การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19
The Expansion of Organized Cybercrime During The COVID-19 Pandemic

ฐกฤต แก้วทับทิม
คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล

Takrit Kaewtubtim
Faculty of Social Sciences and Humanities, Mahidol University

Received March 15, 2021 | Revised September 27, 2021 | Accepted September 28, 2021

บทความวิชาการ (Academic Article)

บทคัดย่อ

บทความฉบับนี้ นำเสนอแนวโน้มการขยายตัวของอาชญากรรมไซเบอร์ที่กระทำโดยองค์กรอาชญากรรม ซึ่งมีความเชื่อมโยงกับการใช้อินเทอร์เน็ตของประชาชนทั่วโลกที่มากขึ้นในช่วงการระบาดของโรคโควิด-19 และมาตรการจำกัดการแพร่ระบาดของโรคโควิด-19 ของรัฐ โดยทำการสำรวจพัฒนาการขององค์กรอาชญากรรมไซเบอร์ในยุคปัจจุบัน และความเชื่อมโยงขององค์กรอาชญากรรมกับอาชญากรรมไซเบอร์ที่มุ่งเน้นแสวงประโยชน์จากสถานการณ์โรคโควิด-19 โดยได้สรุปตัวอย่างอาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมมีแนวโน้มเป็นผู้กระทำการสูงขึ้น 4 ประเภท ได้แก่ (1) การฉ้อโกงทางอินเทอร์เน็ตผ่านวิธีการฟิชชิ่งและสแกมมิ่ง (2) การใช้ไวรัสเรียกค่าไถ่ (3) การแทรกซึมตลาดการค้าทางออนไลน์ และ (4) การละเมิดสิทธิมนุษยชนโดยอาศัยช่องทางอินเทอร์เน็ต เช่น การค้ามนุษย์ และการแสวงประโยชน์ทางเพศ พร้อมกันนี้ บทความได้นำเสนอถึงความท้าทายและข้อเสนอแนะเกี่ยวกับการป้องกันและปราบปรามองค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโรคโควิด-19 ที่ได้จากการสำรวจวรรณกรรมที่มีอยู่ในปัจจุบันเพื่อประโยชน์ในการพัฒนาปราบปรามองค์กรอาชญากรรมไซเบอร์ในบริบทของประเทศไทยต่อไป

คำสำคัญ: องค์กรอาชญากรรม, อาชญากรรมไซเบอร์, การระบาดของโรคโควิด-19, ความมั่นคงปลอดภัยไซเบอร์

Abstract

This article presents the expanding trend of organized cybercrime threat that correlates with the increased uses of the internet during the COVID-19 pandemic and the states' COVID-19 restrictions. The article surveys the evolution of organized cybercrime in a modern era and the connection between organized crime and cybercrimes that exploit the profits out of the COVID-19 pandemic. Example of 4 types of cybercrimes that are increasingly committed by organized crime includes (1) internet frauds such as scamming

and phishing, (2) ransomware, (3) infiltration of online marketplaces, and (4) human rights violations such as human trafficking and sexual exploitation. Furthermore, the challenges and recommendations relating to the prevention and suppression of organized cybercrime during the COVID-19 identified from the current literature are summarized for the benefits of further development in the suppression of organized cybercrime in the context of Thailand.

Keywords: Organized Crime, Cybercrime, COVID-19 Pandemic, Cybersecurity

บทนำ

อาชญากรรมไซเบอร์ เป็นอาชญากรรมที่ทุกคนสามารถตกเป็นเหยื่อได้ และส่งผลกระทบต่อชีวิตความเป็นอยู่ของประชาชนได้ในวงกว้าง (DSI's Bureau of Development and Logistics, 2021) เนื่องมาจากรูปแบบอาชญากรรมที่ใช้เทคโนโลยีสมัยใหม่ คอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต และอุปกรณ์อิเล็กทรอนิกส์ เป็นช่องทางในการกระทำผิด (UNODC, 2019) อย่างไรก็ตาม ในสถานการณ์ปัจจุบันที่โลกต้องเผชิญกับความผันผวนครั้งใหญ่จากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 หรือโรคโควิด-19 (COVID-19) ทำให้การเกิดอาชญากรรมไซเบอร์มีสูงขึ้นด้วยปัจจัยหลายประการ แต่ประเด็นที่น่าสังเกต คือ ผู้ก่ออาชญากรรมไซเบอร์ที่แสวงประโยชน์จากวิกฤตโรคโควิด-19 มิได้มีเป็นเพียงอาชญากรไซเบอร์รายบุคคลเท่านั้น แต่กลับมีแนวโน้มว่าองค์กรอาชญากรรมได้ขยายตัวและปรับตัวเข้าสู่วงการอาชญากรรมไซเบอร์เพิ่มมากขึ้นด้วย (Radoini, 2020; Marelli, 2020; Ahmed, 2020; Thailand Institute of Justice, 2020; Zivotic & Trajkovski, 2020) ซึ่งองค์กรอาชญากรรมที่ประกอบอาชญากรรมไซเบอร์นั้นมีความสามารถทางบุคลากรและเงินทุนในการก่ออาชญากรรมได้มากกว่า อีกทั้งองค์กรอาชญากรรมไซเบอร์ยังมีรูปแบบการกระทำผิดแบบข้ามชาติ จึงน่าจะสร้างความเสียหายให้แก่ประชาชนและเศรษฐกิจได้สูงกว่า และพึงเล็งเห็นได้ว่าประเทศไทยย่อมได้รับผลกระทบจากปัญหาในลักษณะเดียวกันนี้ด้วย ผู้เขียนจึงมีแนวคิดว่า ควรมีการสำรวจถึงข้อมูลและวรรณกรรมที่เกี่ยวข้องกับการขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19 เพื่อให้เห็นสภาพปัญหาในภาพรวมและนำไปสู่การปราบปรามองค์กรอาชญากรรมไซเบอร์ในบริบทของประเทศไทยต่อไป

ดังนั้น วัตถุประสงค์ของบทความนี้ จึงมีดังต่อไปนี้

1) สำรวจข้อมูลและวรรณกรรมที่มีอยู่ในปัจจุบันที่เกี่ยวข้องกับการขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโรคโควิด-19

2) สำรวจและนำเสนอถึงพัฒนาการและการปรับตัวขององค์กรอาชญากรรมสู่อาชญากรรมไซเบอร์

3) สำรวจและสรุปตัวอย่างประเภทของอาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมมีแนวโน้มขยายตัวเข้ามาเป็นผู้กระทำผิดในช่วงการระบาดของโรคโควิด-19

4) สรุปปัญหาในการป้องกันและปราบปรามองค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโรคโควิด-19 ที่พบจากการสำรวจวรรณกรรมข้างต้น

5) นำเสนอข้อเสนอแนะที่ได้จากการสำรวจข้อมูลการขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโรคโควิด-19 เพื่อนำไปใช้ประโยชน์ในการบริบทของการป้องกันปราบปรามองค์กรอาชญากรรมไซเบอร์ในประเทศไทยต่อไป

อย่างไรก็ดี บทความฉบับนี้ยังมีข้อจำกัดอยู่บางประการ คือ เนื่องจากเป็นประเด็นใหม่ที่ยังคงดำเนินอยู่อย่างต่อเนื่องในสถานการณ์ปัจจุบัน ข้อมูลการอ้างอิงบางส่วนจึงมาจากผลการรายงานขององค์กรและสถาบันที่เกี่ยวข้องที่ได้รวบรวมสถิติและสรุปข้อสังเกตเอาไว้ ประกอบกับผลการศึกษาเชิงวิชาการในประเด็นดังกล่าวเป็นการเฉพาะยังคงอยู่ในวงจำกัด โดยการระบาดของโรคโควิดและลักษณะการกระทำผิดขององค์กรอาชญากรรมไซเบอร์เองที่ตรวจจับได้ยากได้เป็นอุปสรรคทำให้ไม่อาจทำการศึกษาได้ในระยะเวลาอันสั้น โดยเฉพาะอย่างยิ่งในการศึกษาเชิงประจักษ์ (empirical study) ดังนั้น วรรณกรรมส่วนใหญ่ที่ได้อ้างอิงกล่าวถึงในบทความฉบับนี้จึงมีลักษณะเป็นการศึกษาในเชิงทฤษฎีและประเมินแนวโน้มจากข้อมูลล่าสุดที่มีอยู่จากในข่าวสารและบทความวารสารเป็นส่วนใหญ่

พัฒนาการขององค์กรอาชญากรรมไซเบอร์

องค์กรอาชญากรรม (organized crime) นั้นมีการให้คำนิยามอยู่มากมาย โดยอาจสรุปคำนิยามทั่วไปว่าหมายถึง องค์กรที่อาชญากรดำเนินการร่วมกันอย่างต่อเนื่องและมีเหตุมีผล เพื่อสร้างกำไรจากกิจกรรมที่ผิดกฎหมายซึ่งมักจะเป็นกิจกรรมที่เป็นที่ต้องการของสาธารณะชนสูง โดยองค์กรสามารถอยู่รอดได้ด้วยการทุจริตของเจ้าหน้าที่รัฐและการใช้วิธีการข่มขู่ คุกคาม หรือใช้กำลังความรุนแรงเพื่อปกป้องการปฏิบัติการขององค์กรนั้น (UNODC, 2018) ขณะที่องค์กรอาชญากรรม ตามพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 หมายถึง “คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม”

ส่วนคำว่า อาชญากรรมไซเบอร์ (cybercrime) หมายถึง การกระทำที่มีคอมพิวเตอร์เป็นเครื่องมือหรือมีคอมพิวเตอร์เป็นเป้าหมายในการกระทำผิด โดยเฉพาะอย่างยิ่งการกระทำผิดผ่านทางอินเทอร์เน็ต ซึ่งอาชญากรรมไซเบอร์มีทั้งการประกอบอาชญากรรมที่มีอยู่เดิมอยู่แล้วและพัฒนามาใช้ช่องทางออนไลน์เพื่อสามารถปฏิบัติการได้ง่ายขึ้น เช่น การฉ้อโกงผ่านอีเมล โทรศัพท์ออนไลน์ โปรแกรม การขายสินค้าปลอมผ่านเว็บไซต์ การเผยแพร่ภาพลามกอนาจารของเด็ก การละเมิดทรัพย์สินทางปัญญา และด้วยเทคโนโลยีใหม่ ก็ได้เกิดอาชญากรรมไซเบอร์ที่เฉพาะตัวขึ้นมาเพิ่มเติม ที่เรียกกันว่า อาชญากรรมไซเบอร์โดยแท้ (pure cybercrime) อันหมายถึง อาชญากรรมไซเบอร์ที่ถ้าไม่มีอินเทอร์เน็ตหรือคอมพิวเตอร์ก็ไม่สามารถเกิดขึ้นได้ เช่น การโจมตีข้อมูลบนเครือข่ายของบุคคล องค์กร และรัฐบาล แล้วนำมาใช้แสวงประโยชน์อันมิชอบ รวมถึงการเจาะระบบเพื่อเข้าถึงสกุลเงินดิจิทัล และการก่อการร้ายผ่านการโจมตีระบบคอมพิวเตอร์ที่ส่งผลต่อสาธารณะเป็นวงกว้าง เป็นต้น (Denni, 2019)

