การทำให้ภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย: ศึกษากรณีแก๊งคอลเซ็นเตอร์และการรับมือต่อปัญหาของกองบัญชาการตำรวจไซเบอร์ในช่วงปีพ.ศ.2563-2567

THAILAND'S SECURITIZATION OF CYBER THREATS: A CASE STUDY OF CALL-CENTER GANGSTERS AND THE RESPONSE OF CYBER CRIME INVESTIGATION BUREAU DURING 2020 - 2024

พงศ์ศักร์ ฉันทสิริสวัสดิ์

บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ

2566

การทำให้ภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย: ศึกษากรณีแก๊งคอลเซ็นเตอร์และการรับมือต่อปัญหาของกองบัญชาการตำรวจไซเบอร์ในช่วงปีพ.ศ.2563-2567

พงศ์ศักร์ ฉันทสิริสวัสดิ์

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
รัฐศาสตรมหาบัณฑิต สาขาวิชาการทูตและความสัมพันธ์ระหว่างประเทศ
คณะสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
ปีการศึกษา 2566

THAILAND'S SECURITIZATION OF CYBER THREATS: A CASE STUDY OF CALL-CENTER GANGSTERS AND THE RESPONSE OF CYBER CRIME INVESTIGATION BUREAU DURING 2020 - 2024

PONGSAK CHANTASIRISAWAT

A Master's Project Submitted in Partial Fulfillment of the Requirements

for the Degree of MASTER OF POLITICAL SCIENCE

(Diplomacy and International Relations)

Faculty of Social Sciences, Srinakharinwirot University

2023

สารนิพนธ์

เรื่อง

การทำให้ภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย: ศึกษากรณีแก๊งคอลเซ็นเตอร์และการรับมือต่อปัญหาของกองบัญชาการตำรวจไซเบอร์ในช่วงปีพ.ศ.2563-2567

ของ

พงศ์ศักร์ ฉันทสิริสวัสดิ์

ได้รับอนุมัติจากบัณฑิตวิทยาลัยให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญารัฐศาสตรมหาบัณฑิต สาขาวิชาการทูตและความสัมพันธ์ระหว่างประเทศ
ของมหาวิทยาลัยศรีนครินทรวิโรฒ

(รองศาสตราจารย์ นายแพทย์ฉัตรชัย เอกปัญญาสกุล)
คณบดีบัณฑิตวิทยาลัย

คณะกรรมการสอบปากเปล่าสารนิพนธ์

..... ที่ปรึกษาหลัก
(รองศาสตราจารย์ ดร.ศิพิมพ์ ศรบัลลังก์)

..... ประธาน
(อาจารย์ ดร.ศิบดี นพประเสริฐ)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.จิราพร ร่วมพงษ์พัฒนะ)

ชื่อเรื่อง	การทำให้ภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย: ศึกษากรณีแก๊งคอลเซ็นเตอร์และการรับมือต่อปัญหาของกองบัญชาการตำรวจไซเบอร์ในช่วงปีพ.ศ.2563-2567
ผู้วิจัย	พงศ์ศักร์ ฉันทสิริสวัสดิ์
ปริญญา	รัฐศาสตรมหาบัณฑิต
ปีการศึกษา	2566
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร. ศิพิมพ์ ศรบัลลังก์

สารนิพนธ์เรื่อง “การทำให้ภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย : ศึกษากรณีแก๊งคอลเซ็นเตอร์และการรับมือต่อปัญหาของกองบัญชาการตำรวจไซเบอร์ในช่วงปี พ.ศ.2563-2567” ฉบับนี้ มีวัตถุประสงค์สำคัญ 2 ประการ คือ 1) เพื่อศึกษากระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง และ 2) เพื่อศึกษาแนวทางการรับมือเพื่อจัดการปัญหาภัยคุกคามทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจไซเบอร์ โดยงานวิจัยชิ้นนี้เป็นงานวิจัยเชิงคุณภาพ ซึ่งผู้วิจัยได้เก็บรวบรวมข้อมูลทั้งจากเอกสารและบทความที่เกี่ยวข้อง ตลอดจนผู้ให้ข้อมูลคนสำคัญ โดยใช้แนวคิดการทำให้เป็นปัญหาความมั่นคง (securitization) เป็นกรอบในการวิเคราะห์ผลการศึกษา สำหรับผลการศึกษาพบว่า กระบวนการทำให้แก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงเป็นส่วนหนึ่งของการทำให้ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของรัฐไทย โดยผ่านตัวแสดงที่ทำหน้าที่ในการกำหนดประเด็นความมั่นคง (securitizing actor) ที่สำคัญ ได้แก่ นายกรัฐมนตรี ทั้งสองคนในช่วงปีพ.ศ.2563-2567 คือ พลเอกประยุทธ จันทรโอชา และนายเศรษฐา ทวีสิน ผ่านการถ่ายทอดชุดวาทกรรมที่ทำให้ปัญหาดังลกล่าวกลายเป็นปัญหาความมั่นคงที่สำคัญของไทย โดยกระบวนการทำให้เป็นปัญหาความมั่นคงดังกล่าวในกรณีของแก๊งคอลเซ็นเตอร์ยังได้นำไปสู่แนวทางในการรับมือของกองบัญชาการตำรวจไซเบอร์อย่างเป็นระบบด้วย

คำสำคัญ : การทำให้เป็นประเด็นความมั่นคง ภัยคุกคามทางไซเบอร์

Title	THAILAND'S SECURITIZATION OF CYBER THREATS: A CASE STUDY OF CALL-CENTER GANGSTERS AND THE RESPONSE OF CYBER CRIME INVESTIGATION BUREAU DURING 2020 - 2024
Author	PONGSAK CHANTASIRISAWAT
Degree	MASTER OF POLITICAL SCIENCE
Academic Year	2023
Thesis Advisor	Associate Professor Dr. Sipim Sornbanlang

The individual study titled "THAILAND'S SECURITIZATION OF CYBER THREATS: A CASE STUDY OF CALL-CENTER GANGSTERS AND THE RESPONSE OF THE CYBER CRIME INVESTIGATION BUREAU DURING 2020-2024" aims to achieve two primary objectives: (1) To examine the securitization of the call-center gangster problem, and (2) To analyze the response of the Cyber Crime Investigation Bureau to the call-center gangsters. Employing a qualitative research methodology, the study gathers data from a range of documents, related articles, and key informants. The analysis is framed using the concept of securitization. The findings indicate that the securitization of call-center gangsters is a component of Thailand's broader cyber threat securitization strategy. This process involves key securitizing actors, including the two Prime Ministers during the 2020-2024 period: General Prayuth Chan-o-cha and Mr. Settha Thaweesin. Through their speech acts, these leaders have elevated the issue of call-center gangsters to the level of national security concern. Consequently, this securitization has prompted a systematic response from the Cyber Crime Investigation Bureau.

Keyword : Securitization Cyber Threat

กิตติกรรมประกาศ

ผู้วิจัยขอขอบพระคุณผู้มีส่วนทำให้สารนิพนธ์ฉบับนี้สำเร็จได้อย่างสมบูรณ์ ได้แก่ รศ.ดร. ศิพิมพ์ ศรบัลลังก์ ที่ปรึกษาสารนิพนธ์ ที่ได้กรุณาให้ข้อเสนอแนะที่เป็นประโยชน์และสนับสนุนให้ผู้วิจัยได้พัฒนาทักษะในการวิจัยอย่างสม่ำเสมอ นอกจากนี้ ผู้วิจัยยังขอขอบพระคุณคณาจารย์ทุกท่านในหลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชาการทูตและความสัมพันธ์ระหว่างประเทศ ภาควิชารัฐศาสตร์ คณะสังคมศาสตร์ มศว ที่ได้ให้ความรู้ตลอดการศึกษาในระดับปริญญาโทของผู้วิจัย ทำให้ผู้วิจัยได้เปิดโลกทัศน์ด้านการทูต การต่างประเทศ และความมั่นคง ตลอดจนได้จุดประกายให้ผู้วิจัยได้สนใจในหัวข้อความมั่นคงทางไซเบอร์และนำไปสู่การทำสารนิพนธ์ในเรื่องดังกล่าว อย่างไรก็ตาม การเรียน ณ มศว แห่งนี้จะไม่สำเร็จได้เลยหากผู้วิจัยไม่มีกัลยาณมิตรในหลักสูตร MAIR SWU รุ่นที่ 1 ที่ได้ช่วยเหลือเกื้อกูล และนำพาให้พวกเราบรรลุเป้าหมายของการเรียนได้เป็นอย่างดี ผู้วิจัยจึงขอขอบคุณกัลยาณมิตรทุกท่านที่มีส่วนร่วมในการศึกษาและการทำสารนิพนธ์ของผู้วิจัยทั้งหมด มา ณ ที่นี้ ด้วย

พงศ์ศักร์ ฉันทสิริสวัสดิ์

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

No table of figures entries found.

บทที่ 1

ความสำคัญของปัญหา คำถาม สมมติฐาน และวัตถุประสงค์

1.1 ความสำคัญของปัญหา

ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงในรูปแบบใหม่ที่ทวีความสำคัญมากขึ้นในปัจจุบัน ดังจะเห็นได้จากปัญหาอาชญากรรมทางไซเบอร์ การหลอกลวงเงินจากคอลเซ็นเตอร์ การโจมตีทางดิจิทัล ฯลฯ ขณะเดียวกัน ในช่วงหลายปีที่ผ่านมามีการทำธุรกรรมออนไลน์เพิ่มมากขึ้นเรื่อย ๆ วิถีชีวิตประจำวันของประชาชนเข้าสู่โลกออนไลน์มากขึ้น ส่งผลทำให้เจอกับความสุ่มเสี่ยงและอาชญากรรมในโลกออนไลน์มากขึ้นเช่นกัน ทั้งนี้ จะเห็นได้ว่าท่ามกลางความเปลี่ยนแปลงตลอดหลายปีที่ผ่านมานี้ การมีอาชญากรรมไซเบอร์เพิ่มมากขึ้น ทำให้องค์กรตำรวจต้องปรับตัวในการทำงาน เพื่อรับมือกับภัยคุกคามดังกล่าว และนำไปสู่การจัดการปัญหาต่างๆที่เกี่ยวข้องได้อย่างมีประสิทธิภาพมากขึ้น ดังจะเห็นได้จากการออกกฎหมายที่เกี่ยวข้อง การตั้งหน่วยงานรับผิดชอบกับภัยคุกคามทางไซเบอร์ การตั้งหน่วยงานที่ชื่อว่า กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)" หรือเป็นที่รู้จักในชื่อ "กองบัญชาการตำรวจไซเบอร์" เมื่อปี พ.ศ. 2563 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ. 2563

ในช่วงที่ผ่านมาจะพบกรณีปัญหาภัยคุกคามทางไซเบอร์ในรูปแบบอาชญากรรมจากแก๊งคอลเซ็นเตอร์เพิ่มขึ้นเรื่อย ๆ โดยประชาชนจำนวนมากตกเป็นเหยื่อและสูญเสียเงินจำนวนมาก โดยจากข้อมูลของศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติพบว่า มีการรับแจ้งความคดีออนไลน์ระหว่าง 1 มีนาคม 2565 – 31 กรกฎาคม 2566 ถึง 302,836 เรื่อง สร้างความเสียหายกว่า 4 หมื่นล้านบาท (สำนักข่าวอิศรา, 2566) โดยส่วนใหญ่จะมีรูปแบบคล้ายคลึงกันคือการแอบอ้างเป็นเจ้าหน้าที่รัฐและหลอกให้เหยื่อโอนเงินให้ภายในระยะเวลาอันรวดเร็ว ซึ่งกล่าวได้ว่าปรากฏการณ์ที่เกิดขึ้นนี้ได้ส่งผลทำให้กองบัญชาการตำรวจไซเบอร์มีมาตรการในการทำให้ปัญหาดังกล่าวเป็นปัญหาความมั่นคงและนำไปสู่มาตรการต่างๆของกองบัญชาการตำรวจไซเบอร์ในการรับมือกับปัญหานี้ซึ่งถือเป็นปัญหาที่สำคัญยิ่งในปัจจุบัน ทำให้เกิดคำถามต่อผู้วิจัยว่า กองบัญชาการตำรวจไซเบอร์มีกระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงอย่างไร และจากการทำให้ประเด็นดังกล่าวเป็นปัญหาความมั่นคงนี้ กองบัญชาการตำรวจ

ไซเบอร์ได้มีแนวทางในการจัดการกับปัญหาดังกล่าวอย่างไร เพื่อให้หน่วยงานสามารถรับมือกับปัญหาได้อย่างมีประสิทธิภาพและช่วยให้ประชาชนไม่ต้องตกเป็นเหยื่ออาชญากรรมไซเบอร์ในรูปแบบดังกล่าวอีก

ปัญหาแก๊งคอลเซ็นเตอร์ ถือเป็นอาชญากรรมทางเศรษฐกิจที่พบเห็นได้มากขึ้นเรื่อย ๆ ในยุคดิจิทัล และแม้ว่าภาครัฐและสื่อมวลชนจะพยายามสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามชนิดนี้อย่างต่อเนื่อง แต่ก็ยังพบว่ามีประชาชนตกเป็นเหยื่อถูกหลอกโดยแก๊งคอลเซ็นเตอร์อยู่เสมอ จะเห็นได้ว่ากลุ่มคอลเซ็นเตอร์เองก็มีพัฒนาการของการก่ออาชญากรรมที่เปลี่ยนแปลงไปเรื่อย ๆ เมื่อวิธีการหนึ่งถูกตีแผ่ ก็จะมีการพัฒนาวิธีการหลอกลวงใหม่เพิ่มขึ้นมา อีกทั้งยังวางแผนเน้นหลอกเหยื่อกลุ่มผู้สูงอายุ ผู้ที่ไม่มีความรู้ด้านเทคโนโลยีมากนัก กลุ่มผู้เปราะบางต่าง ๆ ไม่เพียงเฉพาะการหลอกลวงโดยตรงผ่านทางโทรศัพท์เท่านั้น ปัญหาของแก๊งคอลเซ็นเตอร์เกี่ยวข้องกับกลุ่มอาชญากรรมข้ามชาติ เกี่ยวข้องกับการค้ามนุษย์ และขบวนการฟอกเงินด้วย ความเสียหายทางเศรษฐกิจในระดับปัจเจกบุคคลและความเสียหายต่อเศรษฐกิจในภาพรวมของประเทศทำให้ปัญหาการหลอกลวงทางโทรศัพท์กลายเป็นอาชญากรรมทางเศรษฐกิจข้ามชาติที่เป็นภัยร้ายแรง (อาริยา สุขโต, 2565)

1.2 **คำถามการวิจัย**

1) การทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงของกองบัญชาการตำรวจมีกระบวนการอย่างไร
2) การทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงนำไปสู่แนวทางในการรับมือเพื่อจัดการกับปัญหาดังกล่าวของกองบัญชาการตำรวจไซเบอร์อย่างไร

1.3 **สมมติฐาน**

กระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง (Securitization) ของกองบัญชาการตำรวจไซเบอร์ได้สร้างความตระหนักรู้ถึงภัยคุกคามจากอาชญากรรมประเภทนี้จากการกล่าวถึงมูลค่าความเสียหายที่เกิดจากปัญหาดังกล่าวจำนวนมาก นำไปสู่แนวทางการรับมือเพื่อจัดการปัญหาภัยคุกคามทางไซเบอร์โดยกองบัญชาการตำรวจไซเบอร์อย่างเป็นระบบ

1.4 วัตถุประสงค์ในการวิจัย

1) เพื่อศึกษากระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมมั่นคง
2) เพื่อศึกษาแนวทางการรับมือเพื่อจัดการปัญหาภัยคุกคามทางไซเบอร์จากแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจไซเบอร์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) ทำให้เข้าใจบทบาทหน้าที่และกลไกการทำงานของตำรวจไซเบอร์และแนวทางในการจัดการปัญหาภัยคุกคามทางไซเบอร์ของไทยในกรณีแก๊งคอลเซ็นเตอร์
2) ทำให้ผู้มีหน้าที่เกี่ยวข้องมีความตื่นตัวในการปกป้องและจัดการภัยคุกคามทางไซเบอร์
3) ทำให้ประชาชนตระหนักรู้และตื่นตัวในการป้องกันภัยคุกคามทางไซเบอร์มากขึ้น

1.6 แนวคิดและทฤษฎีที่ใช้ในการวิจัย

ในการวิจัยนี้ ผู้วิจัยจะใช้ทฤษฎีหลักในการวิจัยคือแนวคิดการทำให้เป็นปัญหาความมั่นคง (securitization) ซึ่งมีองค์ประกอบ 6 ประการ คือ (Barry Buzan, 1998)[1]

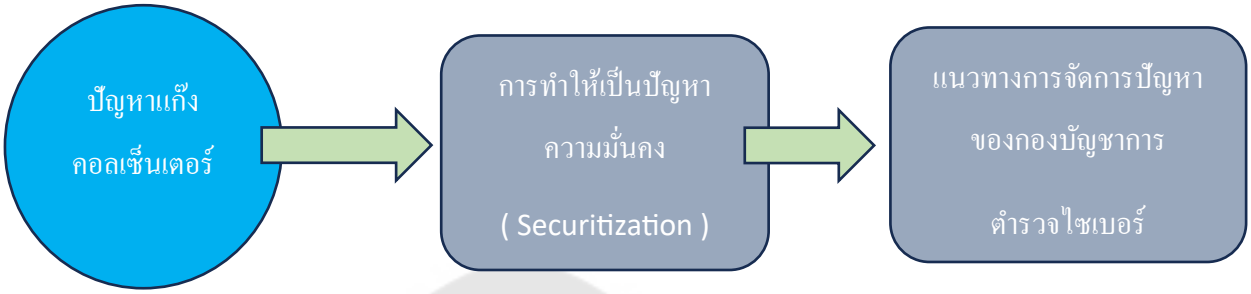
1) Existential threat หมายถึง สิ่งที่เป็นภัยคุกคาม
2) Referent object หมายถึง สิ่งที่เป็นวัตถุอ้างอิงหรือได้รับการคุกคามจากสิ่งๆหนึ่ง
3) Securitizing actor หมายถึง ตัวแสดงที่ทำหน้าที่ทำให้เป็นปัญหาความมั่นคง
4) Speech act หมายถึง วาทกรราที่ใช้ในการทำให้เป็นปัญหาความมั่นคง
5) Audience หมายถึง ผู้ฟังที่คล้อยตามวาทกรรมของตัวแสดงที่ทำหน้าที่ทำให้เป็นปัญหาความมั่นคง
6) Facilitating conditions หมายถึง เงื่อนไขที่ทำให้การทำให้เป็นปัญหาความมั่นคงสำเร็จ

โดยหากจะศึกษาเกี่ยวกับกระบวนการทำให้เป็นปัญหาความมั่นคงจะต้องอธิบายถึงองค์ประกอบทั้ง 6 ประการดังกล่าวข้างต้นให้ครบถ้วน โดยหากกระบวนการทำให้เป็นปัญหาความมั่นคงประสบผลสำเร็จ จะนำไปสู่แนวทางในการจัดการปัญหาดังกล่าวของรัฐในเวลาต่อมา

1.7 กรอบคิดในการวิจัย

งานวิจัยนี้ ได้ใช้ทฤษฎีหลักในการวิเคราะห์ คือ ทฤษฎีการทำให้เป็นปัญหาความมั่นคง เพื่อสะท้อนให้เห็นถึงกระบวนการในการกำหนดปัญหาภัยคุกคามทางไซเบอร์ กรณีแก๊งคอลเซ็น

เตอร์ ให้เป็นปัญหาความมั่นคงของรัฐ และนำไปสู่มาตรการในการจัดการปัญหาของหน่วยงานตำรวจคือกองบัญชาการตำรวจไซเบอร์ โดยมีกรอบคิดในการวิจัย ดังต่อไปนี้



ตาราง 1 แสดงกรอบคิดการทำให้เป็นประเด็นความมั่นคงในการวิจัย

งานวิจัยชิ้นนี้เป็นงานวิจัยเชิงคุณภาพ โดยประกอบไปด้วยการเก็บข้อมูลจาก 2 ส่วนที่สำคัญ ได้แก่ แหล่งข้อมูลปฐมภูมิ และแหล่งข้อมูลทุติยภูมิ โดยข้อมูลแบบทุติยภูมิจะทำการค้นคว้าข้อมูลจากอินเตอร์เนต หนังสือ บทความ และเอกสารที่เกี่ยวข้องต่างๆ เกี่ยวกับประเด็นปัญหาความมั่นคงทางไซเบอร์และกรณีแก๊งคอลเซ็นเตอร์ ขณะที่แหล่งข้อมูลปฐมภูมิจะเป็นการค้นคว้าข้อมูลจากการสัมภาษณ์ผู้ที่เกี่ยวข้องกับกระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงของกองบัญชาการตำรวจไซเบอร์ และผู้ตกเป็นเหยื่อแก๊งคอลเซ็นเตอร์ โดยเป็นผู้สูญเสียเงินหรือทรัพย์สินมูลค่าตั้งแต่ 1,000,000 บาทขึ้นไป

สำหรับขอบเขตการวิจัย ผู้วิจัยได้กำหนดเป็น 2 ส่วนดังนี้

1) ขอบเขตด้านเวลา: กำหนดขอบเขตการศึกษาในช่วง พ.ศ.2563 - 2567 นับตั้งแต่มีการก่อตั้งหน่วยงานกองบัญชาการตำรวจไซเบอร์
2) ขอบเขตด้านพื้นที่: กำหนดพื้นที่ในการศึกษาในพื้นที่ประเทศไทย เนื่องจากกรณีแก๊งคอลเซ็นเตอร์มีเหยื่อจากทั่วประเทศ

1.8 นิยามศัพท์

แก๊งคอลเซ็นเตอร์ หมายถึง อาชญากรรมทางเศรษฐกิจรูปแบบหนึ่งที่มีลักษณะเป็นการฉ้อโกงประชาชน โดยมักอาศัยช่องทางความตื่นกลัวและความโลภของเหยื่อเป็นปัจจัยหลักในการ

หลอกลวงให้หลงเชื่อ ส่วนใหญ่มักใช้วิธีการหลอกลวงเหยื่อผ่านการพูดคุยทางโทรศัพท์ประกอบกับการใช้แอปพลิเคชั่นทางการเงิน ซึ่งหากเหยื่อหลงเชื่อจะนำมาซึ่งการสูญเสียเงินจำนวนมากในคราวเดียว (อาริยา สุขโต, 2565)

บทที่ 2

บททบทวนวรรณกรรมและเอกสารที่เกี่ยวข้อง

แต่เดิมนั้น รัฐมองปัญหาภัยคุกคามในด้านนี้เป็นอาชญากรรมรูปแบบเดิม ในลักษณะ การหลอกลวง ฉ้อโกง กรรโชกทรัพย์ แต่เมื่อกลุ่มผู้กระทำผิดได้พัฒนารูปแบบการกระทำผิดด้วยการนำระบบคอมพิวเตอร์ หรือเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้องมาใช้ในกระบวนการ เป็นการกระทำผิดที่มีรูปแบบเป็น Organized Crime มากขึ้นจนพัฒนามาเป็นลักษณะของอาชญากรรมข้ามชาติเกี่ยวข้องกับปัญหาอื่น ๆ แบบข้ามชาติ รัฐจึงต้องมีการปรับตัวเพื่อรับมือกับภัยคุกคามดังกล่าว โดยต้องทำให้ประเด็นดังกล่าวเป็นปัญหาความมั่นคง มีการออกกฎหมาย และจัดตั้งหน่วยงานรับผิดชอบเพื่อรับมือกับภัยคุกคามใหม่นี้ ตลอดจนมีความร่วมมือกับฝ่ายต่างประเทศเพื่อร่วมกันแก้ไขปัญหาในกรณีที่การกระทำผิดในประเทศไทยมีฐานการกระทำผิดอยู่ในประเทศอื่น

ประเด็นด้านความมั่นคงทางไซเบอร์นับเป็นประเด็นการศึกษาใหม่ ที่ยังคงมีงานวิชาการที่เกี่ยวข้องอย่างจำกัด งานวิชาการส่วนใหญ่ที่พบเป็นการศึกษาเกี่ยวกับผลกระทบจากปัญหาความมั่นคงทางไซเบอร์ต่อภาคส่วนต่างๆ อาทิ ผลกระทบต่อภาคการเงินการธนาคาร และผลกระทบต่อคนในสังคมยุคดิจิทัลที่ต้องเผชิญกับภัยคุกคามทางไซเบอร์ในรูปแบบที่แตกต่างหลากหลาย นอกจากนี้ยังพบงานวิชาการในประเด็นที่เกี่ยวข้องกับกฎหมาย โดยเน้นไปที่การศึกษากฎหมายความผิดเกี่ยวกับคอมพิวเตอร์และอาชญากรรมทางไซเบอร์ รวมไปถึงการศึกษากฎหมายดิจิทัล[ii] อย่างไรก็ตาม แม้ว่าประเด็นความมั่นคงทางไซเบอร์จะเป็นประเด็นที่มีความสำคัญอย่างมากในบริบทโลกปัจจุบัน ทว่า งานวิชาการที่ศึกษาเกี่ยวกับความมั่นคงทางไซเบอร์ในมุมมองของรัฐยังมีไม่มากนัก โดยการศึกษาส่วนใหญ่มุ่งเน้นไปที่การรับมือภัยคุกคามทางไซเบอร์ของบางหน่วยงานของรัฐ โดยมีงานศึกษาที่เกี่ยวกับการรับมือของกระทรวงกลาโหมและกองทัพไทย ดังจะเห็นได้จากงานของ นิรุจ ดวงปัญญา และธาราทิพย์ กัลยาณมิตร ได้ศึกษาถึงแนวทางการพัฒนากองทัพไทยในด้านการรักษาความมั่นคงทางไซเบอร์ (สาวตรี สุขศรี, 2563) และงานของ ศิวลีย์ สิริโรจน์บริรักษ์ที่ได้ศึกษามาตรการการรักษาความมั่นคงทางไซเบอร์ของกระทรวงกลาโหม (ศิวลีย์ สิริโรจน์บริรักษ์, 2557) อย่างไรก็ตาม งานวิชาการที่ศึกษาถึงบทบาทของตำรวจซึ่งเป็นส่วนหนึ่งของฝ่ายความมั่นคงในการรับมือกับภัยคุกคามทางไซเบอร์ซึ่งเกี่ยวข้องกับชีวิตประจำวันของประชาชนยังมี

อยู่น้อยมากหรือแทบจะไม่มีเลย โดยแม้ว่าจะได้มีการก่อตั้ง “ตำรวจไซเบอร์” หรือกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีภายใต้การกำกับดูแลของสำนักงานตำรวจแห่งชาติ (บช.สอท.) ขึ้น แต่ก็ยังไม่มีงานวิชาการใดที่มีการศึกษาถึงบทบาทของตำรวจในการรับมือกับปัญหาความมั่นคงไซเบอร์อย่างเฉพาะเจาะจง

ในส่วนของภารกิจและความรับผิดชอบของ "กองบัญชาการตำรวจไซเบอร์" ซึ่งอยู่ภายใต้การกำกับของสำนักงานตำรวจแห่งชาตินั้นมีหน้าที่ในการรับผิดชอบสืบสวนสอบสวน รวบรวมพยานหลักฐานในคดีที่มีความซับซ้อนหรือเป็นอาชญากรรมทางเทคโนโลยีที่สำคัญ ได้แก่ (สุภาพิชญ์ ถิระวัฒน์, กองบัญชาการตำรวจไซเบอร์, 2564)

