การพัฒนาผู้บังคับใช้กฎหมายในการต่อสู้อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

โดย

นางจตุพร แสงหิรัญ
อัยการผู้เชี่ยวชาญพิเศษ
สำนักงานอัยการสูงสุด

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 57
ประจำปีการศึกษา พุทธศักราช 2557 – 2558

บทคัดย่อ

เรื่อง การพัฒนาผู้บังคับใช้กฎหมายในการต่อสู้อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

ลักษณะวิชา การเมือง

ผู้วิจัย นางจตุพร แสงหิรัญ หลักสูตร วปอ. รุ่นที่ 57

จากความก้าวหน้าทางเทคโนโลยีและผู้คนทั่วโลกใช้คอมพิวเตอร์ Smartphone ติดต่อสื่อสาร ทำธุรกิจค้าขายกันตลอด 24 ชั่วโมง โดยขาดความรู้ความเข้าใจในระบบคอมพิวเตอร์ ไม่รู้วิธีการใช้อย่างถูกต้อง หรือประมาทเลินเล่อไม่ระมัดระวังการเก็บรักษาข้อมูลสำคัญหรือหลงเชื่อข้อมูลข่าวสารโดยไม่พิจารณาตรวจสอบให้รอบคอบ จะทำให้ตกเป็นเหยื่อของอาชญากรที่มุ่งร้าย ทำให้อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์จะทวีจำนวนมากขึ้น ภัยอันตรายจะกระทบถึงตัวบุคคลได้ง่ายและรวดเร็ว รูปแบบการกระทำผิดมีความหลากหลาย สลับซับซ้อน อำพรางตนไม่ให้ติดตามจับกุมได้โดยง่าย ต้องใช้เจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์โดยตรงในการแกะรอย ติดตามคนร้าย ค้นหาข้อมูล รวบรวมพยานหลักฐานต่างๆ และการกระทำความผิดจะเป็นลักษณะข้ามชาติ ไร้พรมแดน คนร้ายมีความเชี่ยวชาญด้านการใช้คอมพิวเตอร์สามารถฉ้อโกงหลอกลวงทรัพย์สินของผู้เสียหายได้ทีละจำนวนมาก กระทำผิดในลักษณะต่างๆ ได้ง่าย รวดเร็วก่อให้เกิดปัญหาแก่ผู้บังคับใช้กฎหมายในด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การติดตามตัวคนร้ายมาลงโทษ

ปรากฏว่าผู้บังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญในด้านกฎหมาย มีทักษะและประสบการณ์การสืบสวนสอบสวน พร้อมทั้งความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์ การใช้เทคโนโลยีสมัยใหม่ ยังมีจำนวนน้อยมาก ต้องรับภาระรับผิดชอบสำนวนคดีจำนวนมาก ขาดขวัญและกำลังใจที่ดี เส้นทางความก้าวหน้าไม่ชัดเจน การเลื่อนตำแหน่ง การโยกย้าย ทำให้กำลังเจ้าหน้าที่ขาดแคลน ต้องใช้เวลาฝึกฝนคนที่ย้ายมาอยู่ใหม่ นอกจากนั้นยังขาดงบประมาณในการจัดหาอุปกรณ์ที่มีประสิทธิภาพ และค่าใช้จ่ายที่เกี่ยวข้องในการบริหารจัดการคดี การฝึกอบรมยังไม่ทั่วถึงและมีน้อยเกินไปไม่ต่อเนื่อง ขาดการฝึกอบรมร่วมกันระหว่างผู้บังคับใช้กฎหมาย ประชุมระหว่างหน่วยงานภาครัฐและหน่วยงานเอกชนที่เกี่ยว การแบ่งปันข้อมูลข่าวสารระหว่างหน่วยงาน เจ้าหน้าที่จึงไม่เพียงพอที่จะต่อสู้กับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบันและแนวโน้มที่จะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ

คำนำ

ทุกวันนี้การดำเนินชีวิตของผู้คนในโลกนี้เปลี่ยนแปลงไป เทคโนโลยีเข้ามามีส่วนในชีวิตประจำวันของคน ไม่ว่าจะเป็นการติดต่อสื่อสาร การทำธุรกิจการค้า กิจกรรมทางสังคม การศึกษา เป็นต้น ผู้คนทั่วโลกสามารถติดต่อสื่อสารได้อย่างสะดวกรวดเร็ว ราคาถูก เข้าถึงได้ง่าย โดยใช้ Smartphone คอมพิวเตอร์ในรูปแบบต่างๆ ผ่านทางระบบอินเตอร์เน็ต