ปัจจุบันได้มีการใช้คำว่า องค์กรอาชญากรรมไซเบอร์ (organized cybercrime) ซึ่งเป็นการรวมกันของทั้งสองคำข้างต้น เพื่ออธิบายถึงการกระทำผิดอาญาที่เกี่ยวข้องกับคอมพิวเตอร์และอินเทอร์เน็ตที่ดำเนินการให้เป็นไปตามวัตถุประสงค์ของคณะบุคคลหนึ่ง ๆ (UNODC, 2019) อย่างไรก็ตามมีการตั้งข้อสังเกตว่า ความหมายขององค์กรอาชญากรรมเดิมที่มุ่งเน้นถึงองค์ประกอบความผิดที่มีแรงจูงใจมาจากผลประโยชน์ทางวัตถุหรือตัวเงินเพียงอย่างเดียว อาจไม่สามารถอธิบายปรากฏการณ์องค์กรอาชญากรรมไซ

เบอร์ที่เกิดขึ้นในศตวรรษที่ 20 ที่บรรดาแฮ็กเกอร์หรือผู้มีทักษะทางคอมพิวเตอร์ที่ได้มารวมตัวประกอบอาชญากรรมในลักษณะนี้ บางส่วนมีการสานสัมพันธ์กันบนพื้นฐานของแรงจูงใจไม่ว่าจะเป็นในเชิงของความตื่นเต้นเร้าใจที่ได้กระทำผิด ภราดรภาพ (comradeship) หรือคุณค่าที่ไม่ใช่ตัวเงินอย่างอื่นที่กลุ่มอาชญากรนั้นมีร่วมกัน อย่างเช่น ความคลั่งไคล้ในสิ่งผิดกฎหมายบางประเภท การคลั่งลัทธิ เป็นต้น การรวมกลุ่มบางอย่างเพื่อกระทำผิดในโลกออนไลน์ก็มิได้มีวัตถุประสงค์ที่จะสนองตอบต่อความต้องการหรือประโยชน์สมาชิกในกลุ่มแต่อย่างใด และไม่มีการใช้ความรุนแรงหรือการติดสินบน (Grabosky, 2015)

ในเชิงโครงสร้าง องค์กรอาชญากรรมไซเบอร์ที่ประกอบอาชญากรรมไซเบอร์โดยแท้นั้นมีวิวัฒนาการโครงสร้างองค์กรที่แตกแยกไปจากแนวคิดองค์กรอาชญากรรมแบบมาเฟียที่เป็นที่คุ้นเคยกันอย่างสิ้นเชิง (Tropina, 2012) ซึ่งไม่ได้มาจากครอบครัวมาเฟียหรือองค์กรอาชญากรรมแบบเก่าที่มีลำดับชั้นการบังคับบัญชา หรือมีการดำเนินงานมาหลายรุ่นคนหรือหลายปี หรืออาศัยสายสัมพันธ์ทางครอบครัวหรือการเข้าร่วมกลุ่มแล้วไต่เต้าเข้าสู่ตำแหน่งให้สูงขึ้น โดยอาชญากรทางคอมพิวเตอร์ที่เข้ามาสู่วงจรขององค์กรอาชญากรรมไม่ได้มีความสัมพันธ์หรือรู้จักกันในชีวิตจริงมาแต่แรก ส่วนใหญ่จะทำงานกันคนเดียว (Standalone) มาก่อน แทบไม่มีการเจอหน้ากันจริง บางครั้งผู้ร่วมกระทำการในองค์กรเดียวกันยังไม่เคยเจอกันทางออนไลน์เสียด้วย (Tropina, 2010) แต่บุคคลเหล่านี้ทราบถึงทักษะของแต่ละรายจนมีการขยายเป็นเครือข่ายที่รู้จักกันในวงการ มีความยืดหยุ่นสูง และมีฉากหน้าที่หลากหลายในการปฏิบัติการ และจากการศึกษาองค์กรอาชญากรรมที่กระทำผิดเกี่ยวกับการเงินร้ายแรงในประเทศเนเธอร์แลนด์ จำนวน 18 คดี พบว่า ปัจจุบัน องค์กรอาชญากรรมไซเบอร์ไม่ได้เป็นเพียงแค่การรวมกลุ่มของอาชญากรผู้โดดเดี่ยว (Loners) การร่วมงานกันแบบเพื่อนร่วมงาน (colleagues) ที่ต่างคนต่างแยกกันกระทำผิดและมีความร่วมมือกันแบบหลวม ๆ อีกต่อไปแล้ว หรือเป็นกลุ่มเพื่อน (peers) ที่ร่วมกันกระทำผิดแต่มีความสัมพันธ์กันระยะสั้น หากแต่ส่วนใหญ่ได้พัฒนาองค์กรที่ซับซ้อนขึ้นมาเป็นลักษณะของเป็นทีมงาน (teams) ซึ่งเป็นองค์กรที่มีการแบ่งงานกันทำอย่างชัดเจน มีการร่วมกันกระทำผิดมาเป็นระยะเวลานานพอสมควร และสุดท้ายคือเป็นองค์กรอย่างเป็นทางการ (formal organization) ที่มีโครงสร้างองค์กรที่กระทำผิดร่วมกันมาอย่างยาวนาน มีจำนวนสมาชิกมาก มีการบริหารจัดการ แบ่งงานอย่างเป็นสัดส่วน ทำให้อัตราการประสบความสำเร็จในการกระทำผิดสูง ซึ่งเป้าหมายของสมาชิกของทีมงาน คือ อำนาจหรือผลประโยชน์ทางการเงิน และการหลีกเลี่ยงการถูกจับได้จากรัฐ (Leukfeldt & Holt, 2020) โดยในรูปแบบองค์กรที่ซับซ้อนขึ้นมาเหล่านี้ จะมีสมาชิกหลัก หรือผู้ยุยงหลัก (core members หรือ core enablers) ที่มีบทบาทคล้ายกับผู้ประกอบการ ซึ่งมักจะไม่ได้เป็นผู้ลงมือกระทำผิดโดยตรง ทำการนัดแนะเพื่อหาบุคคลที่มีทักษะเฉพาะด้านที่ต้องใช้ในการประกอบอาชญากรรมไปร่วมงานทั้งทางออนไลน์ (เช่น การเข้ารหัสรักษาความปลอดภัย) และออฟไลน์ (เช่น การนำรหัสหรือข้อมูลไปเปลี่ยนเป็นเงินสดที่ธนาคารท้องถิ่น) เพื่อให้การประกอบภารกิจเป้าหมายสำเร็จได้ง่ายขึ้น หลังจากนั้น ก็จะแยกย้ายกันไป มีการกลบร่องรอยทางออนไลน์อีกทั้งบางเครือข่ายก็จะติดต่อกันเฉพาะผู้ที่ได้รับการไว้วางใจเท่านั้น ไม่มีคนนอก (Leukfeldt & Holt, 2020; Tropina, 2010) ทำให้เป็นการยากต่อการติดตามของหน่วยงานฝ่ายปราบปรามอาชญากรรมไซเบอร์

กระนั้น การเกิดขึ้นและมีอยู่ขององค์กรอาชญากรรมแบบใหม่นี้ไม่ได้เป็นการแทนที่องค์กรอาชญากรรมแบบดั้งเดิมแต่อย่างใด หากแต่องค์กรอาชญากรรมแบบมาเฟียท้องถิ่นเดิมเหล่านี้ ได้ปรับตัวและเปลี่ยนเป้าหมายจากโลกทางกายภาพ ย้ายมาปฏิบัติการในโลกออนไลน์แทน ดังจะเห็นได้ชัดเจนขึ้นในช่วงการระบาดของโรคโควิด-19 ที่ผ่านมา (Ahmed, 2020) องค์กรอาชญากรรมท้องถิ่นหรือเหล่ากลุ่ม

มาเฟีย รวมไปถึงองค์กรอาชญากรรมที่เดิมจำกัดอยู่เพียงธุรกิจที่มีหน้าร้าน หรือจำเป็นต้องหยุดขบวนการลักลอบขนสิ่งของผิดกฎหมายอย่างยาเสพติดหรือแรงงานลักลอบเข้าเมืองเพราะการสั่งห้ามเดินทางข้ามชายแดนของแต่ละประเทศ ต่างปรับตัวหันมาใช้อินเทอร์เน็ตในการสนับสนุนการประกอบอาชญากรรมในพื้นที่ เช่น กลุ่มอิทธิพล (cartels) หลายกลุ่มในประเทศเม็กซิโก อิตาลี แอฟริกาใต้ ญี่ปุ่น ฯลฯ อาศัยความลำบากของประชาชนในพื้นที่ที่ได้รับผลกระทบจากโรคโควิด-19 ไปทำการช่วยเหลือบริจาคสิ่งของ แล้วนำมาเขียนเผยแพร่บนสื่อโซเชียลมีเดียของตนเองเพื่อเป็นการแอบแฝงประชาสัมพันธ์เครือข่ายของตนเองในพื้นที่ อันเป็นการแสดงอำนาจในการรักษาเขตแดนขององค์กรของตน และเพื่อหาช่องทางในการเพิ่มอำนาจและเส้นทางธุรกิจ (Marelli, 2020; UNODC, n.d.)