1) คดีเกี่ยวกับทรัพย์ซึ่งมีมูลค่าความเสียหายตั้งแต่ 30 ล้านบาทขึ้นไป
2) คดีเกี่ยวกับทรัพย์ที่มีจำนวนผู้เสียหายรวมกันตั้งแต่ 50 คนขึ้นไป
3) คดีเกี่ยวกับทรัพย์ที่มีทั้งมูลค่าความเสียหาย 10 ล้านบาทขึ้นไปและมีจำนวนผู้เสียหายตั้งแต่ 10 คนขึ้นไป
4) คดีที่มีการกระทำความผิดเป็นขบวนการหรือกลุ่มบุคคลซึ่งต้องใช้เครื่องมือพิเศษในการสืบสวนสอบสวนและรวบรวมพยานหลักฐาน
5) คดีที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติ
6) คดีที่ส่งผลเสียหายร้ายแรงต่อระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ
7) คดีที่สำนักงานตำรวจแห่งชาติมีนโยบายป้องกันและปราบปรามเป็นพิเศษ

อย่างไรก็ตาม จะเห็นได้ว่ากรณีที่เกี่ยวข้องกับแก๊งคอลเซ็นเตอร์นั้นเป็นอาชญากรรมทางเทคโนโลยีที่ในบางครั้งอาจไม่ได้ก่อให้เกิดมูลค่าความเสียหายถึง 30 ล้านบาทขึ้นไป แต่เป็นคดีที่สร้างความเสียหายอย่างกว้างขวาง เนื่องจากพบประชาชนจำนวนมากที่ตกเป็นเหยื่อในปัจจุบัน ทำให้ในช่วงปี 2565-2566 นี้กองบัญชาการตำรวจไซเบอร์ได้มีส่วนในการทำให้ประเด็นดังกล่าวเป็นปัญหาความมั่นคงทางไซเบอร์ที่สำคัญ เพื่อให้ประชาชนได้มีการตระหนักรู้ถึงผลกระทบจากการตกเป็นเหยื่อและนำไปสู่แนวทางในการรับมือกับภัยคุกคามทางไซเบอร์และการกำหนดมาตรการป้องกันทั้งในระดับส่วนบุคคลและในระดับรัฐ

ทั้งนี้ ในการศึกษาบทบาทของตำรวจไซเบอร์ในการรับมือกับภัยคุกคามในรูปแบบใหม่: ศึกษาการทำให้ปัญหาแก๊งคอลเซนเตอร์เป็นปัญหาความมั่นคงนั้น เพื่อศึกษาสภาพที่เป็นอยู่ในประเด็นเรื่องภัยคุกคามทางไซเบอร์ ซึ่งเป็นภัยคุกคามในรูปแบบใหม่ ผู้วิจัยจึงเลือกทบทวนวรรณกรรมเพื่อศึกษารากฐานและพัฒนาการของการศึกษาด้านความมั่นคงระหว่างประเทศ (International Security Studies) จนกระทั่ง พัฒนาการของประเด็นด้านความมั่นคงและกระบวนการทำให้เป็นปัญหาความมั่นคง (securitization) ของประเด็นต่าง ๆ เพื่อเป็นกรอบแนวคิดในการศึกษา

2.1 วรรณกรรมที่ศึกษาเกี่ยวกับความมั่นคงระหว่างประเทศ

ในส่วนของนิยามขอบเขตการศึกษาด้านความมั่นคงระหว่างประเทศ งานเขียนของ Barry Buzan ใน The Evolution of International Security Studies (Buzan & Hansen, 2009, pp. 8-9) ได้อธิบายพัฒนาการของการศึกษาด้านความมั่นคงระหว่างประเทศ และนิยามความหมายของประเด็นด้านความมั่นคงไว้ว่า คำว่า “ความมั่นคง” ไม่มีนิยามที่เป็นสากล (no universal definition) โดยในปี ค.ศ. 1983 Buzan ยังคงเห็นว่า ประเด็นเรื่องความมั่นคง ยังคงเป็น underdeveloped concept ที่ยังไม่ได้รับความสนใจอย่างกว้างขวางไปกว่ากลุ่มนโยบาย กลุ่มผลประโยชน์ และประเด็นถกเถียงในเรื่องดังกล่าวยังคงอยู่ในขอบเขตของการทหาร ต่อมาการศึกษาด้านความมั่นคงระหว่างประเทศผลจึงค่อย ๆ พัฒนาขึ้นจากการถกเถียงในเชิงประวัติศาสตร์ วัฒนธรรม (Williams, 2007) สำหรับ Buzan ในการศึกษาความมั่นคงระหว่างประเทศจะมีโครงสร้างการศึกษาที่จะเป็นกรอบและเครื่องมือในการทำความเข้าใจอยู่บนพื้นฐานของคำถาม 4 ประเด็น ได้แก่

1. การตั้งคำถามว่าจะมอง “รัฐ” มีความสำคัญในฐานะ referent object ที่ต้องถูกปกป้อง เพราะความมั่นคงเป็นการ “สร้าง” สิ่งที่ต้องถูกทำให้มั่นคง (be secured) ขึ้นมา ไม่ว่าจะเป็น ชาติ รัฐ บุคคล กลุ่มชาติพันธุ์ สิ่งแวดล้อม หรือ โลก ทั้งนี้ เพราะ ความมั่นคงแห่งชาติ และ ความมั่นคงระหว่างประเทศ ต่างให้ความสำคัญกับ “รัฐชาติ” ในฐานะ referent object ดังนั้น ข้อถกเถียงสำคัญของการศึกษาความมั่นคงระหว่างประเทศ คือ ตัวแสดงไหนที่ถูกกำหนดให้เป็น referent

object สำหรับความมั่นคงต้องถูกทำให้มั่นคง เพราะความมั่นคงของรัฐ (State security) มักจะถูกมองว่าเป็นปัจจัยหลักที่ทำให้ referent object อื่น ๆ ในรัฐมั่นคงและปลอดภัย

2. การตั้งคำถามว่าจะรวมภัยคุกคามภายใน (internal threats) เข้ามาเป็นภัยคุกคามเช่นเดียวกับภัยคุกคามภายนอก (external threats) หรือไม่ ซึ่งแต่เดิมการมองประเด็นด้านความมั่นคงจะผูกโยง ภัยคุกคาม (threats) เข้ากับขอบเขตของรัฐ ถึงได้มีแนวคิดเรื่อง ความมั่นคงของชาติขึ้น ซึ่งมีนัยของภายในและภายนอกชัดเจน ช่วงก่อนสงครามโลก ผลประโยชน์แห่งชาติที่เกี่ยวข้องกับความมั่นคงแห่งชาติถูกมองว่าเป็นการอยู่รอดจากภัยคุกคามจากสภาพเศรษฐกิจที่ตกต่ำจากการปฏิรูปสังคม และประเด็นเรื่องปากท้องภายในประเทศ มากกว่าภัยคุกคามจากภายนอก ต่อมาในช่วงสงครามโลก ความมั่นคงแห่งชาติกลับถูกคุกคามโดย การรุกรานจากภายนอก เช่นเดียวกับช่วงสงครามเย็นที่ความมั่นคงแห่งชาติถูกคุกคามจากอุดมการณ์ทางการเมืองภายนอก ซึ่งการเปลี่ยนแปลงทัศนะในการมองภัยคุกคามนี้ได้ถูกทำให้เป็นสถาบันกลายเป็นแนวคิดเรื่อง “ความมั่นคงระหว่างประเทศ” ที่เกิดขึ้นคู่ไปกับ “ความมั่นคงแห่งชาติ” และมีความเชื่อมโยงกันมากขึ้น โดยสงครามเย็นสิ้นสุดลง ภัยคุกคามภายนอกโดยสหภาพโซเวียตได้ลดบทบาทลงไปจากวาทกรรมด้านความมั่นคงของฝ่ายชาติตะวันตกและสหรัฐอเมริกา ประกอบกับกระแสโลกาภิวัตน์ได้ทำให้เส้นแบ่งของความเป็นภายนอกและภายในไม่ชัดเจนดังเช่นที่ผ่านมา ซึ่งส่งผลกระทบต่อการศึกษาด้านความสัมพันธ์ระหว่างประเทศและความมั่นคงระหว่างประเทศที่ต้องมองโลกเปลี่ยนไป

3. การตั้งคำถามต่อการมองความมั่นคงเหนือไปจากด้านการทหารและการใช้กำลัง โดยมีการนำมิติด้านเศรษฐกิจ การเมืองภายในประเทศ ความมั่นคงทางพลังงาน วิทยาศาสตร์และเทคโนโลยี อาหาร และทรัพยากรธรรมชาติ ซึ่งประเด็นเหล่านี้ เริ่มถูกหยิบยกขึ้นมาในฐานะที่เป็นปัจจัยที่ส่งผลกระทบต่อการใช้ หรือ ควบคุมการใช้กำลังทหาร มิได้ถูกมองเป็นประเด็นด้านความมั่นคงโดยตรง ซึ่งต่อมาในช่วงสงครามเย็น ตั้งแต่ทศวรรษที่ 1980 เริ่มมีการหยิบยกเรื่องความมั่นคงพื้นฐานของมนุษย์เข้ามาเป็นประเด็นด้านความมั่นคง และกลายเป็นส่วนหนึ่งของการศึกษาความมั่นคงระหว่างประเทศ โดยนักวิชาการที่เกี่ยวข้องเริ่มเรียกร้องให้รวมประเด็นด้านสิ่งแวดล้อม

และความมั่นคงทางเศรษฐกิจเข้ามา (Buzan & Hansen, 2009, p. 12) และจากนั้นจึงขยายไปสู่ประเด็นทั่วไปอื่น ๆ ในเชิงสังคม เศรษฐกิจ สิ่งแวดล้อม สุขภาพ การพัฒนา

ขอบเขตของการศึกษาความมั่นคงระหว่างประเทศยังคงมีความไม่แน่นอนว่าครอบคลุมถึงจุดไหน และมีความเชื่อมโยงกับการศึกษาความสัมพันธ์ระหว่างประเทศที่ขีดเส้นแบ่งได้ยาก ในทศวรรษต้น ๆ หลังสิ้นสุดสงครามโลกครั้งที่ 2 เส้นแบ่งระหว่างความมั่นคงระหว่างประเทศและความสัมพันธ์ระหว่างประเทศยังพอระบุได้ชัดเจนว่า การศึกษาความมั่นคงระหว่างประเทศจะมีจุดเน้นอยู่ที่การใช้กำลังทหารในความสัมพันธ์ระหว่างประเทศ โดยระบุภัยคุกคามของรัฐเป็นภัยด้านการทหาร และค่อยๆ ขยายขอบเขตขึ้นภายหลังการสิ้นสุดของสงครามเย็น โดยเฉพาะในช่วงทศวรรษที่ 1990

โดยที่การศึกษาด้านความมั่นคงระหว่างประเทศมีความเกี่ยวพันกับการศึกษาความสัมพันธ์ระหว่างประเทศอย่างใกล้ชิด Buzan มองว่า แนวคิดเรื่อง ความสัมพันธ์ระหว่างประเทศเป็นแนวคิดที่ต้องศึกษาควบคู่กันไปกับการศึกษาด้านความมั่นคง (parallel concepts) ดังนั้น รัฐ และเส้นเขตแดนจึงมีความสำคัญ และได้พัฒนาขึ้นมาควบคู่กับการพัฒนาระบบระหว่างประเทศ ทั้งนี้ เพราะในการนิยามความมั่นคงจำเป็นต้องยึดโยงอยู่กับรัฐและเขตแดนในแง่ที่ว่าความมั่นคงสำหรับใคร เพื่ออะไร สำหรับการศึกษารัฐศาสตร์ ประวัติศาสตร์แสดงให้เห็นถึงพัฒนาการของรัฐตั้งแต่รัฐโบราณในยุคกลาง (medieval state) จนมาเป็นรัฐอธิปไตย (sovereign state) หรือรัฐสมัยใหม่ (modern state) ที่รัฐมีอำนาจอธิปไตยเด็ดขาดเหนือดินแดน (territory) ซึ่งระบบความสัมพันธ์ระหว่างประเทศที่รัฐมีอำนาจอธิปไตยเด็ดขาดเหนือดินแดนนี้เองที่ทำให้เกิดหลักการไม่ละเมิดซึ่งกันและกันในประเด็นภายในประเทศ หรือ non-interference in domestic ที่กลายมาเป็นเงื่อนไขสำคัญของการสร้างเสถียรภาพและระเบียบในสังคมระหว่างประเทศ (Buzan & Hansen, 2009, p. 42)

ในบทที่ 2 ของ The Evolution of International Security Studies นั้น Buzan ได้จัดประเภทแนวคิดด้านความมั่นคง (concepts of security) และให้รายละเอียดความเหมือนและต่าง ๆ ของแต่ละแนวคิดไว้ 11 แนวคิด (Buzan & Hansen, 2009, pp. 37-38) ได้แก่

(1) Conventional Constructivism ที่วิเคราะห์พฤติกรรมของรัฐโดยให้ความสำคัญกับปัจจัยด้านความคิด วัฒนธรรม ความเชื่อ บรรทัดฐาน และอัตลักษณ์

(2) Critical Constructivism เป็นกลุ่มที่มองความมั่นคงกว้างกว่ารัฐ แต่ยังคงให้ความสำคัญกับความมั่นคงด้านการทหาร

(3) The Copenhagen School เป็นกลุ่มที่มองภัยคุกคามกว้างขึ้น และมี referent object กว้างขึ้นมากกว่าแค่ รัฐ แต่ยังรวมถึง สังคม กลุ่มอัตลักษณ์ และสนใจการวิเคราะห์ประเด็นความมั่นคงในระดับภูมิภาค โดยกลุ่ม Copenhagen School เน้นการศึกษาการทำให้เป็นความมั่นคง (securitization) ที่เป็นกระบวนการทางสังคมที่ได้สร้าง (construct) ภัยคุกคามขึ้นมา

(4) Critical Security Studies ที่ย้ำความสำคัญของความมั่นคงของมนุษย์ (human security)เหนือความมั่นคงของรัฐ (state security)

(5) Feminist Security studies ที่เน้นศึกษาการสนับสนุนของผู้หญิงในการกำหนดนโยบายความมั่นคงของรัฐ ปัญหาด้านความมั่นคงของผู้หญิงในสังคมแบบ state-centric และชี้ให้เห็นถึงมิติของความเป็นใหญ่ของชายในการกำหนดนโยบายทางการทหารและด้านความมั่นคง

(6) Human Security ที่เน้นการมอง “มนุษย์” ในฐานะ referent object ด้านความมั่นคงที่เห็นว่าการศึกษาความมั่นคงระหว่างประเทศต้องครอบคลุมถึงประเด็นเรื่องความยากจน การพัฒนา ภาวะอดอยาก หรือประเด็นอื่น ๆ ที่จะเป็นภัยต่อมนุษย์

(7) Peace Research ที่มองประเด็นความมั่นคงในอีกมุมหนึ่ง คือให้ความสำคัญกับแง่มุมของสันติภาพมากกว่าการใช้กำลัง (the use of force)ในความมั่นคงระหว่างประเทศ มีวัตถุประสงค์เพื่อลดและกำจัดการใช้กำลัง ให้ความสำคัญกับการลดอาวุธ และควบคุมการแข่งกันสะสมอาวุธ

(8) Post-colonial Security Studies ที่ท้าทายการมองความมั่นคงในกรอบของตะวันตก และเห็นว่าต้องศึกษาประเด็นด้านความมั่นคงจากมุมมองของประเทศกำลังพัฒนาที่มีประสบการถูกล่าอาณานิคม

(9) Poststructuralist Security Studies ที่มองว่าอำนาจอธิปไตยของรัฐและความมั่นคงเป็นผลผลิตทางการเมืองที่ถูกสร้างขึ้น วิพากษ์วิจารณแนวคิดที่มองความมั่นคงแบบเน้นรัฐที่กีดกันมิให้ประเด็นอื่น ๆ เป็นประเด็นด้านความมั่นคง

(10) Strategic Studies ที่เป็นการศึกษาแบบดั้งเดิมที่มองประเด็นด้านความมั่นคงเป็นเรื่องการเมือง การทหาร และให้ความสำคัญกับพลวัตรทางการทหาร สงคราม และเป็นมุมมองแบบเน้นรัฐ

(11) (Neo) Realism ที่มองเรื่องความมั่นคงในเชิงโครงสร้างและขั้วอำนาจ โดยให้ความสำคัญกับการป้องปราม การแข่งขันสะสมอาวุธ ถือเป็นการศึกษาด้านความมั่นคงกระแสหลักหนึ่ง ซึ่ง Stephen M. Walt นักวิชาการในสำนักสัจนิยม ได้มีมุมมองขอบเขตการศึกษาความมั่นคงว่าเป็นเรื่องของสงครามภัยคุกคาม และการใช้กำลังทหาร

จากหนังสือ Security Studies ของ Paul D. Williams เช่นเดียวกันกับมุมมองของ Barry Buzan นิยามของ “ความมั่นคง” ไม่มีคำตอบที่เห็นตรงกันเป็นฉันทามติ เพราะความมั่นคงของแต่ละบุคคลอาจไม่เหมือนกัน (security undoubtedly means different things to different people) หากมองในเชิงนามธรรม นักวิชาการที่ศึกษาความสัมพันธ์ระหว่างประเทศได้นิยามความมั่นคงว่าเป็นประเด็นที่เกี่ยวข้องกับการขจัดและบรรเทาภัยคุกคามไปจนถึงการรักษาคุณค่า (alleviation of threats to cherished values) และแน่นอนว่า “ความมั่นคง” เป็นประเด็นทางการเมือง เพราะเป็นตัวกำหนดว่า ใครจะต้องได้อะไรเมื่อไหร่และอย่างไรในการเมืองโลก และแม้ว่า Paul D. Williams จะเห็นตรงกันกับ Barry Buzan ว่าการศึกษาความมั่นคงมีพื้นฐานอยู่ที่การถกเถียงของคำถามสี่ข้อที่ได้กล่าวไปข้างต้น เขาเห็นว่า คำตอบต่อคำถามพื้นฐานทั้งสี่ข้อนั้นได้เปลี่ยนแปลงไป และจะเปลี่ยนแปลงไปเรื่อย ๆ ตามกาลเวลา และในงานเขียนของ Paul D.

Williams เอง เขาได้ตั้งคำถามพื้นฐานสำคัญต่อ “ความมั่นคง” เพื่อเป็นกรอบในการศึกษา (William, 2008, pp. 5-10) สี่ข้อ เช่นเดียวกัน ได้แก่

(1) ความมั่นคงคืออะไร? ต่อคำถามนี้ แม้ว่าความมั่นคง (security) และความอยู่รอด (survival) จะมีความเกี่ยวข้องกัน แต่ทั้งสองสิ่งนี้มิใช่สิ่งเดียวที่ใช้ทดแทนกันได้ “ความอยู่รอด” ถือเป็นสถานะของการคงอยู่ (existential condition) ในขณะที่ “ความมั่นคง” คือ ความสามารถที่จะแสวงหาและรักษาความทะเยอทะยานทางการเมืองและสังคมได้ ดังนั้น นิยามของ “ความมั่นคง” จึงเป็นไปตามที่ Ken Booth อธิบายไว้ (William, 2008, หน้า 6) คือ เป็น ความอยู่รอด พลัส (survival-plus) ซึ่ง พลัส ที่ว่า คือ การที่สามารถมีอิสระจากภัยคุกคามที่เป็นอันตรายต่อชีวิต และมีทางเลือกในชีวิต นอกจาก ความมั่นคงตามมุมมองของ Ken Booth ความมั่นคงอาจถูกนิยามได้อีกหลายมุมมอง โดยอีกสองมุมมองที่ได้รับการยอมรับอย่างแพร่หลาย คือ

<u>หนึ่ง</u> ความมั่นคงในฐานะการสะสมซึ่งอำนาจ (accumulation of power) มองความมั่นคงในเชิงวัตถุ ในฐานะที่ ในการมีความมั่นคง จะต้องครอบครองสิ่งของบางอย่าง เช่น ทรัพย์สิน เงิน อาวุธ หรือ กองทัพ กล่าวคือ อำนาจคือเครื่องมือสู่การมีความมั่นคง ยิ่งมีอำนาจมากเท่าใดจะยิ่งมีความมั่นคงมากเท่านั้น โดยเฉพาะอำนาจทางการทหาร

<u>สอง</u> ความมั่นคงในฐานะอิสรภาพในการกระทำ โดยเน้นที่ความสัมพันธ์ระหว่างตัวแสดงต่าง ๆ มากกว่า ยกตัวอย่างเช่น สำหรับสหรัฐอเมริกา การครอบครองอาวุธนิวเคลียร์ของอิหร่านถูกมองว่าเป็นภัยคุกคาม แต่กลับไม่รู้สึกว่าการครอบครองอาวุธนิวเคลียร์ของอินเดียหรือปากีสถานเป็นภัยคุกคาม ทั้งนี้ เพราะ ความมั่นคงเป็นเรื่องของความสัมพันธ์ระหว่างตัวแสดงมากกว่าการครอบครองอำนาจดังในแนวทางที่หนึ่ง

(2) ความมั่นคงของใคร? ต่อคำถามนี้ คือ การหา referent object เช่นเดียวกับการตั้งคำถามของ Barry Buzan ซึ่งจากการศึกษาที่ผ่านมาก่อนหน้า แนวคิดเรื่องความมั่นคงให้ความสำคัญกับผู้คน (people) และภายหลังในการศึกษาความสัมพันธ์ระหว่างประเทศ ความมั่นคงถูกผูกโยงอยู่กับ “รัฐ” จนถูกควบรวบกับแนวคิดเรื่อง “ความมั่นคงของชาติ” (national security) เกิดเป็นการถกเถียงที่สำคัญของการศึกษาด้านความมั่นคงคือ แท้จริงแล้วความมั่นคง

ควรให้ความสำคัญกับ ความมั่นคงของมนุษย์ (human security) เฉกเช่นเดียวกับ ความมั่นคงของชาติหรือไม่ โดยความมั่นคงของมนุษย์นั้น มิได้จำกัดอยู่เพียงเรื่องของอาวุธ แต่เกี่ยวข้องกับศักดิ์ศรีความเป็นมนุษย์ ความปลอดภัยจากโรคภัยไข้เจ็บ ความปลอดภัยจากความขัดแย้งระหว่างชาติพันธ์ การมีสิทธิมีเสียงในสังคม เป็นการผสมผสานมิติเชิงสังคมเข้ามาในการศึกษาความมั่นคง เฉพาะเจาะจงไปที่กลุ่มทางสังคม (social groups) มากไปกว่า ความมั่นคงของชาติในภาพรวม เกิดเป็นระดับการวิเคราะห์ (level of analysis) ที่มีหลายระดับตั้งแต่ระดับที่เล็กที่สุดอย่างปัจเจกบุคคลไปถึงกลุ่มอัตลักษณ์และระดับกลุ่มในระบบระหว่างประเทศ (Williams P7) ในภายหลัง นักวิชาการเริ่มให้ความสำคัญกับ “โลก” (planet Earth) ซึ่งหมายถึง สิ่งแวดล้อม ระบบนิเวศของโลก ที่มนุษย์อาศัยอยู่ เพิ่มขึ้นนอกเหนือไปจากกลุ่มที่อาศัยอยู่บนโลกใบนี้ เพราะสิ่งมีชีวิตบนโลกต่างต้องพึ่งพาโลกใบนี้ ซึ่งเป็นจุดเริ่มต้นของการหันมาสนใจประเด็นสิ่งแวดล้อมอย่าง การเปลี่ยนแปลงสภาพภูมอากาศ และปัญหาโลกร้อนมากขึ้น

(3) ประเด็นด้านความมั่นคงคืออะไร? (What is a security issue?) คือ การตั้งคำถามว่าอะไรบ้างที่ถูกทำให้เป็นประเด็นด้านความมั่นคง และมีกระบวนการประกอบสร้าง (construct) ประเด็นด้านความมั่นคงนั้นอย่างไร คำถามนี้มีความสำคัญในฐานะที่ ความมั่นคงของแต่ละคนที่มีความแตกต่างกันทั้งในแง่ของ เพศสภาพ อายุ ความเชื่อทางศาสนา ชนชั้นทางสังคม เชื้อชาติ ชนชาติ สถานที่ ๆ อาศัยอยู่ ย่อมมีความแตกต่างกัน ข้อห่วงกังวลของแต่ละกลุ่มนำมาซึ่งการสร้างภัยคุกคาม (construct threat agendas) ที่แตกต่างกัน ยกตัวอย่าง เช่น การเกิดฝนอาจมิใช่ภัยคุกคามสำหรับพื้นที่ที่มีความแห้งแล้งและต้องการน้ำ ในขณะที่อาจเป็นภัยคุกคามสำหรับพื้นที่ลุ่มที่อาจทำให้เกิดปัญหาน้ำท่วมได้ หรืออย่างเช่น ประเทศหมู่เกาะย่อมได้รับผลกระทบจากการเพิ่มขึ้นของระดับน้ำทะเลในระดับที่ส่งผลต่อความอยู่รอดของเกาะที่อาจจมลงไปในทะเล มากกว่าประเทศที่อยู่ในภาคพื้นทวีป ดังนั้น การศึกษาด้านความมั่นคงจึงจำเป็นต้องศึกษาและทำความเข้าใจกระบวนการประกอบสร้างภัยคุกคามจากผู้แทนของกลุ่มต่าง ๆ และจำเป็นต้องทำความเข้าใจว่าประเด็นของกลุ่มต่าง ๆ มิได้มีอำนาจเท่ากันในทางการเมือง ยกตัวอย่างเช่น การกำหนดประเด็นด้านความมั่นคงของคณะมนตรีความมั่นคงของสหประชาชาติย่อมมีน้ำหนักและมีผลต่อการเมืองโลกมากกว่าการกำหนดประเด็นด้านความมั่นคงจากสภาความมั่นคงของประเทศใด

ประเทศหนึ่ง สำหรับกระบวนการกำหนดภัยคุกคามนี้เอง องค์กรสหประชาชาติเป็นหนึ่งในพื้นที่ของการประกอบสร้างดังกล่าว โดยเมื่อปี ค.ศ. 2004 UN Secretary-General's High-level Panel on Threats, Challenges and Change ได้จัดทำรายงาน A More Secure World ขึ้น โดยรายงานดังกล่าวระบุ การจัดกลุ่มภัยคุกคามในโลกปัจจุบันออกมาเป็น 6 กลุ่ม คือ (1) ภัยคุกคามทางเศรษฐกิจและสังคม ที่ประกอบด้วย ความยากจน การแพร่ระบาดของการติดเชื้อ สภาวะสิ่งแวดล้อมถดถอย (2) ความขัดแย้งระหว่างรัฐ (inter-state conflict) (3) ความขัดแย้งภายในประเทศ อย่าง สงครามกลางเมือง การฆ่าล้างเผ่าพันธุ์ หรือ ความรุนแรงอื่น ๆ ในระดับสูง (other large-scale atrocities) (4) อาวุธนิวเคลียร์ อาวุธรังสี อาวุธเคมี และอาวุธชีวภาพ (5) การก่อการร้าย (6) องค์กรอาชญากรรมข้ามชาติ (UN High-level Panel 2004:2 / William 8)

