

บทที่ 1

บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

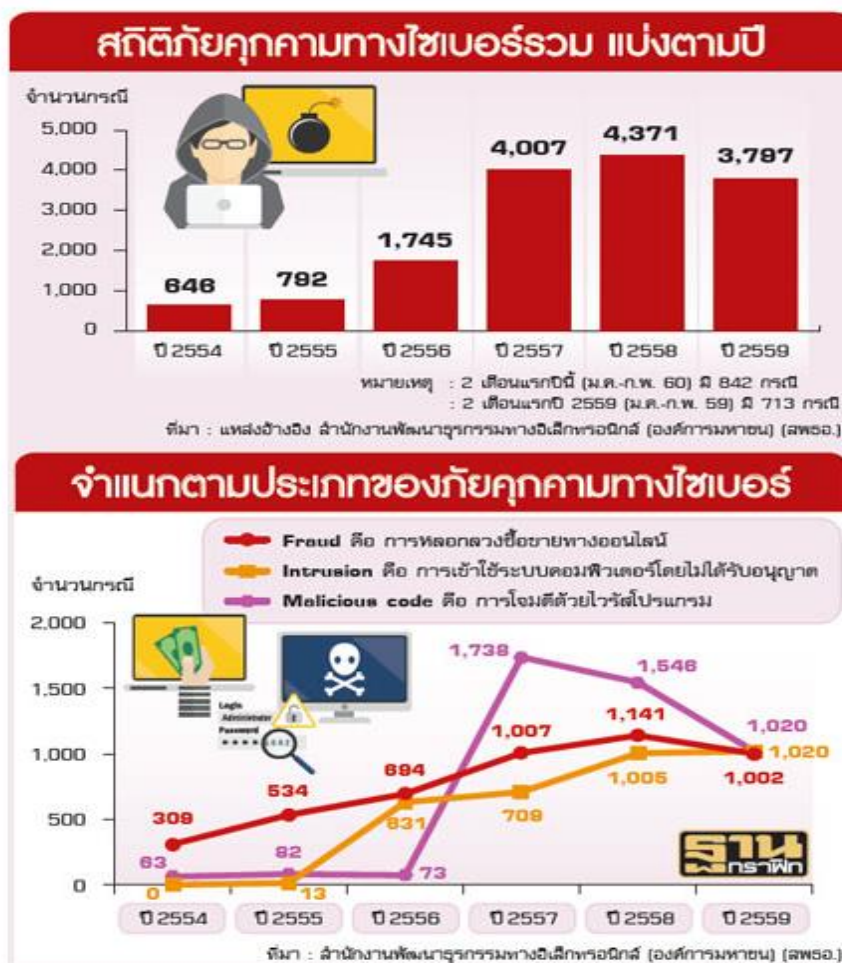
เทคโนโลยีสารสนเทศถือเป็นเครื่องข่ายการติดต่อสื่อสารที่มีความสำคัญมากในปัจจุบัน ในสมัยก่อนเชื่อกันว่า มีเพียงความเชื่อ ความศรัทธา ค่านิยม และศาสนาเท่านั้น ที่จะสามารถทำให้ชีวิตคนเปลี่ยนแปลงได้ เพิ่งจะมา 200 ปีหลังจากที่ผ่านมา ที่ทำให้มนุษย์ตระหนักว่าเทคโนโลยีเป็นตัวการสำคัญที่ทำให้ชีวิตไม่เหมือนเดิม โดยเฉพาะอย่างยิ่ง ในช่วง 40 ปีที่ผ่านมา เทคโนโลยีทำให้โลกเกิดการเปลี่ยนแปลงขนาดใหญ่ นับตั้งแต่มีการปฏิวัติอุตสาหกรรมครั้งที่ 3 ในปี ค.ศ. 1969 ที่เทคโนโลยีสารสนเทศเริ่มเป็นพลังสำคัญในการเปลี่ยนแปลง วิธีการดำรงชีวิตของผู้คนเปลี่ยนไป วิวัฒนาการของเทคโนโลยีก็เปลี่ยนแปลงไปไม่หยุด จนถึงยุคปฏิวัติอุตสาหกรรมครั้งที่ 4 ในปัจจุบัน มีการผสมผสานของเทคโนโลยีต่าง ๆ โดยมีเทคโนโลยี คอมพิวเตอร์ และวิทยาศาสตร์สาขาต่าง ๆ เป็นแกนนำ ปัจจุบันมีคำเรียกบรรดาเทคโนโลยีที่เกิดขึ้นใหม่นี้ว่า เทคโนโลยีเปลี่ยนโลก (Disruptive Technologies) (วราภรณ์ สามโกเศศ, 2563, ออนไลน์) ไม่อาจปฏิเสธได้ว่าเทคโนโลยีใหม่ ๆ ที่เกิดขึ้นนั้น ได้เข้ามามีบทบาทสำคัญในการดำเนินชีวิตของมนุษย์ในสังคมปัจจุบันเป็นอย่างมาก มนุษย์ใช้เทคโนโลยีสารสนเทศเข้ามาทำกิจกรรมทางด้านต่าง ๆ มากมาย เช่น มีการใช้คอมพิวเตอร์ในการทำงาน การค้นหาข้อมูลผ่านทางอินเทอร์เน็ต หรือรับส่งข้อมูลระหว่างกัน ตลอดจนการใช้โทรศัพท์เคลื่อนที่ (Mobile Phone) หรือโทรศัพท์มือถือในการติดต่อสื่อสาร เป็นต้น ขณะที่เทคโนโลยีถือว่ามีอิทธิพลและก่อให้เกิดการเปลี่ยนแปลงรูปแบบการดำเนินชีวิตต่อคนในสังคมโลกเป็นอย่างมาก แต่ในอีกมุมหนึ่งเทคโนโลยีเป็นเรื่องที่ทุกคนมีเสรีภาพอย่างมากที่จะสามารถทำอะไรก็ได้ เนื่องจากหลายเรื่องที่มีมนุษย์กระทำผ่านเทคโนโลยีสารสนเทศ เราไม่อาจจะทราบได้ว่าใครเป็นใคร มีตัวตนหรือไม่มีตัวตน ดังนั้นจึงอาจส่งผลให้เกิดการใช้เทคโนโลยีอย่างเกินขอบเขต จนทำให้เกิดความเสียหายหรือมีการกระทำผิดกฎหมาย เช่น การใช้อินเทอร์เน็ตเป็นเครื่องมือในการทำร้ายผู้อื่น เกิดการละเมิดสิทธิเสรีภาพส่วนบุคคล รวมทั้งมีส่วนก่อให้เกิดการทำความผิดทางอาญา ซึ่งถือว่าเป็นเรื่องที่สำคัญและร้ายแรงในสังคมปัจจุบัน เพราะเป็นสิ่งที่ประชาชนทุกคนมีโอกาสที่จะสัมผัสในชีวิตประจำวัน (อังสุมารินทร์ ภูสีม่วง, 2563, ออนไลน์)

