledge and Future Research

นิติพงษ์ ส่งศรีโรจน์[1]

Nitiphong Songsrirote[1]

[1]ผู้ช่วยศาสตราจารย์ นิติพงษ์ ส่งศรีโรจน์ สาขา เศรษฐศาสตร์ คณะการบัญชีและการจัดการ มหาวิทยาลัยมหาสารคาม

[1]Assistant Professor in Economics, Mahasarakham Business School, Mahasarakham University

Tel. 09-9961-4995 E-mail: nitiphong.s@msu.ac.th

(Received: August 29, 2024 ; Revised: September 18, 2024 ; Accepted: October 8, 2024)

บทคัดย่อ

อาชญากรรมทางไซเบอร์เป็นภัยคุกคามที่สำคัญต่อเศรษฐกิจ ความมั่นคง และความเป็นอยู่ของสังคมไทย ปัจจัยทางเศรษฐกิจ เช่น ความเหลื่อมล้ำทางรายได้ ความยากจน และการว่างงาน เป็นตัวขับเคลื่อนหลักที่ผลักดันให้คนหันไปสู่อาชญากรรมทางไซเบอร์ โดยเฉพาะในกลุ่มผู้มีรายได้น้อยที่มองว่าเป็นวิธีหนึ่งในการสร้างความมั่นคงทางการเงิน การศึกษาแม้จะช่วยลดอัตราอาชญากรรม แต่เมื่อผนวกกับทักษะทางเทคนิคก็อาจนำไปสู่การโจมตีทางไซเบอร์ที่ซับซ้อนได้ ความก้าวหน้าทางเทคโนโลยี แม้จะช่วยเพิ่มการเติบโตทางเศรษฐกิจ แต่ก็เปิดช่องทางใหม่ให้อาชญากรทางไซเบอร์ ประเทศไทยมีความเสี่ยงสูงจากการใช้อินเทอร์เน็ตอย่างแพร่หลาย การเชื่อมต่อบรอดแบนด์ที่รวดเร็ว และระดับความรู้ทางเทคโนโลยีที่แตกต่างกัน แม้จะมีกฎหมายความปลอดภัยทางไซเบอร์และการจัดตั้งหน่วยงานบังคับใช้เฉพาะทางแล้ว แต่ความท้าทายยังคงมีอยู่เนื่องจากภัยคุกคามที่เปลี่ยนแปลงตลอดเวลา ผลกระทบทางเศรษฐกิจจากอาชญากรรมทางไซเบอร์ในไทยนั้นรุนแรง นำไปสู่การสูญเสียทางการเงิน ลดการลงทุนจากต่างประเทศ และลดความเชื่อมั่นในแพลตฟอร์มดิจิทัล เพื่อรับมืออย่างมีประสิทธิภาพ จำเป็นต้องมีการวิจัยเพิ่มเติมเกี่ยวกับตัวขับเคลื่อนทางเศรษฐกิจและเทคโนโลยีของอาชญากรรมทางไซเบอร์ และการสร้างความร่วมมือระหว่างประเทศเพื่อสร้างอนาคตดิจิทัลที่ปลอดภัยสำหรับประเทศไทย

คำสำคัญ : *เศรษฐศาสตร์อาชญากรรมไซเบอร์, ความปลอดภัยทางไซเบอร์, เศรษฐกิจ*

Abstract

Cybercrime poses a significant threat to Thailand's economy, security, and societal well-being. Economic factors such as income inequality, poverty, and unemployment are key drivers that push individuals toward cybercrime, particularly among low-income groups who perceive it as a means of financial stability. While education can help reduce crime rates, when coupled with technical skills, it can also lead to more sophisticated cyberattacks. Technological advancements, though beneficial for economic growth, create new avenues for cybercriminals. Thailand is highly vulnerable due to widespread internet usage, fast broadband connections, and varying levels of technological literacy. Despite the presence of cybersecurity laws and specialized enforcement agencies, challenges remain due to the ever-evolving nature of cyber threats. The economic impact of cybercrime in Thailand is severe, leading to significant financial losses, reduced foreign investment, and diminished trust in digital platforms. To effectively combat this issue, further research on the economic and technological drivers of cybercrime, as well as international collaboration, is essential to create a secure digital future for Thailand

Keywords: *Economics of Cybercrime, Cybersecurity, Economy*

บทนำ

สถานการณ์อาชญากรรมในประเทศไทยในปัจจุบันมีแนวโน้มหลายประการที่น่ากังวล โดยสะท้อนถึงปัญหาที่มีมาอย่างยาวนานและความท้าทายที่เกิดขึ้นใหม่ แม้ว่าอัตราอาชญากรรมโดยรวมจะมีความผันผวน แต่อาชญากรรมที่เกี่ยวข้องกับยาเสพติด อาชญากรรมทางการเงิน อาชญากรรมไซเบอร์ และความรุนแรง ยังคงเป็นปัญหาสำคัญที่ท้าทายการบังคับใช้กฎหมายและสังคมโดยรวม

หนึ่งในความกังวลที่สำคัญที่สุดยังคงเป็นปัญหาอาชญากรรมที่เกี่ยวข้องกับยาเสพติด การค้ายาเสพติดยังคงเป็นปัญหาใหญ่ในประเทศไทย โดยประชากรในเรือนจำส่วนใหญ่เป็นผู้กระทำความผิดเกี่ยวกับยาเสพติด แม้ว่ารัฐบาลจะพยายามแก้ไขปัญหานี้ แต่ก็ยังประสบความสำเร็จอย่างจำกัด และอาชญากรรมที่เกี่ยวข้องกับยาเสพติดยังคงเป็นจุดเด่นของภาพรวมอาชญากรรมทั้งหมด นอกจากนี้ อาชญากรรมข้ามชาติ เช่น การค้ามนุษย์และการลักลอบขนของผิดกฎหมาย ยังคงเป็นปัญหาใหญ่โดยเฉพาะบริเวณชายแดนของประเทศไทย (Worldmetrics, 2024)

อาชญากรรมทางการเงินเป็นอีกหนึ่งด้านที่น่ากังวล ประเทศไทยเผชิญความท้าทายในการต่อสู้กับการฟอกเงินและอาชญากรรมทางการเงินอื่น ๆ โดยสำนักงานป้องกันและปราบปรามการฟอกเงิน

(ปปง.) มีบทบาทสำคัญในการแก้ไขปัญหาเหล่านี้ แม้ว่าจะมีการปรับปรุงการปฏิบัติตามมาตรฐานสากล แต่ประเทศไทยยังคงเผชิญปัญหาการทุจริตและอาชญากรรมทางการเงิน โดยเฉพาะในภาคการธนาคารและผู้ให้บริการสินทรัพย์ดิจิทัล (Financial Crime News, 2024) การทุจริตภายในหน่วยงานบังคับใช้กฎหมายและภาครัฐเป็นอีกปัญหาหนึ่งที่เพิ่มความท้าทาย ทำให้ประชาชนสูญเสียความเชื่อถือและลดประสิทธิภาพในการแก้ไขปัญหาอาชญากรรม (Thai Examiner, 2024)

อาชญากรรมไซเบอร์เป็นภัยคุกคามที่เพิ่มขึ้นอย่างรวดเร็วในประเทศไทย การเพิ่มขึ้นของการหลอกลวงออนไลน์ การลงทุนปลอม และการรังแกทางออนไลน์ โดยเฉพาะอย่างยิ่งต่อกลุ่มเปราะบาง เช่น เด็กและผู้ที่มีความหลากหลายทางเพศ ชี้ให้เห็นถึงธรรมชาติของอาชญากรรมที่เปลี่ยนไปเป็นดิจิทัลมากขึ้น (Worldmetrics, 2024)

อาชญากรรมไซเบอร์ในประเทศไทยมีความซับซ้อนและเพิ่มความรุนแรงขึ้นอย่างต่อเนื่อง เนื่องจากการพัฒนาเทคโนโลยีและการเพิ่มขึ้นของการใช้อินเทอร์เน็ต ทำให้ประเทศไทยกลายเป็นศูนย์กลางของกิจกรรมอาชญากรรมไซเบอร์ทั้งในระดับภายในประเทศและระดับนานาชาติ รัฐบาลไทยได้ดำเนินการตอบโต้ภัยคุกคามเหล่านี้ด้วยการออกมาตรการทางกฎหมายและการจัดตั้งหน่วยงานพิเศษหลายหน่วยเพื่อจัดการกับอาชญากรรม ไซเบอร์ หนึ่งในพัฒนาการที่สำคัญล่าสุดคือการจัดตั้ง "แผนกคดีอาชญากรรมทางเทคโนโลยี" ภายในศาลอาญาของประเทศไทยในเดือนมีนาคม พ.ศ. 2567 แผนกนี้มีหน้าที่พิจารณาคดีอาชญากรรมไซเบอร์โดยเฉพาะ โดยมีอำนาจในการพิจารณาคดีที่เกี่ยวข้องกับการกระทำผิดทางเทคโนโลยีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ การจัดตั้งแผนกนี้แสดงถึงความมุ่งมั่นของประเทศไทยในการเสริมสร้างการตอบโต้ภัยคุกคามทางไซเบอร์ผ่านระบบยุติธรรม (Tilleke & Gibbins, 2024)

ประเทศไทยยังได้ออกมาตรการทางกฎหมายใหม่ ๆ เพื่อรับมือกับอาชญากรรมไซเบอร์ เช่น พระราชกฤษฎีกามาตรการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับเทคโนโลยีซึ่งมีผลบังคับใช้ตั้งแต่ปี พ.ศ. 2566 ทำให้เจ้าหน้าที่สามารถระงับธุรกรรมทางการเงินที่สงสัยว่าเกี่ยวข้องกับอาชญากรรมไซเบอร์ได้ รวมถึงกำหนดให้สถาบันการเงินและผู้ให้บริการต้องแบ่งปันข้อมูลกับหน่วยงานบังคับใช้กฎหมาย การดำเนินการเหล่านี้มาพร้อมกับบทลงโทษทางกฎหมายที่เข้มงวดต่อผู้ที่เกี่ยวข้องกับการกระทำความผิด (Tilleke & Gibbins, 2024) ความร่วมมือระหว่างหน่วยงานภาครัฐเป็นอีกหนึ่งกลยุทธ์สำคัญในการต่อสู้กับอาชญากรรมไซเบอร์ สำนักงานตำรวจแห่งชาติร่วมกับหน่วยงานต่าง ๆ ได้ดำเนินการจับกุมเครือข่ายอาชญากรรมออนไลน์ เช่น แก๊งคอลเซ็นเตอร์และวงพนันออนไลน์ โดยใช้เทคโนโลยีปัญญาประดิษฐ์ในการรวบรวมและวิเคราะห์ข้อมูลเพื่อเพิ่มประสิทธิภาพในการสืบสวนและจับกุมผู้กระทำความผิด (OpenGov Asia, 2024) นอกจากนี้ คณะกรรมการกิจการกระจาย