บางส่วนก็เปลี่ยนมาประกอบอาชญากรรมแบบดั้งเดิมโดยผ่านทางอินเทอร์เน็ตแทน เช่น การตั้งเว็บไซต์และบริษัทขายของปลอม ของลอกเลียนแบบ หรือของที่ไม่มีคุณภาพ (EUROPOL & EUIPO, n.d.) การสร้างโปรแกรมบนโทรศัพท์เพื่อปล่อยกู้เงินนอกระบบดอกเบี้ยแพง โดยมีหัวหน้าองค์กรเป็นชาวจีนที่ตั้งฐานปฏิบัติการในประเทศไทย (Laohong, 2021) เป็นต้น บางส่วนก็อาศัยแผนการธุรกิจขายให้ธุรกิจ (Business-to-Business หรือ B2B) ที่หยิบยืมมาจากธุรกิจที่ถูกกฎหมาย แต่มาปรับใช้กับการขายสินค้าและบริการที่ผิดกฎหมายแทน ในลักษณะของอาชญากรขายให้อาชญากร (Criminal-to-Criminal หรือ C2C) เช่น การสร้างเครือข่ายเซิร์ฟเวอร์ขึ้นมาซึ่งอาชญากรที่เป็นสมาชิกสามารถเข้าระบบเพื่อไปใช้เครื่องมือในการเจาะหรือทำลายระบบหรือล้วงข้อมูลหลายประเภท เช่น ไวรัส โทรจัน คีย์ล็อกเกอร์ ฯลฯ ที่สร้างความเสียหายให้แก่ระบบข้อมูล แล้วเข้าไปใช้ข้อมูลเพื่อการกระทำผิดอื่น ๆ ต่อไป หรือการสร้างเครือข่ายบ็อทเน็ต (botnets) ที่ทำให้สามารถควบคุมเครื่องคอมพิวเตอร์ที่ถูกเจาะระบบและติดตั้งบ็อทแล้ว เพื่อประกอบอาชญากรรมอย่างการฟิชชิ่ง (phishing) ได้ทั่วโลก (Tropina, 2010)

ดังนั้น คำนิยามขององค์กรอาชญากรรมไซเบอร์จึงมีความหมายที่กว้างมากไปกว่าองค์กรอาชญากรรมในรูปแบบเจ้าพ่ออย่างที่เคยมีมาและมีความหลากหลายทั้งในรูปแบบองค์กร รูปแบบการกระทำผิด และมูลเหตุจูงใจของการกระทำผิดด้วย จึงจำเป็นต้องใช้วิธีการและมาตรการป้องกันและปราบปรามอาชญากรรมที่แตกต่างและละเอียดอ่อนขึ้น

การระบาดของโรคโควิด-19 กับการขยายตัวขององค์กรอาชญากรรมไซเบอร์

การระบาดของโรคโควิด-19 (COVID-19) ที่เริ่มมาตั้งแต่ปลายปี พ.ศ. 2562 และกระจายตัวไปอย่างรวดเร็วทั่วโลกจนถึงขณะนี้ ได้สร้างผลกระทบต่อวิถีชีวิตและเศรษฐกิจของประชากรทุกพื้นที่เป็นอย่างมาก โดยข้อมูลจากเว็บไซต์กูเกิล (Google) ณ วันที่ 5 มีนาคม พ.ศ. 2564 มีผู้ติดเชื้อทั่วโลกไปแล้วมากกว่า 116 ล้านคน ด้วยการแพร่ระบาดที่ยังคงมีอย่างต่อเนื่อง ทำให้รัฐบาลของแต่ละประเทศจำเป็นต้องออกมาตรการปิดเมือง (lockdown) มารับมือและป้องกันการแพร่ระบาดให้ชะลอตัวลง โดยมุ่งเน้นไปที่การเว้นระยะห่างทางสังคม การสั่งงดเว้นการออกจากบ้าน การปรับเปลี่ยนให้ทำงานอยู่กับบ้านแทนการจำกัดการเดินทางข้ามเขต การงดการเดินทางข้ามประเทศ การสั่งปิดสถานที่สาธารณะและสถานประกอบการที่เสี่ยงต่อการแพร่กระจายเชื้อโรค (Zivotic & Trajkovski, 2020) ดังนั้น ประชาชนจึงอยู่อาศัยกับบ้านและต้องพึ่งพาอินเทอร์เน็ตในการใช้ชีวิตมากขึ้น ทั้งเพื่อการทำงานและการสันทนาการเพื่อลดความเครียด (ETDA, 2020) และกลุ่มอุตสาหกรรมและธุรกิจที่ต้องใช้ระบบคอมพิวเตอร์ในการดำเนินการ โดยเฉพาะอย่างยิ่งระบบจัดเก็บข้อมูลส่วนบุคคลและข้อมูลการเงินที่มีความอ่อนไหวสูง (Volz

& McMillan, 2020) เมื่อมีการใช้อินเทอร์เน็ตที่สูงขึ้น โอกาสในการประสบกับอาชญากรรมไซเบอร์ก็ย่อมสูงขึ้นไปด้วย

ทั้งนี้ เหยื่อขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโรคโควิด-19 มักเป็นกลุ่มเสี่ยงที่ขาดความรู้ความเข้าใจในการใช้คอมพิวเตอร์และอินเทอร์เน็ตที่สามารถถูกหลอกหรือตกเป็นเหยื่อได้ง่าย ซึ่งสามารถตกเป็นเหยื่อได้ทุกเพศทุกวัย เพราะแต่ละวัยมีความรับรู้ด้านเทคโนโลยีที่แตกต่างกัน (DSI's Bureau of Development and Logistics, 2021) โดยเฉพาะในเด็ก เยาวชน และผู้สูงอายุ ที่ใช้อินเทอร์เน็ตกันมากขึ้นเพื่อเรียนหรือติดต่อกับครอบครัว (ETDA, 2020) นอกจากนี้ยังมีกลุ่มผู้บริโภคที่ตกเป็นเหยื่อของอาชญากรรมดั้งเดิมที่หันมาใช้อินเทอร์เน็ตเป็นช่องทางหาเหยื่อใหม่แทน อย่าง เว็บไซต์ขายสินค้าปลอมหรือบริการที่ผิดกฎหมาย เป็นต้น (UNODC, n.d.; Marelli, 2020) ซึ่งเป็นการฉวยโอกาสจากความวิตกกังวลและความเปราะบางของผู้คนในช่วงที่ต้องเผชิญกับวิกฤติและความไม่แน่นอน

ขณะเดียวกัน การสั่งปิดธุรกิจชั่วคราวและจำกัดการเดินทาง ได้ส่งผลกระทบโดยตรงต่อธุรกิจ 6 ประเภทมากที่สุด ได้แก่ ธุรกิจท่องเที่ยว ซึ่งรายได้ลดลงถึงร้อยละ 73 ธุรกิจบันเทิง ธุรกิจรับจ้างและบริการ ธุรกิจการผลิต และธุรกิจอาหาร (Chankisen, 2021) ซึ่งในกลุ่มธุรกิจเหล่านี้ ไม่ได้มีเพียงเฉพาะธุรกิจที่ดำเนินการอย่างถูกกฎหมายเท่านั้น แต่ยังมีธุรกิจที่แอบแฝงอยู่ขององค์กรอาชญากรรม (organized crime) ซึ่งมีทั้งองค์กรภายในประเทศและองค์กรข้ามชาติที่ได้รับผลกระทบจากการระบาดของโรคโควิด-19 ด้วย เนื่องจากกลุ่มอาชญากรเหล่านี้ ได้อาศัยแสวงประโยชน์จากการขยายตัวของธุรกิจต่าง ๆ โดยเฉพาะอย่างยิ่งธุรกิจท่องเที่ยวทั้งในต่างประเทศและในประเทศไทย ไม่ว่าจะเป็นในรูปแบบของการฟอกเงินและเลี่ยงการเสียภาษีผ่านบริษัทนำเที่ยว เช่น กรณีธุรกิจทัวร์ศูนย์เหรียญ ที่มีการสวมบัตรประชาชนคนไทยตั้งบริษัทจำนวนมาก (Matichon Online, 2020) การเปิดร้านค้าหรือร้านอาหารเพื่อเป็นธุรกิจบังหน้าการฟอกเงิน การค้าประเวณี การฉ้อโกงนักท่องเที่ยวในหลากหลายรูปแบบ การใช้บัตรเครดิตปลอมของขบวนการโจรกรรมข้อมูล บัตรเครดิต (กลุ่มสกิมเมอร์) มารูดซื้อของในร้านค้าหรือกดเงินสดในแหล่งท่องเที่ยวอย่างพื้นที่อโศก สุขุมวิท พัทยา ฯลฯ (Somkamnerd & Terdudomtham, 2019) อันจะเห็นได้ว่าเป็นรูปแบบการกระทำผิดที่ต้องอาศัยธุรกิจที่มีหน้าร้านจริง (brick-and-mortar retail) และหาเหยื่อกันภายในพื้นที่ หรืออาศัยนักท่องเที่ยวที่เข้ามาในพื้นที่จำนวนมากเป็นตัวขับเคลื่อนกลไกอาชญากรรมขององค์กร ดังนั้น การที่นักท่องเที่ยวไม่สามารถเดินทางมาได้เพราะการระบาดของโรคโควิด-19 ก็ส่งผลต่อรายได้ของธุรกิจมืดเหล่านี้เช่นกัน

จากปัจจัยที่เป็นผลมาจากการระบาดของโรคโควิด-19 และมาตรการของรัฐบาลที่ใช้เพื่อพยายามควบคุมการแพร่เชื้อดังกล่าวมาข้างต้น ทำให้ระบบเศรษฐกิจถูกแปลงมาอยู่ในรูปแบบดิจิทัลมากขึ้น ส่งผลให้เกิดกระแสการขยายตัวของอาชญากรรมไซเบอร์ที่มากขึ้นด้วย (Radoini, 2020; Marelli, 2020; Ahmed, 2020; Thailand Institute of Justice, 2020) ซึ่งเปรียบเสมือนเป็นการแพร่ระบาดของโรคร้ายซ้ำสองที่จะมีอัตราการเติบโตรวดเร็วและมีผลร้ายในระยะยาวต่อวิถีชีวิตยิ่งไปกว่าการระบาดของโรคโควิด-19 อย่างหลีกเลี่ยงไม่ได้ จากรายงานการประเมินการคุกคามของอาชญากรรมร้ายแรงและองค์กรอาชญากรรมในสหภาพยุโรป ประจำปี พ.ศ. 2564 (European Union Serious and Organised Crime Threat Assessment 2021) ของสำนักงานสหภาพยุโรปเพื่อความร่วมมือในการบังคับใช้กฎหมายหรือยูโรโพล (EUROPOL) ซึ่งรวบรวมข้อมูลและสถิติที่ยูโรโพลดำเนินภารกิจสอดส่องความเคลื่อนไหวขององค์กรอาชญากรรมแล้ววิเคราะห์เกี่ยวกับสภาพปัญหาขององค์กรอาชญากรรมในช่วงปีที่ผ่านมา ได้สรุปผลพบว่าองค์กรอาชญากรรมในภาคพื้นยุโรปใช้เทคโนโลยีเป็นเครื่องมือสำคัญในการกระทำความผิด ผ่านการใช้การ