ปัจจุบันปัญหาอาชญากรรมนับวันจะมีแต่เพิ่มมากขึ้นและมีรูปแบบที่หลากหลาย โดยอาศัยความเจริญก้าวหน้าของระบบเทคโนโลยีคอมพิวเตอร์และระบบสารสนเทศ จึงทำให้ช่องทางการกระทำความผิดมีความหลากหลายสลับซับซ้อนและเป็นอันตรายต่อผู้คนเป็นวงกว้างทั้งในระดับความมั่นคงภายใน ภายนอกประเทศ เพราะเป้าหมายสำคัญของอาชญากรรมทางเทคโนโลยี โดยเฉพาะอาชญากรรมทางคอมพิวเตอร์ (Criminal Cyber) (มหาวิทยาลัยราชภัฏสวนสุนันทา, 2558, ออนไลน์) คือ การโจรกรรม แก๊ง ลักลอบ เผยแพร่ หรือแสวงหาประโยชน์ต่าง ๆ โดยมีขอบซึ่งสามารถส่งผลกระทบต่อเศรษฐกิจ การเงิน การเมือง การปกครองของสังคม จึงอาจกล่าวได้ว่าอาชญากรรมทางเทคโนโลยีมีผลกระทบมากกว่าอาชญากรรมโดยทั่วไป ซึ่งอาชญากรรมทางเทคโนโลยีมักจะมีการพัฒนาวิธีการใหม่ๆ ขึ้นมาเสมอและยากต่อการติดตามจับกุมตัวผู้กระทำผิดเพื่อบำบัดคดี

สำหรับประเทศไทย หากมองในภาพรวมระดับประเทศ เราจะพบว่า กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ถือเป็นหน่วยงานหลักที่ดูแลงานด้านเทคโนโลยีสารสนเทศ เพื่อกำหนดนโยบายของประเทศ ส่วนอาชญากรรมต่าง ๆ ที่กระทำผ่านช่องทางเทคโนโลยีมีมากมายหลายรูปแบบ เป็นหน้าที่ของสำนักงานตำรวจแห่งชาติ ที่จะต้องป้องกันและปราบปราม สืบสวน และสอบสวน อาชญากรรมที่กระทำผ่านช่องทางเทคโนโลยีสารสนเทศ เพื่อความสงบสุขของสังคมที่ได้รับผลกระทบจากเทคโนโลยีสารสนเทศที่เกิดขึ้นในปัจจุบัน และที่จะเกิดขึ้นในอนาคต

เทคโนโลยีสารสนเทศ มีความก้าวหน้าและเปลี่ยนแปลงไปอย่างรวดเร็วในปัจจุบัน ส่งผลให้การปฏิบัติงานของตำรวจต้องเผชิญกับปัญหาและอุปสรรคที่สลับซับซ้อนมากขึ้นเป็นทวีคูณ เจ้าหน้าที่ตำรวจจึงจำเป็นต้องมีการปรับตัวให้ทันกับอาชญากรรมที่เปลี่ยนแปลงไปอย่างรวดเร็วเช่นกัน มิฉะนั้น จะไม่สามารถป้องกันและปราบปรามอาชญากรรม ที่นับวันจะใช้เทคโนโลยีสารสนเทศเข้ามามีส่วนร่วมในการประกอบอาชญากรรมที่เพิ่มสูงขึ้นเรื่อย ๆ ได้

ข้อมูลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ) ระหว่างปี พ.ศ. 2554-2559 พบว่า การกระทำความผิดทางอาญาที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศมีจำนวนที่เพิ่มมากขึ้น