(4) การนำมาซึ่งความมั่นคง (How can security be achieved?) ต่อคำถามนี้ เป็นการศึกษาเพื่อทำความเข้าใจการได้มาซึ่งความมั่นคงว่ามีกระบวนการอย่างไร และ มีตัวแสดงใดบ้างที่เกี่ยวข้อง โดยให้ความสำคัญกับตัวแสดงทุกระดับ ทั้งตัวแสดงระดับรัฐ ระดับองค์การระหว่างประเทศ และตัวแสดงที่ไม่ใช่รัฐ เช่น กลุ่มเคลื่อนไหวทางสังคม องค์กรอาชญากรรมข้ามชาติ และในบางกรณีปัจเจกบุคคลมีความสามารถที่จะนำมาซึ่งความมั่นคงได้ เนื่องจากมีอำนาจทางการทหาร หรือ มีอำนาจในการสื่อสารต่อสังคมในประเด็นด้านความมั่นคง

อาจกล่าวได้ว่าแนวคิดด้านความมั่นคงศึกษาที่ได้รับความนิยมในช่วงสงครามเย็นค่อนไปในทางการเมืองและมีความเป็นสัจนิยมสูง โดยเน้นศึกษาที่ รัฐ (state) กลยุทธ (strategy) วิทยาศาสตร์ (science) และ status quo ทั้งนี้ เพราะสถานการณ์ของโลกในตอนนั้นเกี่ยวโยงกับการแข่งขันของมหาอำนาจ อาวุธนิวเคลียร์และการป้องปราม แต่พัฒนาการที่สำคัญทางวิชาการของการศึกษาความมั่นคงในกระแสหลักเกิดขึ้นในปี ค.ศ. 1983 ผ่านหนังสือ People, States and Fear ของ Barry Buzan ที่นำเสนอว่า ความมั่นคงมิได้จำกัดอยู่เพียงแค่รัฐเท่านั้นแต่เกี่ยวข้องกับมนุษย์โดยส่วนรวม (human collectivities) โดย Buzan ได้เสนอกรอบความคิดที่เห็นว่า ความมั่นคงของมนุษย์โดยส่วนรวมนั้นได้รับผลกระทบจากปัจจัยที่สำคัญ 5 Sectors ได้แก่ (William, 2008, pp. 2-4)

(1) ด้านการทหาร ที่เกี่ยวข้องกับปฏิสัมพันธ์ระหว่างศักยภาพทางการทหารเชิงรุก (offensive) และศักยภาพทางทหารเชิงป้องกัน (defensive) กับการรับรู้ (perception) ของรัฐต่อความตั้งใจ (intentions) ของรัฐอื่น

(2) ด้านการเมือง ที่เน้นเสถียรภาพในเชิงองค์กรของรัฐ ระบบการปกครอง อุดมการณ์ทางการเมืองที่สร้างความชอบธรรมให้แก่รัฐ

(3) ด้านเศรษฐกิจ ที่เกี่ยวข้องกับการเข้าถึง (access) ทรัพยากร เข้าถึงเงินทุนและตลาดที่จำเป็นต่อการรักษาระดับสวัสดิการของรัฐ และอำนาจของรัฐ

(4) ด้านสังคม ที่เกี่ยวข้องกับปัจจัยด้านวัฒนธรรม พัฒนาการของภาษา ศาสนา อัตลักษณ์แห่งชาติ และบรรทัดฐานต่าง ๆ

(5) ด้านสิ่งแวดล้อม ที่เกี่ยวข้องกับระบบนิเวศของโลกที่จำเป็นต่อการดำรงอยู่ของมนุษย์

แนวคิดของ Buzan ได้ขยายขอบเขตการศึกษาด้านความมั่นคงออกมากว้างขึ้นนอกเหนือจากมิติด้านการทหารแบบดั้งเดิม

2.1.1.1 <u>ภัยคุกคามรูปแบบใหม่ (non-traditional threats)</u> ภายหลังการสิ้นสุดของสงครามเย็น การศึกษาด้านความมั่นคงระหว่างประเทศเริ่มมีการเปลี่ยนแปลงไปจากเดิมที่เป็นการเน้นศึกษาที่รัฐ (state centric) มาเป็นการศึกษาที่กว้างขึ้นและลึกขึ้น ตั้งแต่ช่วงทศวรรษที่ 1980 ถึงทศวรรษที่ 1990 โดยมีการทำให้ referent object ของความมั่นคงลึกไปกว่าเพียงแค่รัฐ และขยายกรอบแนวคิดเรื่องความมั่นคงให้กว้างขึ้นนอกเหนือไปจากภาคการทหาร และให้ความสำคัญกับปัญหาภายในและภัยคุกคามข้ามพรมแดนเท่าเทียมกับภัยคุกคาม ซึ่งภายหลังในช่วงทศวรรษที่ 1990 จนถึงทศวรรษที่ 2000 แนวคิดดังกล่าวได้พัฒนาไปเป็นสาขาต่าง ๆ ในสำนัก Constructivism (Buzan & Hansen, 2009, pp. 187-189)

2.1.1.2 <u>ความมั่นคงของมนุษย์ (Human Security)</u> การสิ้นสุดลงของสงครามเย็นได้เปลี่ยนแปลงการตั้งคำถามต่อประเด็นด้านความมั่นคงและเปลี่ยนแปลงตัวแสดงที่เกี่ยวข้องกับประเด็นด้านความมั่นคงไปจากเดิม บริบทของโลกที่เปลี่ยนแปลงไปเป็นแรงขับเคลื่อนให้ประเด็น

ด้านความมั่นคงเปลี่ยนไปจากเดิม อีกหนึ่งในการเปลี่ยนแปลงสำคัญของการศึกษาด้านความมั่นคงคือ การที่ โครงการพัฒนาแห่งสหประชาชาติ (United Nations Development Programme หรือ UNDP) ได้จัดทำรายงานประจำปีเรื่อง Human Security ขึ้นมาในปี ค.ศ. 1994 (UNDP, 1994) โดยรายงานดังกล่าวได้ขยายขอบเขตของความมั่นคงไปครอบคลุมจากที่ให้ความสำคัญอยู่ที่ การปกป้องเขตแดน การรักษาผลประโยชน์แห่งชาติ การป้องปรามอาวุธนิวเคลียร์ และการป้องกันความขัดแย้งในโลก ไปถึงการรักษาความมั่นคงของมนุษย์ โดยมีมนุษย์เป็นศูนย์กลาง (people-centred) ซึ่งเป็นการเปลี่ยนแปลง referent object ของความมั่นคงจากเดิมที่เป็นรัฐ มาเป็น มนุษย์ ให้ความสำคัญกับความเป็นอยู่ของมนุษย์ในสังคมอย่างมีเสรีภาพ มีทางเลือก และสามารถเข้าถึงโอกาสทางการตลาดและโอกาสทางสังคม ตลอดจนสามารถดำรงชีวิตอยู่ในสถานการณ์ความขัดแย้งหรือในสถานการณ์ที่มีสันติภาพ (Buzan & Hansen, 2009, p. 203) การนิยาม Human Security ของ UNDP นี้เองที่ได้ทำให้ประเด็นด้านความมั่นคงขยายตัวขึ้นและได้รับการยอมรับอย่างกว้างขวางจากรัฐต่าง ๆ จนกระทั่งทุกวันนี้ โดยมีประเด็นด้านความมั่นคงใหม่ๆ ที่ได้รับความสนใจ เช่น ความมั่นคงทางอาหาร ความมั่นคงทางสุขภาพ สิ่งแวดล้อม การเพิ่มขึ้นของประชากร ความเท่าเทียมทางสังคม การอพยพย้ายถิ่น ปัญหายาเสพติด ปัญหาการก่อการร้าย

ในส่วนที่เกี่ยวกับเรื่องความมั่นคงของมนุษย์ หรือ Human Security รายงานประจำปีของ UNDP ข้างต้นได้จัดหมวดหมู่ประเด็นความมั่นคงของมนุษย์ออกเป็น 7 กลุ่ม (UNDP, 1994) ได้แก่

1) ความมั่นคงทางเศรษฐกิจ (Economic security) หมายถึง การที่มนุษย์มีรายได้ที่มั่นคงทั้งจากการทำงาน หรือการที่รัฐมีความช่วยเหลือทางการเงินในระดับพื้นฐานสำหรับประชาชนที่เพียงพอต่อการดำรงชีพ โดยให้ความสำคัญกับการสร้างอาชีพให้ประชาชนสามารถมีรายได้เพื่อดำรงชีพได้เอง

2) ความมั่นคงทางอาหาร (Food security) หมายถึง ความสำคัญเรื่องอาหารในฐานะปัจจัย 4 การสร้างความมั่นคงทางอาหารคือการให้ประชาชนสามารถเข้าถึง (access) ถึงอาหารได้อย่างเพียงพอ

3) ความมั่นคงทางสุขภาพ (Health security) หมายถึง การมีสุขภาวะที่ดี สุขภาพแข็งแรก ปลอดภัยจากโรคภัยและเชื้อโรคต่าง ๆ ภาวะความปลอดภัยหลังคลอดบุตร อัตราการรอดชีวิตของทารกแรกเกิดที่เพิ่มขึ้น และอัตราการเสียชีวิตจากโรคภัยและเชื้อโรคที่ลดลง

4) ความมั่นคงด้านสิ่งแวดล้อม (Environmentally friendly) หมายถึง สิ่งแวดล้อมที่เป็นมิตรต่อมนุษย์ ไม่เป็นอันตรายต่อการดำรงชีพ มีน้ำและอากาศที่สะอาดสำหรับมนุษย์

5) ความมั่นคงในชีวิตส่วนตัว (personal security) หมายถึง ความปลอดภัยของปัจเจกบุคคลที่จะไม่ถูกคุกคามหรือได้รับอันตรายในชีวิตจากการกระทำของรัฐ เช่น เกิดสงคราม และการกระทำของบุคคลอื่นหรือตนเอง เช่น การถูกทำร้ายร่างกายโดยบุคคลอื่น หรือ พฤติกรรมทำร้ายตัวเอง ความมั่นคงด้านนี้ครอบคลุมถึง การถูกทำร้ายโดยบุคคลในครอบครัวและการปกป้องเด็กจากการถูกละเมิดด้วย (child abuse)

6) ความมั่นคงในชุมชน (Community security) หมายถึง ความปลอดภัยของกลุ่มคน เช่น กลุ่มชาติพันธ์ กลุ่มศาสนา ที่รวมตัวกันเป็นชุมชน เช่น กลุ่มคนพื้นเมือง และกลุ่มผู้อพยพ

7) ความมั่นคงในทางการเมือง (Political security) หมายถึง ระบอบการเมืองที่เคารพสิทธิมนุษย์ชนขั้นพื้นฐานของประชาชน

การขยายกระบวนทัศน์ด้านความมั่นคงครั้งนี้ทำให้รัฐเปลี่ยนมุมมองเรื่องความมั่นคงไปจากเดิมที่ให้ความสำคัญกับภัยคุกคามจากภัยนอก มาเป็นการมองภัยคุกคามภายในต่อที่ส่งผลกระทบต่อความมั่นคงของมนุษย์ในชีวิตประจำวันด้วย และมองประเด็นเหล่านี้เชื่อมโยงกัน เป็นปัจจัยที่พึ่งพากันและกัน

อาจกล่าวได้ว่าแนวคิดเรื่องความมั่นคงของมนุษย์ได้เปลี่ยนแปลงมุมมองที่ว่า รัฐ คือ referent object ด้านความมั่นคง มาเป็น ปัจเจกบุคคล ในฐานะ referent object ด้านความมั่นคง

ในขณะเดียวกัน ตัวแสดงที่จะนำมาซึ่งภัยคุกคามก็เพิ่มขึ้น นอกจากตัวแสดงภายนอกอย่างรัฐอื่นหรือแม้กระทั่งรัฐของตนแล้ว ความเชื่อมโยงของโลกที่เป็นผลจากโลกาภิวัตน์ได้เปิดทางให้กลุ่มองค์กรอาชญากรรม (Organized Crime) เข้ามาสร้างภัยคุกคามต่อความมั่นคงของมนุษย์ โดยกลุ่มองค์กรอาชญากรรมตามความหมายของอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร (United Nations Convention Against Transnational Organized Crime) ที่มีขึ้นในปี ค.ศ. 2000 ได้ให้นิยามไว้ว่า หมายถึง “กลุ่มที่มีการจัดโครงสร้างของบุคคลตั้งแต่สามคนหรือมากกว่า ที่ดำรงอยู่เป็นระยะเวลาหนึ่ง และมีการประสานการดำเนินงานระหว่างกัน โดยมีเป้าหมายในการกระทำอาชญากรรมร้ายแรงหนึ่งอย่างหรือมากกว่าเพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงิน หรือผลประโยชน์ทางวัตถุอย่างอื่น ไม่ว่าโดยทางตรงหรือทางอ้อม” ซึ่งอนุสัญญาฯ ดังกล่าวได้ระบุนิยามของอาชญากรรมร้ายแรงไว้ด้วยว่า คือ “การกระทำความผิดซึ่งมีโทษจำคุกขั้นสูงเป็นเวลาอย่างน้อย 4 ปี หรือมากกว่า” และระบุรูปแบบหรือลักษณะที่ถือว่าเป็นอาชญากรรมข้ามชาติไว้ว่า ได้แก่ 1) เป็นความผิดที่กระทำในประเทศมากกว่าหนึ่งประเทศ 2) ความผิดนั้นกระทำลงในประเทศหนึ่งแต่ส่วนสำคัญของการตระเตรียมการวางแผนการสั่งการ หรือการควบคุมได้กระทำในอีกประเทศหนึ่ง 3) ความผิดนั้นกระทำลงในประเทศหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งมีส่วนเกี่ยวข้องกับการกระทำความผิดทางอาญาในอาณาเขตของประเทศมากกว่าหนึ่งประเทศ 4) ความผิดนั้นกระทำลงในประเทศหนึ่ง แต่มีผลกระทบที่สำคัญเกิดขึ้นในอีกประเทศหนึ่ง (สักกรินทร์ นิยมศิลป์, 2558, หน้า 236-237) และตามนิยามขององค์การสหประชาชาติ อาชญากรรมข้ามชาติแบ่งได้เป็น 18 ประเภท ได้แก่ การฟอกเงิน การก่อการร้าย การโจรกรรมงานศิลปะและผลงานทางวัฒนธรรม การละเมิดทรัพย์สินทางปัญญา การค้าอาวุธเถื่อน โจรสลัดในทะเล โจรสลัดบนบก การหลอกลวงในธุรกิจประกัน อาชญากรรมคอมพิวเตอร์ อาชญากรรมสิ่งแวดล้อม การค้ามนุษย์ การค้าอวัยวะมนุษย์ การค้ายาเสพติด การหลอกเรื่องล้มละลาย การแทรกซึมองค์กรธุรกิจ การคอร์รัปชั่น การให้สินบนเจ้าหน้าที่รัฐ และความผิดอื่น ๆ (สักกรินทร์ นิยมศิลป์, 2558, หน้า 237)

ในส่วนของประเทศไทย กฎหมายที่เกี่ยวข้องกับอาชญากรรมข้ามชาติ คือ พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556

ซึ่งพระราชบัญญัติดังกล่าวให้นิยามของ “องค์กรอาชญากรรม” ไว้ว่าคือ คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม ส่วน “องค์กรอาชญากรรมข้ามชาติ” คือ องค์กรอาชญากรรมที่มีการกระทำความผิดซึ่งมีลักษณะอย่างหนึ่งอย่างใด ดังต่อไปนี้ 1) ความผิดที่กระทำในเขตแดนของรัฐมากกว่าหนึ่งรัฐ 2) ความผิดที่กระทำในรัฐหนึ่ง แต่การตระเตรียม การวางแผน การสั่งการ การสนับสนุนหรือการควบคุมการกระทำความผิดได้กระทำในอีกรัฐหนึ่ง 3) ความผิดที่กระทำในรัฐหนึ่ง แต่เกี่ยวข้องกับองค์กรอาชญากรรมที่มีการกระทำความผิดมากกว่าหนึ่งรัฐ 4) ความผิดที่กระทำในรัฐหนึ่ง แต่ผลของการกระทำที่สำคัญเกิดขึ้นในอีกรัฐหนึ่ง (พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556, 2556)

ในส่วนที่เกี่ยวกับอาชญากรรมข้ามชาติ หน่วยงานที่เกี่ยวข้องต่าง ๆ ได้จัดประเภทอาชญากรรมที่เข้าข่ายเป็นอาชญากรรมข้ามชาติไว้เพื่อประโยชน์ในการป้องกันและติดตามสืบสวน โดยองค์การตำรวจสากล (International Criminal Organization: INTERPOL) ได้จัดแบ่งอาชญากรรมข้ามชาติออกเป็น 16 ประเภท (Interpol, n.d.) ได้แก่

1) การทุจริต (Corruption) เพราะโลกาภิวัตน์ทางเศรษฐกิจทำให้ปัญหาการทุจริตเป็นอาชญากรรมที่ไร้พรมแดน (borderless crime)
2) การปลอมแปลงสกุลเงินหรือเอกสาร (Counterfeit currency and documents)
3) อาชญากรรมต่อเด็ก (Crimes against children)
4) อาชญากรรมที่เกี่ยวข้องกับมรดกทางวัฒนธรรม (Cultural heritage crime)
5) อาชญากรรมไซเบอร์ (Cybercrime)
6) การลักลอบขนส่งยาเสพติด (Drug Trafficking)
7) อาชญากรรมสิ่งแวดล้อม (Environmental crime)
8) อาชญากรรมทางการเงิน (Financial crime)
9) การลักลอบค้าอาวุธ (Firearms trafficking)

10) การค้ามนุษย์และการลักลอบขนส่งผู้อพยพ (Human trafficking and migrant smuggling)

11) การลักลอบค้าของเถื่อน (Illicit goods)

12) อาชญากรรมทางทะเล (Maritime crime) เช่น โจรสลัด การลักพาตัว การปล้นเรือสินค้า การกระทำใด ๆ ที่ส่งผลต่อเสรีภาพในการเดินเรือ และเป็นภัยคุกคามต่อเส้นทางการค้าโลก

13) องค์กรอาชญากรรม (Organized crime)

14) การก่อการร้าย (Terrorism)

15) การโจรกรรมยานพาหนะ (Vehicle crime) ที่เป็นส่วนหนึ่งของการค้ายานพาหนะเถื่อน

16) อาชญากรรมสงคราม (War crimes) เช่น การฆ่าล้างเผ่าพันธุ์ อาชญากรรมต่อมนุษยชาติ (crimes against humanity)

ทั้งนี้ ในส่วนของอาเซียน ประเทศสมาชิกได้จัดประเภทอาชญากรรมข้าม8ชาติไว้ 8 ประเภท ได้แก่ 1) การก่อการร้ายสากล 2) การลักลอบค้ายาเสพติด 3) การค้ามนุษย์ 4) การฟอกเงิน 5) การลักลอบค้าอาวุธ 6) การกระทำอันเป็นโจรสลัด 7) อาชญากรรมเศรษฐกิจระหว่างประเทศ และ 8) อาชญากรรมคอมพิวเตอร์ (ฉัตรชัย ศรีเมืองกาญจนา, 2562) (ฉัตรชัย ศรีเมืองกาญจนา, อาชญากรรมข้ามชาติกับความมั่นคงของประเทศไทย)

สำนักงานตำรวจแห่งชาติของไทยยังได้ระบุประเภทของอาชญากรรมที่เข้าข่ายเป็นอาชญากรรมข้ามชาติไว้ 11 ประเภท (สักกรินทร์ นิยมศิลป์, 2558) ได้แก่

1) การก่อการร้ายข้ามชาติ (International terrorism)
2) การปลอมแปลงหลักฐานเกี่ยวกับตัวบุคคล หรือการขโมยอัตลักษณ์บุคคล (Identity fraud)
3) การลักลอบค้าอาวุธเถื่อน (Arms smuggling)
4) การลักลอบขนคนข้ามชาติ หรือลักลอบขนแรงงานต่างด้าวข้ามชาติ (people smuggling or illegal labour)
5) การฟอกเงิน (Money laundering)
6) การลักลอบค้ายาเสพติด (Drug trafficking)

7) การลักลอบค้ามนุษย์หรือการประพฤติผิดทางเพศต่อเด็ก (Human trafficking or pedophile)
8) อาชญากรรมทางเศรษฐกิจและคอมพิวเตอร์ (Financial crime and cybercrime)
9) อาชญากรรมร้ายแรง หรือเหตุการณ์ร้ายแรงอื่น ๆ ในต่างประเทศ (International violent crimes or referrals)
10) อาชญากรรมร้ายแรง หรือเหตุการณ์ร้ายแรงอื่น ๆ ในประเทศไทย (Thailand's other violent crimes or incidents)
11) อาชญากรรมอื่น ๆ (Other crimes)

จากการจัดประเภทอาชญากรรมข้ามชาติขององค์กรระหว่างประเทศต่าง ๆ ข้างต้นจะเห็นว่า อาชญากรรมไซเบอร์ อาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมทางเทคโนโลยีมีความเกี่ยวข้องเป็นอาชญากรรมข้ามชาติที่มิอาจแก้ไขปัญหาได้ด้วยความพยายามของรัฐใดรัฐหนึ่งเพียงรัฐเดียว แต่จำเป็นต้องมีความร่วมมือระหว่างประเทศในการแก้ไขปัญหาร่วมกัน

2.2 แนวคิดและทฤษฎีที่เกี่ยวข้อง

ในการศึกษาเรื่องความมั่นคง แนวคิดด้านความสัมพันธ์ระหว่างประเทศที่เป็นกรอบแนวคิดในการอธิบายการนิยามความมั่นคงได้อย่างน่าสนใจ คือ แนวคิดของโธมัส ฮอบส์ ใน Leviathan ที่อธิบายเหตุผลของการมีความสัมพันธ์กันภายในรัฐเพื่อให้เกิด "ความมั่นคง" กล่าวคือ ฮอบส์ (Thomas Hobbes) ได้อธิบายว่า ในสภาวะธรรมชาติ (state of nature) ที่ไม่มีอำนาจกลาง (authority) ที่จะเป็นหลักประกันให้แก่ความอยู่รอดของปัจเจกบุคคล (individual) จากการแข่งขันกันที่อาจถูกแย่งของในครอบครองหรือทรัพยากรที่มีอยู่อย่างจำกัดได้ตลอดเวลา ซึ่งสถานะดังกล่าวเป็นปัญหาของความอยู่รอด (survival) และความปลอดภัยในชีวิตของปัจเจกบุคคล ทำให้ปัจเจกบุคคลตกอยู่ในสถานะแห่งความหวาดกลัวตลอดเวลา จึงได้มีการตกลงกันเพื่อให้เกิดอำนาจขององค์อธิปัตย์ (sovereign) เป็นสถาบันที่จะรับประกันความมั่นคงให้ปัจเจกบุคคล เกิดเป็นสิ่งที่เรียกว่า "สัญญา" หรือสัญญาประชาคม ระหว่างปัจเจกบุคคลกับรัฐ ที่ปัจเจกบุคคลมอบสิทธิของตนให้แก่รัฐเพื่อแลกกับความปลอดภัย และได้รับการปกป้องจากรัฐที่ปัจเจกบุคคลยอมรับว่ามีอำนาจเหนือปัจเจกบุคคล (Buzan & Hansen, 2009, p. 25) ซึ่งสำหรับฮอบส์

แล้ว อาร์ บี เจ วอล์คเกอร์ (R.B.J. Walker) มองว่า ฮอบส์เชื่อว่าความกลัวต่อภาวะธรรมชาติของปัจเจกบุคคลนั้นมีความรุนแรงมากจนอะไรก็ตามที่องค์อธิปัตย์กระทำแม้ว่าจะแย่แค่ไหนก็ไม่แย่ไปกว่าสภาวะธรรมชาติที่มีการแข่งขันกันอย่างไม่มีการควบคุม (Walker, 1997) โดยแนวคิดเช่นนี้เองที่มีอิทธิพลต่อนักคิดในกลุ่มเสรีนิยมอย่างเช่น จอห์น ล็อค (John Locke) ที่เห็นต่างออกไป ทำให้เกิดเป็นการถกเถียงในเวลาต่อมา ระหว่างแนวคิดเรื่อง ความมั่นคงของปัจเจกบุคคล (individual security) กับ ความมั่นคงร่วมหรือความมั่นคงของรัฐ (collective/state security) ที่เชื่อมโยงกันอย่างแยกไม่ได้ โดยการแก้ไขปัญหาความมั่นคงของรัฐจะใช้วิธีแตกต่างกับการแก้ไขปัญหาของปัจเจก ในขณะที่ความมั่นคงของปัจเจกบุคคลอยู่ในความสัมพันธ์กับปัจเจกบุคคลด้วยกันจึงถือเป็นความมั่นคงร่วมกัน แน่นอนว่า คำอธิบายในแบบของฮอบส์ใน Leviathan เป็นกรอบความคิดเชิงนามธรรมที่ไม่อาจอธิบายพฤติกรรมของรัฐสมัยใหม่บางรัฐที่ไม่สามารถให้ความมั่นคงกับปัจเจกในรัฐของตนได้ ดังในกรณีโซมาเลีย หรือ เมียนมา

2.2.1 ทฤษฎีสัจนิยม (Realism)

เมื่อพิจารณาถึงพัฒนาการของการศึกษาด้านความมั่นคงที่ผ่านมา ทฤษฎีสัจนิยมนับเป็นทฤษฎีหนึ่งที่มีอิทธิพลต่อการศึกษาด้านความมั่นคง ในแง่ของการวิเคราะห์เรื่องอำนาจ ความกลัว และสภาวะอนาธิปไตย (anarchy) ที่เป็นพื้นฐานของการเกิดความขัดแย้งและสงคราม ซึ่งถือเป็นภัยคุกคามต่อความมั่นคง Colin Elman ในหนังสือ Security Studies an Introduction ได้อธิบายความเชื่อมโยงของทฤษฎีสัจนิยมกับการศึกษาด้านความมั่นคงไว้ ดังนี้

(1) Classical realism โดยสัจนิยมคลาสสิคที่ Colin Elman นำมาศึกษาเป็นกลุ่มสัจนิยมคลาสสิคของศตวรรษที่ 20 โดยเน้นตั้งแต่ช่วงปี ค.ศ. 1939 เป็นต้นมา ผ่านแนวคิดของนักคิดคนสำคัญของสำนักนี้ เช่น Edward Hallett Carr ที่เขียนหนังสือ The Twenty Years' Crisis งานของ Frederick Shuman ในปี ค.ศ. 1933 งานของ Harold Nicolson ในปี ค.ศ. 1939 งานของ Reinhold Niebuhr ในปี ค.ศ. 1940 งานของ Hans Morgenthau ปี ค.ศ. 1948 งานของ George F. Kennan ปี ค.ศ. 1951 โดยสำหรับกลุ่มนี้แล้ว โดยธรรมชาติมนุษย์มีความประสงค์ที่จะมีอำนาจเพิ่มขึ้นเช่นเดียวกันกับรัฐที่จะต้องดำเนินการอย่างต่อเนื่องเพื่อเพิ่มศักยภาพของรัฐเพื่อสิ่งที่

รัฐเห็นว่าเป็นความมั่นคง และด้วยสภาวะอนาธิปไตยของระบบระหว่างประเทศที่ไม่มีอำนาจกลางควบคุมทำให้ทุกรัฐมีความเสี่ยงที่จะตกอยู่ในสภาวะไม่มั่นคง โดยสงครามอาจเกิดขึ้นหากรัฐได้รัฐหนึ่งมีผู้นำที่มีแนวโน้มรุกรานคนอื่น หรือ มีความโลภประสงค์จะขยายอำนาจของตนไปยังรัฐอื่น ซึ่งผู้กำหนดพฤติกรรมของรัฐเหล่านี้จะมีการตัดสินใจอย่างมีเหตุผลด้วยการคำนวนความคุ้มค่าและผลของการกระทำ (Elman, 2008, p. 17)