สิ่งใดที่มีคุณอนันต์ก็มีโทษมหันต์ เช่นกัน หากผู้ใช้ไม่ระมัดระวัง ไม่พิจารณาข้อมูลข่าวสารให้รอบคอบหลงเชื่ออะไรง่ายๆ ที่คนร้ายส่งข้อความมาหลอกลวง หรือไม่ป้องกันตัวก็จะถูกคนร้ายเข้ามาเจาะระบบเอาข้อมูลสำคัญหรือ ทำลายข้อมูลของเราทำให้ผู้ใช้ได้รับความเสียหายในด้านชีวิต ทรัพย์สินและชื่อเสียง

ในการดำเนินคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ในปัจจุบัน ผู้บังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญในด้านกฎหมายและทักษะด้านคอมพิวเตอร์ เทคโนโลยีสมัยใหม่ยังมีจำนวนไม่เพียงพอที่จะรับมือกับปริมาณคดีที่เกิดขึ้นในปัจจุบัน และแนวโน้มคดีที่จะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ จึงมีความจำเป็นอย่างยิ่งที่จะต้องหาแนวทางพัฒนาผู้บังคับใช้กฎหมายให้มีความรู้ความเชี่ยวชาญและมีจำนวนที่เพียงพอที่จะรับมือกับอาชญากรรมด้านนี้อย่างเร่งด่วน

(นางจตุพร แสงหิรัญ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 57
ผู้วิจัย

กิตติกรรมประกาศ

เอกสารวิจัยฉบับนี้สำเร็จลงได้ด้วยดี ก็ด้วยความกรุณาช่วยเหลือ สนับสนุนในข้อมูลและคำแนะนำที่เป็นประโยชน์ยิ่ง

ขอขอบคุณผู้ให้ข้อมูลสำคัญในการวิจัย ที่ผู้วิจัยได้ไปทำการสัมภาษณ์ทุกท่าน และคณะอาจารย์ที่ปรึกษางานวิจัย, พลตรี กฤษฎา สุทธานินทร์ ,นาวาอากาศเอก ภาณุ ไชยศิลป์ และนายธรัมย์ ชาลีจันทร์ อัยการผู้เชี่ยวชาญพิเศษ ซึ่งเป็นผู้ทรงคุณวุฒิที่ให้ข้อคิดและคำแนะนำ รวมทั้งผู้ซึ่งมีส่วนในการรวบรวมและจัดพิมพ์รูปเล่มที่ทำให้เอกสารวิจัยฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี จึงขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

(นางจตุพร แสงหิรัญ)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 57
ผู้วิจัย

สารบัญ

		หน้า
บทคัดย่อ		ก
คำนำ		ข
กิตติกรรมประกาศ		ค
สารบัญ		ง
สารบัญตาราง		ฉ
สารบัญแผนภาพ		ช
บทที่ 1	บทนำ	1
	ความเป็นมาและความสำคัญของปัญหา	1
	วัตถุประสงค์ของการวิจัย	7
	ขอบเขตของการวิจัย	7
	วิธีดำเนินการวิจัย	7
	ประโยชน์ที่ได้รับจากการวิจัย	8
บทที่ 2	แนวคิด ทฤษฎี ในการพัฒนาผู้บังคับใช้กฎหมายและกฎหมาย ที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรม ที่เกี่ยวข้องกับคอมพิวเตอร์	9
	คำศัพท์ที่เกี่ยวข้อง	9
	กฎหมายที่เกี่ยวข้อง	14
	หลักการพัฒนาผู้บังคับใช้กฎหมาย	28
บทที่ 3	วิธีการศึกษา	29
	บทสัมภาษณ์ผู้บริหาร	29
บทที่ 4	ผลการศึกษา	81
	ผลการศึกษา	86
	ปัญหาในการดำเนินคดีชั้นพนักงานอัยการ	86
	แนวทางในการพัฒนาผู้บังคับใช้กฎหมาย	90

สารบัญ (ต่อ)

	หน้า
บทที่ 5 สรุปและข้อเสนอแนะ	91
สรุป	91
ข้อเสนอแนะ	93
บรรณานุกรม	96
ประวัติย่อผู้วิจัย	97

สารบัญตาราง

ตารางที่		หน้า
2 – 1	เปรียบเทียบความแตกต่างระหว่างการศึกษา การพัฒนาบุคคล และการฝึกอบรม	12
2 – 2	ความผิดเกี่ยวกับการกระทำต่อคอมพิวเตอร์	16
2 – 3	ความผิดเกี่ยวกับการใช้คอมพิวเตอร์กระทำความผิด	16
2 – 4	ความผิดเกี่ยวกับคอมพิวเตอร์กระทำนอกราชอาณาจักรไทย	17
2 – 5	อำนาจหน้าที่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550	17
3 – 1	สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี 2556 ของ บก.ปอท.	30
3 – 2	สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี 2557 ของ บก.ปอท.	31
4 – 1	สถิติภัยคุกคามปี 2554	81
4 – 2	สถิติภัยคุกคามปี 2555	82
4 – 3	สถิติภัยคุกคามปี 2556	82
4 – 4	สถิติภัยคุกคามปี 2557	83
4 – 5	สถิติภัยคุกคามปี 2558	83
4 – 6	ประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดย eCSIRT	84