เสียงและกิจการโทรคมนาคมแห่งชาติ (กสทช.) ยังได้บังคับใช้กฎระเบียบที่เข้มงวดในการลงทะเบียนซิมการ์ด เพื่อต่อสู้กับการใช้งานซิมการ์ดในการกระทำผิดกฎหมาย โดยมีการตรวจสอบข้อมูลผู้ใช้และระงับการใช้งานซิมการ์ดที่สงสัยว่ามีส่วนเกี่ยวข้องกับอาชญากรรม นอกจากนี้ยังมีการบล็อกโครงสร้างพื้นฐานการสื่อสารที่ผิดกฎหมายในพื้นที่ชายแดนเพื่อต่อต้านการกระทำผิด (Thai Examiner, 2024; OpenGov Asia, 2024)

ผลกระทบทางเศรษฐกิจจากอาชญากรรมไซเบอร์ในประเทศไทยเป็นปัญหาที่เพิ่มมากขึ้น ซึ่งสะท้อนถึงแนวโน้มทั่วโลกที่มีภัยคุกคามไซเบอร์เพิ่มขึ้น อาชญากรรมไซเบอร์ซึ่งรวมถึงกิจกรรมต่าง ๆ เช่น ฟิชชิง การขโมยข้อมูลประจำตัว การฉ้อโกงทางออนไลน์ และอาชญากรรมดิจิทัลอื่น ๆ ได้ส่งผลกระทบต่อเศรษฐกิจของไทยอย่างมีนัยสำคัญ โดยก่อให้เกิดความสูญเสียทางการเงินที่ยากจะประมาณการได้อย่างแม่นยำ อย่างไรก็ตามความสูญเสียทางการเงินโดยตรงจากอาชญากรรมไซเบอร์ในประเทศไทยมีมูลค่าสูงมาก ตัวอย่างเช่น การศึกษาเกี่ยวกับการฉ้อโกงในการทำธุรกรรมทางอินเทอร์เน็ตพบว่าความเสียหายทางเศรษฐกิจรวมจากกิจกรรมดังกล่าวมีมูลค่าประมาณ 214,488.2 ล้านบาท หรือเทียบเท่ากับประมาณ 7.15 พันล้านดอลลาร์สหรัฐ (Kraiwanit & Srijaem, 2021) ตัวเลขนี้ชี้ให้เห็นถึงภาระทางเศรษฐกิจที่อาชญากรรมไซเบอร์ก่อให้เกิดขึ้นในเศรษฐกิจไทย โดยส่งผลกระทบต่อทั้งธุรกิจและบุคคล (Kraiwanit & Srijaem, 2021)

อาชญากรรมไซเบอร์ไม่เพียงแต่ทำให้เกิดความสูญเสียทางการเงินโดยตรงเท่านั้น แต่ยังส่งผลกระทบต่อสภาพแวดล้อมทางธุรกิจในประเทศไทยในวงกว้างอีกด้วย การออกกฎระเบียบด้านความมั่นคงทางไซเบอร์ เช่น พระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ สะท้อนให้เห็นถึงการยอมรับของรัฐบาลถึงภัยคุกคามที่เกิดจากอาชญากรรมไซเบอร์ อย่างไรก็ตาม แม้กฎระเบียบเหล่านี้มีเป้าหมายเพื่อบรรเทาภัยคุกคามไซเบอร์ แต่ ก็ยังเพิ่มภาระให้กับธุรกิจ อาจทำให้การลงทุนจากต่างประเทศลดลงและส่งผลกระทบต่อข้อตกลงการค้าของประเทศไทย (Emerald Expert Briefings, 2018) ผลกระทบทางเศรษฐกิจจากกฎระเบียบเหล่านี้มีความซับซ้อน เนื่องจากต้องสร้างสมดุลระหว่างความปลอดภัยและการเติบโตทางเศรษฐกิจ (Emerald Expert Briefings, 2018)

ประสบการณ์ของประเทศไทยเป็นส่วนหนึ่งของแนวโน้มระดับโลก ซึ่งอาชญากรรมไซเบอร์ได้กลายเป็นภัยคุกคามทางเศรษฐกิจที่สำคัญ โดยเฉพาะอย่างยิ่งในประเทศกำลังพัฒนา Kshetri (2013) ระบุว่าประเทศในกลุ่ม Global South ซึ่งรวมถึงประเทศไทยมีอัตราการเติบโตของอาชญากรรมไซเบอร์สูงที่สุดในช่วงระหว่างปี 2005 ถึง 2009 ซึ่งมีการโจมตีไซเบอร์เพิ่มขึ้นถึงร้อยละ 570 การเติบโตอย่างรวดเร็วของกิจกรรมอาชญากรรมไซเบอร์นี้ยิ่งทำให้ความสูญเสียทางเศรษฐกิจเพิ่มขึ้น เนื่องจากธุรกิจและบุคคลพยายามปกป้องตนเองจากภัยคุกคามไซเบอร์ที่ซับซ้อนขึ้นเรื่อย ๆ (Kshetri, 2013)

แม้ว่าประเทศไทยจะได้ดำเนินมาตรการต่าง ๆ เพื่อจัดการกับอาชญากรรมไซเบอร์ แต่ความท้าทายยังคงมีอยู่เนื่องจากลักษณะที่ซับซ้อนและเปลี่ยนแปลงตลอดเวลาของภัยคุกคามไซเบอร์ อย่างไรก็ตาม การดำเนินการเชิงรุกของประเทศไทยผ่านการปฏิรูปกฎหมาย การบูรณาการเทคโนโลยี และการประสานงานระหว่างหน่วยงานต่าง ๆ ถือเป็นแนวทางสำคัญที่จะช่วยเสริมสร้างความปลอดภัยทางไซเบอร์ในอนาคต ดังนั้น บทความนี้จึงมีความมุ่งหมายในการนำเสนอสถานะองค์ความรู้และการวิจัยในอนาคตเพื่อเป็นแนวทางในการศึกษาวิจัยเพื่อนำมาใช้แก้ปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ โดยเฉพาะอย่างยิ่งการมุ่งเน้นที่แนวคิดทางด้านเศรษฐศาสตร์

ความหมายและทฤษฎีเกี่ยวกับอาชญากรรมไซเบอร์

การก่ออาชญากรรมไซเบอร์กลายเป็นปัญหาที่เร่งด่วนมากขึ้นสำหรับทั้งนักวิจัยและผู้กำหนดนโยบาย การทำความเข้าใจแรงจูงใจและพฤติกรรมของอาชญากรไซเบอร์เป็นสิ่งสำคัญสำหรับการพัฒนากลยุทธ์ในการป้องกันอย่างมีประสิทธิภาพ ทฤษฎีทางอาชญาวิทยา จิตวิทยา และเศรษฐศาสตร์ได้ถูกนำมาใช้เพื่ออธิบายปัจจัยเบื้องหลังที่ทำให้บุคคลกระทำอาชญากรรมไซเบอร์ โดยผู้เขียนจะได้นำเสนอถึงความหมายของอาชญากรรม ไซเบอร์และทฤษฎีต่างๆ ที่เกี่ยวข้องดังนี้

ความหมายของอาชญากรรมไซเบอร์

อาชญากรรมทางไซเบอร์เป็นคำที่มีคำจำกัดความแตกต่างกันไปตามบริบท แต่โดยทั่วไปหมายถึงกิจกรรมที่ผิดกฎหมายที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และเครือข่าย Gordon & Ford (2006) ได้กำหนดให้อาชญากรรมทางไซเบอร์แบ่งออกเป็น 2 ประเภท ได้แก่ ประเภทที่ 1 ซึ่งส่วนใหญ่ใช้เทคโนโลยีเป็นพื้นฐาน และประเภทที่ 2 ซึ่งเน้นที่มนุษย์เป็นหลัก นอกจากนี้ Thangamuthu et al. (2020) กล่าวว่าอาชญากรรมทางไซเบอร์หมายถึงการกระทำที่ละเมิดกฎหมายซึ่งก่อให้เกิดอันตรายต่อบุคคลหรือกลุ่มบุคคลผ่านการใช้เทคโนโลยีสารสนเทศ เช่น การโจรกรรมข้อมูลและการกลั่นแกล้งทางไซเบอร์ ในขณะเดียวกัน Gupta และ Mata-Toledo (2016) โต้แย้งว่าอาชญากรรมทางไซเบอร์อาจส่งผลกระทบต่อสภาพจิตใจของผู้เสียหายในระยะยาวทั้งในแง่ของสุขภาพจิตและสถานะทางเศรษฐกิจ เช่น ในกรณีที่ข้อมูลส่วนบุคคลถูกขโมยและมีการฉ้อโกงทางอินเทอร์เน็ต สรุปได้ว่า อาชญากรรมทางไซเบอร์ หมายถึง การกระทำที่ผิดกฎหมายโดยใช้คอมพิวเตอร์และเครือข่ายเป็นเครื่องมือในการกระทำความผิด ซึ่งสามารถแบ่งออกได้เป็นสองประเภทคือ การกระทำที่ใช้เทคโนโลยีเป็นหลัก และการกระทำที่มีมนุษย์เป็นองค์ประกอบหลัก การกระทำเหล่านี้อาจส่งผลกระทบทั้งในด้านร่างกาย จิตใจ และการเงินของผู้เสียหาย เช่น การโจรกรรมข้อมูลส่วนบุคคล การกลั่นแกล้งทางไซเบอร์ หรือการฉ้อโกงทางอินเทอร์เน็ต ซึ่งอาจทำให้เกิดผลกระทบระยะยาวต่อสุขภาพจิตและเศรษฐกิจของผู้เสียหาย

ทฤษฎีเกี่ยวกับอาชญากรรมไซเบอร์

ทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory: SLT) เป็นหนึ่งในกรอบการทำงานที่มีอิทธิพลมากที่สุดในการทำความเข้าใจอาชญากรรมไซเบอร์ ตามทฤษฎีนี้ บุคคลมักจะกระทำพฤติกรรมทางอาญาโดยการเรียนรู้พฤติกรรม ค่านิยม และทัศนคติจากกลุ่มเพื่อน ทฤษฎีนี้มีความเกี่ยวข้องอย่างมากในการอธิบายว่าชุมชนออนไลน์ โดยเฉพาะชุมชนที่สนับสนุนการแฮ็กและอาชญากรรมไซเบอร์อื่นๆ สามารถมีอิทธิพลต่อบุคคลในการกระทำพฤติกรรมเบี่ยงเบนได้อย่างไร การวิจัยได้แสดงให้เห็นว่าการเชื่อมโยงกับกลุ่มเพื่อนที่มีพฤติกรรมเบี่ยงเบนจะเพิ่มโอกาสในการกระทำอาชญากรรมไซเบอร์โดยเฉพาะเมื่อรวมกับการขาดการควบคุมตนเอง (Stalans & Donner, 2018).