(2) Neorealism หรือสัจนิยมใหม่ โดยนักคิดคนสำคัญของแนวคิดนี้ คือ Kenneth Waltz ในงานเขียน Theory of International Politics ที่มอง ระบบระหว่างประเทศเป็นโครงสร้าง ที่อาจแบ่งได้เป็น 3 ส่วน คือ ระเบียบ (ordering principle) ที่เป็นสภาวะความเป็นอนาธิปไตย ที่ไม่มีอำนาจกลางควบคุม ตัวแสดงในระบบที่มีหน้าที่เหมือนกัน (functionally alike) และส่วนที่ 3 คือ อำนาจที่แตกต่างกัน สำหรับ Kenneth Waltz สองส่วนแรกเป็นลักษณะของโครงสร้างระบบระหว่างประเทศสิ่งที่จะดำรงอยู่อย่างไม่เปลี่ยนแปลง แต่สิ่งที่ทำให้โครงสร้างระบบระหว่างประเทศเปลี่ยนแปลงไปคือ ส่วนที่ 3 คือ การกระจายอำนาจ (distribution of capabilities ที่จะเป็นตัวกำหนด โครงสร้างของระบบออกมาเป็นลักษณะขั้วอำนาจ และเป็นปัจจัยสำคัญที่จะกำหนดพฤติกรรมของรัฐ

(3) Defensive structural realism ที่พัฒนามาจากแนวคิดแบบสัจนิยมใหม่ โดยเพิ่มมิติของการตัดสินใจอย่างมีเหตุผลของรัฐ ว่าในโครงสร้างระหว่างประเทศที่เป็นขั้วอำนาจนั้น รัฐจะสะสมอำนาจเพื่อป้องกันตนมากกว่าเพื่อรุกราน โดยรัฐจะดำเนินการรักษาความมั่นคงด้วยคานอำนาจ (balance of power) เช่น การสร้างระบอบพันธมิตรเพื่อปกป้องตนเอง เพราะการมีอำนาจมากเกินไปอาจทำให้รัฐกลายเป็นภัยคุกคามต่อรัฐอื่นได้

(4) Offensive structural realism ที่เห็นต่างกับ Defensive structural realism ในเรื่องการสะสมอำนาจว่า อำนาจเพื่อปกป้องตนเองนั้นไม่เพียงพอในสภาวะความไม่แน่นอนของระบอบระหว่างประเทศ รัฐใดๆ อาจใช้อำนาจเพื่อทำร้ายรัฐอื่นได้ ดังนั้นรัฐควรมีอำนาจมากพอที่จะรุกรานผู้อื่นได้ถึงจะปลอดภัย

2.2.2 ทฤษฎีเสรีนิยม (Liberalism)

เสรีนิยมมีความแตกต่างจากสัจนิยม โดยนักคิดเสรีนิยมสนใจเรื่องสันติภาพมากกว่าสงคราม นักคิดที่สำคัญของสำนักนี้คือ Immanuel Kant ที่เชื่อว่า รัฐที่เป็นสาธารณรัฐ จะเป็นผู้ผลิตสันติภาพ (peace producers) เพราะรัฐที่สร้างบนพื้นฐานของกฎหมายย่อมจะพยายามสร้างระบอบระหว่างประเทศที่มีกฎหมายกำกับ (Navari, 2008, pp. 29-39)

(1) Douce commerce ที่เชื่อว่าแรงจูงใจจากโอกาสในการค้าระหว่างประเทศจะนำมาซึ่งความร่วมมือระหว่างประเทศที่ทำให้รัฐจะมีพฤติกรรมเพื่อสันติภาพมากกว่าความขัดแย้ง กล่าวคือ การพึ่งพากันของรัฐต่าง ๆ โดยเฉพาะทางเศรษฐกิจจะทำให้เกิดสันติภาพในโลก
(2) Democratic peace thesis ที่ชื่อว่า รัฐเสรีจะไม่ทำสงครามระหว่างกันเอง ดังนั้นหากรัฐต่าง ๆ เป็นประชาธิปไตย โลกก็จะมีสันติภาพ ดังที่เรียกว่า “democratic peace”
(3) Neoliberal institutionalism ที่ให้ความสำคัญกับบทบาทของสถาบันระหว่างประเทศในการบรรเทาความขัดแย้ง อย่างบทบาทของสหประชาชาติในการเป็นผู้ไกล่เกลี่ยความขัดแย้งระหว่างรัฐ แม้ว่าสถาบันระหว่างประเทศจะไม่สามารถเปลี่ยนสภาวะอนาธิปไตยของระบบระหว่างประเทศได้อย่างสมบูรณ์ แต่ก็สามารถเปลี่ยนบรรยากาศระหว่างประเทศที่ช่วยกำหนดพฤติกรรมของรัฐให้มีความร่วมมือกันมากขึ้น และสำหรับ constructivist institutionalism ความเป็นสถาบันระหว่างประเทศมิได้จำกัดอยู่เพียงองค์การที่มีโครงสร้างชัดเจน แต่รวมถึงบรรทัดฐานระหว่างประเทศ กฎหมายระหว่างประเทศด้วย

2.2.3 **ทฤษฎีประกอบสร้าง** (constructivism)

ในทฤษฎีนี้ผู้วิจัยจะขอทับศัพท์เป็น ทฤษฎี constructivism ที่ให้ความสำคัญกับบทบาทของแนวความคิด อุดมการณ์ที่ทำหน้าที่ประกอบสร้างทางสังคมให้การเมืองโลก ดังที่ Alexander Wendt ได้นำเสนอไว้ในบทความเรื่อง “Anarchy is What States Make of it” และมีส่วนทำให้ความมั่นคงศึกษาขยายขอบเขตออกไปผ่านสำนักคิดแบบ Copenhagen School ที่มีสมมติฐานหลักว่า “ความมั่นคง” เป็นสิ่งที่สังคมสร้างขึ้น (McDonald, 2008, pp. 60-67) โดย Matt McDonal ได้ยกตัวอย่าง กรณีการบุกอิรักในปี ค.ศ. 2003 ที่แสดงให้เห็นถึงกระบวนการประกอบสร้าง (construct) โดยความเข้าใจในอัตลักษณ์ที่ต่างกันในสังคม ซึ่งจะสามารถอธิบายได้ว่า

เพราะอะไรอังกฤษและสหรัฐอเมริกาถึงมองว่า การที่อิรัก โดยซัดดัม ฮุสเซน อาจจะกำลังพัฒนาอาวุธนิวเคลียร์ในช่วงปี ค.ศ. 2002 – 2003 เป็นภัยคุกคาม มากกว่ารัฐที่ครอบครองอาวุธนิวเคลียร์อยู่แล้วอย่าง รัสเซีย จีน ฝรั่งเศส ปากีสถาน อินเดีย หรืออิสราเอล และเป็นภัยคุกคามมากพอที่จะตัดสินใจมีปฏิบัติการทางทหารเพื่อแทรกแซงและเปลี่ยนแปลงระบอบซัดดัม ฮุสเซน ซึ่งคำอธิบายของนักคิดในสำนักทฤษฎี constructivism มองย้อนไปถึงประวัติศาสตร์ความขัดแย้งระหว่างกันตั้งแต่สมัยสงครามอ่าวครั้งที่ 1 ทำให้ผู้นำทางการเมืองในอังกฤษและสหรัฐอเมริกามองว่า ระบอบของซัดดัม ฮุสเซนทำให้อิรักเป็น rouge state และเป็นภัยคุกคามต่อความมั่นคง นอกจากนี้ นักคิดในสำนักทฤษฎีประกอบสร้างยังเห็นว่า “ความมั่นคง” เป็นผลผลิตของการเจรจาต่อรองระหว่างตัวแสดงจากกลุ่มต่าง ๆ ซึ่งในที่นี้รวมถึงสาธารณชนด้วย มิได้จำกัดอยู่เพียงแต่ผู้กำหนดนโยบายเท่านั้น ดังนั้น สุนทรพจน์ ถ้อยแถลงจากการประชุม การให้สัมภาษณ์ หรือข้อคิดเห็นจากบุคคลผู้มีชื่อเสียง ก็สามารถสร้างประเด็นความมั่นคงขึ้นมาได้

The Copenhagen School เกิดขึ้นมาจากสำนัก constructivism เพื่อพัฒนาทฤษฎีหรือกรอบแนวคิดสำหรับการศึกษาความมั่นคงจากมุมมองแบบ constructivist แบบดั้งเดิม โดยเป็นชื่อ Copenhagen School เพราะเกิดขึ้นที่ Copenhagen Peace Research Institute ในเดนมาร์ก นำโดย Barry Buzan และ Ole Waever ซึ่งมุมมองของสำนักนี้พัฒนาขึ้นจากบริบทของโลกในช่วงหลังสงความเย็นที่ขยายขอบเขตของการนิยามความมั่นคงให้ครอบคลุมในประเด็นที่เคยถูกละเลย อย่างเรื่อง การเปลี่ยนแปลงของสิ่งแวดล้อม ความยากจน และ สิทธิมนุษยชน (McDonald, 2008, p. 68; Mitra, 2010) และหนึ่งในแนวคิดสำคัญของ Copenhagen School คือ กระบวนการทำให้เป็นความมั่นคง หรือ Securitization ซึ่งถูกนำเสนอในรายละเอียดโดย Ole Waever ในปี ค.ศ. 1995 ซึ่งเป็นกระบวนการที่ตัวแสดง (actor) ได้ประกาศประเด็นใดประเด็นหนึ่ง (particular issue) พลวัตรการเปลี่ยนแปลง หรือ ตัวแสดงใด ๆ ให้เป็น ภัยคุกคามที่ดำรงอยู่ (existential threat) ต่อ referent object หนึ่ง ซึ่งหากการประกาศหรือกำหนดนี้ได้รับการยอมรับจากผู้ฟังที่เกี่ยวข้อง (relevant audience) ประเด็นดังกล่าวก็จะทำให้เกิดมาตรการฉุกเฉินเพื่อตอบรับวิกฤตดังกล่าว ทั้งนี้ ในกระบวนการทำให้ประเด็นใด ๆ เป็นประเด็นด้านความมั่นคงจะมีการใช้ speech act ซึ่งเป็นการผ่านการกระทำทางคำพูด โดยใช้ภาษาของความมั่นคงและภัยคุกคาม

เพื่อทำให้ประเด็นนั้นกลายเป็นภัยคุกคาม ดังเช่นในกรณีที่ ผู้นำทางการเมือง หรือผู้มีอำนาจอ้างว่ากล่าวในฐานะผู้แทนของรัฐหรือประเทศ และสร้างการรับรู้ของสาธารณะว่าเป็นสถานการณ์ที่ต้องมีมาตรการฉุกเฉินรับมือ เช่น การสั่งเคลื่อนพลทหาร เป็นต้น ตัวอย่างที่เห็นได้ชัด คือ การทำให้ทำให้ประเด็นเรื่องผู้อพยพ (immigrants) ที่มิได้ถูกมองว่าเป็นประเด็นด้านความมั่นคงมาก่อน กลายเป็นประเด็นด้านความมั่นคงสำหรับรัฐประชาธิปไตย โดยมีการใช้ภาษาบรรยายภาพให้กลุ่มผู้อพยพเป็นภัยคุกคามที่ต้องรับมือ

2.3 วรรณกรรมที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์

ด้วยพัฒนาการทางเทคโนโลยีที่ก้าวหน้าขึ้น เทคโนโลยีสารสนเทศกลายเป็นเครื่องมือในการติดต่อสื่อสาร ทำธุรกรรมต่าง ๆ ทำให้เกิดเป็นอีกหนึ่งสภาพแวดล้อม ที่เปลี่ยนแปลงลักษณะทางสังคมของมนุษย์ซึ่งนำมาซึ่งภัยคุกคามต่อความมั่นคงของมนุษย์ในอีกรูปแบบหนึ่ง การเปลี่ยนแปลงที่ว่า คือ การเกิดขึ้นของการเปลี่ยนแปลงสู่ยุคดิจิทัล การเกิดขึ้นของคอมพิวเตอร์และระบบอินเทอร์เน็ตได้สร้าง cyberspace หรือพื้นที่สมมติในโลกดิจิทัล ซึ่งเป็นพื้นที่ที่มิได้มีขอบเขตทางกายภาพเหมือนเส้นเขตแดนของประเทศหรือเขตพื้นที่ส่วนตัวเหมือนในโลกแห่งความจริง

ในหนังสือของ Ananda Mitra เรื่อง Digital Security Cyber Terror and Cyber Security ได้อธิบายความท้าทายแรก ๆ ของโลกดิจิทัล คือ ปัญหาการระบุตัวตนของบุคคลในโลกดิจิทัล และโอกาสในการเกิดการขโมยอัตลักษณ์ในโลกดิจิทัล ซึ่งปัญหานี้ยังคงดำรงอยู่เช่นทุกวันนี้ ที่หลาย ๆ ครั้ง ไม่มีการคุ้มครองปกป้องข้อมูลส่วนบุคคลที่ดีพอ ทำให้ข้อมูลส่วนตัวที่ผู้คนกรอกไปในโลกอินเทอร์เน็ตเพื่อลงทะเบียนเข้ารับบริการมีโอกาสถูกนำไปใช้ในทางที่ผิดได้ อีกทั้ง ยังสามารถสวมรอยดำเนินการแทนกันได้ ในอีกกรณีหนึ่ง คือ การกดยอมรับข้อตกลงการใช้บริการที่อนุญาตให้ผู้ให้บริการเก็บข้อมูลและนำข้อมูลดังกล่าวไปเผยแพร่หรือขายต่อ (Mitra, 2010, pp. 13-14) นอกจากนี้ การปฏิสัมพันธ์ระหว่างกันของผู้คนในโลกอินเทอร์เน็ตมีแนวโน้มที่จะถูกหลอกลวงได้ง่าย เพราะ ผู้คนสามารถสร้างตัวตนปลอม หรือ นามแฝงขึ้นมาในโลกดิจิทัลได้ และการทำความรู้จักกันในโลกอินเทอร์เน็ตเป็นเพียงการทำความรู้จักกันจากข้อมูลที่เจ้าตัวป้อนเข้ามาในระบบซึ่งอาจสร้างขึ้นได้

บทความเรื่อง “พลวัตความมั่นคงทางไซเบอร์ของประเทศไทย” โดย กนกนก โพธิ์หอม ในวารสารมุมมองความมั่นคง ประจำเดือนมิถุนายน-กันยายน 2564 เขียนเกี่ยวกับการกำหนดคำนิยามของ ความมั่นคงทางไซเบอร์ของไทยไว้ว่า หน่วยงานที่เกี่ยวข้องด้านพลเรือนจะมองความมั่นคงทางไซเบอร์ในมุมมองที่กว้างกว่า คือ เป็น “การกระทำความผิดหรือทำลายความมั่นคงของประเทศผ่านระบบคอมพิวเตอร์” ในขณะที่หน่วยงานที่เกี่ยวข้องทางการทหาร เช่น กองทัพ มองว่าเป็น “การกระทำใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมีจุดหมายเพื่อประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่น ๆ ที่เกี่ยวข้อง” (กนกนก โพธิ์หอม, 2564, หน้า 48-49)

สำหนับนิยามของคำว่า ความมั่นคงไซเบอร์ สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU ได้ให้คำจำกัดความว่า ความมั่นคงไซเบอร์ คือ “ชุดเครื่องมือ นโยบาย วิธีคิดเกี่ยวกับความมั่นคง การรักษาความปลอดภัย แนวทาง วิธีการจัดการความเสี่ยง การลงมือปฏิบัติ การฝึกอบรม วิธีปฏิบัติที่เป็นเลิศ การสร้างความเชื่อมั่นและเทคโนโลยีที่สามารถนำมาใช้ปกป้องสิ่งแวดล้อมทางไซเบอร์และทรัพย์สินขององค์กรและผู้ใช้ทรัพย์สินขององค์กรและผู้ใช้ประกอบการไปด้วยอุปกรณ์ที่เชื่อมต่อด้วยคอมพิวเตอร์ บคุลากร โครงสร้างพื้นฐานแอพพลิเคชั่นการให้บริการระบบโทรคมนาคมและองค์รวมของข้อมูลที่ถูกส่งผ่านหรือรักษาไว้ในสิ่งแวดล้อมทางไซเบอร์ ความมั่นคงไซเบอร์มุ่งที่จะทำให้ได้มาและรักษาไว้ซึ่งความมั่นคงของทรัพย์สินขององค์กรและผู้ใช้จากความเสี่ยงในสิ่งแวดล้อมทางไซเบอร์ วัตถุประสงค์ด้านความมั่นคง โดยทั่วไปประกอบด้วย 1) การรักษาสภาพความพร้อมใช้งานของข้อมูล (Availability) 2) การรักษาความครบถ้วนสมบูรณ์ของข้อมูล (Integrity) ซึ่งรวมถึงการยืนยันตัวตน (Authenticity) และการห้ามปฏิเสธความรับผิดชอบของทั้งผู้รับและผู้ส่งข้อมูล (Non-repudiation) และ 3) การรักษาความลับของข้อมูล (Confidentiality) (วศิน ปั้นทอง, หน้า 14)

David Wall นักวิชาการด้าน Criminal Justice and Information Technology และผู้อำนวยการ Centre of Criminal Justice Studies ที่มหาวิทยาลัยลีดส์ ได้กล่าวถึงการถกเถียงเรื่องนิยามคำว่า อาชญากรรมไซเบอร์ (Cybercrime) ไว้ว่า อาจแบ่งได้เป็น 3 กลุ่มใหญ่ ๆ คือ

กลุ่มที่หนึ่ง มองว่า อาชญากรรมไซเบอร์ คือ อาชญากรรมแบบดั้งเดิม (traditional) ที่ใช้คอมพิวเตอร์มาเป็นวิธีการหนึ่งของการก่ออาชญากรรม ซึ่งอาจเป็นการสื่อสาร หรือการหาข้อมูลเกี่ยวกับเหยื่อ หรือทำให้บุคคลใดเสื่อมเสีย ซึ่งกลุ่มนี้มองว่า แม้ไม่มีอินเทอร์เน็ต อาชญากรรมเหล่านี้ก็ยังคงอยู่เพียงแต่เปลี่ยนรูปแบบการสื่อสาร

กลุ่มที่สอง มองว่าอาชญากรรมไซเบอร์ คือ อาชญากรรมดั้งเดิมที่เทคโนโลยีสาระสนเทศช่วยสร้างโอกาสใหม่ในการก่ออาชญากรรมระดับโลก เช่น การหลอกลวงทางการเงินระดับโลก สื่อลามกระดับโลก เป็นต้น ซึ่งหากไม่มีอินเทอร์เน็ตกระบวนการเหล่านี้ก็จะยังคงอยู่ในรูปแบบอื่น เพียงแต่เป็นในระดับที่ไม่แพร่หลายเป็นระดับโลก

กลุ่มที่สาม มองว่า อาชญากรรมไซเบอร์นั้นเป็นผลผลิตของอินเทอร์เน็ตที่สร้างโอกาสการก่ออาชญากรรมให้เกิดขึ้นในพื้นที่ไซเบอร์ เช่น การขโมยลิขสิทธิ์ การหลอกลวงทางอินเทอร์เน็ต และหากไม่มีอินเทอร์เน็ต อาชญากรรมเหล่านี้จะหายไป ซึ่งในการทำความเข้าใจอาชญากรรมไซเบอร์ David Wall ยังมีข้อสังเกตว่า ลักษณะเด่นของอาชญากรรมไซเบอร์อาจจำแนกได้เป็น 3 แบบ (Wall, 2004) ดังนี้

1) Computer integrity crimes ที่เป็นอาญชากรรมที่โจมตีระบบ (assault the integrity network) โดยตรงเพื่อเข้าถึงข้อมูลหรือกลไกของระบบ เช่นการ แฮคระบบ การโจมตีระบบด้วยไวรัส
2) Computer related crimes ที่เป็นอาญชากรรมที่ใช้ระบบคอมพิวเตอร์เพื่อเข้าถึงเหยื่อด้วยความตั้งใจที่จะหลอกเอาเงิน สินค้า หรือบริการจากเหยื่อ) เช่น เว็บไซต์ phishing เป็นต้น
3) Computer content crimes ที่เป็นอาชญากรรมที่เกี่ยวข้องกับ ข้อมูลผิดกฎหมายในระบบคอมพิวเตอร์ เช่น การขายและเผยแพร่สื่อลามก หรือ การเผยแพร่ข้อมูลที่สร้างให้เกิดอาชญากรรมที่เกิดจากความเกลียดชัง (hate crime)

นอกจากการจำแนกประเภทอาชญากรรมไซเบอร์ของ David Wall ข้างต้น เขายังได้เสนอว่าองค์ประกอบหลักของอาชญากรรมไซเบอร์มีอยู่ 4 ประการ ได้แก่ 1) การรุกล้ำทางไซเบอร์ (Cyber-trespass) เช่น การเจาะระบบโดยไม่ได้รับอนุญาต 2) การหลอกลวงในพื้นที่ไซเบอร์ (Cyber-deception) เช่น การหลอกขอข้อมูลรหัสบัตรเครดิต การละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาใน

พื้นที่ไซเบอร์ หรือที่เรียกว่า cyber piracy 3) สื่อลามกในพื้นที่ไซเบอร์ (Cyber-pornography/obscenity) รวมถึงที่เกี่ยวข้องกับเด็กและเยาวชนด้วย และ 4) ความรุนแรงทางไซเบอร์ (Cyber-violence) ซึ่งคือ การข่มขู่คุกคามหรือใช้พื้นที่ไซเบอร์แสดงประทุษวาจาต่อผู้อื่น (วศิน ปั้นทอง)

เมื่อพิจารณาจากลักษณะเด่นและประเภทของอาชญากรรมไซเบอร์ตามแนวคิดของ David Wall จะพบว่า อาชญากรรมไซเบอร์ มุ่งกระทำต่อ referent object ใน 3 ระดับ คือ ระดับปัจเจกบุคคลโดยมีเป้าหมายคุกคามต่อผู้คนและทรัพย์สินส่วนบุคคล เป็นเป้าหมายทางเศรษฐกิจระดับภาคธุรกิจเอกชนผ่านการเจาะระบบ ขโมยข้อมูลต่าง ๆ ซึ่งยังคงจำกัดอยู่ในระดับเป้าหมายทางเศรษฐกิจ และระดับรัฐ ที่อาจมีการกระทำบนฐานของอุดมการณ์ทางการเมือง หรือการโจมตีระบบที่มีลักษณะข้ามพรมแดนชาติ

2.4 วรรณกรรมที่เกี่ยวข้องกับความมั่นคงทางไซเบอร์ของไทย

รัฐต่าง ๆ เริ่มให้ความสำคัญกับประเด็นด้านความมั่นคงทางไซเบอร์มากขึ้นตามพัฒนาการทางเทคโนโลยี สำหรับประเทศไทย ประเด็นทางไซเบอร์ก็เป็นหนึ่งในเรื่องที่รัฐให้ความสำคัญด้วยการทำให้เป็นความมั่นคง (Securitization) โดยในบริบทการจัดการภัยคุกคามทางไซเบอร์ของประเทศไทยนั้น ไทยมีการดำเนินการกำหนดมาตรการป้องกันภัยคุกคามทางไซเบอร์แบบองค์รวม เน้นการให้ความรู้ตระหนักถึงภัยคุกคามที่อาจเกิดขึ้น วิธีการป้องกันและรับมือกับภัยที่อาจเกิดขึ้น โดยเฉพาะในการทำธุรกรรมใดๆ ทางออนไลน์ เน้นป้องกันอาชญากรรมที่จะเกิดผลกระทบต่อระบบเศรษฐกิจและหน่วยงานโดยตรง ซึ่งอาชญากรรมในลักษณะนี้ อาชญากรมีวัตถุประสงค์เพื่อหลอกลวงและหวังผลประโยชน์ทางเศรษฐกิจเท่านั้น มิได้หวังทำลายความมั่นคงของรัฐ จึงถูกมองว่าเป็น ภัยคุกคามภายในรัฐ (Intra State Threat) การดำเนินคดีหรือดำเนินการจัดการเป็นอำนาจของรัฐไทยที่ดำเนินการติดตามได้อย่างเต็มที่ ซึ่งมุมมองนี้ของไทยแตกต่างจากประเทศอื่น ๆ ที่ให้ความสำคัญกับการป้องกันภัยคุกคามทางไซเบอร์ที่มาจากภายนอกประเทศ (Inter State Threat)

สำหรับประเทศไทย เพื่อรับมือกับภัยคุกคามทางไซเบอร์ ได้มีการจัดทำแผนยุทธศาสตร์และกฎหมายภายในประเทศเพื่อบริหารจัดการรักษาความมั่นคงทางไซเบอร์ โดยหน่วยงานด้านความมั่นคงของไทยที่เกี่ยวข้องได้ร่วมกันวางกรอบการทำงานโดยจัดทำยุทธศาสตร์ชาติ และแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นด้านความมั่นคง พ.ศ. 2561 – 2580 จัดทำเป็น ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564 (National Cybersecurity Strategy 2017 – 2021) เพื่อเป็นกรอบดำเนินการด้านความมั่นคงทางไซเบอร์ของไทย (กนกนก โพธิ์หอม, 2564)

ในส่วนของกฎหมายมีการจัดทำพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดนโยบาย มาตรการ แนวทางรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ การจัดทำพระราชบัญญัติฉบับนี้สะท้อนให้เห็นว่า ภาครัฐ มองว่า ประเด็นด้านไซเบอร์เป็นประเด็นความมั่นคงที่รัฐต้องรับมือ จึงได้มีการจัดตั้ง “สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบตามพระราชบัญญัติด้วย ต่อมา ได้มีการออกพระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เพื่อรับมือกับปัญหาเรื่องการหลอกลวงทางโทรศัพท์ หรือที่เรียกกันในภาษาชาวบ้านว่าแก๊งคอลเซ็นเตอร์ ซึ่งการหลอกลวงทางโทรศัพท์นี้ พระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ให้เป็นนิยาม “อาชญากรรมทางเทคโนโลยี” ไว้ว่า หมายความว่า การกระทำหรือความพยายามกระทำผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกงกรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562)

นายรุ่งโรจน์ กิตติถาวรกุล ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย ได้เผยแพร่บทความในข่าวสารจุฬาฯ เรื่อง “รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว” โดยนำเสนอนิยามคำว่า อาชญากรรมทางไซ

เบอร์ หรือ Cybercrime ว่า เป็นการกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย และ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย (นายรุ่งโรจน์ กิตติถาวรกุล, ม.ป.ป.) ซึ่งรูปแบบของอาชญากรรมสอดคล้องกับรูปแบบอาชญากรรมของไซเบอร์ของ David Wall คือ เป็นการโจมตีระบบคอมพิวเตอร์โดยตรง (hack) แก้ไข ทำลาย ขโมยข้อมูลในระบบคอมพิวเตอร์ มีการหลอกลวงให้เสียงทรัพย์ (scam) โดยรูปแบบอาชญากรรมทางไซเบอร์ที่พบมาเป็น 3 อันดับแรกในปี พ.ศ. 2565 ได้แก่