สารบัญแผนภาพ

หน้า

แผนภาพที่

2 – 1	รูปแบบและฐานความผิดทางอาชญากรรมทางคอมพิวเตอร์ กฎหมายลำดับรองภายใต้ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550	18
2 – 2	ผังการมีคำร้องขอความช่วยเหลือไปยังต่างประเทศ (กรณีมีสนธิสัญญา)	26
2 – 3	แผนผังการมีคำร้องขอความช่วยเหลือไปยังต่างประเทศ (กรณีไม่มีสนธิสัญญา)	27
3 – 1	สถิติหลักฐานทางเทคโนโลยีที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้รับในปี 2557	58
3 – 2	สถิติหลักฐานทางเทคโนโลยีที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้รับในปี 2558	59

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

คอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพมากในการทำงาน มีการพัฒนาระบบการทำงานโปรแกรมรูปแบบใหม่ๆ และทันสมัยขึ้นตลอดเวลา เพื่ออำนวยความสะดวกให้แก่ผู้ใช้ ปัจจุบันคอมพิวเตอร์เป็นสิ่งที่มีความสำคัญและเป็นสิ่งจำเป็นในการใช้ชีวิตประจำวันของคนทั่วไป คนทั่วโลกใช้คอมพิวเตอร์ในติดต่อสื่อสารกันได้โดยง่ายและรวดเร็ว ใช้ในการทำธุรกิจการค้าหลากหลายรูปแบบ ซึ่งปริมาณการใช้คอมพิวเตอร์สูงขึ้นทุกปี โดยคอมพิวเตอร์ในปัจจุบันมีทั้งแบบตั้งโต๊ะ แบบพกพาเคลื่อน ที่ได้ รวมทั้งโทรศัพท์แบบพกพาที่มีการพัฒนาเทคโนโลยีจนสามารถทำงานได้เช่นเดียวกับคอมพิวเตอร์

เมื่อคอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพมากในการใช้งาน จึงเป็นช่องทางให้ผู้ที่ประสงค์ร้ายใช้คอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้องในการกระทำความผิด

คอมพิวเตอร์มีบทบาทหรือเกี่ยวข้องในการกระทำความผิด ดังนี้คือ

1. คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets) เช่น การกระทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์ โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน

2. การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดในฐานความผิดอื่นๆ (Computer as Tools)

3. การใช้คอมพิวเตอร์เก็บข้อมูลต่างๆ ที่เกี่ยวข้องกับการกระทำความผิดอีกด้วย (Computer as Storage)

ด้วยระบบการทำงานของคอมพิวเตอร์และโครงข่ายการสื่อสารทางอินเตอร์เน็ตที่รวดเร็วและทันสมัยทำให้การติดต่อสื่อสารทำได้ง่าย รวดเร็ว ไร้พรมแดน คนร้ายกับผู้เสียหายอาจอยู่ห่างกันคนละซีกโลกแต่ก็ถูกหลอกลวง ถูกฉ้อโกงได้ มีลักษณะของการกระทำที่สลับซับซ้อน สามารถสร้างความเสียหายได้อย่างมากและรวดเร็ว เกิดขึ้นที่ไหนเมื่อไหร่ก็ได้ ทั้งในและนอก

ราชอาณาจักร กฎหมายที่มีอยู่ในปัจจุบันอาจไม่คลอบคลุมถึงรูปแบบการทำกระผิดใหม่ที่เกิดขึ้นจากการพัฒนาทางเทคโนโลยี ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อชื่อเสียง ทรัพย์สินของผู้อื่นและความมั่นคงต่อประเทศชาติ

เมื่อเกิดเหตุขึ้นแล้วยากต่อการติดตามผู้กระทำความผิดมาลงโทษได้โดยง่าย เนื่องจากไม่เห็นตัวผู้กระทำผิด ต้องใช้เวลาในการสืบสวนสอบสวนกว่าจะได้ทราบว่าคนร้ายเป็น ใครอยู่ที่ใดและมีขั้นตอนการทำงานที่สลับซับซ้อน ต้องใช้เจ้าหน้าที่ที่มีความรู้ ความเชี่ยวชาญในด้านคอมพิวเตอร์มาช่วยในการติดตามคนร้าย ตรวจพิสูจน์การทำงานและหาข้อมูลพยานหลักฐานที่สำคัญในคดีที่อยู่ในคอมพิวเตอร์

ในปัจจุบันมีรูปแบบอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ หลากหลายรูปแบบที่ทำให้ผู้เสียหายต้องสูญเสียทรัพย์สิน เสื่อมเสียชื่อเสียง ได้รับความอับอาย บางรายถึงกับเสียชีวิต เช่น

1. ในเรื่องการฉ้อโกง/การหลอกลวงในรูปแบบต่างๆ

ลักษณะของการกระทำความผิดเช่น การที่คนร้ายโฆษณาขายสินค้าหลอกลวงทางเว็บไซต์ โดยแท้จริงแล้วไม่มีเจตนาจะขาย และหรือส่งมอบสินค้าดังกล่าว เป็นความผิดฐานฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา มาตรา 343 และยังเป็นความผิดฐานนำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1)

และในทางกลับกันการที่คนร้ายสั่งซื้อสินค้าทางอินเตอร์เน็ตโดยหลอกลวง แต่แท้จริงแล้วคนร้ายไม่มีเจตนาที่จะชำระเงินค่าสินค้าแก่ผู้ขาย การกระทำดังกล่าวก็เป็นความผิดฐานฉ้อโกงตามประมวลกฎหมายอาญา มาตรา 341 และยังเป็นความผิดฐานนำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1)

2. การส่งจดหมายอิเล็กทรอนิกส์ (E - mail) หลอกลวง

ลักษณะการกระทำความผิดคือคนร้ายจะใช้วิธีการส่งจดหมายอิเล็กทรอนิกส์ หรือผ่านทางเว็บไซต์ที่สามารถติดต่อสื่อสารได้ทางสังคมออนไลน์ไปหลอกลวงผู้เสียหายด้วยข้อความเท็จต่างๆ ทำให้ผู้เสียหายหลงเชื่อตามข้อความที่ส่งหลอกลวง หลังจากผู้เสียหายหลงเชื่อข้อความที่หลอกลวงแล้ว คนร้ายก็จะใช้วิธีส่งข้อมูลหลอกลวงทางอินเตอร์เน็ตให้ผู้เสียหายทำการโอนเงินเข้าบัญชีของกลุ่มคนร้ายที่เปิดขึ้นมา เมื่อเงินโอนเข้าบัญชีแล้ว คนร้ายก็จะถอนเงินดังกล่าวไป แล้วเลิกการติดต่อกับผู้เสียหาย ซึ่งการกระทำดังกล่าวเป็นความผิดฐานฉ้อโกงประชาชน ตามประมวลกฎหมายอาญา มาตรา 343 และยังเป็นความผิดฐานนำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบ

คอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1)

3. หมิ่นประมาท เผยแพร่ด้วยภาพหรือข้อความให้ผู้อื่นอับอายอับอาย

ลักษณะการกระทำผิดจะเป็นการใช้การลงข้อความหมิ่นประมาท รูปภาพที่ไม่เหมาะสมในสื่อสังคมออนไลน์ เช่น เฟสบุ๊ค ไลน์ เว็บไซต์ต่างๆ หรือส่งจดหมายอิเล็กทรอนิกส์ (อีเมล์) ไปยังบุคคลที่สามซึ่งหากบุคคลต่างๆ สามารถเข้าดูข้อความดังกล่าวได้ การกระทำของผู้ต้องหาย่อมเป็นความผิดฐาน หมิ่นประมาทโดยการโฆษณา ตามประมวลกฎหมายอาญา มาตรา 328 และยังเป็นความผิดฐาน นำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1),16

4. เจาะระบบคอมพิวเตอร์ผู้อื่น เข้าไปแก้ไขข้อมูล เปลี่ยนแปลงข้อมูลทางการเงินเพื่อให้ได้ทรัพย์สิน แก้ไขบัญชีธนาคารเพื่อให้โอนเงินเข้าบัญชีคนร้าย

ลักษณะของการกระทำความผิดคนร้ายได้เข้าสู่ระบบคอมพิวเตอร์ และเข้าถึงข้อมูลคอมพิวเตอร์ของธนาคาร หรือบัญชีเงินฝากของผู้เสียหาย ที่มีมาตรการในการป้องกันการเข้าถึงโดยมิชอบแล้วทำการแก้ไขข้อมูลคอมพิวเตอร์ของธนาคารหรือผู้เสียหาย เพื่อทำการโอนเงินออกจากบัญชีของผู้เสียหาย นอกจากการลักเงินในบัญชีของธนาคารดังกล่าวออกมา จะเป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 334 หรือ 335 แล้วยังเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 5 , 7 , 9 หากการกระทำดังกล่าวมีการใช้บัตรอิเล็กทรอนิกส์ของธนาคารหรือผู้เสียหายในการเข้าสู่ระบบเช่น รหัสผู้ใช้ รหัสผ่าน การกระทำดังกล่าวยังเป็นความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตามประมวลกฎหมายอาญา มาตรา 269/5 , 269/7 ด้วย