ทฤษฎีกิจกรรมประจำวัน (Routine Activity Theory: RAT) เป็นอีกหนึ่งทฤษฎีที่สำคัญในการทำความเข้าใจอาชญากรรมไซเบอร์ **ทฤษฎีกิจกรรมประจำวัน**กล่าวว่าอาชญากรรมมักเกิดขึ้นเมื่อผู้กระทำผิดที่มีแรงจูงใจพบกับเป้าหมายที่เหมาะสมในขณะที่ไม่มีผู้คุ้มกันที่สามารถป้องกันได้ ในบริบทของอาชญากรรมไซเบอร์ ทฤษฎีนี้ช่วยอธิบายถึงช่องโหว่ที่เกิดจากกิจกรรมออนไลน์ประจำวัน เช่น การใช้เครือข่ายที่ไม่ปลอดภัยหรือการแชร์ข้อมูลส่วนบุคคลบนโซเชียลมีเดีย ทฤษฎีนี้ชี้ให้เห็นว่าความสามารถในการมองเห็นและการเข้าถึงของเป้าหมายในโลกออนไลน์สามารถเพิ่มความเสี่ยงต่อการตกเป็นผู้เสียหายและส่งเสริมพฤติกรรมอาชญากรรม (Leukfeldt & Yar, 2016).

ทฤษฎีภาวะไร้ระเบียบของสถาบัน (Institutional Anomie Theory: IAT) ทฤษฎีนี้ได้ขยายทฤษฎี**ภาวะไร้ระเบียบ**ดั้งเดิมโดยเน้นถึงบทบาทของแรงกดดันทางสังคมโดยเฉพาะในสังคมทุนนิยม ทฤษฎีภาวะไร้ระเบียบของสถาบันแสดงให้เห็นว่าการมุ่งมั่นต่อความสำเร็จและผลประโยชน์ที่เป็นตัวเงินร่วมกับสถาบันทางสังคมที่อ่อนแอลง อาจทำให้บุคคลต่างๆ มีส่วนร่วมในอาชญากรรมทางไซเบอร์เพื่อบรรลุเป้าหมายของตน การศึกษาเชิงประจักษ์พบว่าภาวะไร้ระเบียบแบบแผนของสถาบันในระดับสูงมีความสัมพันธ์กับโอกาสที่เพิ่มขึ้นในกิจกรรมทางอาชญากรรมทางไซเบอร์ โดยเฉพาะในบริบทที่ให้ความสำคัญกับความสำเร็จทางเศรษฐกิจ (Dearden, Parti, & Hawdon, 2021).

ทฤษฎีการเลี่ยงความรู้สึกผิดชอบชั่วดี (Moral Disengagement Theory) ทฤษฎีนี้ได้อธิบายกลไกทางจิตวิทยาที่ทำให้บุคคลสามารถกระทำพฤติกรรมที่ผิดศีลธรรมโดยไม่รู้สึกผิดหรือเสียใจ ในบริบทของอาชญากรรมไซเบอร์ ทฤษฎีนี้อธิบายว่าผู้กระทำความผิดมักจะแก้ตัวการกระทำของตนโดยการลดทอนความเป็นมนุษย์ของผู้เสียหายหรือการลดทอนผลกระทบของการกระทำของตนให้เบาลง การเลี่ยงความรู้สึกผิดชอบชั่วดีนี้มักจะได้รับการสนับสนุนโดยความไม่เปิดเผยตัวตนที่โลกออนไลน์มอบให้ซึ่งสามารถลดความรู้สึกถึงความเสียหายของการกระทำทางอาชญากรรมไซเบอร์ (Rogers, 2011).

ทฤษฎีวัฒนธรรมย่อย (Subcultural Theories) ทฤษฎีนี้ได้นำเสนอการสำรวจบทบาทของบรรทัดฐานทางวัฒนธรรมและสังคมเฉพาะกลุ่มออนไลน์ที่สนับสนุนพฤติกรรมเบี่ยงเบน ทฤษฎีเหล่านี้ชี้ให้เห็นว่าชุมชนออนไลน์บางแห่ง เช่น ชุมชนแฮกเกอร์ สร้างบรรทัดฐานและค่านิยมที่สนับสนุนและเฉลิมฉลองการกระทำที่ผิดกฎหมาย สภาพแวดล้อมเช่นนี้ไม่เพียงแต่ให้ความรู้ทางเทคนิคและเครื่องมือ แต่ยังมีการสนับสนุนทางสังคมที่กระตุ้นให้สมาชิกดำเนินการอาชญากรรมไซเบอร์ (Stalans & Donner, 2018).

ทฤษฎีเศรษฐศาสตร์อาชญากรรมไซเบอร์ (Theory of Cybercrime Economics) การวิเคราะห์อาชญากรรมเชิงเศรษฐศาสตร์ได้ริเริ่มโดย Becker (1968) เป็นกรอบแนวคิดที่มีประโยชน์สำหรับการทำความเข้าใจอาชญากรรมไซเบอร์ **ทฤษฎีการวิเคราะห์ต้นทุนและผลประโยชน์ (Cost-Benefit Analysis)** ได้แสดงให้เห็นว่าผู้กระทำความผิดในอาชญากรรมไซเบอร์มักจะตัดสินใจเข้าร่วมกิจกรรมที่ผิดกฎหมายหลังจากประเมินผลตอบแทนที่อาจได้รับเทียบกับความเสี่ยงที่จะถูกจับและถูกลงโทษ ทฤษฎีนี้เป็นประโยชน์ในการทำความเข้าใจว่าผู้กระทำความผิดในอาชญากรรมไซเบอร์ตัดสินใจอย่างไร โดยเฉพาะอย่างยิ่งในแง่ของทรัพยากรที่จัดสรรเพื่อหลีกเลี่ยงการตรวจจับและเพิ่มผลกำไรสูงสุด แบบจำลองทางเศรษฐศาสตร์ยังช่วยอธิบายระดับการลงทุนที่เหมาะสมในด้านความปลอดภัยทางไซเบอร์และผลกระทบของการคุกคามทางกฎหมายที่มีต่อพฤติกรรมของผู้กระทำความผิดในอาชญากรรมไซเบอร์ (Kshetri, 2006).

การศึกษาพฤติกรรมของอาชญากรไซเบอร์นั้นได้รับประโยชน์จากมุมมองทฤษฎีที่หลากหลาย โดยแต่ละทฤษฎีล้วนให้ความเข้าใจเกี่ยวกับแรงจูงใจและกลไกที่อยู่เบื้องหลังอาชญากรรมไซเบอร์และสร้างความเข้าใจในปัจจัยที่ผลักดันให้บุคคลกระทำอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งในมุมมองทางเศรษฐศาสตร์ที่มีต่อการก่ออาชกรรมไซเบอร์

องค์ความรู้ของการวิจัยทางเศรษฐศาสตร์อาชญากรรมไซเบอร์

การสำรวจปัจจัยที่มีผลต่อกิจกรรมของอาชญากรทางไซเบอร์ในประเทศไทยจากมุมมองทางเศรษฐกิจ ได้ให้ข้อมูลเชิงลึกเกี่ยวกับปัจจัยทางเศรษฐกิจและสังคม เทคโนโลยี และกฎหมายที่มีส่วนทำให้เกิดอาชญากรรมทางไซเบอร์ในประเทศไทย การสำรวจผลการวิจัยจะช่วยให้ผู้กำหนดนโยบายธุรกิจ และนักวิจัยเข้าใจสาเหตุและพัฒนากลยุทธ์ในการต่อต้านอาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ ผู้เขียนได้นำเสนอข้อเสนอแนะเชิงนโยบายจากงานวิจัยต่างๆ ในการจัดการกับปัญหาอาชญากรรมไซเบอร์โดยผ่านทางปัจจัยต่างๆ ที่มีต่ออาชญากรทางไซเบอร์

ปัจจัยทางเศรษฐกิจและสังคม

ปัจจัยทางเศรษฐกิจและสังคมมีบทบาทสำคัญในการมีอิทธิพลต่อกิจกรรมอาชญากรทางไซเบอร์ในประเทศไทย การศึกษาต่างๆ ได้เน้นย้ำถึงผลกระทบของความไม่เท่าเทียมกันของรายได้ ระดับการศึกษา และความยากจนที่มีต่ออาชญากรรมทางไซเบอร์

1) ความไม่เท่าเทียมกันของรายได้และความยากจน

อาชญากรรมทางไซเบอร์ในประเทศไทยมักขับเคลื่อนด้วยความเหลื่อมล้ำทางเศรษฐกิจ บุคคลจากภูมิหลังทางเศรษฐกิจและสังคมที่ต่ำกว่าอาจหันไปหาอาชญากรรมทางไซเบอร์เพื่อเป็นหนทางในการเอาชีวิตรอดหรือหากำไรทางการเงินอย่างรวดเร็ว การศึกษาโดย Park et al. (2019) ระบุว่าความไม่เท่าเทียมกันของรายได้ที่สูงขึ้นมีความสัมพันธ์กับกิจกรรมอาชญากรรมทางไซเบอร์ที่เพิ่มขึ้น เนื่องจากบุคคลในกลุ่มรายได้ต่ำอาจมองว่าอาชญากรรมทางไซเบอร์เป็นทางเลือกที่เหมาะสมในการทำให้สถานะทางการเงินดีขึ้น (Park et al., 2019). และกรณีการศึกษาในประเทศไทย พบว่าความไม่เท่าเทียมกันทางเศรษฐกิจเป็นปัจจัยที่สำคัญที่นำไปสู่การเพิ่มขึ้นของอาชญากรรมทางไซเบอร์ โดยเฉพาะอย่างยิ่งในภูมิภาคที่มีความยากจนและโอกาสทางเศรษฐกิจน้อยลง ความไม่เท่าเทียมกันในรายได้ยังส่งผลให้คนส่วนหนึ่งมีแรงจูงใจในการเข้าร่วมกิจกรรมอาชญากรรมทางไซเบอร์ (Kraiwanit & Srijaem, 2021). การศึกษาของ Apichaimongkol & Phakdee (2024) ชี้ให้เห็นว่าเมื่อประชาชนขาดโอกาสทางเศรษฐกิจ ทำให้มีความเสี่ยงต่อการเข้าร่วมกิจกรรมทางอาชญากรรมทางไซเบอร์ได้ง่ายขึ้น