1) การหลอกลวงโดยการแอบอ้างให้ตนเป็นบุคคลอื่น หรือคนที่น่าเชื่อถือ เพื่อเข้าถึงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับของเหยื่อ เช่น การส่งอีเมลล์ (E-mail) ส่งข้อความทางโทรศัพท์ (SMS) เพื่อหลอกให้กรอกข้อมูลส่วนบุคคล หรือส่งลิงก์เว็บไซต์ปลอมให้คนคลิกเข้าไปเพื่อหลอกให้กรอกข้อมูลโดยสมัครใจหรือแฝงโปรแกรมดูดข้อมูลส่วนบุคคลอย่างไม่สมัครใจ ผ่าน Ransomware ที่อาจสามารถเข้าสู่ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ผ่านการเข้าเว็บไซต์ที่ไม่ปลอดภัย หรือการดาวน์โหลดไฟล์ driver จากอินเทอร์เน็ต
2) การละเมิดข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต โดยมีการเปลี่ยนแปลงแก้ไขหรือทำให้เสียหาย หรือนำข้อมูลส่วนบุคคลไปเผยแพร่ต่อผู้อื่น ซึ่งภัยคุกคามทางไซเบอร์ในลักษณะนี้มักเกิดจากการบุกรุก และ/หรือการโจมตีระบบผ่านทางช่องโหว่ (hack)
3) การหลอกลวงในการซื้อขายสินค้าและบริการออนไลน์ เช่น ขายสินค้าปลอม ขายสินค้าละเมิดลิขสิทธิ์แต่อ้างว่าเป็นสินค้าแท้ หรือหลอกให้ชำระเงินผ่านทางระบบออนไลน์แต่ไม่ได้รับสินค้าหรือบริการตามที่ตกลงกันไว้

บทที่ 3

ปัญหาภัยคุกคามทางไซเบอร์และการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง

พัฒนาการทางเทคโนโลยีได้เปลี่ยนแปลงวิถีชีวิตของผู้คนไปจากเดิมมาก การเกิดพื้นที่ทางไซเบอร์เพื่อใช้ประโยชน์ในด้านต่าง ๆ เพิ่มขึ้น ไม่ว่าจะเป็นด้านธุรกรรมทางการเงิน ผ่านระบบอินเทอร์เน็ตแบงค์กิ้ง (internet banking) ด้านการซื้อขายสินค้าออนไลน์ (e-commerce) ซึ่งเกี่ยวข้องกับการชำระเงินผ่านบัตรเครดิตในระบบออนไลน์หรือระบบอินเทอร์เน็ตแบงค์กิ้ง การลงทะเบียนรับบริการทางออนไลน์ต่าง ๆ การลงทะเบียนเพื่อใช้บริการแอพพลิเคชั่นผ่านสมาร์ทโฟน พื้นที่ทางไซเบอร์กลายเป็นพื้นที่ที่มีมูลค่าสูงขึ้นและส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจ โดยเฉพาะเมื่อการใช้โทรศัพท์สมาร์ทโฟนแพร่หลายขึ้น ผู้คนทำธุรกรรมผ่านแพลทฟอร์มดิจิทัลมากขึ้น ทั้งในด้านการติดต่อ สื่อสาร กิจกรรมสันทนาการ การเดินทาง (transportation) ระบบนำทาง (navigation systems) แม้กระทั่งเรื่องสาธารณสุขก็สามารถกระทำออนไลน์ได้ กระแสโลกาภิวัตน์และสถานการณ์ในโลกอย่างการแพร่ระบาดของโรคโควิด-19 เป็นปัจจัยเร่งให้โลกก้าวสู่สังคมดิจิทัลรวดเร็วขึ้นในหลาย ๆ ด้าน แน่นอนว่าเมื่อโลกดิจิทัลเริ่มเข้ามามีบทบาทในชีวิตประจำวันของประชาชนมากขึ้น ผลคือ ปฏิสัมพันธ์ทางสังคมและกิจกรรมทางเศรษฐกิจที่เกิดขึ้นผ่านระบบดิจิทัลนี้เองที่ทำให้พื้นที่ไซเบอร์ มีความสำคัญขึ้น ข้อมูลส่วนบุคคลต่าง ๆ เข้าไปอยู่ในพื้นที่ไซเบอร์ ในบทนี้ จึงจะกล่าวถึงปัญหาแก๊งคอลเซ็นเตอร์และกระบวนการที่ทำให้ปัญหาดังกล่าวกลายเป็นปัญหาความมั่นคง โดยประกอบไปด้วย การทำให้ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทยหน่วยงานที่เกี่ยวข้องในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ของไทย และกระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง ตามลำดับ

3.1 การทำให้ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของไทย

โดยที่ผลกระทบจากภัยคุกคามทางไซเบอร์ส่งผลกระทบโดยตรงในชีวิตประจำวันของประชาชนมากขึ้นเรื่อย ๆ ประเด็นเรื่องความมั่นคงทางไซเบอร์ถูกทำให้เป็นประเด็นด้านความ

มั่นคง (securitization) โดยรัฐไทยให้ความสำคัญกับพื้นที่ไซเบอร์เนื่องจากมองว่าที่เป็นพื้นที่ที่มีมูลค่าทางเศรษฐกิจที่ส่งผลต่อประชาชนโดยตรง จึงถือเป็นผลประโยชน์แห่งชาติ และระบุให้ประเด็นเรื่อง “ความมั่นคงทางไซเบอร์” เป็นประเด็นความมั่นคงที่รัฐต้องให้ความสำคัญ ดังที่จะเห็นได้จากกระบวนการตรากฎหมาย ดังนี้

1. พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 สะท้อนให้เห็นถึงการรับรู้ (perception) ของรัฐไทย ว่า ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญ โดยกฎหมายดังกล่าวระบุว่า “พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล.....” แต่เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัติดังกล่าวเป็นไปเพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่งนิยามตามพระราชบัญญัตินี้ ระบุว่า “ไซเบอร์” คือ ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป และให้นิยามคำว่า “ภัยคุกคามทางไซเบอร์” ว่า คือ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562, 2562)

2. พระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เพื่อรับมือกับปัญหาเรื่องการหลอกลวงทางโทรศัพท์ หรือที่เรียกว่าแก๊งคอลเซ็นเตอร์ การออกกฎหมายเป็นพระราชกำหนด แทนที่จะออกเป็นพระราชบัญญัติโดยรัฐสภา สะท้อนให้เห็นว่า กฎหมายนี้มีความรีบด่วน และถือว่ามีความจำเป็นในเรื่องที่จะรักษาความมั่นคงในทางเศรษฐกิจ ความปลอดภัยของประเทศ ในลักษณะเดียวกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีบางบทบัญญัติที่เกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคลที่

รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติแห่งกฎหมาย ซึ่งเหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพบุคคลเป็นไปเพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ซึ่งแต่ละวันมีผู้ถูกหลอกลวงจำนวนมากและมีมูลค่าความเสียหายสูงมากสมควรมีมาตรการเพื่อป้องกันและปราบปรามอาชญากรรมประเภทนี้ให้หมดไปโดยเร็ว อันเป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจหลีกเลี่ยงได้ เพื่อรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ และความมั่นคงในทางเศรษฐกิจของประเทศ (พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566, 2566)

เหตุผลและความจำเป็นในการตรากฎหมายแสดงให้เห็นว่ารัฐให้ความสำคัญกับภัยคุกคามจากปัญหาแก๊งคอลเซ็นเตอร์มากขึ้นข้อมูลจากรายงานจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ พบว่า ในปี พ.ศ. 2564 ประเทศไทยมีการหลอกลวงผ่านโทรศัพท์มากกว่า 6.4 ล้านครั้ง เพิ่มขึ้นกว่าร้อยละ 270 จากปี พ.ศ. 2563 และมีการส่งข้อความขนาดสั้นหรือเอสเอ็มเอส (SMS) หลอกลวงเพิ่มขึ้นถึงร้อยละ 57 และในปี พ.ศ. 2564 มีผู้เสียหายเข้าแจ้งความกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กว่า 1,600 คน มูลค่าความเสียหายสูงกว่า 1,000 ล้านบาท โดยระบุว่ามูลเหตุจูงใจการกระทำผิด คือ รายได้ที่ได้รับจากการก่อเหตุมีมูลค่าเป็นจำนวนมหาศาล ในขณะที่บทลงโทษตามกฎหมายไม่มีความรุนแรง อาจกล่าวได้ว่า การที่บทลงโทษตามกฎหมายยังไม่มีความรุนแรงเป็นเหตุให้เกิดการกระทำผิดมากขึ้นเรื่อย ๆ รัฐจึงได้ออกพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ขึ้นมาเพื่อรับมือกับภัยคุกคามดังกล่าว (อาริยา สุขโต, 2565) ซึ่งบริบทในขณะนั้น ที่ประชุมคณะรัฐมนตรีเห็นว่ามีอาชญากรรมหลอกลวงประชาชนให้โอนเงินผ่านการติดต่อทางโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ขยายตัวรวดเร็วมาก และเกิดเป็นความเสียหายในวงกว้าง ทั้งในแง่ของจำนวนคดีเฉลี่ยต่อวัน และมูลค่าความเสียหายที่สูงกว่า 22,000 ล้านบาท จึงจำเป็นต้องออกกฎหมายเฉพาะที่ให้อำนาจสถาบันการเงินหรือผู้ประกอบธุรกิจสามารถระงับการทำธุรกรรมใด ๆ ที่ต้องสงสัยว่าเป็นธุรกรรมที่กระทำผิดทางอาญา โดยเฉพาะการหลอกลวงประชาชนให้โอนเงินไปยังบัญชีผู้อื่นที่อยู่ในขบวนการเป็นทอด ๆ อย่าง

รวดเร็วผ่านบัญชีม้า เพื่อให้เจ้าหน้าที่สามารถระงับการทำธุรกรรมหรืออายัดเงินได้ทันท่วงที (สรวิศ บุญมี, 2566)

พระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีบทบัญญัติที่จัดการกับองค์ประกอบหนึ่งของปัญหาคอลเซ็นเตอร์ คือ การสกัดกั้นการเปิดบัญชีม้า หรือ เบอร์ม้า ที่ทำให้ไม่สามารถติดตามระบุตัวตนไปถึงผู้กระทำผิดตัวจริงได้ โดยกฎหมายกำหนดบทลงโทษต่อผู้ที่รับจ้างเปิดบัญชีหรือเบอร์โทรศัพท์ให้ผู้อื่น ระบุว่า “เจ้าของบัญชีม้า หรือเบอร์ม้า ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ รวมถึงผู้ที่เป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใดๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ บัญชีเงินอิเล็กทรอนิกส์ ตลอดจนเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่ 2 - 5 ปี หรือปรับตั้งแต่ 200,000 - 500,000 บาท หรือทั้งจำทั้งปรับ” (กรมประชาสัมพันธ์, 2566)

กรณีการเปิดบัญชีม้าแสดงให้เห็นว่า ปัญหาแก๊งคอลเซ็นเตอร์นอกจากจะถือเป็น Computer related crime ตามการนิยามของ David Wall แล้วยังมีความเกี่ยวข้องกับการฟอกเงินด้วย เนื่องจากการเปิดบัญชีม้าถือเป็นการกระทำที่สนับสนุนให้เกิดการกระทำผิดฐานฉ้อโกงบุคคลอื่น

3.2 หน่วยงานที่เกี่ยวข้องในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ของไทย

ในกระบวนการทำให้เป็นประเด็นความมั่นคงนอกจากด้านกฎหมายแล้วภาครัฐต้องจัดตั้งหน่วยงานรับผิดชอบเพื่อดำเนินการรับมือกับภัยคุกคามที่เกิดขึ้นนั้นด้วย ในส่วนของประเทศไทยได้มีการจัดตั้งหน่วยงานที่เกี่ยวข้อง ดังนี้

3.2.1 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

สกมช. เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีหน้าที่ประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน เพื่อป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ โดย สกมช. มีอำนาจหน้าที่หลัก 16 ประการ (สกมช., (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, n.d.) ได้แก่

(1) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(2) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(3) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(4) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

(5) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

(6) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(7) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ

(8) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(9) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

(10) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

(11) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

(12) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

(13) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

(14) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(15) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ตามระยะเวลาที่คณะกรรมการกำหนด

(16) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมายเพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจ

ทั้งนี้ อำนาจหน้าที่ 16 ประการของ สกมช. เน้นไปที่การจัดทำนโยบายและแผน สร้างความตระหนักรู้ รายงานสถานการณ์ ประเมินความเสี่ยงของสถานการณ์ด้านไซเบอร์ และเป็นหน่วยงานรับผิดชอบหลักในการรักษาความมั่นคงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ แต่มิได้มีอำนาจจับกุม ดำเนินคดีกับผู้กระทำผิดในอาชญากรรมทางเทคโนโลยีที่ส่งผลต่อปัจเจกบุคคล

3.2.2 กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)

บช.สอท. หรือเป็นที่รู้จักในชื่อ "กองบัญชาการตำรวจไซเบอร์" เกิดขึ้นเพื่อรับมือกับการกระทำความผิดในหลายลักษณะ เช่น การหลอกลวงจำหน่ายสินค้าออนไลน์ การขโมยข้อมูลส่วนบุคคลเพื่อนำไปทำธุรกรรมทางอิเล็กทรอนิกส์ของธนาคาร การนำข้อมูลเข้าสู่ระบบคอมพิวเตอร์โดยมิชอบ หรือการนำเข้าข้อมูลอันเป็นเท็จซึ่งกระทบต่อสิทธิของผู้อื่น ความมั่นคง และความสงบเรียบร้อยของสังคม อีกทั้ง เพื่อรับมือกับคดีอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ ที่มีความสลับซับซ้อนขึ้น มีมูลค่าความเสียหายมากขึ้น และมีแนวโน้มเพิ่มมากขึ้น โดยก่อนหน้าที่จะมี บช.สอท. นั้น สำนักงานตำรวจแห่งชาติได้มีส่วนราชการระดับ “กองบังคับการ” รับผิดชอบการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีกระจายอยู่ในหลายหน่วยงาน ได้แก่ (1) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) สังกัดกองบัญชาการตำรวจสอบสวนกลาง เป็นหน่วยงานเฉพาะด้านที่รับผิดชอบคดีอาชญากรรมทางเทคโนโลยี (2) กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) สังกัดสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบการตรวจสอบและวิเคราะห์การกระทำความผิด (3) ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) สำนักงานตำรวจแห่งชาติ รับผิดชอบแก้ไขปัญหา ป้องกัน ปราบปราม อาชญากรรมทางเทคโนโลยี อย่างไรก็ดี โครงสร้างในลักษณะดังกล่าวยังไม่สามารถรองรับคดีอาชญากรรมทางเทคโนโลยีที่เกิดขึ้นทั่วราชอาณาจักรและมีแนวโน้มเพิ่มมากขึ้นได้ จึงได้ปรับโครงสร้างองค์กรจัดตั้งเป็นหน่วยงานระดับ “กองบัญชาการ” ขึ้นมาเป็น บช.สอท หรือ "กองบัญชาการตำรวจไซเบอร์" เพื่อเพิ่มศักยภาพในการวิเคราะห์สาเหตุ รูปแบบ เครือข่ายการกระทำอาชญากรรมทางเทคโนโลยีสารสนเทศได้อย่างเป็น

ระบบ ทำหน้าที่เป็นหน่วยงานหลักในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีที่มีความสลับซับซ้อนที่มีประชาชนได้รับความเสียหายเป็นจำนวนมาก และมีมูลค่าความเสียหายสูง ให้การสนับสนุนสถานีตำรวจในการป้องกันปราบปรามคดีอาชญากรรมทางเทคโนโลยีในเบื้องต้น หากเป็นคดีที่ไม่สลับซับซ้อน และเป็นศูนย์กลางประสานความร่วมมือกับหน่วยงานต่าง ๆ ในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี

นอกจากนี้ ยังได้มีการปรับปรุงโครงสร้างและกำหนดอำนาจหน้าที่ของกองบังคับการและศูนย์ที่เกี่ยวข้องกับการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีที่มีอยู่เดิมเพื่อให้สอดคล้องกับสถานการณ์ปัจจุบัน โดยอำนาจหน้าที่ของ กองบัญชาการตำรวจไซเบอร์ คือ เป็นฝ่ายอำนวยการด้านยุทธศาสตร์ให้สำนักงานตำรวจแห่งชาติในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และการเสนอแนะการปฏิบัติงานตามอำนาจหน้าที่ ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง ดำเนินการเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี โดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษ สนับสนุนส่วนราชการหรือหน่วยงานอื่นในการสืบสวนสอบสวน รวมทั้งสนับสนุนการพัฒนาบุคลากรด้านการสืบสวนสอบสวนของสำนักงานตำรวจแห่งชาติให้มีความรู้ ความสามารถ ในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์การกระทำความผิดทางเทคโนโลยี และดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล ตรวจสถานที่เกิดเหตุ และเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยต่าง ๆ เป็นต้น (สุภาพิชญ์ ถิระวัฒน์, กองบัญชาการตำรวจไซเบอร์, 2564)

ปัจจุบัน "กองบัญชาการตำรวจไซเบอร์" รับผิดชอบสืบสวนสอบสวน รวบรวมพยานหลักฐานในคดีที่มีความซับซ้อนหรือเป็นอาชญากรรมทางเทคโนโลยีที่สำคัญที่มีมูลค่าสูงและมีผู้เสียหายจำนวนมากตามเงื่อนไขที่กำหนด ในกรณีที่เป็นคดีอาชญากรรมทางเทคโนโลยีที่ไม่ซับซ้อน เช่น อาชญากรรมทั่วไปที่คนร้ายใช้เครื่องคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ตกระทำผิด

จะอยู่ในความรับผิดชอบของสถานีตำรวจท้องที่โดยมีกองบัญชาการตำรวจไซเบอร์ทำหน้าที่สนับสนุนข้อมูลที่ต้องสืบค้นทางเทคโนโลยี รวมทั้งประสานหน่วยงานที่เกี่ยวข้องเพื่อสืบค้น พิสูจน์ทราบตัวคนร้าย ทั้งนี้เพื่อให้ประชาชนที่ได้รับความเดือดร้อนได้รับการช่วยเหลืออย่างมีประสิทธิภาพ (สุภาพิชญ์ ถิระวัฒน์, กองบัญชาการตำรวจไซเบอร์, 2564)

3.2.3 คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

กมช. เป็นคณะกรรมการที่จัดตั้งตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมีรองนายกรัฐมนตรีที่ได้รับมอบหมายเป็นประธานกรรมการ และมีรัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เลขาธิการสภาความมั่นคงแห่งชาติ ผู้บัญชาการตำรวจแห่งชาติ ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม เป็นกรรมการโดยตำแหน่ง และมีกรรมการผู้ทรงคุณวุฒิร่วมด้วย ซึ่ง กมช. นี้มีอำนาจหน้าที่ในเชิงนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นหลัก (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, ม.ป.ป.) เป็นหน่วยงานด้านนโยบาย ติดตามและประเมินผลเชิงนโยบายมากกว่าเป็นหน่วยงานปฏิบัติป้องกันและปราบปราม อย่างไรก็ดี องค์ประกอบของ กมช. แสดงให้เห็นว่า รัฐตระหนักรู้ถึงภัยคุกคามด้านความมั่นคงทางไซเบอร์และมีความพยายามในระดับนโยบายเพื่อจัดการกับปัญหาดังกล่าว โดย กมช. มีอำนาจหน้าที่ในการเสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วย

จากที่ได้กล่าวมาทั้งหมด จะเห็นได้ว่าการทำให้ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงของรัฐ ได้นำมาซึ่งการก่อตั้งหน่วยงานที่มีภารกิจเกี่ยวข้องกับการรับมือในปัญหาดังกล่าว ที่สำคัญ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท. หรือกองบัญชาการตำรวจไซเบอร์) และ คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยในส่วนของกองบัญชาการตำรวจไซเบอร์นั้น จะมีภารกิจสำคัญในคดีที่มีความซับซ้อนหรือเป็นอาชญากรรมทางเทคโนโลยีที่สำคัญที่มีมูลค่าสูง และมีผู้เสียหายจำนวนมาก ปัญหาแก๊ง

คอลเซ็นเตอร์ซึ่งเป็นหนึ่งในปัญหาภัยคุกคามทางไซเบอร์ที่สำคัญจึงได้ถูกทำให้เป็นปัญหาความมั่นคงของไทยด้วยเช่นเดียวกัน

3.3 กระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง

ปัญหาการหลอกลวงทางโทรศัพท์หรือการหลอกลวงโดยใช้ระบบคอมพิวเตอร์ถือเป็นรูปแบบหนึ่งของอาชญากรรมข้ามชาติในตัวของมันเองในฐานะอาชญากรรมไซเบอร์ที่มีการจัดตั้งเป็นองค์กร (organized crime) อีกทั้งยังมีความเกี่ยวข้องกับอาชญากรรมข้ามชาติประเภทอื่น ๆ ด้วย ไม่ว่าจะเป็น การค้ามนุษย์ การฟอกเงิน หรือแม้กระทั่งขบวนการยาเสพติด ซึ่งนอกจากความเสียหายที่เกิดขึ้นโดยตรงต่อมูลค่าทางเศรษฐกิจของประชาชน ต่อระบบเศรษฐกิจของประเทศ ปัญหาดังกล่าวยังส่งผลกระทบต่อภาพลักษณ์ของประเทศในระดับระหว่างประเทศด้วย ทั้งนี้เพราะตัวชี้วัดหนึ่งของ Global Competitive Index (GCI) ที่จัดอันดับศักยภาพการแข่งขันทางเศรษฐกิจของประเทศต่าง ๆ มีประเด็นเรื่องอิทธิพลของกลุ่มมาเฟียหรือองค์กรอาชญากรรมเป็นตัวชี้วัดด้วย ในฐานะที่อิทธิพลจากกลุ่มองค์กรอาชญากรรมสามารถเข้ามาคุกคามระบบเศรษฐกิจและพัฒนาการทางเศรษฐกิจของประเทศได้ ในส่วนนี้ จึงจะได้กล่าวถึงลักษณะของปัญหาภัยคุกคามจากแก๊งคอลเซ็นเตอร์ พัฒนาการของปัญหาแก๊งคอลเซ็นเตอร์ และกระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง ตามลำดับ

3.3.1 ลักษณะของปัญหาภัยคุกคามจากแก๊งคอลเซ็นเตอร์

เนื่องจากงานวิจัยฉบับนี้เน้นศึกษา “ปัญหาแก๊งคอลเซ็นเตอร์” ดังนั้น เพื่อศึกษากระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาด้านความมั่นคง หรือ securitization ผู้วิจัยขอนำเสนอรูปแบบการทำงานของกลุ่มมิจฉาชีพที่ทำการหลอกลวงผ่านทางโทรศัพท์ หรือที่เรียกกันในภาษาชาวบ้านว่า “ปัญหาแก๊งคอลเซ็นเตอร์” อาชญากรรมประเภทนี้มีลักษณะการกระทำเป็นขบวนการ ข้อมูลจากบทความภัยอาชญากรรมแก๊งคอลเซ็นเตอร์ เผยแพร่โดยหอสมุดรัฐสภา ระบุว่า ขบวนการดังกล่าวพัฒนาการมาจากการหลอกลวงเหยื่อให้หลงเชื่อทางโทรศัพท์แล้วให้

เหยื่อไปที่ตู้เอทีเอ็มและให้ทำการโอนเงินแก่คนร้าย โดยอาจหลอกลวงเหยื่อใน 2 ลักษณะ (อาริยา สุขโต, 2565) คือ

1) การหลอกลวงด้วยความโลภ ในลักษณะเหมือนแก๊งตกทอง ด้วยการหลอกลวงผู้เสียหายว่าได้รับคืนภาษี ได้รับเงินรางวัล ได้รับเงินมรดกแต่จะต้องจ่ายค่าบริการเบื้องต้นหรือค่าธรรมเนียมต่าง ๆ ไปก่อนถึงจะได้เงินก้อนใหญ่ แต่ตนไม่มีเงิน เมื่อเหยื่อหลงเชื่อด้วยความโลภอยากได้เงินหรือทรัพย์สินนั้นก็จะหลงเชื่อโอนเงินไปให้มิจฉาชีพก่อน
2) การหลอกลวงด้วยความกลัว ด้วยการว่าเหยื่อเป็นหนี้ต่าง ๆ เช่น หนี้ค่าโทรศัพท์ หนี้บัตรธนาคาร หรือมีบัญชีธนาคารพัวพันกับยาเสพติด บัญชีธนาคารจะต้องถูกอายัดและถูกตรวจสอบโดยสำนักงานป้องกันและปราบปรามการฟอกเงิน สวมรอยเป็นเจ้าหน้าที่ของรัฐหลอกให้เหยื่อดำเนินธุรกรรมตามที่คนร้ายแจ้ง

3.3.2 พัฒนาการของปัญหาแก๊งคอลเซ็นเตอร์

แต่เดิมปัญหาภัยคุกคามแก๊งคอลเซ็นเตอร์ถูกมองเป็น อาชญากรรมข้ามชาติที่เป็นกลุ่มต่างชาติใช้ประเทศไทยเป็นฐานปฏิบัติการหลอกลวงเหยื่อในประเทศอื่น โดยขบวนการหรือแก๊งที่มีบทบาท คือ แก๊งคอลเซ็นเตอร์ ที่ส่วนใหญ่เป็นผู้กระทำผิดชาวไต้หวัน มาเลเซีย และจีน ซึ่งก่อนจะมาเป็นคอลเซ็นเตอร์ อาชญากรกลุ่มนี้รู้จักกันในชื่อ เอทีเอ็มเกมส์ (ATM Game) ที่สร้างกลโกงต่อประชาชนโดยการแอบอ้างเป็นผู้อื่นหลอกลวงให้เหยื่อเชื่อทางโทรศัพท์และเดินทางไปโอนเงินให้คนร้ายผ่านตู้เอทีเอ็ม (สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์วิจัยและนวัตกรรม, 2564) และพัฒนาการต่อมาจนเป็นอาชญากรรมที่มีการจัดตั้งกลุ่มคนมานั่งโทรศัพท์หลอกเหยื่อ ในลักษณะ คอลเซ็นเตอร์ และตั้งแต่ปี พ.ศ. 2550 เป็นต้นมา เริ่มมีปฏิบัติการในประเทศไทยที่หลอกลวงเหยื่อคนไทยมากขึ้นเรื่อย ๆ

กล่าวได้ว่า ภัยคุกคามจากการหลอกลวงทางโทรศัพท์แพร่กระจายมากขึ้นและทำได้ง่ายดายขึ้นตามพัฒนาการทางเทคโนโลยี ในยุคสมัยก่อนหน้าคนร้ายจะต้องหลอกให้เหยื่อไปกระทำธุรกรรมที่ตู้เอทีเอ็ม แต่ในสถานการณ์ที่ผู้คนมีแอพพลิเคชั่นธนาคารอยู่ในมือถือสมาร์ทโฟน อาชญากรรมการหลอกลวงผ่านทางโทรศัพท์จึงแพร่หลายขึ้น ผู้คนตกเป็นเหยื่อของกลุ่มมิจฉาชีพ