5. การขโมยข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ต่างๆ ทำธุรกรรมทางการเงิน/แอบอ้างเป็นตัวเรา

ลักษณะในการกระทำความผิดโดยคนร้ายได้แอบเอาข้อมูลที่ผู้เสียหายใช้ในอินเตอร์เน็ต ซึ่งจะมีการเชื่อมโยงไปยังเว็บไซต์ต่างๆ เช่น การเข้าเว็บไซต์ดูดวงซึ่งเราจะกรอกข้อมูลวันเดือนปีเกิด เบอร์โทรศัพท์มือถือ ชื่ออีเมล์ที่ติดต่อเราได้ในเว็บไซต์ดังกล่าว บางครั้งเราอาจคิดว่าเว็บไซต์ดังกล่าวเป็นของหน่วยงานที่น่าเชื่อถือไม่น่าจะกระทำความผิดอาญา แต่ในความจริงในการทำธุรกิจของเว็บไซต์ดังกล่าวอาจต้องใช้พนักงานในการควบคุมดูแลระบบเว็บไซต์ของหน่วยงานซึ่งบุคคลดังกล่าวอาจเป็นมิจฉาชีพแฝงตัวเข้ามาในหน่วยงานก็เป็นได้ ดังนั้นข้อมูลส่วนบุคคลซึ่งอาจเป็นความ ลับของเราก็จะไม่เป็นความลับอีกต่อไป โลกของความปลอดภัยนั้นหาได้ยากบนโลก

ออนไลน์ ข้อมูลต่างๆ ถูกโอนถ่ายจากเว็บหนึ่งสู่เว็บหนึ่งทั้งที่เจ้าของข้อมูลรู้ตัวและไม่รู้ตัว การเข้าถึงข้อมูลส่วนบุคคลสามารถทำได้ง่ายขึ้นไม่ว่าจะเป็นการหาชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ ข้อมูลเหล่านี้ง่ายต่อการถูกเปิดเผย การที่สมัครเพื่อเป็นสมาชิกเว็บไซต์หนึ่งเว็บไซต์ บัญชีอี-เมล์หนึ่งอี-เมล์ มีข้อมูลส่วนตัวที่จำเป็นที่จะต้องให้ และใครจะรู้บ้างว่าข้อมูลเหล่านั้นจะถูกเก็บ หรือถูกส่งต่อไปยังที่ใดต่อไป โดยเฉพาะในปัจจุบันโลกของสังคมออนไลน์ (Social Network) ได้ถือว่าเป็นฐานข้อมูลอย่างดีให้กับองค์กรธุรกิจมากมาย เพื่อหาผลประโยชน์ในการใช้เป็นฐานข้อมูลลูกค้า ซึ่งเป็นประโยชน์แก่ผู้สุจริตที่ใช้งานอินเตอร์เน็ต แต่ในทางกลับกันหากคนร้ายได้เข้าถึงข้อมูลดังกล่าว คนร้ายก็จะสามารถนำข้อมูลส่วนบุคคลของเราไปกระทำความผิดทางอาญา ไม่ว่าจะกระทำความผิดโดยตรงกับเรา หรือกระทำความผิดหลอกลวงผู้อื่นโดยใช้ฐานข้อมูลเราไปหลอกลวงผู้เสียหาย เช่น การสั่งซื้อสินค้าทางอินเตอร์เน็ต โดยใช้หมายเลขบัตรเครดิต วันเดือนปีเกิด เบอร์โทรศัพท์ ของเราในการซื้อสินค้า ซึ่งเมื่อนำข้อมูลส่วนบุคคลดังกล่าวไปใช้ในการสั่งซื้อสินค้าหรือบริการทางอินเตอร์เน็ต การกระทำดังกล่าวจะเป็นความผิดฐาน ใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตามประมวลกฎหมายอาญา มาตรา 269/5 , 269/7 เป็นการฉ้อโกงโดยแสดงตนเป็นคนอื่นต่อเจ้าของสินค้า ตามประมวลกฎหมายอาญา มาตรา 342 และยังเป็นความผิดฐานนำข้อมูล คอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1) อีกด้วย