สื่อสารแบบเข้ารหัส การใช้เครือข่ายสังคมออนไลน์ และโปรแกรมส่งข้อความ เพื่อเข้าถึงกลุ่มเป้าหมายของอาชญากรรมให้มากขึ้น โดยเฉพาะอย่างยิ่งในการขายสินค้าผิดกฎหมายหรือการเผยแพร่ข้อมูลที่บิดเบือน รวมถึงใช้เป็นช่องทางในการส่งต่อเครื่องมือในการประกอบอาชญากรรมให้แก่อาชญากรรายอื่น และการล่วงละเมิดทางสิทธิมนุษยชน (EUROPOL, 2021)

นอกจากนี้ ข้อมูลสถิติขององค์การตำรวจสากล (INTERPOL) แสดงให้เห็นหลักฐานของการขยายตัวของอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งการโจมตีทางไซเบอร์ขององค์กรอาชญากรรมหลายกลุ่มที่เกิดความถี่ขึ้นอย่างมาก ในช่วงสองสัปดาห์แรกของเดือนเมษายน พ.ศ. 2563 ที่เป็นช่วงซึ่งการแพร่ระบายของโรคเริ่มรุนแรงและขยายวงกว้างมากขึ้น เมื่อเปรียบเทียบการโจมตีทางไซเบอร์ในช่วงก่อนการแพร่ระบาดของโรคโควิด-19 ที่แทบไม่มีการโจมตีในลักษณะเดียวกันนี้เลย (INTERPOL, 2020a) โดยการขยายตัวในครั้งนี้ ส่วนหนึ่งมาจากการเปลี่ยนกลุ่มเป้าหมายเหยื่อขององค์กรอาชญากรรมรูปแบบดั้งเดิม มาสู่โลกออนไลน์มากขึ้นเพื่อชดเชยการสูญเสียแหล่งรายได้เดิมและฉวยโอกาสจากความเปราะบางของผู้คนในช่วงวิกฤติ และช่องโหว่ความปลอดภัยของอินเทอร์เน็ตและระบบคอมพิวเตอร์ที่ยังไม่ได้มีความพร้อมต่อการรองรับสังคมไซเบอร์อย่างเต็มตัวในระยะเวลาอันสั้น (Marelli, 2020; Ahmed, 2020) ดังนั้น การขยายตัวขององค์กรอาชญากรรมไซเบอร์ ถือว่าเป็นภัยคุกคามต่อความมั่นคงของทั้งประเทศไทยและสังคมโลกที่ต้องเฝ้าระวังอย่างใกล้ชิด

ตัวอย่างประเภทการกระทำผิดเกี่ยวกับคอมพิวเตอร์ขององค์กรอาชญากรรมที่ขยายตัวขึ้นในช่วงการแพร่ระบาดของโรคโควิด-19

อาชญากรรมไซเบอร์เป็นอาชญากรรมที่ไม่ได้จำกัดเฉพาะพื้นที่ใดพื้นที่หนึ่งเท่านั้น หากแต่เป็นอาชญากรรมที่ไร้พรมแดน (borderless) และในหลายกรณีก็มีลักษณะเป็นอาชญากรรมข้ามชาติ (transnational) ที่ผู้กระทำผิดและเหยื่อไม่ได้อยู่ในพื้นที่เดียวกันหรือประเทศเดียวกัน อีกทั้งในการกระทำผิดครั้งหนึ่งอาจกระทำลงและมีผลร้ายในเขตอำนาจของหลายประเทศจนยากที่จะติดตามหรือระบุให้แน่ชัดว่าเป็นความผิดในประเทศใด องค์กรอาชญากรรมไซเบอร์จึงเป็นความเสี่ยงต่อเสถียรภาพของเศรษฐกิจและสังคมในทุกประเทศซึ่งผู้เชี่ยวชาญและรัฐบาลต่างก็พยายามหาวิธีการป้องกันและปราบปราม แต่เนื่องด้วยสถานการณ์การแพร่ระบาดของโรคโควิด-19 ส่งผลให้มีผู้ใช้อินเทอร์เน็ตสูงมากขึ้นทั้งในกลุ่มประชาชนและองค์กรทั้งหลาย (ETDA, 2020) ซึ่งทางองค์การตำรวจสากลได้มีการประกาศเตือนถึงภัยจากอาชญากรรมไซเบอร์ที่มีแนวโน้มจะขยายตัวมากขึ้นในช่วงวิกฤติการณ์ โดยส่วนหนึ่งเป็นผลมาจากการเปลี่ยนกลยุทธ์ขององค์กรอาชญากรรมในการกระทำผิดให้เข้าถึงกลุ่มเป้าหมายได้มากขึ้นในทางออนไลน์ (INTERPOL, 2020a) ซึ่งองค์กรเหล่านี้มีความสามารถในการปรับตัวและใช้ประโยชน์จากสถานการณ์ยากลำบากได้เป็นอย่างดี

จากการสำรวจข้อมูลเบื้องต้น พบว่ามีประเภทของการกระทำผิดที่มีอัตราขยายตัวขึ้นอย่างต่อเนื่องในช่วงที่มีการระบาดของโรคโควิด-19 ที่มีแนวโน้มว่าองค์กรอาชญากรรมไซเบอร์เป็นผู้กระทำความผิดหรือสนับสนุนอยู่เบื้องหลัง ดังนี้

1) การฟิชชิ่ง (phishing) และการสแกมมิ่ง (scamming)

เป็นวิธีการฉ้อโกงทางอินเทอร์เน็ตอย่างหนึ่งซึ่งใช้อีเมลหรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล ข้อมูลบัตรเครดิต ชื่อผู้ใช้ (username) รหัสผ่าน (passwords) ที่ใช้เข้าสู่ระบบเว็บไซต์ทางการเงินหรือโซเชียลมีเดียหรือเว็บไซต์ที่มีความน่าสนใจต่อพวกอาชญากรสูงประเภทอื่น เพื่อนำข้อมูลไปใช้

ในทางมิชอบและสร้างความเสียหายในหลายด้าน ซึ่งวิธีการฟิชชิ่งที่ใช้มีอยู่หลากหลายรูปแบบและเพิ่มความแยบยลมากขึ้นอย่างต่อเนื่อง โดยเฉพาะเมื่อใช้เพื่อเข้าไปล้วงข้อมูลจากระดับองค์กรใหญ่หรือบุคคลสำคัญ ซึ่งบางครั้งก็จะมีการใช้โปรแกรมคอมพิวเตอร์มัลแวร์ (malware) ต่าง ๆ ร่วมด้วย เช่น ไวรัส โทรจัน เวิร์ม ที่จะบุกเข้าโจมตีคอมพิวเตอร์ของเหยื่อหลังจากคลิกที่ลิ้งค์ในอีเมลหรือเข้าชมเว็บไซต์ เพื่อเข้าไปล้วงข้อมูล รวมถึงทำลายระบบให้เสียหายด้วย (Council of Europe, 2020; Radoini, 2020)

จากการวิเคราะห์ข้อมูลของกูเกิล โดย แอตลาส วีพีเอ็น (Atlas VPN) พบว่า มีการเพิ่มจำนวนของเว็บไซต์ฟิชชิ่ง จากเดิมมีอยู่ประมาณ 149,000 เว็บไซต์ในเดือนมกราคม พ.ศ. 2563 ไปเป็นจำนวนมากกว่า 522,000 เว็บไซต์ ภายในเดือนมีนาคม พ.ศ. 2563 หรือเพิ่มขึ้นมากกว่าร้อยละ 350 ในระยะเวลาเพียงแค่ 3 เดือน (Radoini, 2020) อันเป็นช่วงเริ่มต้นการระบาดของโรคโควิด-19 และเริ่มมีมาตรการสั่งปิดเมืองและจำกัดการเดินทางกันแล้ว

การใช้เว็บไซต์ให้ข่าวเท็จหรือแอบอ้างว่าเป็นเว็บไซต์เกี่ยวกับข้อมูลของโรคโควิด-19 ทั้งที่เป็นข้อมูลเท็จ (false Information หรือ misinformation) ก็เป็นอีกทางหนึ่งของการแสกมมิ่งและฟิชชิ่ง โดยองค์การอนามัยโลก ได้ประกาศแจ้งเตือนให้เพิ่มความระมัดระวังในการอ่านเว็บไซต์เหล่านี้ และอย่าหลงเชื่อทำการสั่งซื้อสินค้า โอนเงิน หรือให้ข้อมูลส่วนบุคคลแก่เว็บไซต์ปลอมที่ดูน่าเชื่อถือเหล่านี้ เพราะบางครั้งเว็บไซต์หรืออีเมลที่เป็นธุรกิจจริงได้ถูกองค์กรอาชญากรรมเข้าระบบและยึดหรือถูกปลอมไปเป็นหน้าฉากในการฉ้อโกงแล้ว ทำให้ถูกฉ้อโกงจากการหลอกขายสินค้าที่ไม่มีของที่จะขายจริง เช่น กรณีบริษัทเยอรมนีถูกหลอกขายหน้ากากอนามัย 10 ล้านชิ้นจากประเทศไอร์แลนด์ผ่านการแอบอ้างบริษัทเนเธอร์แลนด์ขายหน้ากากที่มีอยู่จริงแต่ถูกโคลนนิ่ง (cloning) เป็นอีกเว็บไซต์หนึ่งไปหลอกผู้ซื้อ (EUROPOL, 2020) หรือมีการหลอกให้โอนเงินเข้าบัญชีหลอกเพื่อจ่ายเป็นค่ารักษาพยาบาลที่ตกลงกัน ซึ่งคาดกันว่ามีผู้ตกเป็นเหยื่อของการสแกมมิ่งในลักษณะนี้เป็นมูลค่าความเสียหายมหาศาลแล้ว (Global Initiative Against Transnational Organized Crime, 2020)