ภาพประกอบที่ 1.1 สถิติภัยคุกคามทางไซเบอร์

ที่มา: สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ), 2560, ออนไลน์

ปัจจุบันคดีอาชญากรรมจำนวนมากที่กระทำผ่านเครือข่ายทางอินเทอร์เน็ต เช่น การฉ้อโกงหลอกลวงซื้อขายทางออนไลน์, การหลอกให้โอนเงิน, การกระจายข่าวปลอมที่แชร์ผ่านโซเชียลเน็ตเวิร์ค (Fake News), การหลอกลวงผู้หญิงหรือเพศอื่น ๆ ด้วยการพูดคุยผ่านการแชท การส่งข้อความ (Romance Scam), การเข้าถึงโจมตีหรือทำลายข้อมูลคอมพิวเตอร์เพื่อเรียกค่าไถ่ เป็นต้น ซึ่งคดีเหล่านี้ล้วนแต่มีความซับซ้อน การสืบสวน สอบสวน จำเป็นต้องดำเนินการโดยผู้เชี่ยวชาญ และมีความเร่งด่วน

สำนักงานตำรวจแห่งชาติได้มีการจัดตั้งหน่วยงานเพื่อดูแลคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่มีปริมาณเพิ่มขึ้นทั้งคดีที่ส่งผลต่อความเดือดร้อนของประชาชนโดยตรง

และคดีที่เกี่ยวข้องกับความมั่นคงของประเทศ ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

นับตั้งแต่มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้ ประชาชนสามารถแจ้งความได้ที่สถานีตำรวจใกล้บ้าน(คู่มือการปฏิบัติแนวทางป้องกันและเพื่อหลีกเลี่ยง) ซึ่งหลังจากการประกาศใช้พระราชบัญญัติฉบับดังกล่าวได้มีการรวบรวมสถิติผู้เสียหายเข้าแจ้งความร้องทุกข์เกี่ยวกับคดีการกระทำความผิดทางเทคโนโลยีสารสนเทศ กับกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) สำนักงานตำรวจแห่งชาติ รายละเอียดปรากฏตามภาพประกอบที่ 1.2 ดังนี้

สถิติผู้เสียหายเข้าแจ้งความร้องทุกข์ต่อ ศูนย์บริการประชาชน บก.ปอท. ปี 2561-2563				
ประเภท	ปี 2561	ปี 2562	ปี 2563	
การกระทำความผิดโดยมีระบบเป็นเป้าหมาย	623	697	319	มูลค่าความเสียหาย ปี 2561 527,309,998
แฮกเพื่อปรับเปลี่ยน/ขโมย/ทำลายข้อมูล	499	516	256	ประชาชนเข้าร้องทุกข์ปี 2561 2,718 คดี
แฮกเพื่อหลอกโอนเงิน	124	181	63	
กระทำความผิดโดยมีระบบเป็นเครื่องมือ	973	1,235	624	มูลค่าความเสียหาย ปี 2562 573,575,640
หลอกขายสินค้า/บริการ	573	857	441	ประชาชนเข้าร้องทุกข์ปี 2562 3,200 คดี
หลอกโอนเงินผ่านอีเมล (E-mail Scam)	71	51	36	
หลอกโอนเงินผ่านโทรศัพท์	85	0	0	มูลค่าความเสียหาย ปี 2563 126,210,787
แบล็กเมลล์(ข่มขู่)	94	57	25	
หลอกเกี่ยวกับความรัก(Romance Scam)	90	81	42	ประชาชนเข้าร้องทุกข์ปี 2563 1,293 คดี
ปลอมเป็นบุคคลอื่นเพื่อหลอกโอนเงิน	60	189	80	
กระทำความผิดโดยเผยแพร่เนื้อหาไม่เหมาะสม	1,122	1,268	350	ข้อมูล ณ 29 ก.พ. 2563
หมิ่นประมาท	1,122	1,268	442	
รวมทั้งสิ้น	2,718	3,200	1,293	

ภาพประกอบที่ 1.2 สถิติผู้เสียหายเข้าแจ้งความร้องทุกข์

ที่มา: กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2563, ออนไลน์

จากปัญหาอาชญากรรมทางเทคโนโลยีสารสนเทศ ที่มีจำนวนคดีเพิ่มมากขึ้น ผู้เสียหายต้องเดินทางไปร้องทุกข์ยังกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ซึ่งหลายคดีมีการส่งเรื่องคืนให้สถานีตำรวจท้องที่เกิดเหตุ เป็นผู้รับผิดชอบทำการสอบสวน มีบางคดีที่ผู้เสียหายไปร้องทุกข์ที่สถานีตำรวจท้องที่เกิดเหตุ ซึ่งเป็นคดีที่ไม่ยุ่งยากหรือซับซ้อน กลับมีการส่งคดีไปให้ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี เป็นผู้ดำเนินการ ขณะเดียวกันบางคดีกองบังคับการปราบปรามการกระทำความผิด

เกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้ส่งกลับมาให้สถานีตำรวจเป็นผู้ดำเนินการ ซึ่งมีรายละเอียด ดังนี้

ตารางที่ 1.1 กรณีผู้เสียหายมาแจ้งที่ศูนย์รับเรื่องร้องทุกข์กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) แล้ว ปอท. ส่งเรื่องให้ สภ./สน. ท้องที่ดำเนินการ