6. การทำปลอมหน้า website ผู้อื่น

ลักษณะการกระทำความผิด คนร้ายจะมีการทำหน้าเว็บไซต์ให้เหมือนกับเว็บไซต์ที่แท้จริง เช่น เว็บไซต์ธนาคาร A หลังจากนั้นคนร้ายจะส่งข้อความหลอกลวงไปยังบุคคลทั่วไป ซึ่งเป็นผู้เสียหายทางอีเมล์ โดยแจ้งว่าบัญชีของผู้ถูกหลอกลวงว่ามีปัญหา หรือธนาคารได้มีการปรับปรุงระบบหรือเปลี่ยนแปลงพัฒนาระบบรักษาความปลอดภัยใหม่ เพื่อความปลอดภัยทางบัญชีเงินฝากลูกค้า จึงให้ผู้เสียหายทำรายการ/แก้ปัญหา โดยให้ผู้เสียหาย Click Link ในอีเมล์ดังกล่าว ซึ่งจะเชื่อมต่อไปยัง Website ปลอม ซึ่งมีลักษณะเหมือนกับหน้าจอ A-Cyber Banking ทุกประการ โดยเป็น URL ที่ไม่ใช่ของธนาคาร โดยให้มีชื่อของเว็บไซต์ปลอมที่จะมีชื่อที่คล้ายคลึงกับ URL ของธนาคาร เมื่อผู้เสียหายหลงเชื่อเชื่อมต่อไปยังหน้าเว็บไซต์ปลอมก็จะหลงเชื่อกรอกข้อมูลส่วนบุคคลของผู้เสียหาย ไม่ว่าจะเป็นหมายเลขบัญชีเงินฝาก รหัสความปลอดภัย และข้อมูลส่วนบุคคลต่างๆ คนร้ายก็จะเก็บข้อมูลของผู้เสียหายดังกล่าวไปทำรายการโอนเงินผ่านระบบ e-banging ของธนาคารทำการโอนเงินของผู้เสียหายไป ซึ่งการกระทำดังกล่าวของผู้ต้องหาเป็นความผิดฐานนำข้อมูลคอมพิวเตอร์อันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ตาม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 14(1) เมื่อได้ข้อมูลทางการเงินและข้อมูลส่วนบุคคลของผู้เสียหายแล้ว คนร้ายนำข้อมูลดังกล่าวไปใช้การกระทำดังกล่าวก็จะเป็นความผิดฐานใช้บัตรอิเล็กทรอนิกส์ของผู้อื่นโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชนตามประมวลกฎหมายอาญา มาตรา 269/5 , 269/7 และยังเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาตรา 5,7 ,14(1) อีกต่างหากด้วย

7. การพนันออนไลน์

ลักษณะของการกระทำความผิด คนร้ายจะใช้ช่องทางอินเตอร์เน็ตในการติดต่อสื่อสารกับนักเล่นการพนัน โดยอาจจัดทำเป็นหน้าเว็บไซต์ในการเล่นการพนันไม่ว่าจะเป็นการพนันทายผลฟุตบอล หรือคาสิโนออนไลน์ เป็นต้น ทั้งนี้การเล่นการพนันออนไลน์นั้น เกิดจากผู้เล่นต้องการหลบหลีกการจับกุมจากเจ้าหน้าที่ตำรวจ เพราะไม่ทราบว่าเจ้ามือที่รับแทงพนันดังกล่าวอยู่ที่ใด ซึ่งบางครั้งอาจอยู่นอกประเทศก็เป็นได้ ส่วนการจ่ายเงินพนันใช้วิธีการโอนเงินทางอินเตอร์เน็ตทำให้การจับกุมมีความยาก ซึ่งการกระทำดังกล่าวของผู้เล่นการพนันทางออนไลน์นั้น มีความผิดตามพระราช บัญญัติการพนัน พ.ศ.2478 เท่านั้น แต่สำหรับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นั้นยังไม่มีการบัญญัติว่าการกระทำดังกล่าวเป็นความผิดตามพระราชบัญญัติดังกล่าว

ทุกวันนี้หากใช้คอมพิวเตอร์คลิกเข้าสู่อินเตอร์เน็ต ต้องระมัดระวังในการใช้งาน เพราะในโลกอินเตอร์เน็ตอันกว้างใหญ่ มีภัยอันตรายอย่างมัลแวร์แฝงอยู่ ซึ่งมัลแวร์มีหลายประเภท แต่มีมัลแวร์ชนิดหนึ่งที่จะมาจับเครื่องคอม และไฟล์ของเราเป็นตัวประกัน เรียกเงินค่าไถ่ จนทำให้คนทั่วโลกและไทยตื่นตัวมาก มีหนังสือราชการ ประกาศออกเตือนผู้ใช้คอม เพิ่มความระมัดระวังเป็นพิเศษ มัลแวร์ที่กำลังระบาดตอนนี้คือ Ransomware