ในบริบทของประเทศไทย การฟิชชิ่งและสแกมมิ่งที่แพร่หลายนั้นมีทั้งเว็บไซต์ธนาคารปลอม การหลอกให้ส่งรหัสผ่านครั้งเดียวหรือโอทีพี (OTP) เพื่อเข้าระบบการทำธุรกรรมทางธนาคาร แล้วขโมยโอนเงินออกนอกระบบ การใช้อีเมลหลอกลวงที่มักพบเป็นองค์กรอาชญากรรมจากประเทศแถบแอฟริกากลุ่มคอลเซ็นเตอร์ คือ การหลอกถามข้อมูลเพื่อหาประโยชน์จากข้อมูลนั้นต่อไป เช่น การข่มขู่กรรโชกทรัพย์ ซึ่งในปัจจุบันองค์กรอาชญากรรมต่าง ๆ ใช้เทคโนโลยีในการโทรศัพท์ผ่านอินเทอร์เน็ตหรือวีโอไอพี (Voice Over Internet Protocol หรือ VOIP) ปฏิบัติการทั้งภายในประเทศไทยและอาศัยประเทศไทยปฏิบัติการหลอกลวงเหยื่อในต่างประเทศด้วย โดยในช่วงการระบาดของโควิด-19 มีข่าวการแจ้งเตือนการหลวกลวงของกลุ่มคอลเซ็นเตอร์ว่าจะมีการโอนเงินกระตุ้นเศรษฐกิจเพื่อชดเชยการสั่งปิดช่วงการเฝ้าระวังโรคโควิด-19 ให้ประชาชนจากกรมบัญชีกลาง (Manager Online, 2020a) หรือการใช้สื่อโซเชียลมีเดียของกลุ่มต้มตุ๋นจากไนจีเรียหลอกลวงว่าให้ร่วมลงทุนมีกำไรดี หรือหลอกให้รักและว่าจะใช้ชีวิตร่วมกัน หรือมีทรัพย์สินมีราคาจะขายให้ราคาถูก ซึ่งภายหลังถูกจับและพบเงินหมุนเวียนมากกว่า 280 ล้านบาท (Khoasod Online, 2020) ซึ่งกลุ่มมิจฉาชีพเหล่านี้จะตกทรัพย์โดยให้เหยื่อโอนเงินไปให้เพื่อหวังผลตอบแทนในภายหลัง ประชาชนมักตกเป็นเหยื่อกันมากในช่วงการระบาดของโรคโควิด-19 เพราะหลงเชื่อว่าจะมีโอกาสในการทำเงินในการลงทุนหรือได้เงินชดเชยในช่วงเศรษฐกิจถดถอยจริง หรือเกิดจากความรู้สึกเบื่อหน่ายหรือเปราะบางจากความกดดันที่ต้องอยู่แต่บ้านจนใช้อินเทอร์เน็ตเป็นช่องทางในการแสวงหาความสุขรูปแบบต่าง ๆ เช่น หาคนรัก หรือซื้อของ เป็นต้น

2) ไวรัสเรียกค่าไถ่ (ransomware)

ประเภทของการกระทำผิดอีกอย่างหนึ่งที่มีลักษณะเฉพาะตัว คือ การใช้ไวรัสเรียกค่าไถ่ (ransomware) ซึ่งกลายมาเป็นเครื่องมือที่แพร่หลายในช่วงการระบาดของโรคโควิด-19 ซึ่งไวรัสเรียกค่าไถ่จะมาในหลากหลายรูปแบบ ทั้งเจาะเข้าระบบเพื่อฝังไวรัสเรียกค่าไถ่เอาไว้ในระบบให้ทำงานในภายหลัง หรือการใช้วิธีการฟิชชิ่งหรือสแกมมิ่งไปยังเป้าหมายที่ต้องการ แล้วให้เมื่อคลิกเปิดอีเมลหรือเปิดลิ้งค์ก็จะถูกติดตั้งไวรัสเรียกค่าไถ่ โดยเป้าหมายมีทั้งการเรียกค่าไถ่จากบุคคลธรรมดาเพื่อแลกกับการไม่เปิดเผยข้อมูลส่วนบุคคล และการเรียกค่าไถ่จากองค์กรหรือธุรกิจต่าง ๆ ซึ่งอาจถูกโจมตีเป็นมัลแวร์ไปที่คอมพิวเตอร์ของตำแหน่งบุคคลสำคัญ เช่น ผู้จัดการ หัวหน้า ผู้บริหารองค์กรว่าจะเปิดเผยข้อมูลขององค์กร หรือโจมตีด้วยการเจาะเข้าระบบข้อมูลหรือระบบที่ใช้ดำเนินงานขององค์กรหรือธุรกิจนั้นโดยตรง จนทำให้ระบบถูกปิดและไม่สามารถใช้การได้ และไม่สามารถเข้าถึงฐานข้อมูลต่าง ๆ เช่น ข้อมูลการรักษา ฯลฯ แล้วเรียกค่าไถ่เพื่อให้ระบบสามารถกลับมาใช้ได้เหมือนเดิม ซึ่งในกรณีหลังนี้เป็นปรากฏการณ์ที่เกิดขึ้นบ่อยครั้งขึ้นในสถานพยาบาล ห้องปฏิบัติการทางการแพทย์ และสถานที่ที่ประชาชนเข้าไปใช้บริการตรวจหาเชื้อโรคโควิด-19 หรือสถานที่พัฒนาวัคซีนป้องกันโรคโควิด-19 เช่น โรงพยาบาลหลายแห่งในหลายประเทศโดยเฉพาะในสหรัฐอเมริกา ที่ตกเป็นเป้าหมายในการโจมตีด้วยไวรัสเรียกค่าไถ่ที่คาดว่าเป็นการปฏิบัติการขององค์กรอาชญากรรมแฮ็กเกอร์รัสเซียกลุ่มหนึ่งที่มีความเชี่ยวชาญและพุ่งเป้าไปที่โรงพยาบาลเป็นการเฉพาะ (Volz & McMillan, 2020)

และเมื่อเริ่มมีการกระจายวัคซีนโควิด-19 ไปทั่วโลก องค์การตำรวจสากล ได้ออกประกาศเตือนสีส้มให้ระวังการคุกคามขององค์กรอาชญากรรมที่พุ่งเป้าหมายไปที่วัคซีนโควิด-19 หลังมีรายงานการโจมตีทางไซเบอร์จากองค์กรอาชญากรรมแฮ็กเกอร์เกาหลีเหนือไปยังหลายบริษัทที่ทำการวิจัยวัคซีนและวิธีรักษาโรคโควิด-19 โดยอาจมุ่งหวังว่าจะทำการปลอมหรือขโมยวัคซีนตัวใหม่ไปให้ได้ (INTERPOL, 2020b; McGee, 2020) ซึ่งแสดงให้เห็นว่าไวรัสเรียกค่าไถ่เป็นอาชญากรรมที่ต้องจับตามากเพราะมีผลกระทบต่อความปลอดภัยและสวัสดิภาพของคนไข้ ผู้ประกอบวิชาชีพในสถานพยาบาล ความมั่นคงด้านสาธารณสุขและสิทธิความเป็นส่วนตัวของประชาชน นอกจากนี้ยังเกิดขึ้นกับองค์กรอื่น ๆ ที่เกี่ยวข้องกับการสาธารณสุขอย่างองค์การอนามัยโลก (World Health Organization หรือ WHO) สถาบันการเงิน หน่วยงานรัฐบาล และธุรกิจอื่นที่มีการจัดเก็บข้อมูลส่วนบุคคลอีกด้วย (Council of Europe, 2020; Radoini, 2020) แต่ปัญหาของอาชญากรรมประเภทนี้ คือ เหยื่อมักจะยอมจ่ายค่าไถ่เพื่อให้สามารถเข้าถึงและใช้ระบบได้อีกครั้งหนึ่งโดยลับ ๆ เพราะไม่ต้องการให้สาธารณชนทราบถึงการถูกเจาะระบบอันจะส่งผลต่อภาพลักษณ์หรือการต้องจ่ายค่าเสียหายอีกเป็นจำนวนมากที่ปล่อยให้ข้อมูลรั่วไหล หรือเพื่อให้ผู้เรียกค่าไถ่ลบข้อมูลออกไป แม้ว่าจะไม่มีการยืนยันว่าได้มีการลบข้อมูลจริงหรือไม่ ซึ่งการจ่ายค่าไถ่ ยิ่งเป็นการส่งเสริมให้องค์กรอาชญากรรมเหล่านี้มีปัจจัยในการกระทำผิดในอนาคตและยังไปสนับสนุนให้การขโมยตัวตน (identity theft) และการฉ้อโกงจากข้อมูลส่วนบุคคลยังคงดำเนินต่อไปได้ (Ahmed, 2020)

3) การแทรกซึมตลาดการค้าขององค์กรอาชญากรรมบนโลกออนไลน์

เป็นวิธีการที่องค์กรอาชญากรรมใช้ในการเข้าแสวงหากำไรจากเงื่อนไขหรือสภาวะของตลาดแบบใหม่หรือที่ผิดแผกออกไปจากเดิมได้อย่างรวดเร็วและมีประสิทธิภาพ โดยในช่วงที่เกิดการระบาดของโรคโควิด-19 ได้ทำให้องค์กรอาชญากรรมผันตัวเองมาสู่การแทรกซึม (infiltration) เข้าสู่ตลาด เพื่อเข้ามาหาส่วนแบ่งจากอุปสงค์ของตลาดที่กำลังขาดแคลนสินค้าอย่างอุปกรณ์การแพทย์ต่าง ๆ หน้ากากอนามัย แอลกอฮอล์ล้างมือ เครื่องช่วยหายใจ ชุดป้องกันพีพีอี (PPE) วัคซีนป้องกันโรคโควิด-19 อุปกรณ์ที่ต้องใช้

ในการฌาปณกิจ การทำความสะอาด การค้าทางออนไลน์ สินค้าที่เกี่ยวข้องกับเภสัชกรรม สินค้าและวัตถุดิบเกี่ยวกับการผลิตและจำหน่ายอาหาร เป็นต้น ด้วยการตั้งโรงงานผลิตหรือหาแหล่งผลิตสินค้าที่ต้องการและวางแผนการกระจายสินค้าได้อย่างรวดเร็ว เพราะอาศัยประสบการณ์และความได้เปรียบจากความร่วมมือและช่องทางการค้าที่องค์กรอาชญากรรมมีอยู่แล้วจากธุรกิจมืดอย่างการขายของปลอมหรือของลอกเลียนแบบ (counterfeit goods) และในอีกทางหนึ่ง องค์กรอาชญากรรมได้ใช้วิธีแทรกซึมทางเศรษฐกิจโดยการเข้าหาเจ้าของธุรกิจที่กำลังประสบปัญหาการเงินจากการระบาดของโรคโควิด-19 โดยไปปล่อยเงินกู้แล้วบังคับให้โอนกิจการหรือขอซื้อกิจการ แล้วเข้าเป็นเจ้าของธุรกิจที่ถูกกฎหมายเหล่านี้ ซึ่งทำให้องค์กรสามารถเข้าเป็นส่วนหนึ่งของห่วงโซ่อุปทานอย่างแนบเนียนและยังสามารถใช้ธุรกิจที่ถูกกฎหมายเหล่านี้เป็นฉากหน้าในการฟอกเงินได้อีกทางหนึ่ง (UNODC, n.d.)