ปี	ความผิด	จำนวน
พ.ศ. 2562	ความผิดฐาน นื้อ โกง (ประเภทคดีซื้อสินค้า/ปลอมไลน์-ปลอมเฟซบุ๊ก/ ยืมเงิน/หลอกส่งของมาให้แล้วจ่ายค่าธรรมเนียม ค่าภาษี)	545 เรื่อง
	ความผิดฐานหมิ่นประมาท	313 เรื่อง
	ความผิดฐาน เข้าถึงระบบ, ข้อมูลคอมพิวเตอร์ของผู้อื่น	10 เรื่อง
พ.ศ. 2563	ความผิดฐาน นื้อ โกง (ประเภทคดีซื้อสินค้า/ปลอมไลน์-ปลอมเฟซบุ๊ก/ ยืมเงิน/หลอกส่งของมาให้แล้วจ่ายค่าธรรมเนียม ค่าภาษี)	135 เรื่อง
	ความผิดฐานหมิ่นประมาท	97 เรื่อง
	ความผิดฐาน เข้าถึงระบบ, ข้อมูลคอมพิวเตอร์ของผู้อื่น	4 เรื่อง

ตารางที่ 1.2 คดีที่ผู้เสียหายมาร้องทุกข์ที่ สภ./สน. ท้องที่เกิดเหตุ แล้วมีการส่งเรื่องให้กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีดำเนินการ

ปี	ความผิด	จำนวน
พ.ศ. 2562	ความผิดฐาน นื้อ โกง (ประเภทคดีซื้อสินค้าออนไลน์ / ให้สืบทาตัวคนร้าย/ ให้ตรวจสอบไอพี -ปลอมเฟซบุ๊ก)	630 เรื่อง
	ความผิดฐานหมิ่นประมาท	308 เรื่อง
	ความผิดฐาน เข้าถึงระบบ, ข้อมูลคอมพิวเตอร์ของผู้อื่น	-
พ.ศ. 2563	ความผิดฐาน นื้อ โกง (ประเภทคดีซื้อสินค้า/ปลอมไลน์-ปลอมเฟซบุ๊ก/ ยืมเงิน/ หลอกส่งของมาให้แล้วจ่ายค่าธรรมเนียม ค่าภาษี)	135 เรื่อง
	ความผิดฐานหมิ่นประมาท	45 เรื่อง
	ความผิดฐาน เข้าถึงระบบ, ข้อมูลคอมพิวเตอร์ของผู้อื่น	1 เรื่อง
	ความผิดฐาน ทำให้เสียหาย ทำลายแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมข้อมูลคอมพิวเตอร์ของผู้อื่น	1 เรื่อง

จากฐานความคิดดังกล่าว พนักงานสอบสวนสถานีตำรวจท้องที่เกิดเหตุ ควรจะทำการสอบสวนตามหลักกฎหมาย ทำไมจึงส่งเรื่องให้กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีดำเนินการ

เจ้าหน้าที่ตำรวจ ถือเป็นเจ้าหน้าที่ของรัฐ ที่มีหน้าที่ ดูแล รักษาความปลอดภัยในชีวิตและทรัพย์สิน ป้องกันปราบปรามการกระทำความผิดทางอาญา ที่มีผลกระทบต่อสิทธิ หน้าที่ เสรีภาพในชีวิต ร่างกายและทรัพย์สินของประชาชน เพื่อความสงบเรียบร้อย ในขณะที่คดีต่าง ๆ เหล่านี้ ตามหลักปฏิบัติ เป็นอำนาจหน้าที่ของเจ้าหน้าที่ตำรวจ แต่กลับพบว่าตำรวจเข้ามามีบทบาทในการบังคับใช้กฎหมายอาญาในเรื่องนี้น้อยมาก โดยเฉพาะบทบาทในด้านการป้องกันและปราบปราม สืบสวนสอบสวน การกระทำความผิดทางอาญา ตามประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477 ซึ่งเป็นอำนาจและหน้าที่ของเจ้าหน้าที่ตำรวจ ที่เกี่ยวกับการป้องกันและปราบปรามสืบสวนสอบสวน การกระทำความผิดที่มีโทษทางอาญา หรืออาชญากรรมในรูปแบบต่าง ๆ นั้น ตามประมวลกฎหมายวิธีพิจารณาความอาญา พ.ศ. 2477 ซึ่งได้กำหนดอำนาจและหน้าที่ของเจ้าหน้าที่ตำรวจ เกี่ยวกับการสืบสวนไว้ดังนี้

มาตรา 2 (10) “การสืบสวน หมายรวมถึงการแสวงหาข้อเท็จจริงและหลักฐานซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่ เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด”

มาตรา 17 “พนักงานฝ่ายปกครองหรือตำรวจ มีอำนาจทำการสืบสวนคดีอาญาได้” ทำให้การสืบสวนเจ้าหน้าที่ตำรวจทุกคน ทุกชั้นยศ มีอำนาจในการสืบสวนและสามารถทำการสืบสวนป้องกัน ปราบปราม และจับกุมผู้ที่กระทำความผิดอาญาได้ทั่วราชอาณาจักรไทย โดยการจับกุมการตรวจค้นจะต้องเป็นไปตามที่กฎหมายบัญญัติ เกี่ยวกับการสอบสวน ไว้ดังนี้

มาตรา 2 (11) “การสอบสวน หมายรวมถึงการรวบรวมพยานหลักฐานและการดำเนินการทั้งหลายอื่นตามบทบัญญัติแห่งประมวลกฎหมายนี้ ซึ่งพนักงานสอบสวนได้ทำไปเกี่ยวกับความผิดที่กล่าวหา เพื่อที่จะทราบข้อเท็จจริงหรือพิสูจน์ความผิดและเพื่อจะเอาตัวผู้กระทำความผิดมาฟ้องลงโทษ”