Ransomware เป็นมัลแวร์ที่ออกแบบมาเพื่อเรียกค่าไถ่เหยื่อโดยเฉพาะ โดยส่วนใหญ่เกิดจากการคลิก link อันตราย หรือไปดาวน์โหลดไฟล์ ที่แนบในอีเมลเพื่อเปิดเอกสารแต่กลายเป็นพวกมัลแวร์อันตราย โดยเมื่อคลิกลิงค์ หรือรันไฟล์มัลแวร์ที่แนบมากับอีเมล์ มัลแวร์ ransomware นี้ จะสแกนไฟล์ต่างๆ ทั้งไฟล์ เอกสารทั่วไป, ไฟล์ภาพ ,ไฟล์วีดีโอ ซึ่งเป็นไฟล์ที่เราคุ้นเคยและใช้อยู่ในชีวิตประจำวันแล้ว มัลแวร์จะนำไฟล์ในคอมเราทั้งหมดนี้ไปทำการเข้ารหัส แล้วเปิดหน้าต่างเป็นข้อความขึ้นมาบนเครื่องเพื่อเรียกค่าไถ่ โดยมีข้อความปรากฏว่ากรุณาจ่ายเงินตามจำนวนเงิน ภายในระยะเวลาที่กำหนด ถ้ายอมจ่ายจะได้ตัวถอดรหัสไฟล์เพื่อมาถอดรหัสที่คนร้ายทำการเข้ารหัสไว้ให้เหยื่อสามารถเปิดไฟล์กลับมาใช้ได้ตามเดิม หากไม่จ่ายภายในกำหนดระยะเวลาแล้ว ค่าไถ่จะขึ้น

ราคาแพงขึ้นอีกเท่าตัว แต่ถึงแม้จะจ่ายเงินแล้วก็ไม่แน่ว่าจะได้เอกสารข้อมูลต่างๆ ของเราคืนทั้งหมดหรือไม่

และนอกจากนั้นในอนาคตอันใกล้โลกจะเข้าสู่ยุค Internet of Things = IOT หรือ “อินเตอร์เน็ตในทุกสิ่ง” หมายถึง การที่สิ่งต่างๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเตอร์เน็ตทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเตอร์เน็ต เช่น การสั่งเปิด-ปิดอุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่างๆ ผ่านเครือข่ายอินเตอร์เน็ต เป็นต้น หากวันนั้นมาถึงอย่างเต็มรูปแบบจะเป็นทั้งประโยชน์อย่างมหาศาล และความเสี่ยงไปพร้อมๆ กัน เพราะหากระบบรักษาความปลอดภัยของอุปกรณ์และเครือข่ายอินเตอร์เน็ตไม่ดีพอ จะทำให้ผู้ไม่ประสงค์ดีเข้ามากระทำการที่ไม่พึงประสงค์ต่ออุปกรณ์ข้อมูลสารสนเทศหรือความเป็นส่วนตัวของบุคคลได้ (วารสารไมโครคอมพิวเตอร์ ฉบับเดือนกุมภาพันธ์ 2557)

ดังนั้นผู้บังคับใช้กฎหมายที่เกี่ยวข้อง เช่น ตำรวจ อัยการ เจ้าหน้าที่ผู้ตรวจพิสูจน์พยานหลักฐาน เป็นต้น จึงจำเป็นต้องได้รับการพัฒนาองค์ความรู้และทักษะในส่วนที่เกี่ยวข้องกับกฎหมาย ความรู้ในด้านการสืบสวนสอบสวน การตรวจค้นจับกุม การตรวจยึดของกลาง การได้มาซึ่งพยานหลักฐานที่ชอบด้วยกฎหมายในคดีที่มีคอมพิวเตอร์มาเกี่ยวข้อง และรู้ระบบขั้นตอนการทำงานของคอมพิวเตอร์และโครงข่ายการติดต่อสื่อสารทางอินเตอร์เน็ตและการใช้สื่อสังคมออนไลน์ในรูปแบบต่างๆ ที่มีอยู่ในปัจจุบัน ผู้บังคับใช้กฎหมายต้องทำงานร่วมกันอย่างรวดเร็วใกล้ชิด เพื่อยับยั้งการกระทำผิดและจับกุมผู้กระทำผิดมาลงโทษ แต่ปัจจุบันเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญในอาชญากรรมด้านนี้มีจำนวนน้อย ไม่เพียงพอกับปริมาณคดีที่เพิ่มมากขึ้นในปัจจุบัน ทำให้การดำเนินคดีเป็นไปด้วยความล่าช้า ขาดประสิทธิภาพ การรวบรวมพยานหลักฐานต่างๆ เป็นไปได้ยาก รวมทั้งการติดตามพยานหลักฐานที่อยู่ต่างประเทศซึ่งใช้ระยะเวลานานมาก เจ้าหน้าที่ผู้ตรวจพิสูจน์หลักฐานเกี่ยวกับอาชญากรรมคอมพิวเตอร์มีน้อย ทำให้ต้องรอผลการตรวจพิสูจน์ รอข้อมูลจากผู้ให้บริการอินเตอร์เน็ต ทำให้พยานหลักฐานในสำนวนยังไม่รัดกุมเพียงพอที่จะชี้ชัดไปว่าผู้ใดกระทำผิด ทำที่ไหน ด้วยวิธีใด กระบวนการยุติธรรมเป็นไปอย่างล่าช้า ประชาชนผู้เสียหายไม่ได้รับการชดใช้เยียวยา ไม่เชื่อมั่นว่าเจ้าหน้าที่รัฐจะสามารถจับกุมลงโทษผู้กระทำผิดได้ ขาดความเชื่อมั่นศรัทธาในกระบวนการยุติธรรม จึงยอมสูญเสียทรัพย์สิน ชื่อเสียง ไม่ไปร้องทุกข์กับเจ้าหน้าที่