และเนื่องจากข้อจำกัดในการเดินทาง การกระจายสินค้าส่วนใหญ่จะทำผ่านการขายในร้านค้าออนไลน์ ที่มุ่งเป้าไปยังผู้บริโภคทั่วไป ซึ่งสินค้าที่องค์กรอาชญากรรมผลิตหรือจัดหามาขายนั้นมักมีคุณภาพต่ำกว่ามาตรฐาน หรือไม่มีคุณภาพเลย (Marelli, 2020) โดยเมื่อช่วงเดือนมกราคม พ.ศ. 2564 องค์การตำรวจสากลได้ออกประกาศเตือนสีส้ม ถึงขบวนการปลอมแปลงวัคซีนโควิด-19 ที่จะหลอกขายให้แก่ประชาชน โดยเฉพาะอย่างยิ่งในช่องทางออนไลน์ (INTERPOL, 2020b) ซึ่งได้นำไปสู่การทลายและจับกุมขบวนการปลอมวัคซีนที่ทำมาเพื่อแอบอ้างขายทั้งในร้านค้าทั่วไปและทางออนไลน์ในประเทศแอฟริกาใต้ ซึ่งมีผู้ร่วมขบวนการเป็นชาวจีนและชาวแซมเบีย ขณะที่ประเทศจีนก็ได้ค้นพบและจับกุมแหล่งผลิตวัคซีนโควิด-19 ปลอมจำนวนกว่า 3,000 โดส ที่ทำจากน้ำผสมน้ำเกลือ และผู้ต้องสงสัยอีกกว่า 80 คน (INTERPOL, 2021) นอกจากนี้ หลายองค์กรยังใช้วิธีการกักตุนสินค้าเพื่อทำกำไรจากราคาขายปลีกที่สูงเกินกว่าที่กฎหมายกำหนด และการลักลอบนำเข้าหรือส่งออกสินค้าควบคุมไปยังพื้นที่ต่าง ๆ ดังเห็นได้จากการจับกุมและดำเนินคดีกลุ่มบุคคลที่กักตุนหน้ากากอนามัยและอุปกรณ์การแพทย์ในประเทศไทยเพื่อนำมาขายทางออนไลน์ ทั้งที่เป็นการนำเข้าและการผลิตในประเทศหลายครั้ง โดยองค์กรเหล่านี้มีองค์กรท้องถิ่นและองค์กรข้ามชาติ และมีนักการเมืองเข้ามาเกี่ยวพันเป็นผู้ต้องสงสัยอีกด้วย (PPTVHD36, 2020; Manager Online, 2020b) โดยเครือข่ายอาชญากรรมมากว่าร้อยละ 80 ใช้โครงสร้างธุรกิจที่ถูกกฎหมายในการกระทำอาชญากรรม (EUROPOL, 2021) ซึ่งในปี ค.ศ. 2020 องค์การตำรวจสากลได้เข้าขัดขวางการดำเนินการขององค์กรอาชญากรรมกว่า 37 องค์กรที่ทำการขายอุปกรณ์และเครื่องมือทางการแพทย์และยาที่เป็นอันตรายและผิดกฎหมายมูลค่ามากกว่า 14 ล้าน ดอลลาร์สหรัฐ ทั้งสินค้าที่ไม่มีใบอนุญาตและสินค้าปลอมซึ่งทำการขายผ่านช่องทางออนไลน์กว่า 2,000 เว็บไซต์ (UNODC, n.d.) ซึ่งอาชญากรรมประเภทนี้มีผลกระทบโดยตรงต่อความเป็นอยู่ของประชาชน การหลอกลวงซ้ำเติมสถานการณ์ให้แย่และขาดความมั่นคงยิ่งขึ้นไปอีก และส่งผลเสียต่อสุขภาพในระยะยาวด้วย

4) การละเมิดสิทธิมนุษยชนผ่านเครือข่ายออนไลน์

มาตรการจำกัดการเดินทางทำให้ผู้คนต้องอาศัยค้นหาสิ่งที่ตนเองต้องการจากทางออนไลน์ มาทดแทนในสิ่งที่ขณะนี้ไม่สามารถเข้าถึงได้ตามปกติ ซึ่งไม่ได้จำกัดเฉพาะแต่สินค้าและบริการโดยทั่วไปเท่านั้น แต่กลุ่มคนบางกลุ่มที่มีความต้องการเฉพาะหรือรสนิยมที่ผิดปกติก็เป็นกลุ่มเป้าหมายขององค์กรอาชญากรรมที่จะหาประโยชน์ทางการเงินจากกลุ่มคนประเภทนี้ โดยมาตรการสั่งปิดเมืองที่ขยายออกไปหลายครั้ง ทำให้ยอดการเข้าชมเว็บไซต์ที่เป็นสื่อมีเนื้อหาทางเพศอย่างพอร์นฮับ (PornHub) มีสถิติผู้เข้าชมมากขึ้นอย่างเห็นได้ชัด ซึ่งแม้ว่าพอร์นฮับจะเป็นเว็บไซต์ที่ถูกกฎหมายในสหรัฐอเมริกาและในหลายประเทศ แต่กระแสความต้องการชมเนื้อหาสื่อใหม่ ๆ อาจเป็นแรงจูงใจให้เกิดการแสวงประโยชน์อันมิชอบของ

องค์กรอาชญากรรมที่ช่วงนี้ไม่สามารถหารายได้จากธุรกิจเดิมอย่างการค้าประเวณี หรือยาเสพติดได้ อาจใช้อิทธิพลและการบังคับขู่เข็ญให้ผู้ค้าบริการทางเพศในสังกัดของตนเอง รวมไปถึงบุคคลที่อยู่ในกลุ่มเสี่ยงในท้องที่ขององค์กรอย่างผู้ใช้ยาเสพติด เด็กและเยาวชน หรือผู้ยากไร้ มาเข้าสู่วงจรธุรกิจทางเพศเพื่อทำการแสดงสดหรือถ่ายทำสื่อทางเพศต่าง ๆ โดยที่ไม่เต็มใจหรือไม่มีทางเลือกได้ (Global Initiative Against Transnational Organized Crime, 2020)

อีกธุรกิจหนึ่งที่เป็นอาชญากรรมร้ายแรงทางคอมพิวเตอร์มานานแล้ว แต่ช่วงการระบาดของโรคโควิด-19 ได้ไปเพิ่มโอกาสให้การขยายตัวของการกระทำผิดลักษณะนี้ให้เป็นไปได้ง่ายขึ้น คือ เว็บไซต์และเครือข่ายที่เก็บค่าสมาชิกในการเข้าดูสื่อและเนื้อหาเกี่ยวกับการแสวงประโยชน์ทางเพศจากเด็กโดยมิชอบ (child sexual exploitation) ซึ่งองค์กรอาชญากรรมสามารถเข้ามามีบทบาทในการตอบสนองความต้องการของกลุ่มบุคคลเหล่านี้ โดยอาศัยอิทธิพลและเงินทุนในการไปนำตัวเด็กและเยาวชนมาจากครอบครัวที่ยากจนเพื่อแลกกับเงิน รวมถึงการเข้าถึงเด็กและเยาวชนที่เรียนหนังสือ เล่นเกม และใช้เวลาทางออนไลน์ผ่านโซเชียลมีเดียมากขึ้นในช่วงที่ต้องอยู่บ้าน (ETDA, 2020) หรือไม่ได้รับการดูแลจากผู้ปกครองเพราะผู้ปกครองต้องถูกรักษาตัวในโรงพยาบาลจากโรคโควิด-19 อีกทั้ง เด็กและเยาวชนบางส่วนอาจถูกจำกัดให้อยู่ในสภาพที่ถูกทารุณกรรมโดยที่ไม่มีโอกาสที่บุคคลอื่นหรือหน่วยงานรัฐจะสามารถรับรู้และรายงานการกระทำผิดได้เช่นในขณะที่ยังสามารถไปเรียนได้ ซึ่งเด็กและเยาวชนอาจถูกบังคับให้กระทำการเกี่ยวกับทางเพศหรือถูกชักจูงล่อลวงด้วยวิธีการตระเตรียมเด็กเพื่อวัตถุประสงค์ทางเพศ (child grooming) จากทั้งองค์กรที่เป็นเจ้าของเครือข่ายเองและกลุ่มผู้ใช้เครือข่าย โดยสิ่งที่น่าเป็นห่วงในระยะยาว แม้หลังจากวิกฤตการณ์โรคโควิด-19 จะได้ผ่านพ้นไปแล้ว คือ บุคคลที่มีรสนิยมผิดปกติเหล่านี้ที่อยู่บ้านนานวันเข้าและได้ตัดสินใจเข้าสู่เครือข่ายการแสวงประโยชน์จากเด็กบนโลกออนไลน์จะยังคงเป็นสมาชิกในเครือข่ายอยู่และจะสร้างความเสียหายให้แก่สวัสดิการเด็กและเยาวชนได้มากขึ้นในอนาคตด้วย (Global Initiative Against Transnational Organized Crime, 2020; Radoini, 2020)

ความท้าทายในการป้องกันและปราบปรามองค์กรอาชญากรรมไซเบอร์ในช่วงเวลาการระบาดของโรคโควิด-19

องค์กรอาชญากรรมไซเบอร์นั้นเป็นรูปแบบการกระทำผิดที่ยากต่อการตรวจพบ สืบสวน และติดตามผู้กระทำผิดมาลงโทษอยู่แล้ว ยิ่งเมื่อเกิดสภาวะของโรคระบาดที่กระจายตัวไปในทั่วโลก ยิ่งทำให้การขยายตัวของรูปแบบอาชญากรรมนี้มีจำนวนมากขึ้น และมีความสลับซับซ้อนมากยิ่งขึ้น ด้วยสภาพของปัญหาที่อาชญากรรมไซเบอร์ ยังเป็นอาชญากรรมที่ไม่ค่อยได้ถูกรายงานให้แก่หน่วยงานรัฐทราบ ทำให้สถิติของการเกิดอาชญากรรมรูปแบบนี้จึงคาดการณ์ได้ว่ามีสูงกว่าตัวเลขที่มีอยู่อย่างแน่นอน นั่นหมายถึงปัญหาอาชญากรรมไซเบอร์ โดยเฉพาะอย่างยิ่งที่กระทำลงโดยองค์กรอาชญากรรมจึงเป็นปัญหาที่ยังต้องมีการศึกษาวิจัยเพิ่มเติมอีกมาก (EUROPOL, 2021) ความท้าทายของการป้องกันและปราบปรามยังประสบปัญหาด้วยการขาดกำลังพลที่จะเข้าไปแก้ไขปัญหา (DSI's Bureau of Development and Logistics, 2021) โดยเจ้าหน้าที่ผู้รักษากฎหมายมีจำนวนลดลงจากการติดเชื้อโควิด-19 และต้องรับมือกับปัญหาที่มีความเร่งด่วนเฉพาะหน้า เช่น การเสริมกำลังไปรักษามาตรการป้องกันโรคโควิด-19 และการประท้วงและชุมนุมทางการเมือง (Zivotic & Trajkovski, 2020) อีกทั้ง ยังขาดความเข้าใจในลักษณะการดำเนินงานและแรงจูงใจที่นอกเหนือไปจากเรื่องการเงินขององค์กรอาชญากรรมไซเบอร์ที่มีขอบเขตและความละเอียดอ่อนมากกว่าองค์กรอาชญากรรมแบบดั้งเดิม ซึ่งในการตอบสนองต่อปัญหานี้ ได้มีการเสนอแนะว่า