มาตรา 18 “ในจังหวัดอื่นนอกจากจังหวัดพระนครและจังหวัดธนบุรี พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ปลัดอำเภอ และข้าราชการตำรวจซึ่งมียศตั้งแต่นายร้อยตำรวจตรีหรือเทียบเท่า นายร้อยตำรวจตรีขึ้นไป มีอำนาจสอบสวนความผิดอาญาซึ่งเกิด หรืออ้าง หรือเชื่อว่าได้เกิดภายในเขตอำนาจของตน หรือผู้ต้องหาที่มีที่อยู่ หรือถูกจับกุมภายในเขตอำนาจของตนได้

จากที่กล่าวมาแล้วข้างต้น สรุปได้ว่า อาชญากรรมทางเทคโนโลยีสารสนเทศที่นับวันจะมีจำนวนเพิ่มสูงขึ้น จากการทบทวนวรรณกรรมพบว่า ยังไม่มีการศึกษาอย่างเป็นรูปธรรมเกี่ยวกับ

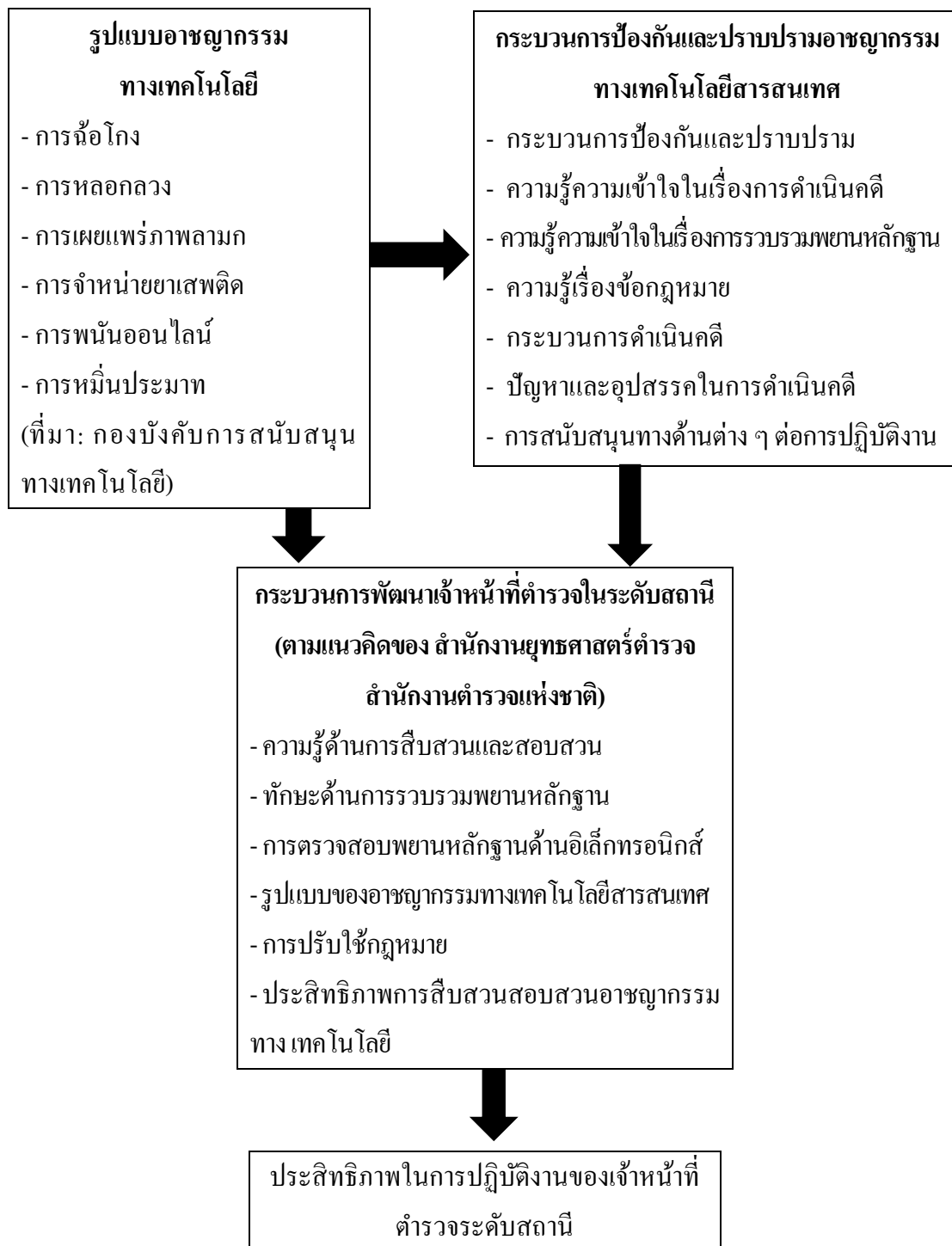
แนวทางการปฏิบัติงานของเจ้าหน้าที่ตำรวจในระดับสถานีเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ ดังนั้นผู้วิจัยจึงสนใจที่ศึกษาเรื่อง “แนวทางการพัฒนาเจ้าหน้าที่ตำรวจในระดับสถานีเพื่อเพิ่มประสิทธิภาพการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ” เพื่อศึกษาว่า รูปแบบ วิธีการ และช่องทางของอาชญากรรมที่กระทำผ่านทางเทคโนโลยีสารสนเทศ กระบวนการจัดการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศของเจ้าหน้าที่ตำรวจในระดับสถานี แนวทางการพัฒนาศักยภาพของเจ้าหน้าที่ตำรวจในระดับสถานีในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ ทั้งนี้เพื่อพัฒนาประสิทธิภาพการปฏิบัติงานของเจ้าหน้าที่ตำรวจในระดับสถานี ในการดำเนินภารกิจการป้องกันและปราบปราม สืบสวน สอบสวน อาชญากรรมทางเทคโนโลยีสารสนเทศ ต่อไป