2) ระดับการศึกษา

ระดับการศึกษามีอิทธิพลต่อความน่าจะเป็นในการมีส่วนร่วมในอาชญากรรมทางไซเบอร์ เนื่องจากระดับการศึกษาที่สูงขึ้นมักเกี่ยวข้องกับโอกาสในการทำงานที่ดีขึ้นและความโน้มเอียงในการก่ออาชญากรรมที่ต่ำกว่า อย่างไรก็ตาม ความสัมพันธ์ระหว่างการศึกษาและอาชญากรรมทางไซเบอร์มีความซับซ้อน เนื่องจากบุคคลที่มีการศึกษาพร้อมทักษะทางเทคนิคอาจใช้ความรู้ของตนในทางที่ผิดเพื่อดำเนินกิจกรรมที่เป็นอันตรายเช่นกัน ผลการวิจัยของ Ramadani (2018) ชี้ให้เห็นว่าในขณะที่การศึกษาสามารถลดการเกิดอาชญากรรมทางไซเบอร์ได้ แต่ก็สามารถช่วยให้บุคคลเข้าร่วมการโจมตีทางไซเบอร์ในรูปแบบที่ซับซ้อนมากขึ้น นอกจากนั้น การศึกษาของ Ungkap & Daengsi (2022) พบว่าระดับการศึกษามีบทบาทสำคัญในการกำหนดพฤติกรรมของบุคคลเกี่ยวกับการใช้งานอินเทอร์เน็ตและการป้องกันภัยคุกคามทางไซเบอร์ การศึกษาที่ต่ำมักจะนำไปสู่ความเสี่ยงสูงต่อการตกเป็นเหยื่อหรือเข้าร่วมในกิจกรรมอาชญากรรมทางไซเบอร์ การเสริมสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์สามารถช่วยลดความเสี่ยงได้

3) การว่างงาน

อัตราการว่างงานเป็นอีกหนึ่งปัจจัยทางเศรษฐกิจและสังคมที่สำคัญซึ่งมีอิทธิพลต่ออาชญากรรมทางไซเบอร์ การว่างงานสูงสามารถนำไปสู่กิจกรรมอาชญากรรมทางไซเบอร์ที่เพิ่มขึ้นเมื่อบุคคลต่าง ๆ แสวงหาวิธีการทางเลือกในการหารายได้ ความเครียดทางเศรษฐกิจที่เกิดจากการว่างงานอาจผลักดันให้บุคคลไปสู่กิจกรรมที่ผิดกฎหมาย เช่น การแฮ็ก การฟิชชิง และการฉ้อโกงทางออนไลน์ (Rungsrisawat et al., 2019; Techatassanasoontorn et al., 2011) และการศึกษาของ Nachaisin (2019) พบว่าการว่างงานและการศึกษาต่ำก็มีส่วนทำให้ผู้คนหันมาใช้อาชญากรรมไซเบอร์เป็นวิธีในการหาเลี้ยงชีพเช่นเดียวกัน

ปัจจัยทางเทคโนโลยี

ความก้าวหน้าทางเทคโนโลยีที่รวดเร็วในประเทศไทยมีทั้งผลดีและผลเสียต่ออาชญากรรมทางไซเบอร์ ในขณะที่เทคโนโลยีช่วยให้เศรษฐกิจเติบโตและพัฒนา แต่ก็สร้างโอกาสให้อาชญากรทางไซเบอร์ใช้ประโยชน์จากช่องโหว่ต่าง ๆ

1) การเข้าถึงอินเทอร์เน็ต

การใช้ประโยชน์จากอินเทอร์เน็ตอย่างแพร่หลายในประเทศไทยได้ทำให้มีการเติบโตของอาชญากรรมทางไซเบอร์มากขึ้น โดยอัตราการเข้าถึงอินเทอร์เน็ตที่สูงจะเพิ่มจำนวนเป้าหมายที่อาจเกิดขึ้นสำหรับอาชญากรทางไซเบอร์ ตามที่ Calderwood และ Popova (2018) ได้กล่าวไว้ ประเทศไทยเป็นหนึ่งในประเทศที่เสี่ยงที่สุดในแง่ของอาชญากรรมทางไซเบอร์ เนื่องจากมีผู้ใช้อินเทอร์เน็ตจำนวนมากและมีการรับรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ค่อนข้างต่ำ (Calderwood & Popova, 2018)

2) การเชื่อมต่อบรอดแบนด์

คุณภาพของการเชื่อมต่ออินเทอร์เน็ตยังส่งผลต่อการแพร่หลายของอาชญากรรมทางไซเบอร์อีกด้วย Park et al. (2019) พบว่าการเชื่อมต่อบรอดแบนด์มีความสัมพันธ์อย่างมีนัยสำคัญกับอัตราการเกิดอาชญากรรมทางไซเบอร์ที่สูงขึ้น การเชื่อมต่ออินเทอร์เน็ตที่รวดเร็วและเชื่อถือได้มากขึ้นทำให้อาชญากรทางไซเบอร์มีเครื่องมือที่จำเป็นในการดำเนินการโจมตีอย่างมีประสิทธิภาพมากขึ้น (Park et al., 2019).

3) ความรู้ความสามารถทางเทคโนโลยี

ระดับความรู้ทางเทคโนโลยีในหมู่ประชากรเป็นอีกหนึ่งปัจจัยสำคัญ ในขณะที่ความรู้ความสามารถทางเทคโนโลยีสามารถเพิ่มศักยภาพให้บุคคลและธุรกิจในการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ แต่ก็สามารถช่วยให้อาชญากรทางไซเบอร์ดำเนินการโจมตีที่ซับซ้อนมากขึ้นได้เช่นกัน การศึกษาของ Machim et al. (2020) ได้เน้นย้ำถึงความสำคัญของความรู้ความสามารถทางเทคโนโลยีในการลดอาชญากรรมทางไซเบอร์ในประเทศไทย โดยเฉพาะอย่างยิ่งในภาคอุตสาหกรรม (Machim et al., 2020).

4) ปัญญาประดิษฐ์

ปัญญาประดิษฐ์ (AI) มีบทบาทสำคัญทั้งในการป้องกันและสนับสนุนอาชญากรรมไซเบอร์ ซึ่งมีผลกระทบทางเศรษฐกิจอย่างมีนัยสำคัญ ปัญญาประดิษฐ์ถูกนำมาใช้ในการเพิ่มประสิทธิภาพด้านความปลอดภัยทางไซเบอร์ โดยการตรวจจับและลดภัยคุกคามได้อย่างรวดเร็วและแม่นยำกว่าวิธีการแบบดั้งเดิม เช่น การใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) สำหรับการตรวจจับการฉ้อโกงและป้องกันการโจมตี (Verma & Gupta, 2020) อย่างไรก็ตาม อาชญากรไซเบอร์สามารถใช้ปัญญาประดิษฐ์ในการขยายขนาดการโจมตีทาง ไซเบอร์ ทำให้เกิดช่องทางใหม่สำหรับการก่ออาชญากรรมไซเบอร์ (Hoanca & Mock, 2020) การวิจัยด้านเศรษฐศาสตร์เกี่ยวกับ AI ในความปลอดภัยทางไซเบอร์ระบุว่าตลาดสำหรับโซลูชันที่ขับเคลื่อนด้วย AI กำลังเติบโตอย่างรวดเร็ว ซึ่งเน้นย้ำถึงความสำคัญในการลดความสูญเสียทางการเงินจากการโจมตีทางไซเบอร์ (Kshetri, 2021)

ปัจจัยด้านกฎหมายและกฎระเบียบ

กรอบกฎหมายและกฎระเบียบในประเทศไทยมีบทบาทสำคัญในการกำหนดแนวทางในการต่อสู้กับอาชญากรรมทางไซเบอร์ ประสิทธิผลของกฎหมายและระเบียบข้อบังคับ รวมถึงความสามารถของหน่วยงานบังคับใช้กฎหมาย มีผลกระทบอย่างมีนัยสำคัญต่อความสามารถในการต่อสู้กับอาชญากรรมทางไซเบอร์

1) กฎหมายความปลอดภัยทางไซเบอร์

ประเทศไทยได้ออกกฎหมายหลายฉบับเพื่อเสริมสร้างการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) เป็นหนึ่งในกฎหมายที่ออกแบบมาเพื่อปกป้องประเทศจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น โดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับสกุลเงินดิจิทัลและธุรกรรมทางการเงินออนไลน์ อย่างไรก็ตาม ประสิทธิผลของกฎหมายดังกล่าวขึ้นอยู่กับการบังคับใช้และการปฏิบัติตามกฎหมาย และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์อาจถูกนำมาใช้เพื่อจำกัดเสรีภาพทางการเมืองแทนที่จะมุ่งเน้นไปที่ความปลอดภัยทางไซเบอร์เพียงอย่างเดียว (Emerald Expert Briefings, 2018) นอกจากนั้นพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSA) ของประเทศไทยมีผลกระทบอย่างมีนัยสำคัญต่ออาชญากรรมไซเบอร์ในเชิงเศรษฐกิจ เนื่องจากกฎหมายเหล่านี้กำหนดให้ธุรกิจต้องมีค่าใช้จ่ายในการปฏิบัติตามกฎระเบียบ โดยการเพิ่มมาตรการปกป้องข้อมูลและโครงสร้างพื้นฐานความปลอดภัยไซเบอร์ ส่งผลโดยตรงต่อค่าใช้จ่ายในการดำเนินธุรกิจและอาจช่วยยับยั้งอาชญากรรมไซเบอร์ได้ โดยทำให้การก่ออาชญากรรมมีความซับซ้อนและมีความเสี่ยงมากขึ้น งานวิจัยชี้ให้เห็นว่ากฎหมายความมั่นคงไซเบอร์อย่างมีบทบาทสำคัญในการลดความเสียหายทางการเงินที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งผ่านการปกป้องจากโครงสร้างพื้นฐานที่สำคัญและข้อมูลส่วนบุคคล (Yamcharoen et al., 2022)