ควรสร้างความร่วมมือกันระหว่างหน่วยงานรัฐด้านการป้องกันและปราบปรามอาชญากรรมกับหน่วยงานด้านการวิจัยที่จะก่อให้เกิดองค์ความรู้ใหม่ไปใช้ในการแก้ไขปัญหานี้ (Leukfeldt & Holt, 2020) ประกอบกับการสร้างความเข้าใจกับเหยื่อบางกลุ่มและสร้างกฎหมายที่เหมาะสมเพื่อไม่ให้เป็นการสนับสนุนองค์กรอาชญากรรมไซเบอร์ไปมากกว่านี้ เช่นในกรณีของการเรียกค่าไถ่ผ่านไวรัสเรียกค่าไถ่ (Ahmed, 2020) นอกจากนี้ ยังต้องหาความสมดุลกันระหว่างการใช้กฎหมายที่มีอยู่เพื่อป้องกันและปราบปรามอาชญากรรมไซเบอร์โดยที่ไม่เป็นการละเมิดต่อสิทธิเสรีภาพส่วนบุคคลของประชาชนและสิทธิที่จะรับรู้ในข้อมูลข่าวสารด้วย ขณะเดียวกันรัฐบาลควรมุ่งเน้นให้ความสำคัญในการสร้างเกราะป้องกันแก่เหยื่อที่ขาดความคุ้มครองซึ่งเป็นกลุ่มที่ถูกโจมตีจากอาชญากรรมไซเบอร์มากที่สุด (Thailand Institute of Justice, 2020; DSI's Bureau of Development and Logistics, 2021)

บทสรุปและข้อเสนอแนะ

1) บทสรุป

องค์กรอาชญากรรมไซเบอร์นั้นสามารถสร้างความเสียหายได้มาก เพราะมีการดำเนินการทั้งการกระทำผิดขององค์กรอาชญากรรมเอง และการที่องค์กรอาชญากรรมไปสนับสนุนส่งเสริมการกระทำผิดทางคอมพิวเตอร์ของอาชญากรรายอื่นอีก รวมทั้งวัตถุประสงค์ของการกระทำผิดอาจจะไม่ได้จำกัดอยู่เฉพาะเพียงการหาประโยชน์ที่เป็นตัวเงินเท่านั้น แต่ยังมีวัตถุประสงค์เพื่อการเมือง เพื่อตอบสนองต่อความต้องการเฉพาะตัวขององค์กรหรือกลุ่มคนนั้น ๆ ด้วย

อย่างไรก็ตาม ในสภาวะของการแพร่ระบาดของโรคโควิด-19 ได้ทำให้องค์กรอาชญากรรมมีการเปลี่ยนแปลงและปรับตัวครั้งใหญ่ในการเปลี่ยนกลุ่มเป้าหมายมาเป็นเหยื่อที่ใช้อินเทอร์เน็ตมากยิ่งขึ้น เนื่องจากองค์กรอาชญากรรมรูปแบบดั้งเดิมที่อยู่ตามแหล่งการค้าและพาณิชย์ หรือที่กระทำการอาชญากรรมในพื้นที่อย่างการลักลอบขนสิ่งผิดกฎหมายต่าง ๆ ก็ได้รับผลกระทบจากมาตรการจำกัดการเดินทางของรัฐบาลเช่นกัน การเปลี่ยนแปลงกะทันหันเช่นนี้ ทำให้การป้องกันและปราบปรามกระทำได้ยากยิ่งขึ้นเพราะอาชญากรรมไซเบอร์มีอัตราการขยายตัวเพิ่มสูงขึ้นอย่างมาก สร้างภาระงานให้แก่หน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปราม (DSI's Bureau of Development and Logistics, 2021)

อีกทั้ง การที่อาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมได้เข้ามามีบทบาทในการกระทำผิดก็เป็นรูปแบบของกลยุทธ์ที่พัฒนาขึ้นมาใหม่ ทำให้ในขณะนี้ยังอาจไม่มีข้อมูลเพียงพอสำหรับการชี้ชัดลงไปว่าวิวัฒนาการขององค์กรอาชญากรรมไซเบอร์จะเป็นไปในทิศทางใดและมีความสลับซับซ้อนในการปกปิดมากเพียงใด

ในช่วงที่มีการแพร่ระบาดของโรคโควิด-19 การกระทำผิดหรือการสนับสนุนการกระทำอาชญากรรมไซเบอร์ใน 4 ประเภทหลักที่เพิ่มขึ้นเพราะการระบาดของโรคโควิด-19 ดังปรากฏสรุปในภาพที่ 1 ดังนี้

ภาพที่ 1 สรุปตัวอย่าง 4 อาชญากรรมไซเบอร์ที่องค์กรอาชญากรรมมีแนวโน้มเป็นผู้กระทำผิด

ซึ่งอาชญากรรมไซเบอร์เหล่านี้มักต้องดำเนินงานเป็นขบวนการเนื่องจากมีความซับซ้อนในการวางแผนและการปฏิบัติการและมีมูลค่าความเสียหายทั้งทางเศรษฐกิจและสังคมสูง จึงเป็นไปได้สูงว่าอาชญากรรมที่เพิ่มขึ้นเหล่านี้ส่วนหนึ่งมาจากการกระทำขององค์กรอาชญากรรมนั่นเอง

ด้วยสภาพปัญหาดังกล่าว นอกจากนี้ การป้องกันที่น่าจะมีประสิทธิภาพมากกว่า คือ การสร้างภูมิคุ้มกันให้แก่ประชาชนในด้านความปลอดภัยทางไซเบอร์ โดยจะเห็นได้ว่าเหยื่ออาชญากรรมไซเบอร์ จะเป็นกลุ่มที่ไม่เข้าใจความเสี่ยงของการใช้อินเทอร์เน็ต อย่างเด็ก เยาวชน ผู้สูงอายุ หรือ ผู้ที่ไม่เคยมีความรู้เกี่ยวกับการใช้อินเทอร์เน็ตอย่างจริงจัง รวมไปถึงกลุ่มองค์กรที่มีการใช้ข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลและข้อมูลด้านการสาธารณสุข โดยเฉพาะที่เกี่ยวข้องกับโรคโควิด-19 เมื่อนำมาประกอบกับสภาวะที่มีความไม่แน่นอนท่ามกลางความผันผวนของข้อมูลที่มีอยู่มากมายในอินเทอร์เน็ต ความวิตกกังวลที่เกี่ยวกับโรคระบาดและเศรษฐกิจ ย่อมเป็นปัจจัยส่งผลให้ผู้ที่ขาดความเข้าใจในความเสี่ยงทางไซเบอร์และกลุ่มองค์กรที่เป็นเป้าหมายของการหาประโยชน์จากโรคโควิด-19 ตกเป็นเหยื่อได้ง่ายขึ้น ดังนั้น ในสภาวะของการแพร่ระบาดของโรคโควิด-19 ซึ่งสร้างข้อจำกัดของรัฐในการบริหารงานอย่างเต็มที่ รัฐควรประชาสัมพันธ์ให้ทราบถึงความเสี่ยงเหล่านี้ให้มากยิ่งขึ้นด้วย

2) ข้อเสนอแนะ

(1) องค์กรอาชญากรรมไซเบอร์เป็นกลุ่มผู้กระทำผิดที่อาศัยความก้าวหน้าทางเทคโนโลยีและอินเทอร์เน็ต ทำให้พื้นที่การประกอบอาชญากรรมของกลุ่มอาชญากรเหล่านั้นเพิ่มขึ้นอย่างไม่มีขีดจำกัด โดยรัฐไม่อาจมองเห็นการกระทำผิดได้อย่างชัดเจนทั้งหมด ทำให้องค์กรอาชญากรรมไซเบอร์กลายเป็นปัญหาทั้งในระดับชาติและระดับนานาชาติที่จำเป็นต้องได้รับการแก้ไขเป็นระบบด้วย ดังนั้น ประเทศไทยควรยกระดับให้การป้องกันปราบปรามองค์กรอาชญากรรมไซเบอร์เป็นนโยบายระดับชาติ โดยเพิ่มความเข้มงวดมากขึ้นในการติดตามและป้องกันการกระทำผิดให้สอดคล้องกับสภาพปัญหาที่อยู่ในระดับข้ามชาติด้วย

(2) การขยายตัวขององค์กรอาชญากรรมไซเบอร์ แม้ไม่ใช่สิ่งใหม่ แต่ก็เป็นปรากฏการณ์ครั้งใหม่ที่องค์กรอาชญากรรมได้สร้างผลกระทบต่อสังคมได้มากขึ้นโดยอาศัยสถานการณ์การแพร่ระบาดของโรคโควิด-19 มาแสวงประโยชน์อันมิชอบกันอย่างเต็มที่โดยที่รัฐอาจไม่สามารถป้องกันและปราบปรามได้อย่างเต็มกำลังเท่าที่ควร (DSI's Bureau of Development and Logistics, 2021) ปัญหานี้ ได้สะท้อนให้เห็นว่า ประเทศไทยจะต้องมีระบบป้องกันทางไซเบอร์ที่ดี ซึ่งหมายถึง การให้ความรู้ความเข้าใจแก่ประชาชน และการสร้างระบบความปลอดภัยทางไซเบอร์ภายในประเทศให้มีประสิทธิภาพ ประกอบกันไปด้วยกับการปราบปรามอาชญากรรมที่ทันสมัยและอยู่บนพื้นฐานของการบูรณาการองค์ความรู้จากทั้งภาคปฏิบัติและภาคการวิจัยมาช่วยในการเอาชนะความพยายามขององค์กรอาชญากรรมไซเบอร์ที่มุ่งหมายจะยึดครองพื้นที่ทางออนไลน์ให้ได้มากขึ้น