2. วัตถุประสงค์ของการวิจัย

การศึกษาวิจัยครั้งนี้ ผู้วิจัยได้กำหนดวัตถุประสงค์หลัก 4 วัตถุประสงค์ คือ

1. เพื่อศึกษาถึงรูปแบบ เทคนิค วิธีการ และช่องทางของอาชญากรรมที่กระทำผ่านทางเทคโนโลยีสารสนเทศ
2. เพื่อศึกษาถึงกระบวนการจัดการเกี่ยวกับการป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยีสารสนเทศของเจ้าหน้าที่ตำรวจในระดับสถานี
3. เพื่อศึกษาแนวทางในการพัฒนาศักยภาพของเจ้าหน้าที่ตำรวจในระดับสถานีในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ
4. เพื่อพัฒนาประสิทธิภาพการปฏิบัติงานของเจ้าหน้าที่ตำรวจในระดับสถานีในการดำเนินภารกิจด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ

3. กรอบแนวคิดของการวิจัย



ภาพประกอบที่ 1.3 กรอบแนวคิดการวิจัย

กรอบแนวคิดที่ใช้ในการศึกษาครั้งนี้ ประกอบด้วย

1) รูปแบบของอาชญากรรมทางเทคโนโลยีสารสนเทศ เป็นการศึกษาถึงรูปแบบอาชญากรรมที่ใช้เทคโนโลยีสารสนเทศเข้ามาเป็นส่วนหนึ่งในการกระทำความผิด ซึ่งเป็นการกระทำที่ส่งผลกระทบต่อความปลอดภัยในชีวิตและทรัพย์สินของประชาชน โดยมีหลักในการพิจารณา ประกอบด้วย

(1) การฉ้อโกง เป็นการหลอกลวงขายสินค้า หรือลงทุนผ่านทางเครือข่ายคอมพิวเตอร์ เช่น การประกาศขายสินค้าทางสื่อออนไลน์ต่าง ๆ การชักชวนให้เริ่มลงทุนแต่ไม่ได้มีกิจการเหล่านั้นจริง

(2) การหลอกลวง เป็นการล่อลวงให้เข้าใจผิด เช่น การล่อลวงให้ผู้หญิงไปค้าประเวณี

(3) การเผยแพร่ภาพลามก เป็นการใช้อุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ เพื่อเผยแพร่ภาพนิ่งหรือภาพเคลื่อนไหวลามกอนาจาร หรือข้อมูลที่มีผลกระทบทางลบต่อวัฒนธรรมของแต่ละสังคม

(4) การจำหน่ายยาเสพติด เป็นการกระทำความผิดทางอาชญากรรมที่ใช้การสื่อสารผ่านเครือข่ายคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ เพื่อใช้ขยายความสามารถในการกระทำความผิด เช่น การใช้อีเมล หรือไลน์ ในการติดต่อสื่อสารกับเครือข่ายยาเสพติด การใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับการค้ายาเสพติด เป็นต้น

(5) การพนันออนไลน์ การใช้อุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ อย่างคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ มาเล่นการพนันที่ไม่ชอบด้วยกฎหมาย ซึ่งเป็นความผิดฐานฟอกเงิน

(6) การหมิ่นประมาท การใช้อุปกรณ์อิเล็กทรอนิกส์ในการเขียนใส่ความผู้อื่นต่อบุคคลที่สาม โดยต้องการให้ผู้นั้นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง

2) กระบวนการจัดการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เป็นการศึกษาถึงการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศทุกประเภท ของเจ้าหน้าที่ตำรวจในระดับสถานี โดยมีหลักในการพิจารณา ประกอบด้วย

(1) กระบวนการป้องกันและปราบปราม เป็นการศึกษาถึงการป้องกันและปราบปรามอาชญากรรมที่กระทำผิดกฎหมายอาญาทุกชนิด จัดทำแผนป้องกันและปราบปรามควบคุมดูแลอบรมให้ความรู้แก่เจ้าหน้าที่ตำรวจผู้ปฏิบัติงานและประชาชนให้เข้าใจ มีความสัมพันธ์อันดีกับตำรวจ และให้ความร่วมมือ ช่วยเหลือในการป้องกันปราบปรามอาชญากรรม ตลอดจนถึงเก็บรวบรวมข้อมูลสถิติอาชญากรรมเพื่อนำไปใช้ในการวางแผนป้องกันและปราบปรามอาชญากรรม

(2) ความรู้ความเข้าใจในเรื่องการดำเนินคดี เป็นการศึกษาถึงการแสวงหาข้อเท็จจริง พยานหลักฐาน ในคดีอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี เพื่อให้เกิดการเรียนรู้และประสิทธิภาพในการทำคดี

(3) ความรู้ความเข้าใจในเรื่องการรวบรวมพยานหลักฐาน เป็นการศึกษาถึงหลักการในการรวบรวมพยานหลักฐาน เพื่อช่วยให้เจ้าหน้าที่ตำรวจในระดับสถานีทราบว่าพยานหลักฐานแบบใดที่สามารถนำมาใช้ประกอบคดี หรือหลักฐานแบบใดควรนำเข้าสู่คดี เพื่อประกอบการพิจารณาตัดสินของศาลในการลงโทษผู้กระทำความผิด