2) ความสามารถของการบังคับใช้กฎหมาย

ความสามารถของหน่วยงานบังคับใช้กฎหมายในการจัดการกับอาชญากรรมทางไซเบอร์เป็นอีกปัจจัยสำคัญ ในหลายกรณีอาชญากรทางไซเบอร์ดำเนินการข้ามชาติ ทำให้ยากต่อการจับกุมและดำเนินคดีของหน่วยงานระดับชาติ หน่วยงานบังคับใช้กฎหมายของประเทศไทยต้องเผชิญกับความท้าทายอย่างมากในการรู้เท่าทันต่อการเปลี่ยนแปลงตลอดเวลาของอาชญากรรมทางไซเบอร์ การศึกษาของ Ter (2017) เกี่ยวกับแนวทางของประเทศสิงคโปร์ในการต่อสู้กับอาชญากรรมทางไซเบอร์ให้ข้อมูลเชิงลึกต่อความสามารถในการบังคับใช้กฎหมายในการจัดการกับภัยคุกคามทางไซเบอร์ (Ter, 2017) กรณีของประเทศไทย แม้ว่าประเทศไทยจะมีกฎหมายด้านความปลอดภัยทางไซเบอร์ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 แต่ยังคงมีช่องว่างในการบังคับใช้กฎหมาย รวมถึงการพัฒนาและปรับปรุงกฎหมายให้ทันสมัยตามการเปลี่ยนแปลงของเทคโนโลยี (Gorian, 2021) อย่างไรก็ดีกฎหมายและกฎระเบียบยังคงเป็นปัจจัยที่สำคัญในการควบคุมและป้องกันอาชญากรรมทางไซเบอร์ (Nachaisin, 2021) การบังคับใช้กฎหมายที่เข้มงวดและเทคโนโลยีตรวจสอบที่มีประสิทธิภาพสามารถลดการเกิดอาชญากรรมไซเบอร์ได้ (Khurunun & Saengthongdee, 2023)

3) ความร่วมมือระหว่างประเทศ

เนื่องจากลักษณะอาชญากรรมทางไซเบอร์ข้ามชาติ ความร่วมมือระหว่างประเทศจึงเป็นสิ่งจำเป็นสำหรับการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ การเข้าร่วมข้อตกลงระหว่างประเทศและการทำงานร่วมกับประเทศต่างๆ สามารถเพิ่มความสามารถในการต่อสู้กับอาชญากรรมทางไซเบอร์ได้ การศึกษาโดย Bukrapue (2015) เกี่ยวกับกิจกรรมฉ้อโกงต่อชาวต่างชาติในประเทศไทยได้ชี้ให้เห็นถึงความจำเป็นของความร่วมมือระหว่างประเทศในการจัดการกับอาชญากรรมทางไซเบอร์ (Bukrapue, 2015) และจากผลการศึกษาของ Kraiwanit & Srijaem (2021) พบว่า ผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์นั้นครอบคลุมถึงการสูญเสียทางการเงินทั้งของผู้ใช้และภาคธุรกิจในประเทศไทย การฉ้อโกงทางอินเทอร์เน็ตและการโจรกรรมข้อมูลสามารถทำให้เกิดความเสียหายหลายล้านบาทต่อปี โดยรายงานล่าสุดระบุว่าความเสียหายทางเศรษฐกิจจากอาชญากรรมทางไซเบอร์มีมูลค่าสูงถึง 214,488.2 ล้านบาท

ผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์

อาชญากรรมทางไซเบอร์มีผลกระทบทางเศรษฐกิจอย่างมีนัยสำคัญต่อประเทศไทย ความสูญเสียทางการเงินที่เกิดขึ้นกับบุคคล ธุรกิจ และรัฐบาลเนื่องจากอาชญากรรมทางไซเบอร์มียังคงมีมากและสูงขึ้นตลอดเวลา

1) ความสูญเสียทางการเงิน

ความเสียหายทางเศรษฐกิจที่เกิดจากอาชญากรรมทางไซเบอร์ในประเทศไทยมีมากมาย Kraiwanit และ Srijaem (2021) ได้ประเมินว่าการฉ้อโกงธุรกรรมทางอินเทอร์เน็ตเพียงอย่างเดียวส่งผลให้เกิดความสูญเสียรวมมูลค่า 214,488.2 ล้านบาท (ประมาณ 7.15 พันล้านเหรียญสหรัฐ) ความสูญเสียเหล่านี้ชี้ให้เห็นถึงความจำเป็นในการดำเนินมาตรการที่มีประสิทธิภาพเพื่อป้องกันและลดอาชญากรรมทางไซเบอร์ (Kraiwanit & Srijaem, 2021) โดยเฉพาะการโจรกรรมทางการเงินและการปลอมแปลงข้อมูล ซึ่งสร้างความเสียหายทั้งต่อธุรกิจและประชาชนทั่วไป (Apichaimongkol & Phakdee, 2024)

2) ผลกระทบต่อการลงทุนจากต่างประเทศ

อาชญากรรมทางไซเบอร์ยังสามารถขัดขวางการลงทุนจากต่างประเทศในประเทศไทย การรับรู้ถึงความเสี่ยงของอาชญากรรมทางไซเบอร์ที่สูงอาจทำให้ประเทศไทยดึงดูดนักลงทุนต่างชาติได้น้อยลง ด้วยความกังวลว่าการลงทุนของตนเองอาจได้รับความเสียหาย การศึกษาโดย Chotewetsin (2023) ได้ชี้ถึงผลกระทบของความเสี่ยงทางการเมืองและไซเบอร์ต่อเศรษฐกิจของประเทศไทยและความสามารถในการดึงดูดนักลงทุนต่างชาติ

3) ต้นทุนค่าเสียโอกาส

นอกเหนือจากการสูญเสียทางการเงินโดยตรงแล้ว อาชญากรรมทางไซเบอร์ยังทำให้เกิดต้นทุนค่าเสียโอกาสจำนวนมากอีกด้วย ความกลัวอาชญากรรมทางไซเบอร์สามารถนำไปสู่การที่บุคคลและธุรกิจหลีกเลี่ยงการใช้บริการออนไลน์ ซึ่งจะจำกัดศักยภาพในการเติบโตทางเศรษฐกิจ Riek et al. (2016) แสดงให้เห็นว่าการรับรู้ความเสี่ยงจากอาชญากรรมทางไซเบอร์มีผลกระทบในทางลบต่อการใช้บริการออนไลน์ เช่น ธนาคาร ช้อปปิ้ง และเครือข่ายสังคมออนไลน์ ซึ่งส่งผลกระทบต่อกิจกรรมทางเศรษฐกิจ (Riek et al., 2016).

ปัจจัยที่มีอิทธิพลต่ออาชญากรรมทางไซเบอร์ในประเทศไทยมีความหลากหลายและเชื่อมโยงกัน สภาพเศรษฐกิจและสังคม ความก้าวหน้าทางเทคโนโลยี และสภาพแวดล้อมทางกฎหมายและกฎระเบียบล้วนมีบทบาทสำคัญต่อการก่ออาชญากรรมทางไซเบอร์ นอกจากนั้นผลกระทบทางเศรษฐกิจของอาชญากรรมทาง ไซเบอร์ทำให้เกิดการสูญเสียทางการเงินจำนวนมากและต้นทุนค่าเสียโอกาส การจัดการอาชญากรรมทางไซเบอร์ให้มีประสิทธิภาพจำเป็นต้องจัดการกับปัจจัยเหล่านี้อย่างครอบคลุม ผ่านการผสมผสานของการแทรกแซงทางเศรษฐกิจและสังคม การปรับปรุงเทคโนโลยี และกรอบกฎหมายที่เข้มงวด ความร่วมมือระหว่างประเทศและความพยายามอย่างต่อเนื่องในการตระหนักรู้และการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ยังคงเป็นสิ่งสำคัญต่อความสำเร็จในการต่อต้านอาชญากรรมทางไซเบอร์

ข้อเสนอแนะเชิงนโยบายต่อปัจจัยที่ส่งผลต่ออาชญากรรมไซเบอร์

การจัดการกับอาชญากรรมทางไซเบอร์นั้นต้องพิจารณาปัจจัยทางสังคม เศรษฐกิจ และโครงสร้างต่างๆ เช่น ความไม่เท่าเทียมกันของรายได้ ความยากจน การศึกษา การว่างงาน ความก้าวหน้าทางเทคโนโลยี และกรอบกฎหมายและระเบียบข้อบังคับ นโยบายที่ครอบคลุมตามประเด็นเหล่านี้ช่วยส่งเสริมสภาพแวดล้อมดิจิทัลที่ปลอดภัยยิ่งขึ้น

ความไม่เท่าเทียมกันของรายได้และความยากจนมีความสัมพันธ์กับการเพิ่มขึ้นของอาชญากรรมทางไซเบอร์ เนื่องจากบุคคลที่ด้อยโอกาสอาจหันไปหาแหล่งรายได้ออนไลน์ที่ผิดกฎหมายเนื่องจากความต้องการทางการเงิน นโยบายที่มุ่งลดมาตรการความไม่เท่าเทียมกันของรายได้ เช่น ระบบภาษีแบบก้าวหน้าและการจัดตั้งโครงการสวัสดิการสังคม ถือเป็นสิ่งสำคัญในการบรรเทาความสิ้นหวังทางเศรษฐกิจที่ทำให้ผู้คนหันไปพึ่งพิงอาชญากรรมทางไซเบอร์ การวิจัยระบุว่าประเทศที่มีรายได้ไม่เท่าเทียมกันมักจะมีอัตราการก่ออาชญากรรมทางไซเบอร์ที่สูงกว่าเนื่องจากการย้ายถิ่นฐานทางสังคมที่จำกัดและมีงานที่เหมาะสมและมีรายได้ดี (Jones & Smith, 2020) (Williams et al., 2019) มาตรการเฉพาะเพื่อปรับปรุงการเข้าถึงการศึกษาและเทคโนโลยีในพื้นที่ที่มีรายได้น้อยสามารถป้องกันไม่ให้ผู้คนหันไปพึ่งอาชญากรรมทางไซเบอร์เพื่อหารายได้

การต่อสู้กับอาชญากรรมทางไซเบอร์ ด้วยนโยบายทางการศึกษาถือเป็นสิ่งสำคัญ เนื่องจากการนโยบายการศึกษาจะช่วยลดอาชญากรรมทางไซเบอร์ได้ นโยบายการศึกษาที่มุ่งการตระหนักรู้ด้านความปลอดภัยทาง ไซเบอร์หรือความรู้ด้านดิจิทัลจะนำไปสู่การก่ออาชญากรรมทางไซเบอร์น้อยลง เนื่องจากจะช่วยให้ได้รับความรู้ที่จำเป็นในการปกป้องตนเอง รวมถึงความเข้าใจผลทางกฎหมายที่เกิดจากการกระทำความผิดทางไซเบอร์ (Parker et al., 2021) รัฐบาล มีภาระผูกพันที่จะนำความปลอดภัยทางไซเบอร์เป็นวิชาหนึ่งในโปรแกรมของสถาบันการศึกษาในระดับต่างๆ เพื่อให้ประชาชนมีความรู้ความเข้าใจเกี่ยวกับปัญหาที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ และในขณะเดียวกันก็เป็นการเสริมสร้างกำลังแรงงานด้านไซเบอร์ (Brown et al., 2021)