ในลักษณะนี้มากขึ้น และมีรูปแบบการหลอกใหม่ ๆ ที่เข้ากับยุคสมัย ไม่ว่าจะเป็นการหลอกลวงให้ร่วมลงทุน อ้างว่าเป็นคนรู้จักหลอกให้โอนเงินให้ด่วน หลอกว่าเป็นบริษัทขนส่งสินค้าเพื่อให้สอดคล้องกับพฤติกรรมของคนสมัยนี้ที่สั่งซื้อสินค้าออนไลน์และอาจหลงเชื่อการหลอกด้วยความกลัว เช่น หลอกเป็นเจ้าหน้าที่รัฐดำเนินคดีกับเหยื่อที่มีชื่อพัวพันกับการส่งสินค้าผิดกฎหมายเป็นต้น การหลอกลวงของแก๊งคอลเซ็นเตอร์อย่างกว้างขวางได้ส่งผลกระทบต่อเศรษฐกิจของประเทศทั้งในแง่ของการสูญเสียเงินโดยตรงของประชาชน ผลกระทบทางอ้อมในการทำให้พัฒนาทางดิจิทัลของประเทศเติบโตได้ช้าลง เนื่องจากผู้คนเกิดความระแวงสงสัยต่อการทำธุรกรรมในโลกอินเทอร์เน็ตมากขึ้น

ในกระบวนการหลอกลวงของแก๊งคอลเซ็นเตอร์อีกหนึ่งปัจจัยที่สำคัญที่สุด คือ การเปิดบัญชีรับเงินโดยใช้ชื่อผู้อื่นเพื่อมิให้สืบถึงตัวผู้กระทำผิดได้ ซึ่งเราเรียกบัญชีในลักษณะนี้ว่า “บัญชีม้า” คือ จ้างหน้าม้ามาเปิดบัญชีให้ โดยเมื่อเกิดเหตุการณ์หลอกให้โอนเงินไปก็จะพบเพียงแค่โอนเงินไปที่บัญชีของบุคคลที่เป็นเจ้าของบัญชี ที่จะอ้างว่ามิได้มีส่วนเกี่ยวข้องกับกระบวนการแก๊งมิจฉาชีพเพียงแต่รับจ้างเปิดบัญชีและมีคนอื่นนำไปใช้ ทำให้เส้นทางการติดตามเงินเป็นไปได้ยากขึ้น โดยธนาคารแห่งประเทศไทย นิยามความหมายคำว่า บัญชีม้าไว้ว่า “บัญชีม้า คือ บัญชีเงินฝากธนาคารของบุคคลอื่น ที่นำมาใช้เป็นช่องทางการทำธุรกรรมทางการเงิน เช่น การถ่ายโอนเงิน การรับเงินการโอนเงิน ซึ่งเงินที่ได้มาจากการกระทำผิด จุดประสงค์การเปิดบัญชีม้าคือ เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวผู้กระทำผิดได้” การเปิดบัญชีม้า คือ การจ้างให้บุคคลอื่นมาเปิดบัญชีแทน หรือรับซื้อบัญชีเงินฝากธนาคารของบุคคลทั่วไป ซึ่งพบว่ามีการขายบัญชีเงินฝากธนาคารกันอย่างเปิดเผย ตั้งแต่ราคา 800 บาท จนถึง 20,000 บาท โดยผู้ที่จะขายบัญชีม้าจะต้องมีการส่งมอบเอกสารให้แก่ผู้ซื้อ เช่น สำเนาบัตรประจำตัวประชาชน ซิมการ์ดโทรศัพท์ เพื่อให้สามารถนำข้อมูลส่วนบุคคลของเจ้าของบัญชีไปผูกกับ mobile banking และทำธุรกรรมออนไลน์ได้ทันที (กรมประชาสัมพันธ์, 2566)

3.4 กระบวนการทำให้แก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง

จากการศึกษาพบว่าหนึ่งในกระบวนการสำคัญที่ทำให้แก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง คือ การก่อตั้งหน่วยงาน กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) หรือ "กองบัญชาการตำรวจไซเบอร์ นอกเหนือจากหน่วยงานที่เกี่ยวข้องอื่น ๆ ได้แก่ กสทช กระทรวงดิจิทัลเพื่อการพัฒนาเศรษฐกิจและสังคม เพื่อให้เป็นหน่วยงานที่ทำหน้าที่ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ โดยเฉพาะปัญหาแก๊งคอลเซ็นเตอร์ซึ่งสร้างมูลค่าความเสียหายที่สูงและมีแนวโน้มเพิ่มมากขึ้นเรื่อย ๆ นอกจากนี้ ยังพบว่า มีตัวแสดงสำคัญที่มีส่วนในการทำให้ปัญหาดังกล่าวกลายเป็นปัญหาความมั่นคง โดยเฉพาะอย่างยิ่ง การกล่าวถึงประเด็นแก๊งคอลเซ็นเตอร์โดยนายกรัฐมนตรีของไทย นับตั้งแต่ พ.ศ.2565 – 2567 ดังตาราง

นายกรัฐมนตรี / ปีพ.ศ.ที่ให้สัมภาษณ์	**ข้อความในการให้สัมภาษณ์ผู้สื่อข่าวเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์**
พลเอกประยุทธ จันทร์โอชา/ 2565	ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาที่สร้างความเสียหายแก่พี่น้องประชาชนอย่างมาก ดังนั้นขอกำชับให้หน่วยงานที่เกี่ยวข้องบูรณาการความร่วมมือปราบปรามมิจฉาชีพและอาชญากรรมออนไลน์อย่างจริงจังและเด็ดขาด เพื่อบรรเทาความเดือดร้อนของพี่น้องประชาชนจากการสูญเสียทรัพย์สิน และนำไปสู่การจับกุมขบวนการดังกล่าว พร้อมทั้งควรสร้างภูมิคุ้มกันแก่ประชาชนให้รู้เท่าทันมิจฉาชีพเหล่านี้ด้วย (ที่มา: The Reporter, 30 มีนาคม 2565)
นายเศรษฐา ทวีสิน/ 2567	นายกรัฐมนตรีกำชับเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์ถึงหน่วยงานที่รับผิดชอบ โดยเฉพาะกองบัญชาการตำรวจไซเบอร์ให้เกิดผลงานที่ชัดเจนโดยเร็ว และต้องไม่ใช่การจับกุมเพียงอาชญากรรายเล็ก แต่ต้องเป็นรายใหญ่ เนื่องจากเป็นประเด็นที่กระทบต่อพี่น้องประชาชน การที่

	ประชาชนถูกหลอกลวงต้มตุ๋น ไม่ใช่ปัญหาของประชาชนที่ถูกหลอกลวง แต่เป็นปัญหาความมั่นคงของประเทศด้วย (ที่มา: เดลินิวส์, 1 เมษายน 2567)

ตาราง 1 แสดงการให้สัมภาษณ์ของนายกรัฐมนตรีไทยเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์

จากข้อมูลข้างต้น แสดงให้เห็นว่าตัวแสดงที่ทำหน้าที่กำหนดประเด็นความมั่นคงของรัฐไทย คือ นายกรัฐมนตรีจากทั้งสองรัฐบาล แม้ในช่วงระยะเวลาที่แตกต่างกันแต่ก็ได้มีบทบาทสำคัญอย่างมากในการทำให้ปัญหาแก๊งคอลเซ็นเตอร์กลายเป็นปัญหาความมั่นคงในระดับประเทศเช่นเดียวกัน โดยได้ถ่ายทอดวาทกรรมที่แสดงให้เห็นถึงความสำคัญของปัญหาและผลกระทบที่เกิดขึ้นต่อประชาชนในสังคม กระทั่งนำไปสู่แนวทางการจัดการเพื่อรับมือและแก้ไขปัญหาดังกล่าว ดังสะท้อนได้จากการก่อตั้งหน่วยงานที่เกี่ยวข้องในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ของไทย ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) หรือกองบัญชาการตำรวจไซเบอร์ และคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยเฉพาะอย่างยิ่ง กองบัญชาการตำรวจไซเบอร์ที่มีหน้าที่ในการดูแลคดีอาชญากรรมทางเทคโนโลยีที่สำคัญที่มีมูลค่าสูง และมีผู้เสียหายจำนวนมาก โดยได้มีการปฏิบัติการร่วมกับหน่วยงานอื่นในการจัดการปัญหาดังกล่าวอย่างเป็นระบบ ไม่ว่าจะเป็น สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช) กระทรวงดิจิทัลเพื่อการพัฒนาเศรษฐกิจและสังคม กรมสืบสวนคดีพิเศษ กระทรวงการคลัง ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานป้องกันและปราบปรามการฟอกเงิน สมาคมธนาคารไทย และสมาคมสถาบันการเงินของรัฐ

จากที่ได้กล่าวมาทั้งหมด จะเห็นได้ว่ากระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคง มีจุดเริ่มต้นมาจากการทำให้ปัญหาภัยคุกคามทางไซเบอร์เป็นปัญหาความมั่นคงก่อน ซึ่งปัญหาแก๊งคอลเซ็นเตอร์นั้นเป็นปัญหาสำคัญอย่างหนึ่งของปัญหาภัยคุกคามทางไซเบอร์ ทำให้กระบวนการทำให้เป็นปัญหาความมั่นคงนี้เริ่มจากตัวแสดงในการกำหนดประเด็น

ความมั่นคง (securitizing actor) โดยเฉพาะอย่างยิ่งผู้นำระดับประเทศอย่างนายกรัฐมนตรีได้ถ่ายทอดชุดวาทกรรมที่แสดงให้เห็นถึงภัยอันตรายจากปัญหาแก๊งคอลเซ็นเตอร์ ตลอดจนผลกระทบและความเสียหายที่เกิดขึ้นต่อประชาชนในสังคม นำไปสู่การการรับมือปัญหาดังกล่าวของหน่วยงานที่เกี่ยวข้อง รวมถึงกองบัญชาการตำรวจไซเบอร์ ซึ่งจะได้กล่าวถึงในบทต่อไป

บทที่ 4

การรับมือกับปัญหาแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจไซเบอร์

ในการศึกษาแนวทางการจัดการปัญหาของกองบัญชาการตำรวจไซเบอร์ หรือกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) หรือกองบัญชาการตำรวจไซเบอร์ ผู้วิจัยได้ศึกษาเกี่ยวกับประเด็นที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของกองบัญชาการตำรวจไซเบอร์ ได้แก่ ภารกิจความรับผิดชอบของกองบัญชาการตำรวจไซเบอร์ โครงสร้างองค์กรของกองบัญชาการตำรวจไซเบอร์ มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การใช้มาตรการป้องกันอาชญากรรมทางเทคโนโลยีแต่ละประเภท การจัดสรรงบประมาณ และแนวทางการจัดการปัญหาแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจ ไซเบอร์ ในช่วงพ.ศ.2563 – 2567 ดังนี้

4.1 หน้าที่ความรับผิดชอบของกองบัญชาการตำรวจไซเบอร์

กองบัญชาการตำรวจไซเบอร์ จัดตั้งขึ้นเมื่อวันที่ 9 กันยายน พ.ศ. 2563 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ (ฉบับที่ 5) พ.ศ. 2563 โดยกล่าวได้ว่าอำนาจหน้าที่ของกองบัญชาการตำรวจไซเบอร์นั้น เปรียบได้กับฝ่ายอำนวยการด้านยุทธศาสตร์ของสำนักงานตำรวจแห่งชาติ ซึ่งมีภารกิจในการวางแผน ควบคุม ตรวจสอบ ให้คำแนะนำ และเสนอแนะการปฏิบัติงานตามอำนาจหน้าที่ ดำเนินการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทั่วราชอาณาจักร รวมถึงปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่น อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทางเทคโนโลยีและความผิดอื่นที่เกี่ยวเนื่อง นอกจากนี้กองบัญชาการตำรวจไซเบอร์ยังมีหน้าที่ในการดำเนินการเกี่ยวกับการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี โดยการใช้เทคโนโลยีสารสนเทศและเครื่องมือพิเศษเพื่อสนับสนุนส่วนราชการหรือหน่วยงานอื่นในการสืบสวนสอบสวน รวมทั้งสนับสนุนการพัฒนาบุคลากรด้านการสืบสวนสอบสวนของสำนักงานตำรวจแห่งชาติให้มีความรู้ ความสามารถ ในการสืบสวนสอบสวนคดีอาชญากรรมทาง

เทคโนโลยี ดำเนินการเกี่ยวกับการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์การกระทำความผิดทางเทคโนโลยี และดำเนินการเกี่ยวกับการพิสูจน์หลักฐานดิจิทัล ตรวจสถานที่เกิดเหตุ และเก็บรวบรวมพยานหลักฐานดิจิทัลเพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวนของหน่วยต่าง ๆ เป็นต้น ทั้งนี้ กล่าวได้ว่าภารกิจความรับผิดชอบของกองบัญชาการตำรวจไซเบอร์ แบ่งออกเป็น 2 ระดับ ดังนี้

1) อาชญากรรมทางเทคโนโลยีที่สำคัญที่มีมูลค่าสูง และมีผู้เสียหายจำนวนมากตามเงื่อนไขที่กำหนด กล่าวคือ มีหน้าที่รับผิดชอบคดีที่มีความเสียหายต่อเศรษฐกิจและสังคมในวงกว้าง ซึ่งปัญหาแก๊งคอลเซ็นเตอร์มักจะถูกจัดอยู่ในคดีกลุ่มนี้ เนื่องจากมีผู้เสียหายจำนวนมากและส่งผลกระทบต่อเศรษฐกิจและสังคมในวงกว้างสร้างความเดือดร้อนให้กับประชาชนจำนวนมาก

2) คดีอาชญากรรมทางเทคโนโลยีที่ไม่ซับซ้อน ให้การสนับสนุนข้อมูลสืบค้นทางเทคโนโลยี รวมทั้งประสานหน่วยงานที่เกี่ยวข้องเพื่อสืบค้น พิสูจน์ทราบตัวคนร้ายให้กับตำรวจท้องที่ซึ่งรับผิดชอบคดี อาชญากรรมทั่วไปที่คนร้ายใช้เครื่องคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ตกระทำผิด

สำหรับงานวิจัยนี้ ผู้วิจัยมุ่งให้ความสำคัญกับการศึกษาแนวทางการจัดการอาชญากรรมทางเทคโนโลยีที่สำคัญและมีมูลค่าสูง และมีผู้เสียหายจำนวนมากตามเงื่อนไขที่กำหนด เช่น คดีเกี่ยวกับทรัพย์ที่มีจำนวนผู้เสียหายรวมกันตั้งแต่ 50 คนขึ้นไป คดีเกี่ยวกับทรัพย์ที่มีทั้งมูลค่าความเสียหาย 10 ล้านบาทขึ้นไปและมีจำนวนผู้เสียหายตั้งแต่ 10 คนขึ้นไป ดังที่ได้กล่าวถึงในส่วนของระเบียบวิธีการวิจัยในบทที่ 1

4.2 **โครงสร้างองค์กรของกองบัญชาการตำรวจไซเบอร์**

โครงสร้างภายในกองบัญชาการไซเบอร์แบ่งออกเป็น 7 กองบังคับการ ดังนี้

1) กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 1 (บก. สอท. 1) รับผิดชอบกรุงเทพมหานคร โดย บก. สอท. 1 ตั้งอยู่ที่ศูนย์ราชการแจ้งวัฒนะ

2) กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 2 (บก. สอท. 2)

รับผิดชอบพื้นที่ภาคกลางตอนล่าง ภาคตะวันออก โดย บก. สอท. 2 ตั้งอยู่ที่จังหวัดนนทบุรี

3) กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 3 (บก. สอท. 3) รับผิดชอบพื้นที่ภาคตะวันออกเฉียงเหนือ โดย บก. สอท. 3 ตั้งอยู่ที่จังหวัดขอนแก่น

4) กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 4 (บก. สอท. 4) รับผิดชอบพื้นที่ภาคกลางตอนบนและพื้นที่ภาคเหนือ โดย บก. สอท. 4 ตั้งอยู่ที่จังหวัดเชียงใหม่

5) กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 5 (บก. สอท. 5) รับผิดชอบพื้นที่ภาคใต้ โดย บก. สอท. 5 ตั้งอยู่ที่จังหวัดสุราษฎร์ธานี

6) กองบังคับการอำนวยการ รับผิดชอบงานอำนวยการด้านธุรการกำลังพล วางยุทธศาสตร์ ส่งกำลังบำรุง ดูแลเรื่องงบประมาณและการเงิน ฝ่ายกฎหมายและวินัย และระบบเทคโนโลยีสารสนเทศองค์กร

7) กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี รับผิดชอบภารกิจสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีร่วมกับฝ่ายปฏิบัติการหรือหน่วยงานอื่นตามที่ได้รับการร้องขอ รวมทั้งพิสูจน์และกู้พยานหลักฐานดิจิทัล ตรวจสถานที่เกิดเหตุเพื่อรวบรวมพยานหลักฐานดิจิทัล เพื่อสนับสนุนการปฏิบัติงานสืบสวนสอบสวน และมีหน้าที่ให้ความรู้ และร่วมกับหน่วยงานของรัฐและเอกชนเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีด้วย โดยเป็นหน่วยงานฝึกอบรมให้ความรู้กับเจ้าหน้าที่ตำรวจในด้านอาชญากรรมคอมพิวเตอร์ การสืบสวนทางเทคนิคการเก็บรักษาพยานหลักฐานทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือสามารถรับฟังในกระบวน การพิจารณาในชั้นศาลได้ ตลอดจนเร่งพัฒนาศักยภาพของบุคลากรในหน่วยงานเพื่อให้มีความเชี่ยวชาญ สามารถให้การสนับสนุนคดีที่มีความซับซ้อน และปฏิบัติภารกิจร่วมกับหน่วยงานอื่น (กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, https://www.hightechcrime.org/staff/History, ม.ป.ป.)

4.3 มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ในการจัดการปัญหาภัยคุกคามทางไซเบอร์กองบัญชาการตำรวจไซเบอร์ได้มีการระบุ (identify) อาชญากรรมทางเทคโนโลยีไว้ 5 ด้าน (กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, วุฒิสภา, ม.ป.ป.) ได้แก่

1) คดีหลอกลวงทางการเงินออนไลน์ เช่น แชร์ลูกโซ่ การลงทุนออนไลน์ ซึ่งรวมถึงกรณีการหลอกลวงจากแก๊งคอลเซ็นเตอร์ ในลักษณะการส่งข้อความสั้น (SMS) จากเครือข่ายโทรศัพท์มือถือต่างๆ การแอบอ้างเป็นเจ้าหน้าที่ของหน่วยงานรัฐและหน่วยงานเอกชนด้วย
2) คดีซื้อขายสินค้าผิดกฎหมาย หลอกลวงขายสินค้าไม่มีมาตรฐานหรือไม่ผ่านพิธีศุลกากรอย่างถูกกฎหมายผ่านช่องทางออนไลน์
3) คดีเผยแพร่ข่าวปลอม และการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ การเข้าถึงระบบโดยมิชอบ (hacking) การเรียกค่าไถ่ข้อมูลและระบบ
4) คดีล่วงละเมิดทางเพศต่อเด็กและสตรีทางอินเตอร์เน็ต
5) การพนันออนไลน์ และอาชญากรรมข้ามชาติ

การจัดประเภทอาชญากรรมทางเทคโนโลยีของกองบัญชาการตำรวจไซเบอร์สะท้อนให้เห็นถึง ความเข้าใจต่อ cyber crime ในมุมมองของผู้บังคับใช้กฎหมายได้อย่างดี โดยประเภทคดีทั้ง 5 สอดคล้องกับแนวคิดที่เกี่ยวข้องกับ cyber crime ดังที่ได้กล่าวถึงในบทที่ 2 เมื่อกำหนดประเภทอาชญากรรมทางเทคโนโลยีที่กองบัญชาการไซเบอร์ให้ความสำคัญแล้ว ได้กำหนดมาตรการป้องกันและมาตรการปราบปราม เพื่อเป็นแนวทางในการปฏิบัติงานโดยมีรายละเอียดดังนี้

4.3.1 มาตรการป้องกัน

ในการปฏิบัติภารกิจกองบัญชาการตำรวจไซเบอร์ได้กำหนดเป็นมาตรการสำคัญ 5 ด้าน ได้แก่

1) เป็นศูนย์ประสานงานกลางในการเฝ้าระวัง และรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานที่สำคัญของตำรวจ

2) ประสานความร่วมมือด้านอาชญากรรมทางเทคโนโลยี กับหน่วยงานอื่น ๆ ทั้งจากภาครัฐและเอกชน ทั้งภายในและต่างประเทศ
3) รวบรวมสถิติอาชญากรรมทางเทคโนโลยี
4) ติดตาม เฝ้าระวัง ป้องกัน สร้างความตระหนักรู้ให้กับประชาชนและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีที่มีการเปลี่ยนแปลงรูปแบบไปอย่างรวดเร็ว
5) พัฒนาบุคลากรด้านการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีให้มีความเชี่ยวชาญและทันสมัยต่อการเปลี่ยนแปลงของเทคโนโลยี

4.3.2 มาตรการปราบปราม

สำหรับการปราบปรามคดีแก๊งคอลเซ็นเตอร์ กองบัญชาการตำรวจไซเบอร์ได้มีกำหนดเป็นมาตรการสำคัญ 3 ด้าน ได้แก่

1) การบังคับใช้กฎหมายที่เกี่ยวข้อง ทั้ง ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่น ๆ ทางอาญาที่เกี่ยวกับอาชญากรรมทางเทคโนโลยี อันเป็นความผิดทางอาญาเกี่ยวกับอาชญากรรมทาง เทคโนโลยี
2) การให้การสนับสนุนสถานีตำรวจในพื้นที่ต่าง ๆ สืบสวนสอบสวนคดีทางเทคโนโลยีที่ไม่ซับซ้อน และ
3) ตรวจพิสูจน์เก็บรวบรวมหลักฐานทางดิจิทัล และ กู้พยานหลักฐานทางดิจิทัล ซึ่งมาตรการการตรวจพิสูจน์เก็บรวบรวมหลักฐานนี้อยู่ในความรับผิดชอบของกองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี

4.4 การใช้มาตรการป้องกันอาชญากรรมทางเทคโนโลยีแต่ละประเภท

ในการศึกษาผลการปฏิบัติงานของกองบัญชาการตำรวจไซเบอร์พบว่า ในด้านการป้องกันการเกิดอาชญากรรมทางไซเบอร์ กองบัญชาการตำรวจไซเบอร์ได้ใช้ประเภทอาชญากรรมทางเทคโนโลยี 5 ประเภท เป็นโจทย์ในการปฏิบัติงาน โดยมีแนวทางป้องกันอาชญากรรมทางเทคโนโลยีประเภทต่าง ๆ รายละเอียดดังนี้

4.4.1 การป้องกันการหลอกลวงทางการเงินออนไลน์ และปัญหาคอลเซ็นเตอร์

กองบัญชาการตำรวจไซเบอร์ได้มีความพยายามในการสร้างความตระหนักรู้ให้แก่ประชาชนเพื่อป้องกันการถูกหลอก โดยได้นำเสนอปัญหาและรูปแบบของการหลอกลวงผ่านสื่อประชาสัมพันธ์ให้เข้าถึงประชาชนในวงกว้าง เช่น เผยแพร่ในเว็บไซต์ทางการของหน่วยงาน คือ เว็บไซต์ https://ccid3.ccib.go.th เพื่อให้ข้อมูลเกี่ยวกับวิธีการหลอก กลเม็ดของกลุ่มมิจฉาชีพ นอกจากเว็บไซต์ทางการแล้วยังได้มีการตั้งเพจ Facebook ของกองบัญชาการตำรวจไซเบอร์เพื่อให้ข้อมูลเตือนภัย สร้างความตระหนักรู้ และรับแจ้งเหตุ ซึ่งนับเป็นช่องทางการติดต่อ 2 ทาง เพื่ออำนวยความสะดวกแก่ประชาชน อย่างไรก็ดี จำนวนผู้ติดตามเพจ Facebook ของกองบัญชาการตำรวจไซเบอร์ ปัจจุบัน (พฤษภาคม 2567) มีผู้ติดตาม 2.1 แสนคน ซึ่งยังคิดเป็นจำนวนไม่มากนักจาก เมื่อเทียบกับจำนวนประชากรของไทย ที่มีอยู่ประมาณ 66.05 ล้านคน (สถานะปี 2566) (Thailand Board of Investment, 2024) และคิดเป็นสัดส่วนไม่ถึงร้อยละ 1 จากจำนวนผู้ใช้ Facebook ในประเทศไทยทั้งหมดประมาณ 48 ล้านบัญชี (Motive Influence, 2566) ซึ่งนอกจากการจัดทำข้อมูลเพื่อเผยแพร่แล้ว กองบัญชาการตำรวจไซเบอร์ยังใช้ช่องทางสื่อมวลชนเพื่อเผยแพร่ข้อมูลแก่ประชาชนเป็น โดยโฆษกกองบัญชาการตำรวจไซเบอร์ได้มีการให้สัมภาษณ์หรือ ออกแถลงการณ์ขอความร่วมมือสื่อมวลชนให้ข้อมูลเตือนภัยแก่ประชาชน และประชาสัมพันธ์แนวทางป้องกันภัยจากมิจฉาชีพแก๊งคอลเซ็นเตอร์อยู่เป็นระยะตามรูปแบบที่เปลี่ยนไปของการกระทำผิด

ในด้านนโยบาย กองบัญชาการตำรวจไซเบอร์รับนโยบายของรัฐบาล และสำนักงานตำรวจแห่งชาติมาปฏิบัติงานเพื่อให้การป้องกันและปราบปรามการกระทำความผิดอาชญากรรมทางเทคโนโลยีในทุกรูปแบบ เช่นตอบสนองโครงการ “ไซเบอร์วัคซีน” ของสำนักงานตำรวจแห่งชาติ โดย รองผู้บัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีร่วมเป็นหัวหน้าคณะทำงานฝ่ายจัดทำเนื้อหาผลิตสื่อ และเผยแพร่ประชาสัมพันธ์ ในโครงการไซเบอร์วัคซีน ซึ่งเป็นการช่วยสร้างเสริมภูมิคุ้มกันด้านภัยอาชญากรรมทางเทคโนโลยีให้แก่ นักเรียน นักศึกษาในสถาบันการศึกษา และประชาชนทั่วไป ให้สามารถมีความรู้ในการป้องกันตนเองและบุคคลใน

ครอบครัว นอกจากนี้ กองบัญชาการตำรวจไซเบอร์ ยังมีแพลทฟอร์มสำหรับการแจ้งความออนไลน์ในคดีอาชญากรรมทางเทคโนโลยีด้วย ที่ https://thaipoliceonline.com อีกทั้งยังสามารถโทรสอบถามข้อมูลได้ที่ สายด่วนตำรวจไซเบอร์ 1441 หรือ 081-866-3000 และมีแชทบอท @police1441 ไว้คอยให้คำปรึกษาเกี่ยวกับคดีอาชญากรรมทางเทคโนโลยี ซึ่งคอยให้บริการตอบคำถามประชาชน ตลอด 24 ชั่วโมง นอกจากมาตรการป้องกันของกองบัญชาการตำรวจไซเบอร์แล้ว ในระดับรัฐบาล นายกรัฐมนตรีก็ให้ความสำคัญกับการป้องกันภัยคุกคามจากแก๊งคอลเซ็นเตอร์ด้วย โดยเมื่อวันที่ 14 พฤษภาคม 2567 ในช่วงระหว่างการประชุมคณะรัฐมนตรี นายชัย วัชรงค์ โฆษกประจำสำนักนายกรัฐมนตรี ได้แถลงภายหลังการประชุมคุณรัฐมนตรีอย่างเป็นทางการนอกสถานที่ หรือ การประชุม คณะรัฐมนตรีสัญจร ว่า นายเศรษฐา ทวีสิน นายกรัฐมนตรีได้มีข้อสั่งการและมอบนโยบายให้หน่วยงานของรัฐที่เกี่ยวข้องแก้ไขปัญหาแก๊งคอลเซ็นเตอร์ โดยมอบให้การไฟฟ้าส่วนภูมิภาค การประปาส่วนภูมิภาค ระงับการให้บริการข้ามพรมแดน เพื่อตัดกำลังของกลุ่มแก๊งคอลเซ็นเตอร์ที่ใช้พื้นที่ชายแดนเป็นฐานการดำเนินการ และขอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ประสานขอความร่วมมือ กับ กสทช. และผู้ประกอบการด้านสื่อสารร่วมมือด้วย ซึ่งมาตรการเหล่านี้จะมีส่วนช่วยลดภาระงานป้องกันให้กับการปฏิบัติงานของกองบัญชาการตำรวจไซเบอร์ด้วย