(4) ความรู้เรื่องข้อกฎหมาย เป็นการศึกษาถึงแนวทางในการแก้ไขกฎหมายรวมถึงการเพิ่มเติมข้อกฎหมายที่มีอยู่ให้ครอบคลุมอาชญากรรมทางเทคโนโลยีสารสนเทศทุกประเภท นอกจากนี้ยังรวมถึงการส่งเสริมความร่วมมือระหว่างประเทศ โดยเฉพาะทางด้านการสืบสวนสอบสวน เพื่อดำเนินคดีกับผู้กระทำความผิด

(5) กระบวนการดำเนินคดี เป็นการศึกษาถึงการร้องทุกข์ กล่าวโทษ สอบสวนฟ้องคดี หรือพิจารณาพิพากษาคดี ตามกฎหมายวิธีพิจารณาความอาญา เกี่ยวกับคดีอาชญากรรมทางเทคโนโลยีสารสนเทศของเจ้าหน้าที่ตำรวจในระดับสถานี

(6) ปัญหาและอุปสรรค เป็นการศึกษาถึงปัญหาและอุปสรรคในการดำเนินคดีอาชญากรรมทางเทคโนโลยีสารสนเทศของเจ้าหน้าที่ตำรวจในระดับสถานี

(7) การสนับสนุน เป็นการศึกษาถึงความต้องการของเจ้าหน้าที่ตำรวจในระดับสถานีต่อการสนับสนุนทางด้านต่าง ๆ ที่เกี่ยวข้องกับการปฏิบัติงาน

3) กระบวนการพัฒนาเจ้าหน้าที่ตำรวจในระดับสถานี

(1) ความรู้ด้านเทคนิคด้านการสืบสวนและสอบสวน เป็นการศึกษาถึงวิธีการให้ความรู้เพื่อให้ผู้ปฏิบัติงานมีความรู้ความเข้าใจ เกี่ยวกับการสืบสวนสอบสวนคดีที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีสารสนเทศ

(2) ทักษะด้านการรวบรวมพยานหลักฐาน เป็นการศึกษาถึงแนวทางในการเรียนรู้หลักการทั่วไปในการรักษาความน่าเชื่อถือของพยานหลักฐาน โดยเฉพาะในส่วนของพยานหลักฐานทางอิเล็กทรอนิกส์

(3) การตรวจสอบพยานหลักฐานทางอิเล็กทรอนิกส์ เป็นการศึกษาถึงแนวทางในการตรวจสอบข้อความที่สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ (สำนักงานคณะกรรมการกฤษฎีกา, 2544, หน้า 2)

(4) รูปแบบของอาชญากรรมทางเทคโนโลยีสารสนเทศ เป็นการศึกษาถึงรูปแบบต่าง ๆ ของอาชญากรรมทางเทคโนโลยีสารสนเทศ เช่น คดีหมิ่นประมาท คดีฉ้อโกงทางคอมพิวเตอร์ คดีการเผยแพร่ภาพลามกอนาจาร คดีเว็บไซต์ขายของผิดกฎหมาย เป็นต้น

(5) การปรับใช้กฎหมาย เป็นการศึกษาถึงการตีความข้อกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีสารสนเทศ

(6) ประสิทธิภาพการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีสารสนเทศ เป็นการศึกษาถึงการจัดการความรู้งานด้านการสืบสวนสอบสวนอาชญากรรมทางด้านเทคโนโลยี

4) ประสิทธิภาพในการปฏิบัติงานของเจ้าหน้าที่ตำรวจระดับสถานี เป็นการศึกษาถึงความสามารถของเจ้าหน้าที่ตำรวจในระดับสถานี ในด้านการป้องกันและปราบปราม สืบสวนสอบสวน ในคดีอาชญากรรมที่มีเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้อง ทั้งในด้านการทำหนังสือสอบถาม หรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิด สามารถเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการ สรุปสำนวนคดีอาชญากรรมทางเทคโนโลยีสารสนเทศได้ตามระยะเวลาที่กำหนด สามารถสืบค้นข้อมูลเว็บไซต์ สืบค้นข้อมูลไอพีแอดเดรส (IP Address) เพื่อสืบค้นข้อมูลว่าผู้ใช้งานคือใคร เป็นต้น

5) ปัญหาและอุปสรรคที่ส่งผลประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีของเจ้าหน้าที่ตำรวจในระดับสถานี เป็นการศึกษาถึงปัญหาและอุปสรรคที่เกิดขึ้นจากการทำงานทางด้านต่าง ๆ ที่เกี่ยวข้องกับการป้องกันและปราบปราม สืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีสารสนเทศ

4. คำถามการวิจัย

การศึกษาวิจัยครั้งนี้มุ่งศึกษาการพัฒนาศักยภาพของเจ้าหน้าที่ตำรวจในระดับสถานีในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ โดยมีคำถามของการวิจัยดังนี้

1. รูปแบบ เทคนิค วิธีการ และช่องทางของอาชญากรรมที่กระทำผ่านทางเทคโนโลยีสารสนเทศ มีลักษณะอย่างไร

2. การบวนการจัดการเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศของเจ้าหน้าที่ตำรวจในระดับสถานี มีวิธีการดำเนินการอย่างไร มีปัญหาและอุปสรรคอย่างไร

3. การพัฒนาศักยภาพเจ้าหน้าที่ตำรวจในระดับสถานีในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ มีแนวทางอย่างไร