อัตราการว่างงานสูงมีความเกี่ยวข้องกับอัตราการก่ออาชญากรรมที่สูงขึ้น รวมถึงอาชญากรรมไซเบอร์ด้วย นโยบายที่มุ่งเน้นการสร้างงานโดยเฉพาะในภาคเทคโนโลยีสามารถช่วยลดปัจจัยที่นำไปสู่การมีส่วนร่วมในการก่ออาชญากรรมไซเบอร์ได้ การส่งเสริมให้บริษัทเอกชนลงทุนในการสร้างงานที่ขับเคลื่อนด้วยเทคโนโลยี และการฝึกอบรมทักษะด้านดิจิทัลจะช่วยลดความดึงดูดใจของอาชญากรรมไซเบอร์ในฐานะช่องทางการทำมาหากิน (Greenfield et al., 2022). นอกจากนี้ การจัดให้มีโอกาสสำหรับผู้ว่างงานในการเรียนรู้ทักษะใหม่ ๆ ในภาคส่วนที่กำลังเติบโตอย่างความปลอดภัยทางไซเบอร์จะไม่เพียงแต่ลดอาชญากรรมเท่านั้น แต่ยังช่วยเติมเต็มช่องว่างทักษะที่มีอยู่ในแรงงานด้านความปลอดภัยไซเบอร์อีกด้วย (Mason et al., 2021)

ปัจจัยทางเทคโนโลยี เช่น ความก้าวหน้าอย่างรวดเร็วของแพลตฟอร์มและเครื่องมือดิจิทัลมีบทบาทสำคัญทั้งในด้านการแพร่กระจายและการป้องกันอาชญากรรมไซเบอร์ นโยบายที่สนับสนุนการพัฒนาและการนำเทคโนโลยีด้านความปลอดภัยไซเบอร์ไปใช้ในวงกว้าง เช่น การเข้ารหัสข้อมูล การยืนยันตัวตนหลายปัจจัย และระบบตรวจจับภัยคุกคามที่ใช้ปัญญาประดิษฐ์ ถือเป็นสิ่งสำคัญ การทำงานร่วมกันระหว่างภาครัฐและภาคเอกชนเพื่อส่งเสริมโครงสร้างพื้นฐานทางเทคโนโลยีที่มีความปลอดภัยจำเป็นต้องมีเพื่อรับมือกับอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ การปรับปรุงข้อกำหนดและมาตรฐานด้านความปลอดภัยไซเบอร์อย่างต่อเนื่องก็มีความสำคัญเพื่อให้สอดคล้องกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว (Clark et al., 2020;Davis & Lee, 2019)

การมีกฎหมายและการบังคับใช้ที่มีประสิทธิภาพเป็นพื้นฐานในการจัดการกับอาชญากรรมไซเบอร์ รัฐบาลต้องมั่นใจว่ากฎหมายมีความทันสมัยเพียงพอที่จะสอดคล้องกับการพัฒนาอย่างรวดเร็วของเทคโนโลยีที่อาชญากรไซเบอร์นำไปใช้ รวมถึงการให้ความร่วมมือระหว่างประเทศในด้านกฎหมาย เนื่องจากอาชญากรรมไซเบอร์มักข้ามเขตแดน นอกจากนี้ การปรับปรุงกรอบกฎหมายที่มีอยู่ให้ครอบคลุมภัยคุกคามทางไซเบอร์ใหม่ ๆ เช่น แรนซัมแวร์ การขโมยสกุลเงินดิจิทัล และการละเมิดข้อมูลก็มีความจำเป็นเช่นกัน (Nelson & Wright, 2021). อีกทั้ง มาตรการด้านกฎระเบียบที่เข้มงวดควรถูกนำมาใช้เพื่อให้แน่ใจว่าองค์กรมีความรับผิดชอบในการรักษามาตรฐานความปลอดภัยไซเบอร์ที่เพียงพอ เพื่อให้พร้อมรับมือกับภัยคุกคามที่อาจเกิดขึ้น (Lewis & Kessler, 2020).

การแก้ไขปัญหาอาชญากรรมไซเบอร์จำเป็นต้องใช้วิธีการที่ครอบคลุมหลายด้าน โดยการมุ่งเน้นไปที่ปัจจัยทางเศรษฐกิจและสังคม เทคโนโลยี และกฎหมายที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรมไซเบอร์ นโยบายที่ลดความไม่เท่าเทียมกันของรายได้ ปรับปรุงการศึกษา และเสริมสร้างกรอบกฎหมายเป็นส่วนสำคัญในการลดอัตราการก่ออาชญากรรมไซเบอร์และสร้างสภาพแวดล้อมดิจิทัลที่ปลอดภัยมากขึ้น.

การวิจัยทางเศรษฐศาสตร์อาชญากรรมไซเบอร์ในอนาคต

ด้วยเหตุที่โลกเข้าสู่ยุคดิจิทัลมากขึ้น การคุกคามจากอาชญากรรมทางไซเบอร์จึงเพิ่มขึ้นอย่างมากซึ่งส่งผลกระทบต่อเศรษฐกิจทั่วโลก ประเทศไทยเช่นเดียวกับประเทศอื่น ๆ ต้องเผชิญกับความท้าทายสำคัญในการต่อสู้กับอาชญากรรมทางไซเบอร์ ซึ่งมีผลกระทบต่อเสถียรภาพทางเศรษฐกิจ ความมั่นคง และความเป็นอยู่ที่ดีของสังคม การทำความเข้าใจปัจจัยทางเศรษฐกิจที่มีผลต่อกิจกรรมอาชญากรรมทางไซเบอร์ในประเทศไทยเป็นสิ่งสำคัญในการพัฒนามาตรการรับมือที่มีประสิทธิภาพ ดังนั้น การให้แนวทางการวิจัยทางเศรษฐศาสตร์ในอนาคตเกี่ยวกับอาชญากรรมไซเบอร์สำหรับประเทศไทยจึงเป็นสิ่งสำคัญ โดยผู้เขียนได้นำเสนอประเด็นต่างๆ ดังนี้

ปัจจัยทางเศรษฐกิจ

สภาวะเศรษฐกิจมีบทบาทสำคัญต่อการเกิดอาชญากรรมทางไซเบอร์ในประเทศไทย เมื่อเศรษฐกิจเติบโตและกลายเป็นดิจิทัลมากขึ้น โอกาสสำหรับอาชญากรทางไซเบอร์ก็เพิ่มขึ้นตามไปด้วย การวิจัยในอนาคตควรมุ่งไปที่การตรวจสอบความสัมพันธ์ระหว่างความไม่เท่าเทียมทางเศรษฐกิจหรือความยากจนกับอัตราการเกิดอาชญากรรมทางไซเบอร์ในประเทศไทย โดยเฉพาะอย่างยิ่ง การทำความเข้าใจว่าความเหลื่อมล้ำทางเศรษฐกิจในระดับภาคส่งผลต่อบุคคลในการเข้าสู่การก่ออาชญากรรมทางไซเบอร์อย่างไร ซึ่งจะช่วยให้ได้ข้อมูลเชิงลึกเกี่ยวกับมาตรการป้องกันอีกด้วย การเป็นหนี้ครัวเรือนของไทย รวมถึงผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์ต่อธุรกิจและผู้บริโภคในประเทศไทยก็เป็นประเด็นที่น่าศึกษา การวิจัยที่มุ่งเน้นไปที่การหาปริมาณค่าใช้จ่ายด้านความปลอดภัย ความสูญเสียทางการเงินและการทำความเข้าใจในภาคส่วนต่าง ๆ ของเศรษฐกิจไทยที่ได้รับผลกระทบจากกิจกรรมอาชญากรรมทางไซเบอร์ ความเชื่อมั่นของผู้บริโภคที่ลดลงในแพลตฟอร์มดิจิทัลก็เป็นประเด็นที่ควรให้ความสนใจ

ความก้าวหน้าทางเทคโนโลยี

แม้ความก้าวหน้าทางเทคโนโลยีจะขับเคลื่อนการเติบโตทางเศรษฐกิจ แต่ก็สร้างช่องทางใหม่ๆ สำหรับอาชญากรทางไซเบอร์ในประเทศไทย การนำเทคโนโลยีดิจิทัลมาใช้อย่างรวดเร็ว รวมถึงอีคอมเมิร์ซ การธนาคารออนไลน์ และโซเชียลมีเดีย ทำให้ประเทศมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์เพิ่มขึ้น การวิจัยในอนาคตควรสำรวจว่าเทคโนโลยีแบบใดที่มีส่วนทำให้เกิดอาชญากรรมทางไซเบอร์เพิ่มขึ้น รวมถึงผลกระทบทางเศรษฐกิจจากอาชญากรรมเหล่านี้ ตัวอย่างเช่น บทบาทของแพลตฟอร์มโซเชียลมีเดียในการอำนวยความสะดวกในการฉ้อโกงทางอินเทอร์เน็ตในประเทศไทย อีกประเด็นที่สำคัญสำหรับการวิจัยในอนาคตคือประสิทธิภาพของเทคโนโลยีและนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ในการลดความสูญเสียทางเศรษฐกิจจากอาชญากรรมทางไซเบอร์ ขณะที่ประเทศไทยยังคงลงทุนในโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ การทำความเข้าใจการวิเคราะห์ต้นทุนและผลประโยชน์ของการลงทุนเหล่านี้จึงเป็นสิ่งสำคัญ การวิจัยควรตรวจสอบประสิทธิภาพทางเศรษฐกิจของมาตรการความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ และความสามารถของมาตรการเหล่านี้ในการป้องกันความสูญเสียทางการเงิน นอกจากนั้น การวิจัยควรมุ่งเน้นไปที่การพัฒนากลไกการป้องกันที่สามารถตอบสนองต่อการใช้ AI ในการก่ออาชญากรรมไซเบอร์และการวิเคราะห์ต้นทุนทางเศรษฐกิจของการใช้ AI ทั้งในด้านการป้องกันและการก่ออาชญากรรม

กรอบนโยบายและผลกระทบทางเศรษฐกิจ

กรอบทางนโยบายมีบทบาทสำคัญในการกำหนดผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์ การวิจัยในอนาคตควรมุ่งเน้นไปที่การประเมินประสิทธิภาพของกฎหมายอาชญากรรมทางไซเบอร์ที่มีอยู่และการบังคับใช้กฎหมายเหล่านั้น แม้ว่าจะมีกฎหมายอาชญากรรมทางไซเบอร์อยู่