จากคำสัมภาษณ์ของเจ้าหน้าที่ตำรวจในสังกัดกองบัญชาการตำรวจไซเบอร์ เกี่ยวกับแนวทางในการแก้ไขปัญหาแก๊งคอลเซ็นเตอร์ พบว่า ในการปฏิบัติงานของตำรวจในภาพใหญ่ คือ ปฏิบัติงานเพื่อ ให้ประชาชนมีความมั่นคงปลอดภัยในชีวิต และทรัพย์สิน อีกทั้งยังเป็นผู้บังคับใช้กฎหมายที่เป็นที่พึ่งของประชาชนที่เดือดร้อนในการปราบปรามผู้กระทำผิด ซึ่งสำหรับปัญหาการหลอกลวงของคอลเซ็นเตอร์ กองบัญชาการตำรวจไซเบอร์ให้ความสำคัญกับการลดความเสี่ยงของประชาชนในการตกเป็นเหยื่อของการหลอกลวงด้วยการสร้างความตระหนักรู้ต่อภัย เตือนภัยสร้างภูมิคุ้มกันทางไซเบอร์ให้กับประชาชนเพื่อป้องกันเหตุ อย่างไรก็ตาม ก็ยังคงไม่สามารถป้องกันเหตุได้เบ็ดเสร็จ เพราะกลุ่มมิจฉาชีพมักจะเลือก กลุ่มผู้สูงอายุ บุคคลเกษียณอายุเป็นเหยื่อเป้าหมาย เนื่องจากคนกลุ่มนี้มิได้คุ้นเคยและเข้าใจเทคโนโลยีสมัยใหม่เท่าที่ควร อีกทั้งยังเป็นกลุ่มคนที่มักจะมีทรัพย์สินเงินเก็บมาก บางคนมีแนวโน้มดื้อรั้น มั่นใจในตัวเอง สติสัมปชัญญะถดถอยไปตามวัย

และอาจมิได้เข้าถึงข้อมูลการเตือนภัยในโลกออนไลน์มากนัก จึงมักทำให้ถูกหลอกได้ง่าย ซึ่งเมื่อเกิดกรณีการหลอกลวงขึ้นแล้วภารกิจที่สำคัญของตำรวจไซเบอร์ คือ การปราบปรามกลุ่มมิจฉาชีพหรือแก๊งคอลเซ็นเตอร์ที่สร้างความเสียหายต่อประชาชนในวงกว้าง หรือมีมูลค่าสูง โดยเมื่อตำรวจไซเบอร์มีปฏิบัติการจับกุมในคดีคอลเซ็นเตอร์แล้ว จะนำเสนอข่าวเปิดเผย รูปแบบ กลลวง และวิธีการหลอกลวงของแก๊งคอลเซ็นเตอร์ให้สาธารณชนได้รับทราบในช่องทางต่าง ๆ เพื่อเป็นการเตือนภัย แต่นอกจากการป้องกันภัยด้วยการสร้างความในแง่ของการตระหนักรู้ของประชาชนทั่วไปไม่ให้ตกเป็นเหยื่อแล้ว ตำรวจไซเบอร์ยังเห็นความสำคัญของการสร้างความตระหนักรู้ในแง่ของกลุ่มคนที่มีแนวโน้มที่จะไปทำงานเป็นคอลเซ็นเตอร์ทำหน้าที่หลอกลวงคนอื่น ทั้งกลุ่มที่สมัครใจไปกระทำผิดและกลุ่มที่ถูกหลอกให้ไปทำงานเป็นคอลเซ็นเตอร์หลอกลวงผู้อื่น ว่าถือเป็นการก่ออาชญากรรมและมีความผิด ควรระมัดระวังตัวมิให้ถูกหลอกไปทำงานเป็นคอลเซ็นเตอร์เพื่อลดจำนวนผู้กระทำผิดในคดีลักษณะนี้ด้วย

4.4.2 การปราบปรามการหลอกลวงทางการเงินออนไลน์ และปัญหาคอลเซ็นเตอร์

ในการตอบสนองต่อนโยบายรัฐบาลและสำนักงานตำรวจแห่งชาติในการแก้ไขปัญหาแก๊งคอลเซ็นเตอร์ กองบัญชาการตำรวจไซเบอร์ได้มีปฏิบัติการปราบปรามหลายครั้ง ไม่ว่าจะเป็นปฏิบัติการตัดวงจรซิม-สาย-เสา โค่นเสาสัญญาณ หรือสถานีเถื่อนชายแดนประเทศเพื่อนบ้าน การจับกุมข้าราชการที่นำข้อมูลไปขายให้แก๊งคอลเซ็นเตอร์ การร่วมมือกับเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมายต่างประเทศทลายแก๊งคอลเซ็นเตอร์ที่คอยหลอกเหยื่อ โดยมีมูลค่าความเสียหายกว่า 3 พันล้านบาท (The Standard, 2566) สำหรับปัญหาคอลเซ็นเตอร์ นอกจากการสร้างความตระหนักรู้ เสริมสร้างภูมิคุ้มกันให้ประชาชนแล้ว ในด้านการปราบปราม กองบัญชาการตำรวจไซเบอร์ มีปฏิบัติการปราบปราม “บัญชีม้า” ซึ่งเป็นหนึ่งในเครื่องมือสำคัญของเส้นทางการเงินของแก๊งคอลเซ็นเตอร์ เพื่อตัดวงจรอาชญากรรมด้วย โดยร่วมกับธนาคารตรวจสอบเส้นทางการเงินที่น่าสงสัยเพื่อสืบสวนไปยังตัวการของแก๊งคอลเซ็นเตอร์ โดยเมื่อเดือนตุลาคม 2565 กองบัญชาการตำรวจไซเบอร์ได้มีปฏิบัติการ “เด็ดปีกมังกร” ซึ่งเป็นปฏิบัติการาจับเครือข่ายแก๊งคอลเซ็นเตอร์ ที่เกี่ยวข้องกับเจ้าหน้าที่รัฐที่ทำการขายข้อมูลส่วนตัวของคนไทยให้กับกลุ่มมิจฉาชีพ โดยใน

ปฏิบัติการดังกล่าวจับผู้ต้องหาได้ 16 รายแบ่งเป็น 3 กลุ่ม คือ กลุ่มรับจ้างเปิดบัญชีม้า กลุ่มรวบรวมเงินจากบัญชีม้าส่งต่อให้นายทุนซึ่งพบว่าเป็นชาวจีน และกลุ่มที่ทำหน้าที่รวบรวมข้อมูลประชาชนเพื่อนำไปใช้ประกอบการหลอกลวง ซึ่งปรากฏว่าเป็นเจ้าหน้าที่ของรัฐที่สามารถเข้าถึงข้อมูลส่วนบุคคลของประชาชนได้ จึงนำไปขายให้กับแก๊งคอลเซ็นเตอร์ ซึ่งทางธนาคารพบการเคลื่อนไหวทางการเงินของบัญชีม้ามายังบัญชีของผู้ต้องหาซึ่งเป็นเจ้าหน้าที่รัฐดังกล่าว จึงประสานการตรวจสอบไปยังตำรวจเพื่อปฏิบัติการจับกุม (เดลินิวส์ออนไลน์, 2565)

ในส่วนของกฎหมาย กองบัญชาการตำรวจไซเบอร์สามารถบังคับใช้กฎหมายตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ในการปราบปรามบัญชีม้าหรือซิมม้าได้ ในส่วนของผู้เปิดบัญชีม้าระบุโทษอยู่ในมาตรา 9 ที่ระบุว่า “ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์หรือบัญชีเงินอิเล็กทรอนิกส์ของตนโดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ” แต่สำหรับผู้จัดหาหรือชักชวนให้คนเปิดบัญชีหรือซิมม้าจะมีโทษสูงกว่า ตามที่มาตรา 10 ของ พระราชกำหนดฯ ระบุว่า “ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืมบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ เพื่อใช้ในการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท” และมาตราที่ 11 ระบุว่า “ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวด้วยประการใด ๆ เพื่อให้มีการซื้อหรือขายหมายเลขโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ (พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566, 2566)

ในระดับประเทศ รัฐบาลโดยนายเศรษฐา ทวีสิน ตระหนักดีถึงปัญหาภัยคุกคามจากปัญหาการหลอกลวงโดยแก๊งคอลเซ็นเตอร์ เนื่องจากเป็นความเดือดร้อนต่อประชาชนโดยตรง จากคำสัมภาษณ์ของนายกรัฐมนตรี เมื่อวันที่ 24 พฤศจิกายน 2566 นายเศรษฐาฯ แจ้งกับสื่อมวลชนว่า ได้มีการหารือกับรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเกี่ยวกับปัญหาแก๊งคอลเซ็นเตอร์แล้ว โดยเฉพาะกลุ่มที่ฝังตัวอยู่บริเวณชายแดนประเทศเพื่อนบ้าน และเห็นว่าจำเป็นต้องได้รับความร่วมมือจากทุกหน่วยงานที่เกี่ยวข้องในการแก้ไขปัญหา การให้สัมภาษณ์ของนายกรัฐมนตรีสะท้อนให้เห็นว่า ปัญหาแก๊งคอลเซ็นเตอร์ถูกทำให้เป็นภัยคุกคามด้านความมั่นคงของไทยที่รัฐบาลให้ความสำคัญมาก ซึ่งนอกจากหน่วยงานอื่น ๆ ที่เกี่ยวข้องแล้ว กองบัญชาการตำรวจไซเบอร์กลายเป็นหน่วยงานรับผิดชอบที่สำคัญในการรับมือกับภัยคุกคามนี้ ดังที่เห็นได้จากข้อสั่งการนายกรัฐมนตรีที่กำหนดเส้นระยะเวลาให้กองบัญชาการตำรวจไซเบอร์ปฏิบัติการปราบปรามแก๊งคอลเซ็นเตอร์ โดยเมื่อ ในวันที่ 1 เมษายน 2567 นายกรัฐมนตรีได้ตรวจเยี่ยมและมอบนโยบายให้กับข้าราชการตำรวจและเจ้าหน้าที่สืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือ บช. สอท. ให้จับตัวการใหญ่ของแก๊งคอลเซ็นเตอร์ให้ได้ โดยนายเศรษฐา ทวีสิน นายกรัฐมนตรี ได้กล่าวกับ บช. สอท. ว่า

> *“วันนี้เอาประชาชนเป็นที่ตั้ง ผลงานของเราจะเป็นที่ประจักษ์ ขอเป็นนิมิตหมายอันดีและเป็นจุดเริ่มต้นใหม่ ของการที่เราเข้ามาดูแลพี่น้องประชาชน ภายใน 30 วันนี้ชัดเจนว่าจะจับอะไรให้ได้ ไม่ว่าจะเป็นหวยออนไลน์ หรืออะไรที่เกิดขึ้น ซึ่งพี่น้องถูกหลอกลวงทุกวันนี้ยังมีอยู่ ขอเลยเรื่องนี้จะต้องทำงานกันอย่างชัดเจนและใกล้ชิด เพราะเทคโนโลยีไปไกลมาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) พร้อมที่จะทำงานร่วมกัน ผมเจอรัฐมนตรีดีอีในวันที่ 2 เมษายน นี้ จะกำชับอย่างเด็ดขาดว่าต้องทำงานร่วมกันอย่ามีการโยนความผิดซึ่งกันและกัน อย่าบอกว่าคนนี้ไม่ให้ความร่วมมือ ไม่มีนะตรงนี้ ผมเชื่อว่ามานั่งตรงนี้แล้วรัฐมนตรีกระทรวงต่าง ๆ ที่เกี่ยวข้องจะต้องให้ความสำคัญกับเรื่องนี้ พวกท่านเองก็ต้องให้ความสำคัญ ผมใช้เวลา`

ประมาณ 5 นาทีที่พูดไป อยากให้ทุกท่านตระหนักดีว่าประชาชนเดือดร้อน เหตุผลที่เรามาทำงานตรงนี้ เพื่อให้ความดูแลพี่น้องประชาชน ไม่ใช่ให้คนผิดลอยอยู่ได้ และยังทำทุกอย่างผิด ๆ อยู่ คิดว่าถึงเวลาแล้ว อยากได้เหตุผลว่าทำไมถึงจับไม่ได้ ต้องจับให้ได้ เพื่อพี่น้องประชาชนจะได้อยู่อย่างมีความสุข อย่าให้ถูกซ้ำเติมตรงนี้ โดยเฉพาะการถูกหลอกลวง เงินหมดไปก็เป็นส่วนหนึ่งของอาชญากร ตรงนี้ถือเป็นสารตั้งต้น ที่ต้องขจัดปัญหานี้ออกไปให้หมดจากสังคมไทย ผมยืนยันเรื่องนี้เป็นเรื่องซีเรียส ยืนยัน 30 วันต้องชัดเจน" (เว็บไซต์รัฐบาลไทย, 2567)

4.4.3 มาตรการป้องกันและปราบปรามคดีซื้อขายสินค้าผิดกฎหมาย หลอกลวงขายสินค้าไม่มีมาตรฐานหรือไม่ผ่านพิธีศุลกากรอย่างถูกกฎหมายผ่านช่องทางออนไลน์

ในส่วนของมาตรการป้องกันคดีซื้อขายสินค้าผิดกฎหมายและหลอกลวงขายสินค้า กองบัญชาการตำรวจไซเบอร์ได้ประชาสัมพันธ์เตือนภัยให้ประชาชนทราบถึงวิธีการหลอกลวงขายสินค้า มิให้ประชาชนตกเป็นเหยื่อของมิจฉาชีพได้โดยง่าย มีการแนะนำให้ประชาชนรวบรวมพยานหลักฐาน เช่น ข้อความการสนทนา หลักฐานการชำระเงิน คำสั่งซื้อสินค้า หลักฐานช่องทางการติดต่อกับผู้ขาย ซึ่งหลังจากประชาสัมพันธ์เตือนภัยไปยังประชาชนแล้ว พบว่าสถานการณ์การหลอกลวงทางออนไลน์ปรับตัวดีขึ้นบ้าง จากการรู้ทันกลลวงของมิจฉาชีพ และการออกกฎหมายที่เข้มงวดขึ้น

กองบัญชาการตำรวจไซเบอร์ได้ร่วมกับสภาผู้บริโภค และ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) จัดการอบรมเพิ่มศักยภาพเครือข่ายและหน่วยงานคุ้มครองผู้บริโภคที่มีเป้าหมายเพื่อติดอาวุธให้ผู้บริโภครู้เท่าทันกลโกงของมิจฉาชีพ โดยจัดการเสวนาในประเด็น “กลโกงซื้อขายออนไลน์กับกฎหมายแพลตฟอร์มที่ต้องรู้” นอกจากนี้ ยังมีโครงการลงทะเบียนเว็บไซต์และบัญชีสื่อสังคมออนไลน์ภาคสมัครใจเพื่อสร้างความมั่นใจให้กับประชาชน ในการซื้อสินค้าออนไลน์ เป็นฐานข้อมูลให้ประชาชนสามารถตรวจสอบความน่าเชื่อถือของเว็บไซต์และบัญชี

สังคมออนไลน์ได้ อย่างไรก็ดี โครงการนี้ยังไม่เป็นที่รู้จักมากนะ และมิได้มีการลงทะเบียนมากพอที่จะเป็นฐานข้อมูลสำคัฐที่ประชาชนจะเข้าไปตรวจสอบ

สำหรับมาตรการปราบปรามฯ เป็นไปตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่มีผลบังคับใช้ตั้งแต่วันที่ 17 มีนาคม พ.ศ. 2566 ที่มีบทกำหนดความผิดและกำหนดโทษสำหรับผู้กระทำผิดอย่างชัดเจน โดยเฉพาะการเชิญชวนโฆษณาซื้อ-ขาย

4.4.4 มาตรการป้องกันและปราบปรามคดีเผยแพร่ข่าวปลอม และการกระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ การเข้าถึงระบบโดยมิชอบ (hacking) การเรียกค่าไถ่ข้อมูลและระบบ

ในการป้องกันการเผยแพร่ข่าวปลอม และการกระทำผิดตาม พระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ กองบัญชาการตำรวจไซเบอร์มีการจัดตั้งศูนย์ประสานงานและแก้ไขปัญหาข่าวปลอม (ANTI FAKE NEWS COORDINATION CENTRE) ทำหน้าที่ ตรวจสอบข้อมูลประสานงาน ผลิต และเผยแพร่ข้อมูลที่ถูกต้อง และสนับสนุนร่วมปฏิบัติหน่วยที่เกี่ยวข้อง อีกทั้งยังทำหน้าที่ด้านปราบปราม โดยศูนย์ประสานงานและแก้ไขปัญหาข่าวปลอมได้ทำหน้าที่รับแจ้งความร้องทุกข์สืบสวนจับกุมผู้กระทำความผิด ติดตาม

4.4.5 มาตรการป้องกันและปราบปรามคดีล่วงละเมิดทางเพศต่อเด็กและสตรีทางอินเตอร์เน็ต

สำหรับคดีประเภทนี้ตำรวจไซเบอร์จะเน้นไปที่การปราบปรามมากกว่า โดยมีหน้าที่ตรวจสอบ สืบสวนสอบสวนบัญชีออนไลน์ต่าง ๆ ที่เผยแพร่หรือนำเข้าสื่อลามกอนาจารเด็กออนไลน์ ซึ่งเป็นความผิดตาม พระราชบัญญัติ การกระทำผิดเกี่ยวกับคอมพิวเตอร์ที่นำเข้าสู่ระบบคอมพิวเตอร์หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

4.4.6 มาตรการป้องกันและปราบปรามคดีการพนันออนไลน์ และอาชญากรรมข้ามชาติ

สำหรับคดีการพนันออนไลน์และอาชญากรรมข้ามชาติจะเป็นปฏิบัติการสืบสวนสอบสวนและปฏิบัติการจับกุม ขยายผลการจับกุมและทำการปิดกั้นเว็บไซต์พนันออนไลน์เป็นส่วนมาก ในส่วนของอาชญากรรมข้ามชาติจะมีความร่วมมือกับหน่วยงานที่เกี่ยวข้องในต่างประเทศ เพื่อแลกเปลี่ยนข้อมูล และเฝ้าระวังตามหมายจับตำรวจสากล (Interpol)

4.5 การจัดสรรงบประมาณ

นับแต่การก่อตั้งหน่วยงานกองบัญชาการตำรวจไซเบอร์ เมื่อวันที่ 9 กันยายน พ.ศ.2563 ผู้วิจัยได้สืบค้นแผนการจัดสรรงบประมาณย้อนหลัง พบว่า ในข้อมูลการจัดสรรงบประมาณประจำปี พ.ศ.2564 ยังไม่ปรากฏชื่อหน่วยงาน บช. สอท. ในแผนการจัดสรร แต่พบข้อมูลการจัดสรรงบประมาณประจำปีของสำนักงานตำรวจแห่งชาติให้ บช. สอท. ตั้งแต่ พ.ศ. 2565 - 2567 โดยมีรายละเอียด ดังนี้

(1) ปีงบประมาณ 2565 ได้รับการจัดสรรจำนวน 166,748,200 บาท เพื่อใช้จ่ายในโครงการ การบังคับใช้กฎหมาย อำนวยความยุติธรรม และบริการประชาชน (กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ, 2564)

(2) ปีงบประมาณ 2566 ได้รับการจัดสรรจำนวน 263,052,480 บาท เพื่อใช้จ่ายในโครงการ การบังคับใช้กฎหมาย อำนวยความยุติธรรม และบริการประชาชน (กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ, 2565)

(3) ปีงบประมาณ 2567 ได้รับการจัดสรรจำนวน 205,881,800 บาท เพื่อใช้จ่ายในโครงการ การบังคับใช้กฎหมาย อำนวยความยุติธรรม และบริการประชาชน (กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ, 2567)

เมื่อพิจารณาจากการจัดสรรงบประมาณในสำนักงานตำรวจแห่งชาติให้กองบัญชาการตำรวจจะเห็นว่าในปีงบประมาณ 2566 ได้รับการจัดสรรงบประมาณเพิ่มขึ้นจากปีก่อนหน้าแสดงให้เห็นว่าภารกิจด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้รับความสำคัญขึ้น และแม้ว่าในปีงบประมาณ 2567 จะได้รับการจัดสรรงบประมาณน้อยกว่าปี 2566 แต่ก็ยังมากกว่า

งบประมาณในปี 2565 ซึ่งนับเป็นแนวโน้มที่เพิ่มขึ้นที่สะท้อนให้เห็นถึงประเด็นด้านภัยคุกคามทางเทคโนโลยีที่ถูกทำให้เป็นประเด็นด้านความมั่นคง

4.6 แนวทางการรับมือกับปัญหาแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจไซเบอร์

ท่ามกลางภารกิจของกองบัญชาการตำรวจไซเบอร์ในการจัดการปัญหาภัยคุกคามทางไซเบอร์ จะเห็นได้ว่าปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาที่มีมูลค่าความเสียหายมากที่สุดและเป็นปัญหาที่เกิดขึ้นอย่างต่อเนื่อง ดังจะเห็นจากข้อมูลสถิติการรับแจ้งความที่มีจำนวนมาก โดยจากสถิติในปีพ.ศ. 2564 พบว่ามีคดีแก๊งคอลเซ็นเตอร์ที่ทำการหลอกลวงเงินจากประชาชนจากกว่า 6 ล้านครั้งซึ่งเพิ่มขึ้นจากปีพ.ศ.2563 ถึง 2.7 เท่าและสร้างมูลค่าความเสียหายถึง 1,600,000,000 บาท (PPTV, 2565, ออนไลน์)[iii] ขณะที่สถิติการรับแจ้งความออนไลน์ระหว่างวันที่ 1 มีนาคม 2565 – 22 เมษายน 2566 พบว่ามีจำนวนทั้งสิ้น 244,567 คดี ซึ่งเฉลี่ยในแต่ละวันจะมีการรับแจ้งคดีการหลอกลวงประมาณ 800 คดีต่อวัน โดยรูปแบบการหลอกลวงแอบอ้างว่าเป็นคอลเซ็นเตอร์ของหน่วยงานของรัฐพบว่ามีจำนวน 20,937 คดี มูลค่าความเสียหาย 3,328,454,052.35 บาท ทั้งนี้ มีหน่วยงานของรัฐที่ถูกแอบอ้างนำไปหลอกลวงประชาชนถึง 13,402 คดี (RTP Cyber Vaccinated, 2566, ออนไลน์)[iv] ดังตาราง

หน่วยงานรัฐที่ถูกแอบอ้าง	**จำนวนคดีที่ได้รับการแจ้งความออนไลน์**
กรมสรรพากร	3,024
ไปรษณีย์ไทย	1,384
สถานีตำรวจ	1,303
สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.)	590
กรมสอบสวนคดีพิเศษ (DSI)	533
กรมศุลกากร	218
สำนักงานตำรวจแห่งชาติ	149
กรมที่ดิน	147

การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย/ส่วนภูมิภาค	113
การประปานครหลวง/ส่วนภูมิภาค	51
กรมพัฒนาธุรกิจการค้า	16
กรมการค้าภายใน	4
กรมการจัดหางาน	3

ตาราง 2 แสดงสถิติการรับแจ้งความคดีแก๊งคอลเซ็นเตอร์ในช่วง 2 มีนาคม 2565 – 22 เมษายน 2566

ที่มา: https://pctpr.police.go.th/knowledge.php

นอกจากนี้ สถิติการรับแจ้งความคดีอาชญากรรมทางเทคโนโลยีทั้งหมดใน พ.ศ.2566 มีทั้งสิ้น 185,814 คดี คิดเป็นมูลค่าความเสียหายถึง 20,000,000,000 บาท (Droindsans, 2567, ออนไลน์) [v] โดยระหว่าง 17 มีนาคม – 31 ธันวาคม 2566 มีผู้ตกเป็นเหยื่อในลักษณะที่แตกต่างกันดังนี้

ลักษณะของการหลอกลวงจากแก๊งคอลเซ็นเตอร์	**จำนวนคดีที่ได้รับแจ้ง**
หลอกลวงซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ	82,902
หลอกให้โอนเงินเพื่อทำงานฯ	20,837
หลอกให้กู้เงิน	17,155
หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	13,093
ข่มขู่ทางโทรศัพท์ (Call center)	8,811
หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	8,283
หลอกให้โอนเงินเพื่อรับรางวัลฯ	5,013
กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ฯ	1,549
หลอกรักแล้วโอนเงิน	1,435
หลอกลวงเกี่ยวกับทรัพย์สินดิจิทัล	1,432
หลอกซื้อขายสินค้าหรือบริการ	479
หลอกให้ลงทุนความผิดตาม พ.ร.ก.กู้ยืมเงิน	141

เข้ารหัสข้อมูลคอมพิวเตอร์ของคนอื่นเพื่อกรรโชกฯ	73

ตาราง 3 ตาราง 4.2 ลักษณะของการหลอกลวงจากแก๊งคอลเซ็นเตอร์ในช่วง 17 มีนาคม -31 ธันวาคม 2566

ที่มา: https://droidsans.com/14-online-cyber-2024-and-aoc-hotline/

จากข้อมูลสถิติการรับแจ้งความของสำนักงานตำรวจแห่งชาติข้างต้น สะท้อนให้เห็นว่าสำนักงานตำรวจแห่งชาติได้มีแนวทางในการรับมือกับภัยคุกคามทางไซเบอร์ โดยไม่เพียงแต่มีการจัดตั้งกองบัญชาการตำรวจไซเบอร์ ซึ่งมีภารกิจในการรับผิดชอบคดีที่มีมูลค่าความเสียหายสูงเท่านั้น แต่ยังได้มีการทำงานร่วมกับคณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี[1] และศูนย์ต่อต้านอาชญากรรมออนไลน์ ซึ่งมีสายด่วนในการรับเรื่องร้องทุกข์จากประชาชน คือ AOC 1441 ตลอดจนทำหน้าที่ในอำนวยความสะดวกให้แก่ประชาชนในการติดต่อประสานงานร้องทุกข์และแจ้งความ ทั้งนี้ ยังได้มีการเพิ่มช่องทางให้แก่ประชาชนสามารถผู้ได้รับความเดือดร้อนจากการตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยีให้สามารถแจ้งความได้โดยตรงผ่านช่องทางออนไลน์ โดยสามารถเข้าแจ้งความได้ที่ เว็บไซต์ https://thaipoliceonline.com

กล่าวได้ว่าการรับมือของกองบัญชาการตำรวจไซเบอร์จำเป็นต้องบูรณาการความร่วมมือกับหลายภาคส่วน เพื่อให้สามารถป้องกันและปราบปรามปัญหาแก๊งคอลเซ็นเตอร์ได้อย่างมีประสิทธิภาพ ตลอดจนลดความเสียหายที่อาจเกิดขึ้นกับประชาชนให้เหลือน้อยที่สุด โดยหน่วยงานที่กองบัญชาการตำรวจไซเบอร์ต้องประสานความร่วมมือในการป้องกันและปราบปรามปัญหาแก๊งคอลเซ็นเตอร์นอกเหนือไปจากการประสานงานร่วมกับคณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยีและศูนย์ต่อต้านอาชญากรรมออนไลน์ สำนักงานตำรวจแห่งชาติ เช่น กระทรวงดิจิทัลเพื่อการพัฒนาเศรษฐกิจและสังคม กระทรวงการคลัง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ธนาคาร รวมถึงผู้ให้บริการเครือข่ายโทรศัพท์ ฯลฯ