4. การพัฒนาประสิทธิภาพการปฏิบัติของเจ้าหน้าที่ตำรวจระดับสถานีในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ มีลักษณะอย่างไร

5. ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ทราบถึงรูปแบบ เทคนิค และวิธีการของอาชญากรรมทางเทคโนโลยีสารสนเทศ
2. ทำให้ทราบถึงกระบวนการจัดการของเจ้าหน้าที่ตำรวจในระดับสถานี ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ
3. ทำให้ทราบถึงแนวทางในการพัฒนาเพื่อเพิ่มประสิทธิภาพเจ้าหน้าที่ตำรวจในระดับสถานี ทั้งงานป้องกันและปราบปราม งานสืบสวน งานสอบสวน อาชญากรรมทางเทคโนโลยีสารสนเทศ
4. ทำให้ทราบถึงการสร้างองค์ความรู้ วิธีการ เครื่องมือของเจ้าหน้าที่ตำรวจในระดับสถานี ในงานป้องกันและปราบปราม งานสืบสวน งานสอบสวน อาชญากรรมทางเทคโนโลยีสารสนเทศ
5. หากมีมาตรการที่มีประสิทธิภาพ ผู้กระทำความผิดก็จะเกิดความกลัว ทำให้อาชญากรรมทางเทคโนโลยีสารสนเทศลดน้อยลง

6. นิยามศัพท์เฉพาะ

เนื่องจากคำสำคัญบางคำที่ใช้ในการวิจัยนี้ มีความหมายที่ไม่คงที่ ขึ้นอยู่กับบริบทและการตีความของนักวิชาการแต่ละคน ผู้วิจัย จึงได้นิยามคำสำคัญที่ใช้ในการวิจัย เพื่อความเข้าใจตรงกันในเบื้องต้น ดังนี้

แนวทางการพัฒนาเพื่อเพิ่มประสิทธิภาพ (Development Approach to Increase Efficiency) หมายถึง การเปลี่ยนแปลงสิ่งใดสิ่งหนึ่งให้ดีขึ้นจนเป็นที่พึงพอใจ

เจ้าหน้าที่ตำรวจ (Police Officer) ตามที่ระบุไว้ในพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ได้ให้ความหมายไว้ว่า ตำรวจคือเจ้าหน้าที่ของรัฐ มีหน้าที่ตรวจตราความสงบ จับกุมและปราบปรามผู้กระทำความผิด ในที่นี้หมายถึง เจ้าหน้าที่ตำรวจที่ปฏิบัติงานในสถานี

ระดับสถานีตำรวจ (Police Station) หมายถึง ระดับของสถานีตำรวจซึ่งแบ่งตามตำแหน่งของหัวหน้าสถานีได้เป็น 3 ระดับ คือ

- 1) ระดับที่มีผู้กำกับการเป็นหัวหน้าสถานี
- 2) ระดับที่มีรองผู้กำกับการเป็นหัวหน้าสถานี
- 3) ระดับที่มีสารวัตรเป็นหัวหน้าสถานี

ป้องกัน (Prevention) หมายถึง มาตรการและกิจกรรมต่าง ๆ ที่กำหนดขึ้นล่วงหน้า ทั้งทางด้านโครงสร้าง (Structural Approach) และที่มิใช่ด้านโครงสร้าง (Non Structural Approach) เพื่อลดหรือควบคุมผลกระทบในทางลบ

ปราบปราม (Suppression) หมายถึง กิจกรรมหรือการปฏิบัติงานในการรักษาความปลอดภัย เพื่อจับกุมผู้กระทำหรือพยายามกระทำความผิด ตลอดจนการรวบรวมพยานหลักฐานในการพิสูจน์ความผิด เพื่อการควบคุมอาชญากรรม

การกระทำความผิด (Commit) หมายถึง การกระทำที่กฎหมายห้ามและถือว่าเป็นความผิดซึ่งมีผลให้ต้องถูกลงโทษตามที่กฎหมายกำหนดไว้

เทคโนโลยีสารสนเทศ (Information Technology) หมายถึง การพัฒนาด้านคอมพิวเตอร์และเทคโนโลยีด้านเครือข่ายการสื่อสารและโทรคมนาคม ซึ่งส่งผลให้เกิดเสรีภาพในการแพร่กระจายข้อมูลข่าวสารอย่างรวดเร็ว

อาชญากรรมทางเทคโนโลยีสารสนเทศ (Hi-Tech Crime) คือ การกระทำการที่ถือว่าเป็นความผิดตามกฎหมายและเป็นการกระทำผ่านหรือโดยอาศัยคอมพิวเตอร์ ไมโครอิเล็กทรอนิกส์ และโทรคมนาคมในการกระทำความผิด ซึ่งมีวัตถุประสงค์มุ่งต่อระบบคอมพิวเตอร์ ข้อมูลของคอมพิวเตอร์ หรือบุคคล

องค์ประกอบในการกระทำความผิด (Component of the Offense) หมายถึง องค์ประกอบความผิดจะกำหนดระดับความร้ายแรงของการกระทำ โดยทั่วไปของพฤติกรรมต้องห้าม ได้แก่ องค์ประกอบในเชิงภาวะวิสัย (Objective Tatbestandsmerkmale) และองค์ประกอบในเชิงอัตวิสัย (Subjective Tatbestandsmerkmale) โดยเฉพาะอย่างยิ่งการกระทำโดยเจตนาหรือการพยายามกระทำความผิด