แล้ว แต่จำนวนการเกิดอาชญากรรมทางไซเบอร์ยังคงเพิ่มขึ้น ซึ่งแสดงให้เห็นถึงช่องว่างที่อาจเกิดขึ้นในกรอบกฎหมายหรือการบังคับใช้กฎหมาย นอกจากนี้ การศึกษาเปรียบเทียบระหว่างประเทศไทยและประเทศอื่น ๆ ที่มีลักษณะทางเศรษฐกิจและเทคโนโลยีที่คล้ายคลึงกันอาจให้ข้อมูลเชิงลึกที่มีคุณค่าเกี่ยวกับแนวทางปฏิบัติที่ดีในการป้องกันอาชญากรรมทางไซเบอร์ การทำความเข้าใจว่าการบังคับใช้กฎระเบียบในสภาพแวดล้อมต่าง ๆ ส่งผลต่อพฤติกรรมอาชญากรทางไซเบอร์และผลลัพธ์ทางเศรษฐกิจอย่างไร สามารถนำไปสู่การพัฒนานโยบายที่มีประสิทธิภาพมากขึ้น บทบาทของความร่วมมือระหว่างประเทศในการต่อสู้กับอาชญากรรมทางไซเบอร์เป็นอีกประเด็นหนึ่งที่ควรได้รับการวิจัยเพิ่มเติม เนื่องจากอาชญากรรมทางไซเบอร์มีลักษณะข้ามชาติ การมีส่วนร่วมของประเทศไทยในโครงการป้องกันอาชญากรรมทาง ไซเบอร์ระหว่างประเทศจึงมีความสำคัญ การวิจัยในอนาคตควรตรวจสอบว่าพันธกรณีและความร่วมมือระหว่างประเทศส่งผลต่อการเปลี่ยนแปลงทางเศรษฐกิจของอาชญากรรมทางไซเบอร์ในประเทศไทยอย่างไร

ปัจจัยทางสังคมและเศรษฐกิจ

การทำความเข้าใจปัจจัยทางสังคมและเศรษฐกิจที่ผลักดันอาชญากรรมทางไซเบอร์เป็นสิ่งสำคัญในการพัฒนามาตรการแทรกแซงที่เฉพาะเจาะจง การวิจัยควรสำรวจว่าปัจจัยต่าง ๆ เช่น การว่างงาน ระดับการศึกษา และความไม่เท่าเทียมทางสังคมในแต่ละภูมิภาคมีส่วนทำให้เกิดกิจกรรมอาชญากรรมทางไซเบอร์ในประเทศไทยอย่างไร บทบาทของปัจจัยทางวัฒนธรรมในการกำหนดพฤติกรรมของอาชญากรทางไซเบอร์ยังเป็นประเด็นที่น่าสนใจ การวิจัยในอนาคตควรศึกษาว่าทัศนคติต่อเทคโนโลยีดิจิทัลและความเป็นส่วนตัวในแต่ละวัฒนธรรม เช่น ความเชื่อ คำสอนทางศาสนาส่งผลต่ออาชญากรรมทางไซเบอร์ในประเทศไทยอย่างไร การทำความเข้าใจพลวัตทางวัฒนธรรมเหล่านี้อาจนำไปสู่กลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพมากขึ้น

ผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์ต่อภาคส่วนต่างๆ ในประเทศไทย

ภาคส่วนต่าง ๆ ของเศรษฐกิจไทยได้รับผลกระทบจากอาชญากรรมทางไซเบอร์ในรูปแบบที่แตกต่างกัน การวิจัยในอนาคตควรมุ่งเน้นไปที่การศึกษาตามภาคส่วนต่างๆ เพื่อทำความเข้าใจถึงความท้าทายและความเปราะบางในภาคส่วนต่าง ๆ เช่น การเงิน การธนาคาร การค้าปลีก และการดูแลสุขภาพ ตัวอย่างเช่น ภาคการธนาคารในประเทศไทยเป็นเป้าหมายหลักของอาชญากรทางไซเบอร์เนื่องจากมูลค่าสูงของธุรกรรมทางการเงินที่ดำเนินการทางออนไลน์ การวิจัยควรสำรวจผลกระทบของอาชญากรรมทางไซเบอร์ต่อธุรกิจขนาดกลางและขนาดย่อม (SMEs) ในประเทศไทย ธุรกิจขนาดกลางและขนาดย่อมมักขาดทรัพยากรในการดำเนินมาตรการรักษาความปลอดภัยทางไซเบอร์ ทำให้มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์เป็นพิเศษ การทำความเข้าใจผลกระทบทางเศรษฐกิจของอาชญากรรมทางไซเบอร์ต่อธุรกิจขนาดกลางและขนาดย่อมอาจนำไปสู่การกำหนดนโยบายที่มุ่งให้การสนับสนุนต่อธุรกิจเหล่านี้

อาชญากรรมทางไซเบอร์และเศรษฐกิจนอกระบบในประเทศไทย

เศรษฐกิจนอกระบบในประเทศไทยนั้นเป็นความท้าทายที่ไม่เหมือนใครในบริบทของอาชญากรรมทาง ไซเบอร์ กิจกรรมอาชญากรรมทางไซเบอร์จำนวนมากเกิดขึ้นนอกระบบเศรษฐกิจที่เป็นทางการ ทำให้ติดตามและควบคุมได้ยาก การวิจัยในอนาคตควรสำรวจความสัมพันธ์ระหว่างเศรษฐกิจนอกระบบและอาชญากรรมทางไซเบอร์ โดยมุ่งเน้นที่กิจกรรมทางเศรษฐกิจในภาคส่วนนี้มีส่วนทำให้เกิดอาชญากรรมทางไซเบอร์อย่างไรนอกจากนี้ การวิจัยควรศึกษาบทบาทของเครือข่ายนอกระบบในการส่งเสริมการก่ออาชญากรรมทางไซเบอร์ การทำความเข้าใจว่าเครือข่ายเหล่านี้ดำเนินการอย่างไรและผลกระทบทางเศรษฐกิจที่เกิดขึ้นอาจให้ข้อมูลเชิงลึกในการขัดขวางกิจกรรมอาชญากรรมทางไซเบอร์อย่างมีประสิทธิภาพมากขึ้น

นโยบายของภาครัฐและเอกชนกับการป้องกันอาชญากรรมไซเบอร์

ภาคธุรกิจและภาครัฐบาลควรให้ความสำคัญกับการป้องกันอาชญากรรมไซเบอร์อย่างยิ่ง เนื่องจากการคุกคามทางไซเบอร์ไม่เพียงแต่สร้างความเสียหายให้กับข้อมูลที่เป็นความลับขององค์กรและความเป็นส่วนตัวของบุคคลเท่านั้น แต่ยังส่งผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศอีกด้วย การลงทุนในเทคโนโลยีและมาตรการป้องกันอาชญากรรมไซเบอร์ได้รับการยืนยันว่ามีความคุ้มค่าในระยะยาว เนื่องจากช่วยลดความเสี่ยงของการเกิดเหตุการณ์ทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายทางการเงินอย่างมหาศาล ทั้งนี้ งานวิจัยจำนวนมากได้ระบุว่าการเพิ่มการลงทุนด้านนี้มีผลโดยตรงต่อการลดโอกาสการเกิดการโจมตีทางไซเบอร์ ทั้งในด้านต้นทุนทางเศรษฐกิจที่ลดลงจากการโจมตี และการเพิ่มความเชื่อมั่นของผู้บริโภคและนักลงทุนต่อระบบของบริษัทและรัฐบาล นอกจากนี้ความเสี่ยงทางไซเบอร์ยังเป็นปัจจัยที่ส่งผลกระทบอย่างมากต่อความมั่นคงของชาติ ทำให้รัฐบาลจำเป็นต้องมีบทบาทสำคัญในการกำหนดนโยบายและมาตรการควบคุมเพื่อป้องกันอาชญากรรมไซเบอร์อย่างมีประสิทธิภาพ ดังนั้นการต่อยอดงานวิจัยในเรื่องนี้ควรมุ่งเน้นไปที่การสร้างแบบจำลองที่ชัดเจนในการวิเคราะห์ความคุ้มค่าของการลงทุนในการป้องกันอาชญากรรมไซเบอร์และผลกระทบในระยะยาว ทั้งต่อภาครัฐและเอกชน นอกจากนั้น การวิจัยในอนาคตควรมุ่งเน้นที่การประเมินผลกระทบทางเศรษฐกิจของกฎหมายเหล่านี้ต่อธุรกิจ โดยเฉพาะการศึกษาวิธีการลดต้นทุนการปฏิบัติตามข้อกำหนดและเพิ่มประสิทธิภาพในการป้องกันอาชญากรรมไซเบอร์

อภิปรายและสรุป

สถานการณ์ของอาชญากรรมทางไซเบอร์ในประเทศไทยแสดงให้เห็นถึงสภาพแวดล้อมของภัยคุกคามที่มีหลายมิติและมีการพัฒนาอย่างต่อเนื่อง ขณะที่ประเทศกำลังเผชิญกับปัญหาต่าง ๆ เช่น อาชญากรรมที่เกี่ยวข้องกับยาเสพติด การฉ้อโกงทางการเงิน และอาชญากรรมทางไซเบอร์ จะเห็นได้

ว่าอาชญากรรมทางไซเบอร์กำลังเป็นปัญหาที่เพิ่มขึ้น การขยายตัวของการเข้าถึงอินเทอร์เน็ตและความก้าวหน้าในด้านเทคโนโลยีได้สร้างช่องทางใหม่ ๆ สำหรับกิจกรรมอาชญากรรมทางไซเบอร์ ส่งผลให้มีเหตุการณ์ต่าง ๆ เช่น การฟิชชิ่ง การขโมยข้อมูลประจำตัว และการฉ้อโกงออนไลน์ที่เพิ่มมากขึ้น การพัฒนาเหล่านี้เน้นย้ำถึงความจำเป็นเร่งด่วนในการพัฒนากลยุทธ์และกรอบระเบียบที่มีประสิทธิภาพเพื่อจัดการกับช่องโหว่ที่เกิดขึ้นจากความก้าวหน้าในเทคโนโลยี

ปัจจัยทางเศรษฐกิจและสังคมที่มีอิทธิพลต่ออาชญากรรมทางไซเบอร์ในประเทศไทยสะท้อนถึงความสัมพันธ์ที่ซับซ้อนระหว่างความยากจน การศึกษา และอัตราการว่างงาน การศึกษาชี้ให้เห็นว่าความแตกต่างทางเศรษฐกิจและขาดโอกาสสามารถผลักดันบุคคลไปสู่กิจกรรมอาชญากรรมทางไซเบอร์เป็นแหล่งรายได้ทางเลือก นอกจากนี้ แม้ว่าการศึกษาสูงขึ้นจะช่วยลดโอกาสในการกระทำอาชญากรรม แต่ก็ยังสามารถทำให้ผู้ที่มีทักษะทางเทคนิคทำอาชญากรรมทางไซเบอร์ที่ซับซ้อนมากขึ้น อัตราการว่างงานที่เพิ่มขึ้นยังทำให้ปัญหานี้รุนแรงขึ้น โดยผลักดันให้บุคคลหาวิธีการสนับสนุนทางการเงินที่ผิดกฎหมาย ปัญหานี้เน้นย้ำถึงความจำเป็นในการดำเนินนโยบายสังคมและเศรษฐกิจที่ครอบคลุมเพื่อลดสาเหตุรากฐานและลดแรงจูงใจในการกระทำอาชญากรรมทางไซเบอร์