อย่างไรก็ตาม จากการศึกษาพบว่า นอกจากการปราบปรามต้นเหตุของปัญหาแก๊งคอลเซ็นเตอร์ที่มีการดำเนินการปราบปรามอย่างเข้มงวดมากขึ้นในช่วงที่ผ่านมา กองบัญชาการตำรวจ

ไซเบอร์ยังได้มุ่งเน้นไปที่การประชาสัมพันธ์ให้กับประชาชนทั่วไปเพื่อนำไปสู่การป้องกันมิให้ประชาชนตกเป็นเหยื่อขบวนการดังกล่าวเพิ่มมากขึ้น ดังจะเห็นได้ว่า กองบัญชาการตำรวจไซเบอร์ได้มีการจัดทำภาพโฆษณาและวีดีทัศน์ขนาดสั้นเพื่อสื่อสารในลักษณะการเตือนภัยให้แก่ประชาชนเกี่ยวกับแก๊งคอลเซ็นเตอร์และในประเด็นที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีอย่างต่อเนื่อง โดยนอกจากจะมีการประสานงานกับศูนย์ต่อต้านอาชญากรรมออนไลน์แล้ว เปิดให้มีการแจ้งความออนไลน์แล้ว ยังได้มีช่องทางติดต่อสื่อสารเพิ่มเติม คือ ช่องทางการสนทนา Line (@police1441) เพื่อให้คำปรึกษาในคดีอาชญากรรมทางเทคโนโลยีด้วย

โดยสรุปแล้ว แนวทางการรับมือต่อปัญหาแก๊งคอลเซ็นเตอร์ของกองบัญชาการตำรวจไซเบอร์ที่ผ่านมานับตั้งแต่ได้มีการก่อตั้งหน่วยในปีพ.ศ.2563 ประกอบไปด้วยมาตรการสำคัญคือการป้องกันและการปราบปราม นอกจากนี้ ยังได้เพิ่มขีดความสามารถในการรับมือกับปัญหาด้วยการบูรณาการความร่วมมือกับหน่วยต่าง ๆ ที่เกี่ยวข้อง เพิ่มช่องทางการรับแจ้งความออนไลน์และช่องทางการติดต่อกับเจ้าหน้าที่ในการให้คำปรึกษาเกี่ยวกับคดีอาชญากรรมทางเทคโนโลยี ตลอดจนได้มีการประชาสัมพันธ์เพื่อให้เกิดการตระหนักรู้ถึงภัยคุกคามทางไซเบอร์และรู้เท่าทันการหลอกลวงของแก๊งคอลเซ็นเตอร์อย่างต่อเนื่อง ซึ่งปัจจุบันจะเห็นได้ว่าประชาชนเริ่มมีการตื่นตัวและเพิ่มความระมัดระวังมากขึ้นในการรับสายโทรศัพท์ หรือการสนทนากับบุคคลแปลกหน้าที่แอบอ้างว่าเป็นหน่วยงานภาครัฐ อย่างไรก็ตาม แม้ว่าจะได้มีการประชาสัมพันธ์เพื่อป้องกันการตกเป็นเหยื่อของแก๊งคอลเซ็นเตอร์มาโดยตลอดตามมาตรการป้องกันอาชญากรรมทางเทคโนโลยีของกองบัญชาการตำรวจไซเบอร์ ทว่า จำนวนของสถิติในการรับแจ้งความยังอยู่ในระดับที่สูง เนื่องจากวิธีการหลอกลวงเหยื่อของแก๊งคอลเซ็นเตอร์ที่มีการเปลี่ยนแปลงไปเรื่อย ๆ ดังนั้น จึงเป็นโจทย์สำคัญของกองบัญชาการตำรวจไซเบอร์ในการหาแนวทางการรับมือที่เหมาะสมต่อพลวัตรของอาชญากรรมทางเทคโนโลยีต่อไป

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะจากการวิจัย

5.1 สรุปผลการวิจัย

ในการศึกษากระบวนการทำให้ปัญหาแก๊งคอลเซ็นเตอร์เป็นปัญหาความมั่นคงของกองบัญชาการตำรวจไซเบอร์ พบว่า ตัวแสดงที่เกี่ยวข้องกับกระบวนการทำให้เป็นปัญหาความมั่นคง (securitization) ของไทย เริ่มจากตัวแสดงในระดับรัฐ ที่รัฐบาลนำโดยนายกรัฐมนตรีและหน่วยงานที่เกี่ยวข้องอื่น ๆ ได้ให้ความสำคัญกับปัญหาแก๊งคอลเซ็นเตอร์ เนื่องจากเป็นปัญหาที่สร้างความเดือดร้อนให้แก่ประชาชนจำนวนมาก และมูลค่าความเสียหายที่สูง จึงเกิดเป็นนโยบายเพื่อแก้ไขปัญหาดังกล่าวมากขึ้นทั้งในแง่ของกลไกการบริหารราชการของรัฐ และการดำเนินการออกกฎหมายที่เกี่ยวข้องเพื่อรับมือกับปัญหา ในส่วนของตัวแสดงในระดับประชาชน เทคโนโลยีที่พัฒนาขึ้นและเปลี่ยนแปลงไปทำให้มิจฉาชีพมองหาวิธีการใหม่ ๆ ในการก่ออาชญากรรม โดยอาชญากรรมหลอกลวงในรูปแบบเดิม ๆ ได้พัฒนาและเปลี่ยนแปลงรูปแบบไปและเข้าถึงประชาชนมากขึ้น และเมื่อมีผู้เสียหายจากอาชญากรรมทางเทคโนโลยีมากขึ้น ก็เกิดเป็นแรงกดดันจากประชาชนต่อรัฐให้แก้ไขปัญหาและบรรเทาความเดือดร้อนให้กับประชาชน

การเกิดขึ้นของกองบัญชาการตำรวจไซเบอร์เป็นส่วนหนึ่งของกระบวนการ securitization ของไทย นับเป็น securitizing actor หรือตัวแสดงที่ทำให้เรื่องอาชญากรรมทางเทคโนโลยีกลายเป็นความมั่นคงของรัฐไทย ที่เกิดจากนิยามด้านความมั่นคงในระดับโลกที่ผ่านมาให้ความสำคัญกับความปลอดภัยของมนุษย์ทั้งในมิติของความปลอดภัยในชีวิตและทรัพย์สิน ซึ่งเป็นแนวโน้มการเปลี่ยนแปลงนิยามของ referent object ในสายตาของรัฐ ที่เปลี่ยนแปลงจากการให้ความสำคัญของ “ความมั่นคงปลอดภัยของรัฐ” มาเป็น “ความมั่นคงปลอดภัย” ของประชาชน ดังนั้นการจัดตั้งหน่วยงานตำรวจขึ้นมาจัดการกับปัญหาอาชญากรรมทางไซเบอร์ และออกกฎหมายที่เกี่ยวข้องเพื่อจัดการกับการกระทำผิดที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี โดยยกระดับการรับมือกับภัยคุกคามด้วยการจัดตั้งหน่วยงานระดับ “กองบัญชาการ” ขึ้นภายใต้สำนักงานตำรวจแห่งชาติ เพื่อรับผิดชอบคดีที่มีความเสียหายมูลค่าสูง ส่งผลกระทบในวงกว้าง

และเป็นหน่วยงานสืบสวน สอบสวน ตรวจสอบหลักฐานเพื่อสนับสนุนการปฏิบัติหน้าที่ตำรวจท้องที่ นับเป็นการสร้างวาทกรรม หรือ speech act ที่ทำให้อาชญากรรมทางเทคโนโลยีเป็นปัญหาด้านความมั่นคงในตัวเอง ในลักษณะเดียวกันกับการทำให้เรื่องอื่น ๆ เป็นประเด็นด้านความมั่นคง เช่น ปัญหายาเสพติด ปัญหาการฟอกเงิน ปัญหาการค้ามนุษย์ เนื่องจากภารกิจหลักของตำรวจคือการรับมือกับภัยคุกคามด้านความมั่นคงอยู่แล้ว ดังนั้นการจัดตั้งหน่วยงานรับผิดชอบเฉพาะเป็นการแสดงให้เห็นว่า เรื่องดังกล่าวมีความสำคัญและส่งผลกระทบต่อความมั่นคงรัฐจึงต้องเข้ามามีบทบาทรับผิดชอบ

เมื่อพิจารณาศึกษาถึงบทบาทของกองบัญชาการตำรวจไซเบอร์ จะเห็นได้ว่า กองบัญชาการตำรวจไซเบอร์ได้สร้างความตระหนักรู้เกี่ยวกับภัยคุกคามจากอาชญกรรมทางเทคโนโลยี โดยเฉพาะปัญหาแก๊งคอลเซ็นเตอร์ ผ่านการสื่อสารกับประชาชนซึ่งเป็น audience ที่รับวาทกรรมที่ทำให้อาชญากรรมทางเทคโนโลยีเป็นปัญหาด้านความมั่นคง ดังที่จะเห็นได้ว่า คำว่า “คอลเซ็นเตอร์” กลายเป็นคำที่มีความหมายเชิงลบในฐานะมิจฉาชีพเป็น “แก๊งคอลเซ็นเตอร์” เพิ่มเติมจากความหมายดั้งเดิมของคอลเซ็นเตอร์ที่สื่อความหมายถึงศูนย์โทรศัพท์สำหรับการบริการลูกค้า โดยในการใช้ภาษาประชาสัมพันธ์ของตำรวจไซเบอร์จะเป็นไปในลักษณะ “เตือนภัยแก๊งคอลเซ็นเตอร์” หรือ “ปฏิบัติการรวบหัวหน้าแก๊งคอลเซ็นเตอร์” เป็นต้น อีกทั้งยังได้มีการระบุ (identify) ประเภทอาชญากรรมทางเทคโนโลยีเพื่อความชัดเจนในการแก้ไขปัญหา และประชาสัมพันธ์ให้ประชาชนเข้าใจ โดยมีแนวทางในการจัดการปัญหาคอลเซ็นเตอร์ 2 มิติ คือ

(1) มาตรการป้องกัน มิให้เกิดเหตุด้วยการบังคับใช้กฎหมายอย่างเข้มงวดเพื่อป้องกันการกระทำผิด และป้องปรามมิให้ประชาชนทั่วไปเข้าร่วมกระบวนการแก๊งคอลเซ็นเตอร์ ในขณะเดียวกันก็สร้างความตระหนักรู้ สร้างภูมิคุ้มกันให้กับประชาชน

(2) มาตรการปราบปราม ด้วยการบังคับใช้กฎหมายสืบสวนและสอบสวน ปฏิบัติการจับกุม ขยายผลการจับกุม มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อปราบปรามแก๊งคอลเซ็นเตอร์

ปัญหาคอลเซ็นเตอร์มีมิติของความเป็นอาชญากรรมข้ามชาติ เพราะอาชญากรรมทางเทคโนโลยีมิได้เกิดขึ้นอยู่ภายในเขตแดนเท่านั้น แต่มีลักษณะ transnational ในส่วนของปัญหาคอลเซ็นเตอร์พบว่า มักจะมีฐานปฏิบัติการอยู่ตามชายแดนหรือในเขตประเทศเพื่อนบ้านของไทย แต่ก่อเหตุหลอกลวงประชาชนในประเทศไทย และประเทศอื่น ๆ ด้วย โดยพบว่า ส่วนมากมีความเกี่ยวข้องกับกลุ่มอาชญากรข้ามชาติ ที่เกี่ยวพันกับการฟอกเงิน หรือการกระทำผิดอื่นร่วมด้วย อย่างเช่น กระบวนการค้ามนุษย์ เว็บพนันออนไลน์ เป็นต้น เพราะในหลาย ๆ กรณีพบว่าบุคคลที่ทำงานในแก๊งคอลเซ็นเตอร์เป็นเหยื่อของกระบวนการค้ามนุษย์ที่ถูกบังคับใช้แรงงานให้ทำหน้าที่เป็นคอลเซ็นเตอร์เพื่อหลอกลวงผู้อื่น โดยหากหลอกไม่ได้ก็จะถูกทำร้ายร่างกาย ลงโทษ ทำให้ปัญหานี้มีความจำเป็นต้องได้รับความร่วมมือจากตำรวจต่างชาติในการแก้ไขปัญหาด้วย ซึ่งกองบัญชาการตำรวจไซเบอร์มีหน่วยงานรับผิดชอบ

การแบ่งส่วนราชการภายใต้กองบัญชาการตำรวจไซเบอร์ครอบคลุมความรับผิดชอบพื้นที่ทุกภาคทั่วประเทศไทย นอกจากนี้ กองบัญชาการไซเบอร์ยังมีความร่วมมือกับหน่วยงานที่เกี่ยวข้องต่างประเทศในการแลกเปลี่ยนข้อมูล ร่วมกับปฏิบัติการจับกุมผู้กระทำผิดด้วย ซึ่งเป็นแนวทางจัดการปัญหาที่ทำให้จำนวนอาชญากรรมจากแก๊งคอลเซ็นเตอร์ลดลง

5.2 **ข้อเสนอแนะจากการวิจัย**

5.2.1 สำหรับหน่วยงานภาครัฐ โดยเฉพาะหน่วยงานที่เกี่ยวข้องกับความมั่นคง การทำความเข้าใจกระบวนการทำให้เป็นความมั่นคง (securitization) จะสามารถใช้วิเคราะห์ประเด็นปัญหาใหม่ๆ ที่อาจเกิดขึ้นในอนาคต เพื่อเป็นข้อเสนอแนะทางนโยบายเพื่อป้องกันเหตุได้ ดังเช่นในกรณีของปัญหาแก๊งคอลเซ็นเตอร์ที่มีพัฒนาการมาจากแก๊งต้มตุ๋น การหลอกลวงทางเศรษฐกิจในรูปแบบเดิม ๆ โดยใช้เทคโนโลยีเข้ามาเป็นเครื่องมือจึงเข้าถึงประชาชนได้ง่ายขึ้นจนกลายเป็นปัญหาระดับชาติ

5.2.2 แม้ว่ากองบัญชาการตำรวจไซเบอร์หรือกองบัญชาการตำรวจสืบสวนและสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) จะกำหนดเงื่อนไขคดีที่เข้าข่ายความรับผิดชอบชัดเจน แต่เป็นการยากสำหรับประชาชนที่จะทราบว่าคดีที่ตนเป็นผู้เสียหายเข้าเงื่อนไขความ

รับผิดชอบของหน่วยงานใดตามการแบ่งงานตามโครงสร้างของสำนักงานตำรวจแห่งชาติ ผู้วิจัยเห็นว่า บทบาทของกองบัญชาการตำรวจไซเบอร์ และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือ บก.ปอท. ที่มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกัน และปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน มีความใกล้เคียงกันโดยมีเงื่อนไขความแตกต่างอยู่ที่มูลค่าความเสียหายเกี่ยวกับคดีที่ต้องเกิน 30 ล้านบาท หรือต้องมีผู้เสียหายรวมกันตั้งแต่ 50 คนขึ้นไป หรือ มูลค่าความเสียหาย 10 ล้านบาทขึ้นไปและมีผู้เสียหายตั้งแต่ 10 คนขึ้นไป หรือ มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติ โดยการที่ทั้งสองหน่วยงานรับทำคดีลักษณะเดียวกันแต่มีจุดแบ่งที่เงื่อนไขข้างต้นทำให้ประชาชนเกิดความสับสนว่าหน่วยงานใดกันแน่ที่เป็นผู้รับผิดชอบ และประชาชนควรติดต่อหน่วยงานใด

บรรณานุกรม

บรรณานุกรม

Buzan, B., & Hansen, L. (2009). *THE EVOLUTION OF INTERNATIONAL SECURITY STUDIES.*

Elman, C. (2008). Realism. In P. D. Williams, *Security Studies: An introduction* (p. 17). Oxford: Routledge.

Interpol. (n.d.). Retrieved from https://www.interpol.int/

McDonald, M. (2008). Constructivism. In P. D. Williams, *Security Studies: An Introduction.* Oxford: Routledge.

Mitra, A. (2010). *Digital Security: Cyber Terror and Cyber Security.* New York: Infobase Publishing.

Motive Influence. (2566). *โซเชียลมีเดีย ที่คนไทยใช้มากสุดปี 2023*. Retrieved from motiveinfluence.com/blog/marketing/โซเชียลมีเดีย-ที่คนไทยใช้มากสุดปี-2023/547

Navari, C. (2008). Liberalism. In P. D. Williams, *Security Studies: An Introduction.* Oxford: Routledge.

Thailand Board of Investment. (2024). *Thailand Board of Investment*. Retrieved from https://www.boi.go.th/index.php?page=demographic

The Standard. (2566). *ตำรวจไซเบอร์เตือนภัยแก๊งคอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่ กสทช. และค่ายมือถือ หลอกให้โอนเงินเพื่อแสดงความบริสุทธิ์ใจ*. Retrieved from The Standard: https://thestandard.co/call-center-gang-warning/

Ullman, R. (1983). 'Redefining Security'. *International Security*, 129–53.

UNDP. (1994). *Human Development Report 1994*. Retrieved from https://hdr.undp.org/system/files/documents/hdr1994encompletenostatspdf.pdf

Walker, R. (1997). The Subject of Security. In K. Krause, & M. C. Williams , *Critical Security Studies: Cases and Concepts* (p. 67). Minneapolis: Minnesota University Press.

Wall, D. (2004). *What are Cybercrime?* Retrieved from Centre of Crime and Justice Studies:

https://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627250408553239.pdf

William, P. D. (2008). *SECURITY STUDIES: AN INTRODUCTION*. OXFORD: ROUTLEDGE.

Williams, M. (2007). *Culture and security: Symbolic power and the politics of international security.* Routledge.

กนกนก โพธิ์หอม. (2564). พลวัตความมั่นคงทางไซเบอร์ของประเทศไทย. *วารสารมุมมองความมั่นคง ฉบับที่ 7 ประจำเดือนมิถุนายน - กันยายน 2564*. เข้าถึงได้จาก https://www.nsc.go.th/wp-content/uploads/Journal/article-00705.pdf)

กรมประชาสัมพันธ์. (2566). *รู้จัก บัญชีม้า ซิมม้า โทษหนัก ทั้งปรับ-จำคุก*. Retrieved from กรมประชาสัมพันธ์: https://www.prd.go.th/th/content/category/detail/id/9/iid/225752

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (n.d.). Retrieved from https://www.mdes.go.th/mission/detail/2458-%E0%B8%84%E0%B8%93%E0%B8%B0%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A3%E0%B8%B1%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A1%E0%B

กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ. (2564). Retrieved from https://policebudget.go.th/drupal/content/%E0%B9%80%E0%B8%A5%E0%B9%88%E0%B8%A1%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%A5%E0%B8%B0%E0%B9%80%E0%B8%AD%E0%B8%B5%E0%B8%A2%E0%B8%94%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%88%E0%B8%B1%E0%B8%94%E0%B8%AA%E0%B8%A3%E0%B8%A3%E0%B8

กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ. (2565). Retrieved from https://policebudget.go.th/drupal/sites/default/files/0.%E0%B8%88%E0%B8%B3%E0%B9%81%E0%B8%99%E0%B8%81%E0%B8%A3%E0%B8%A7%E0%B8%A1%20%E0%B8%9B%E0%B8%B566%28%E0%B8%AA%E0%B9%88%E0%B8

%87%E0%B8%9C%E0%B8%A5%E0%B8%B4%E0%B8%95%2012.1065%29.pdf

กองงบประมาณ สำนักงานงบประมาณการเงินตำรวจ. (2567). Retrieved from https://budgetfinance.police.go.th/filedownload/prachasampan/2024/1.%20PDF%20%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%A5%E0%B8%B0%E0%B9%80%E0%B8%AD%E0%B8%B5%E0%B8%A2%E0%B8%94%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%88%E0%B8%B1%E0%B8%94%E0%B8%AA%E0%B8%A3%E0%B8%A3%E0%B8%

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (n.d.). Retrieved from https://www.hightechcrime.org/staff/History: https://www.hightechcrime.org/staff/History

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (n.d.). *วุฒิสภา*. Retrieved from วุฒิสภา: https://www.senate.go.th/assets/portals/126/fileups/345/files/8%20%E0%B8%AD%E0%B8%B2%E0%B8%8A%E0%B8%8D%E0%B8%B2%E0%B8%81%E0%B8%A3%E0%B8%A3%E0%B8%A1%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B9%80%E0%B8%97%E0%B8%84%E0%B9%82%E0%B8%99%E0%B9%82%E0%B8%A5%E0%B8%A2%E0%B8%B5

ฉัตรชัย ศรีเมืองกาญจนา. (2562). *อาชญากรรมข้ามชาติกับความมั่นคงของประเทศไทย*. เข้าถึงได้จาก สำนักวิชาการ สำนักเลขาธิการสภาผู้แทนราษฎร: https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=55062&filename=house2554#:~:text=%E0%B8%AA%E0%B9%88%E0%B8%A7%E0%B8%99%E0%B8%97%E0%B8%B2%E0%B8%87%E0%B8%94%E0%B9%89%E0%B8%B2%E0%B8%99%E0%B8%AD%E0%B8%87%E0%B8%84%E0%B9%8C%E0%B8%8

เดลินิวส์ออนไลน์. (2565). *ปฏิบัติการ "เด็ดปีกมังกร" ตะลึง พ.ต.ท. ขายข้อมูลแก๊งคอลเซ็นเตอร์... สามารถติดตามต่อได้ที่ : https://www.dailynews.co.th/news/1625011/*. Retrieved from https://www.dailynews.co.th/news/1625011/

นายรุ่งโรจน์ กิตติถาวรกุล. (n.d.). *รู้ เข้าใจและตระหนัก "อาชญากรรมทางไซเบอร์" (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว*. Retrieved from HTTPS://WWW.CHULA.AC.TH/NEWS/138291/

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. (2566). Retrieved from ราชกิจจานุเบกษา: https://www.mdes.go.th/law/detail/6664-%E0%B8%9E%E0%B8%A3%E0%B8%B0%E0%B8%A3%E0%B8%B2%E0%B8%8A%E0%B8%81%E0%B8%B3%E0%B8%AB%E0%B8%99%E0%B8%94%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%9B%E0%B9%89%E0%B8%AD%E0%B8%87%E0%B8%81%E0%B8%B1

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562). Retrieved from ราชกิจจานุเบกษา: https://ratchakitcha.soc.go.th/documents/140A018N0000000000100.pdf

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556. (2556). *พระราชบัญญัติ ป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ*. Retrieved from https://www.ratchakitcha.soc.go.th/DATA/PDF/2556/A/055/1.PDF

วศิน ปั้นทอง. (ม.ป.ป.). *ความมั่นคงไซเบอร์: ประสบการณ์ของต่างประเทศและบทเรียนสำหรับประเทศไทย.* เข้าถึงได้จาก สภาความมั่นคงแห่งชาติ: https://www.nsc.go.th/wp-content/uploads/Journal/article-00102.pdf

เว็บไซต์รัฐบาลไทย. (2567). Retrieved from วันนี้เอาประชาชนเป็นที่ตั้ง ผลงานของเราจะเป็นที่ประจักษ์ ขอเป็นนิมิตหมายอันดีและเป็นจุดเริ่มต้นใหม่ ของการที่เราเข้ามาดูแลพี่น้องประชาชน ภายใน 30 วันนี้ชัดเจนว่าจะจับอะไรให้ได้ ไม่ว่าจะเป็นหวยออนไลน์ หรืออะไรที่เกิดขึ้น ซึ่งพี่น้องถูกหลอกลวงทุกวันนี้ยังมีอย

ศิวลีย์ สิริโรจน์บริรักษ์, (. :. (2557). การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม. *ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ*.

สรวิศ บุญมี. (2566). วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชียฉบับวิทยาศาสตร์และเทคโนโลยี ปีที่ 17 ฉบับที่ 2 ประจ าเดือน พฤษภาคม-สิงหาคม 256619บทคัดย่อแก๊งคอลเซ็นเตอร์เป็นอาชญากรรมทางเศรษฐกิจที่แสวงประโยชน์จากความตื่นกลัว ความโลภ ซึ่งเกิดขึ้นมา

นานระยะหนึ่งแล้ว แต่ได้ขยายวงอย. *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชียฉบับวิทยาศาสตร์และเทคโนโลยี , ปีที่ 17*(ฉบับที่ 2 ประจำเดือน พฤษภาคม-สิงหาคม 2566).

สักกรินทร์ นิยมศิลป์. (2558). อาชญากรรมข้ามชาติ: ภัยคุกคามไทยและอาเซียน. *ความหลากหลายทางประชากรและสังคมในประเทศไทย ณ ปี 2558*. เข้าถึงได้จาก https://ipsr.mahidol.ac.th/wp-content/uploads/2022/03/447-IPSR-Conference-A15-fulltext.pdf

สาวตรี สุขศรี. (2563). กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. *โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์*.

สำนักข่าวอิศรา. (2566). *"คอลเซ็นเตอร์" บุกชายแดนใต้ ยะลาร้องถูกหลอกอื้อ*. Retrieved from https://www.isranews.org/article/south-news/south-slide/122380-gangcallcenter.html#:~:text=เปิดสถิติคดีออนไลน์%2016,ไม่ต่ำกว่า%2010%20ราย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (n.d.). Retrieved from https://www.ncsa.or.th/functions-and-powers-of-the-office.html

สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์วิจัยและนวัตกรรม. (2564). Retrieved from https://researchcafe.tsri.or.th/call-center-crime/

สุภาพิชญ์ ถิระวัฒน์. (2564). *กองบัญชาการตำรวจไซเบอร์.* Retrieved from หอสมุดรัฐสภา: https://library.parliament.go.th/th/radioscript-rr2564-nov1

สุภาพิชญ์ ถิระวัฒน์. (n.d.). *กองบัญชาการตำรวจไซเบอร์.* Retrieved from สำนักเลขาธิการสภาผู้แทนราษฎร : https://library.parliament.go.th/th/radioscript-rr2564-nov1

อาริยา สุขโต. (2565). *ภัยอาชญากรรมแก๊งคอลเซ็นเตอร์.* เข้าถึงได้จาก สำนักงานเลขาธิการสภาผู้แทนราษฎร: https://library.parliament.go.th/th/radioscript/rr2565-jul7

ประวัติผู้เขียน

[i] Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis*, p.25-33.

[iii] เปิดสถิติ แก๊งคอลเซ็นเตอร์ โทรหลอกคนโอนเงิน ตลอดปี 2564 https://www.pptvhd36.com/wealth/stock-investment/171695 (9 พฤษภาคม 2565)

[iv] ตร.จับมือหน่วยงานรัฐ เตือนภัยคอลเซ็นเตอร์ ลวงประชาชน เสียหาย 400 ล้าน https://pctpr.police.go.th/blog/?p=136#:~:text=สำหรับสถิติการหลอกลวงใน,ได้รับแจ้งคดีการ

[v] เปิดสถิติ 14 ที่ภัยออนไลน์ที่คนไทยโดนหลอกมากสุด 2566. https://droidsans.com/14-online-cyber-2024-and-aoc-hotline/ (15 มกราคม 2567)