(3) การป้องกันและปราบปรามควรต้องมีความสมดุลต่อสิทธิเสรีภาพขั้นพื้นฐานของประชาชนโดยทั่วไปที่ไม่ได้มีความเกี่ยวข้องกับองค์กรอาชญากรรมไซเบอร์ เช่น การติดตามข้อมูลการเข้าใช้เว็บไซต์หรือร่องรอยการเงินทางอินเทอร์เน็ต รวมไปถึงการใช้มาตรการติดตามสอดแนมผู้ต้องสงสัยในระดับต่าง ๆ ซึ่งรัฐจำเป็นต้องหามาตรการที่เหมาะสมมาปรับใช้ให้สามารถป้องปรามองค์กรอาชญากรรมได้โดยส่งผลกระทบต่อสิทธิเสรีภาพของประชาชนให้น้อยที่สุด

(4) เพื่อตอบสนองต่อนโยบายการป้องกันและปราบปรามองค์กรอาชญากรรมไซเบอร์ รัฐควรส่งเสริมความร่วมมือทั้งจากฝ่ายที่มีอำนาจหน้าที่และฝ่ายที่รวบรวมศึกษาข้อมูลในเชิงลึก เพื่อนำมาประกอบและวิเคราะห์หาแนวทางในการป้องกันและปราบปรามให้มีประสิทธิภาพยิ่งขึ้น

(5) จากการสำรวจสภาพของปัญหาและข้อมูลในปัจจุบันที่มีอยู่ ผู้เขียนได้พบว่า มีข้อมูลเชิงลึกในการศึกษาด้านองค์กรอาชญากรรมไซเบอร์ในบริบทของประเทศไทยอยู่น้อยมาก และยังไม่พบว่ามีการศึกษาถึงความสัมพันธ์ขององค์กรอาชญากรรมไซเบอร์ในประเทศไทยกับผลกระทบของการระบาดของโรคโควิด-19 ดังนั้น จึงควรมีการศึกษาถึงการปรับเปลี่ยนรูปแบบและวิธีการกระทำผิด เพื่อหาหนทางในการป้องกันและปราบปรามให้องค์กรอาชญากรรมไซเบอร์ลดบทบาทในทางเศรษฐกิจและสังคมยุคใหม่ในบริบทของประเทศไทยเป็นการเฉพาะต่อไป

เอกสารอ้างอิง

Ahmed, J. (2020). **Lockdowns Have Been Hard on Organized Crime, Too And a rise in cyber- ransoms is the result**. Retrieved March 3, 2021. from https://foreignpolicy.com/2020/10/07/ransom-hacking-cybercrime-pandemic-lockdowns-organized-crime/

Chankisen, T. (2021). **74% of Thai business had lower income from COVID-19 and 8 strategies to strengthen the business immunity**. Retrieved March 5, 2021. from https://thestandard.co/74percent-of-thai-businesses-lower-income-from-the-covid-19-crisis/. (In Thai).

Council of Europe. (2020). **Cybercrime and COVID-19**. Retrieved March 1, 2021. from https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19

Denni, M. A. (2019). **Cybercrime**. Retrieved March 3, 2021. from https://www.britannica.com/topic/cybercrime

DSI's Bureau of Development and Logistics. (2021). **The New Normal of Special Investigations**. Retrieved August 31, 2021. from https://www.dsi.go.th/Upload/41a4f341be9acaaf4876ad9fce01066f.pdf. (in Thai).

ETDA. (2020). **Thailand Internet User Behavior 2020**. Retrieved August 31, 2021. from https://www.etda.or.th/th/Useful-Resource/publications/Thailand-Internet-User-Behavior-2020.aspx. (in Thai).

EUROPOL & EUIPO. (n.d.). **Intellectual Property Crime Threat Assessment 2019**. Retrieved March 5, 2021. from https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_IP_Crime_Threat_Assessment_Report/ 2019_IP_Crime_Threat_Assessment_Report.pdf

EUROPOL. (2020). **Corona crimes: multi-million face mask scam foiled by police across Europe**. Retrieved March 5, 2021. from https://www.europol.europa.eu/

newsroom/news/corona-crimes-multi-million-face-mask-scam-foiled-police-across-europe

_____. (2021). **European Union Serious and Organised Crime Threat Assessment 2021.** Retrieved May 5, 2021. from https://www.europol.europa.eu/sites /default/files/documents/socta2021_5.pdf

Global Initiative Against Transnational Organized Crime. (2020). **Crime and contagion: The impact of a pandemic on organized crime**. Retrieved March 4, 2021. from https://globalinitiative.net/wp-content/uploads/2020/03/GI-TOC-Crime-and-Contagion-The-impact-of-a-pandemic-on-organized-crime-1.pdf

Grabosky, P. (2015). Organized Cybercrime and National Security. Smith, R. G., Cheung, R. C.-C., & Lau, L. Y.-C. (Eds.). **Cybercrime Risks and Responses**. (67-80). New York, US: Palgrave Macmillan.

INTERPOL. (2020a). **Cybercrime: COVID-19 Impact**. Retrieved March 5, 2021. from https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cyber crime%20Analysis%20Report-%20August%202020.pdf

_____. (2020b). **INTERPOL warns of organized crime threat to COVID-19 vaccines**. Retrieved March 1, 2021. from https://www.interpol.int/en/News-and-Events/ News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines

_____. (2021). **Fake COVID vaccine distribution network dismantled after INTERPOL alert**. Retrieved March 5, 2021. from https://www.interpol.int/en/ News-and-Events/News/2021/Fake-COVID-vaccine- distribution-network-dismantled-after-INTERPOL-alert

Khoasod Online. (2020). **Immigration Bureau arrested Nigerian call center gang, found over 280M bahts in money circulation**. Retrieved March 3, 2021. from, https://www.khaosod.co.th/update-news/news_4254955. (In Thai).

Laohong, K. (2021). **DSI targets Chinese loan sharks**. Retrieved March 5, 2021. from https://www.bangkokpost.com/thailand/general/2051055/dsi-targets-chinese-loan-sharks

Leukfeldt, E. R. & Holt, Thomas J. (2020). Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline. **International Journal of Offender Therapy and Comparative Criminology**, 64(5), 522-538.

Manager Online. (2020a). **Ministry of Finance warns citizens falling victims to Fake News "Dangerous phone numbers deceive about government aids to steal money from bank account"**. Retrieved March 5, 2021. from https://mgronline.com/stockmarket/detail/9630000119874. (In Thai).

_____. (2020b). **Arrested 2 Chinese guys for hoarding over 60,000 face mask to sell online**. Retrieved March 5, 2021. from https://mgronline.com/crime/detail/9630000036707. (In Thai).

Marelli, F. (2020). How organized crime is expanding during the COVID-19 crisis. **Freedom From Fear (F3) Magazine**, 00(16), 6-10. Retrieved March 5, 2021. from https://issuu.com/unicri/docs/f3_discover_our_fragility

Matichon Online. (2020). **Dissecting the 'money laundering' model, economic crime**. Retrieved March 5, 2021. from https://www.matichon.co.th/economy/news_2491379. (In Thai).

McGee, M. K. (2020). **Interpol: Organized Crime to Capitalise on COVID-19 Vaccines**. Retrieved March 5, 2021. from https://www.bankinfosecurity.com/interpol-a-15499

PPTVHD36. (2020). **CPPD raided "Punyot" for face mask hoarding – selling case**. Retrieved March 3, 2021. from https://www.pptvhd36.com/news/ประเด็นร้อน/123147. (In Thai).

Radoini, A. (2020). Cyber-crime during the COVID-19 Pandemic. **Freedom From Fear (F3) Magazine**, 00(16), 6-10. Retrieved March 5, 2021. from https://issuu.com/unicri/docs/f3_discover_our_fragility

Somkamnerd, N. and Terdudomtham, T. (2019). Transnational Crime: Credit Card Crime Using by Russian and East European (Commonwealth of Independent States) Criminals in Thailand. **Journal of Criminology and Forensic Science**, 5(2), 222-238. (In Thai).

Thailand Institute of Justice. (2020). **Experts are confident cybersecurity threat lurks in the new normal. To thrive, organizations must design resilient system that can function if attacked**. Retrieved March 5, 2021. from https://www.tijthailand.org/en/highlight/detail/cybercrime-covid-19

Tropina, T. (2010). Cyber Crime and Organized Crime. **Freedom From Fear (F3) Magazine**, 00(7), 16-17. Retrieved March 3, 2021. from http://f3magazine.unicri.it/wp-content/uploads/F3_07.pdf

_____. (2012). The Evolving Structure of Online Criminality: How Cybercrime Is Getting Organised. **Eucrim**, 00(4), 158-165. Retrieved March 5, 2021. from https://eucrim.eu/media/issue/pdf/eucrim_issue_2012-04.pdf#page=20

UNODC. (n.d.). **The impact of COVID-19 on organized crime**. Retrieved March 2, 2021. from https://www.unodc.org/documents/data-and-analysis/covid/RB_COVID_organized_crime_july13_web.pdf

_____. (2018). **Defining organized crime**. Retrieved March 3, 2021. from https://www.unodc.org/e4j/en/organized-crime/module-1/key-issues/defining-organized-crime.html

_____. (2019). **Cyber organized crime: What is it?**. Retrieved March 2, 2021. from https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

Volz, D. & McMillan, R. (2020). **Hackers Hit Hospitals in Disruptive Ransomware Attack**. Retrieved March 4, 2021. from https://www.wsj.com/articles/hackers-hit-hospitals - in-disruptive-ransomware-attack-11603992735

Zivotic, I. & Trajkovski, Daniela. (2020). Adaptability of Organized Criminal Groups to the Situation Caused by the Covid 19 Pandemic. **Knowledge International Journal**, 43(5), 1003 - 1006. Retrieved August 31, 2021. From https://ikm.mk/ojs/index.php/KIJ/article/view/4810

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล	**ร้อยตำรวจเอก ฐกฤต แก้วทับทิม ***
ตำแหน่ง/สถานะ	นักศึกษาปริญญาเอก
ที่อยู่หน่วยงาน/สังกัด	หลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาการบริหารงานยุติธรรมและสังคม คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล อ.พุทธมณฑล จ.นครปฐม 73170
ไปรษณีย์อิเล็กทรอนิกส์	takritk@gmail.com

* ผู้ประพันธ์บรรณกิจ (Corresponding Author)