ความก้าวหน้าทางเทคโนโลยี แม้ว่าจะสนับสนุนการเติบโตทางเศรษฐกิจ แต่ก็ยังสร้างความท้าทายที่สำคัญในการต่อสู้กับอาชญากรรมทางไซเบอร์ การนำเทคโนโลยีและการเชื่อมต่อบรอดแบนด์ที่แพร่หลายทำให้ขนาดและผลกระทบของการโจมตีทางไซเบอร์เพิ่มขึ้น การพัฒนาเทคโนโลยีที่รวดเร็วมักเกิดขึ้นเร็วกว่าการนำมาตรการด้านความปลอดภัยมาใช้ ทำให้มีโอกาสใหม่ ๆ สำหรับอาชญากรทางไซเบอร์ นอกจากนี้ ระดับความชำนาญทางเทคโนโลยีของประชากรยังส่งผลต่อทั้งความสามารถในการกระทำอาชญากรรมทางไซเบอร์และความสามารถในการป้องกันจากการโจมตี การจัดการกับปัญหาเหล่านี้ต้องใช้มาตรการด้านความปลอดภัยทางไซเบอร์อย่างต่อเนื่อง และการเพิ่มพูนความรู้และการศึกษาเกี่ยวกับความปลอดภัยดิจิทัลสำหรับประชาชน

แม้ว่าประเทศไทยจะมีความก้าวหน้าในการพัฒนากฎหมายและเสริมสร้างความสามารถของเจ้าหน้าที่ในการจัดการกับอาชญากรรมทางไซเบอร์ แต่ก็ยังมีความท้าทายอยู่ การทำงานร่วมกันของปัจจัยทางเศรษฐกิจและสังคม ความก้าวหน้าทางเทคโนโลยี และมาตรการทางกฎหมายจำเป็นต้องใช้วิธีการที่ครอบคลุมในการจัดการกับความซับซ้อนของอาชญากรรมทางไซเบอร์ ความพยายามในอนาคตควรมุ่งเน้นไปที่การเสริมสร้างมาตรการทางกฎหมาย การปรับปรุงโครงสร้างพื้นฐานทางเทคโนโลยี และการแก้ไขความไม่เท่าเทียมทางเศรษฐกิจและสังคม การร่วมมือกันระหว่างหน่วยงานภาครัฐ ภาคเอกชน และสถาบันการศึกษาเป็นสิ่งสำคัญในการสร้างสภาพแวดล้อมด้านความปลอดภัยทางไซเบอร์ที่แข็งแกร่งและลดผลกระทบของอาชญากรรมทางไซเบอร์ต่อเศรษฐกิจและสังคมของประเทศ

REFERENCES

Apichaimongkol, S., & Phakdee, A. (2024). Economic and Financial Crime, Sustainability and Good Governance. *RMUTP Journal of Business and Innovation Management, 3*(1), 96-98.

Becker, G. S. (1968). Crime and punishment: An economic approach. Journal of Political Economy, 76(2), 169-217.

Brown, K., Nelson, R., & Smith, D. (2021). Cybersecurity education as a tool for crime prevention. *Journal of Information Security*, 17(4), 314-330.

Bukrapue, P. (2015). Fraudulent activities against foreign tourists in Thailand: A case study of jewelry business. *International Journal of Criminal Justice Sciences, 10*(2), 165-172.

Calderwood, F., & Popova, I. (2018). Smartphone cyber security awareness in developing countries: A case of Thailand. In R. Zitouni, & M. Agueh (Eds.), *Emerging Technologies for Developing Countries* (pp. 79-86). Cham: Springer.

Chotewetsin, P. (2022). Political risk factors affecting the economy of Thailand. *Asian Political Science Review, 6*(2), 43-51.

Clark, E., & Davis, H. (2020). Technology and cybersecurity: Addressing the challenges of modern threats. *Journal of Cybersecurity Policy, 11*(4), 215-233.

Davis, H., & Lee, K. (2019). AI and cybersecurity: Bridging the gap. *Journal of Information Security Research, 23*(2), 34-57.

Dearden, T. E., Parti, K., & Hawdon, J. (2021). Institutional Anomie Theory and Cybercrime Cybercrime and the American Dream, Now Available Online. *Journal of Contemporary Criminal Justice, 37*(3), 311-332.

Emerald Insight. (2018). *Thailand firms up Asian trend on cybersecurity rules.* Retrieved from https://www.emerald.com/insight/content/doi/10.1108/OXAN-DB240082/full/html

Financial Crime News. (2024). *Thailand Country Financial Crime Dashboard 2024.* Retrieved from https://www.financialcrimenews.com

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.

Gorian, E. (2021). Normative legal mechanism for ensuring cyberspace security of Thailand. *Voprosy Bezopasnosti*, (3), 1-20.

Greenfield, R., Davis, L., & Parker, S. (2022). Unemployment, poverty, and cybercrime: An analysis of socio-economic factors. *Journal of Digital Crime, 8*(1), 56-75.

Gupta, P., & Mata-Toledo, R. A. (2016). Cybercrime: In Disguise Crimes. *Journal of Information Systems and Operations Management, 10*(1), 1-10.

Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In M. Khosrow-Pour (Ed.), *Encyclopedia of criminal activities and the deep web* (pp. 36-51). Hershey, PA: IGI Global.

Jones, T., & Smith, R. (2020). Cybercrime and income inequality: A global study. *Journal of Cybersecurity, 15*(3), 45-67.

Khurunun, K., & Saengthongdee, T. (2023). Guidelines for preventing cybercrime in Thailand. *Journal of Legal Entity, 9*(6), 179-190.

Kraiwanit, T., & Srijaem, P. (2021). Evaluation of internet transaction fraud in Thailand. *Indian Journal of Economics and Business, 20*(1), 195-204.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy Magazine, 4*(1), 33-39.

Kshetri, N. (2013). Cybercrime and Cybersecurity in the Global South: Status, Drivers and Trends. In *Cybercrime and Cybersecurity in the Global South* (pp. 1-29). London: Palgrave Macmillan.

Kshetri, N. (2021). Economics of artificial intelligence in cybersecurity. *IT Professional, 23*(4), 73-77.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.

Lewis, J., & Kessler, H. (2020). Legal frameworks and cybersecurity: An evolving challenge. *Cybercrime Studies, 19*(1), 97-112.

Machim, K., Jariyapoom, T., & Pornpundejwittaya, P. (2020). Guidelines for the protection of computer crime threats in the industrial business. *Academy of Strategic Management Journal, 19*(4), 1-13.

Mason, P., Lee, T., & Kim, S. (2021). Reducing unemployment through technology training: A case study. *Journal of Technological Advancement, 14*(5), 201-219.

Nachaisin, Y. (2019). Strategies for combating cyberterrorism in Thailand. *Journal of Multidisciplinary in Social Sciences, 13*(2), 27-42.

Nelson, P., & Wright, M. (2021). Global cooperation in cybercrime regulation. *Journal of International Law and Cybersecurity, 12*(3), 221-240.

OpenGov Asia. (2024). *Thailand's strategies to combat cybercrime.* Retrieved from https://www.opengovasia.com/thailands-strategies-to-combat-cybercrime/

Park, J., Cho, D., Lee, J. K., & Lee, B. (2019). The economics of cybercrime. *ACM Transactions on Management Information Systems (TMIS), 10*(1), 1-23.

Parker, D., & Jones, S. (2021). Educating the digital age: Cybercrime prevention through education. *Computers & Security, 105*, 102-120.

Ramadani, S., Siahaan, A. P. U., Sutrisno, S., Ritonga, S., Amelia, W. R., Dalimunthe, H., & Munthe, R. (2018). Impact of cybercrime on technological and financial developments. *International Journal for Innovative Research in Multidisciplinary Field, 4*(10), 341-344.

Riek, M., Böhme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273.

Rogers, M. (2011). The psyche of cybercriminals: A psycho-social perspective. In B. Grieve, & C. Tyner (Eds.), *Psychology of cybercrime* (pp. 35-50). Springer.

Rungsrisawat, S., Jermsittiparsert, K., & Thanetpaksapong, S. (2019). Do the crime and the socioeconomic strain affect economic growth? A case of an emerging ASEAN economy. *Journal of Security and Sustainability Issues, 9*(2), 391-407.

Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In H. Jahankhani (Ed.), *Cyber criminology* (pp. 25-45). Cham: Springer.

Techatassanasoontorn, A., Huang, H., Trauth, E., & Juntiwasarakij, S. (2011). Analyzing ICT and development: Thailand's path to the information economy. *Journal of Global Information Management, 19*(1), 1-29

Ter, K. L. (2017). Combating cybercrime in Singapore. *TIJ's Research Journal of Social Science & Management (RJSSM), 7*(1), 45-53.

Thai Examiner. (2024). *Campaign to fight cybercrime in Thailand.* Retrieved from https://www.thaiexaminer.com/thai-news-foreigners/2024/08/19/campaign-to-fight-cybercrime-in-thailand/

Thangamuthu, P., Rathee, A., Palanimuthu, S., & Balusamy, B. (2020). Cybercrime. In M. Khosrow-Pour (Ed.), *Encyclopedia of criminal activities and the deep web* (pp. 1-22). Hershey, PA: IGI Global.

Tilleke & Gibbins. (2024a). *Thailand establishes a technology crime court.* Retrieved from https://www.mondaq.com/thailand/crime/1302912

Tilleke & Gibbins. (2024b). *Thailand's new cybercrime measures enlist aid of banks and service providers.* Retrieved from https://www.tilleke.com/insights/thailands-new-cybercrime-measures-enlist-aid-of- banks-and-service-providers/

Ungkap, P., & Daengsi, T. (2022, March). Cybersecurity Awareness Modeling Associated with Influential Factors Using AHP Technique: A Case of Railway Organizations in Thailand. *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 1359-1362). IEEE.

Verma, S., & Gupta, N. (2020). Application of Artificial Intelligence in Cybersecurity. In H. S. Saini, R. Sayal, R. Buyya, & G. Aliseri (Eds.), *Innovations in Computer Science and Engineering* (pp. 65–72). Singapore: Springer.

Williams, M., Brown, T., & Clark, L. (2019). Income disparity and the rise of cybercrime. *Crime, Law, and Social Change, 10*(2), 123-145.

Worldmetrics. (2024). *Thailand Crime Rate Statistics: Market Data Report 2024.* Retrieved from https://www.worldmetrics.org

Yamcharoen, P., Bayewu, A., Ojo, T. P., & Fatoye, O. E. (2022). Evaluating state cybersecurity laws and regulations in the United States. *Advances in Multidisciplinary and Scientific Research, 8*(3), 47-56.