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาขั้นตอนการดำเนินการของเจ้าหน้าที่ผู้บังคับใช้กฎหมายในองค์กรต่างๆ ที่เกี่ยวข้อง และวิเคราะห์ปัญหาและอุปสรรคที่เกิดขึ้นในการทำงาน รวมทั้งปัญหาด้านบุคลากร งบประมาณ การบริหารจัดการคดีและองค์กร

2. เสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคต่างๆ เพื่อการพัฒนาบุคลากรผู้บังคับใช้กฎหมายในองค์กรต่างๆ ที่เกี่ยวข้อง ให้มีความรู้ ความเชี่ยวชาญ และมีจำนวนเพียงพอที่จะสามารถในการดำเนินคดีกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ

ขอบเขตของการวิจัย

1. งานวิจัยนี้เริ่มทำในห้วงเวลาตั้งแต่เดือนพฤศจิกายน 2557 ถึง เดือนพฤษภาคม 2558

2. เน้นการวิจัยเฉพาะขั้นตอนการดำเนินคดีกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ รวมทั้งปัญหาและอุปสรรคในการทำงาน การบริหารจัดการคดี บุคลากรในองค์กรดังนี้ สำนักงานตำรวจแห่งชาติ, สำนักงานอัยการสูงสุด, กรมสอบสวนคดีพิเศษ, สถาบันนิติวิทยาศาสตร์, กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

3. เน้นหาแนวทาง วิธีการ การพัฒนาบุคลากรผู้บังคับใช้กฎหมายที่เกี่ยวข้องในแต่ละองค์กร

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์ขั้นตอนการดำเนินคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ รวมทั้งปัญหาและอุปสรรคในการทำงาน การบริหารจัดการคดี บุคลากรและหาแนวทางแก้ไขปัญหาอุปสรรค การพัฒนาบุคลากร การทำงานร่วมกันอย่างมีประสิทธิภาพ รวมทั้งการสัมภาษณ์ผู้บริหาร ผู้ทรงคุณวุฒิ ทั้งภาครัฐและเอกชน ที่มีความรู้ ความเชี่ยวชาญเกี่ยวกับการใช้คอมพิวเตอร์ ด้านอาชญากรรม และในเรื่องการพัฒนาบุคลากร เพื่อศึกษาเปรียบเทียบ และนำเสนอการแนวทางการเพิ่มประสิทธิภาพในการปฏิบัติงานเป็นที่พึงพอใจแก่ประชาชน

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ได้ทราบถึงปัญหาและอุปสรรคต่างๆที่เกิดขึ้นของแต่ละองค์กรที่เกี่ยวข้องในการดำเนินคดีกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์และแนวทางแก้ไข

2. ได้แนวทางในการพัฒนาบุคลากรผู้บังคับใช้กฎหมายให้มีความรู้ ความเชี่ยวชาญและมีปริมาณเพียงพอ ที่จะสามารถดำเนินคดีได้อย่างรวดเร็วขึ้น มีประสิทธิภาพ และเป็นที่เชื่อมั่นศรัทธาของประชาชน

บทที่ 2
แนวคิด ทฤษฎี ในการพัฒนาผู้บังคับใช้กฎหมายและกฎหมาย ที่เกี่ยวข้องกับการดำเนินคดีอาชญากรรม ที่เกี่ยวข้องกับคอมพิวเตอร์

ในเรื่องของอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ มีคำจำกัดความของศัพท์ที่เกี่ยวข้องหลายคำที่ควรศึกษา

คำศัพท์ที่เกี่ยวข้อง

Cyber

ดิกชันนารี American Heritage&Science Dictionary ให้ความหมายของ Cyber ไว้ว่าเป็นคำเสริมหน้า (prefix) ใช้นำหน้าคำเพื่อให้หมายถึง คอมพิวเตอร์ หรือ ข่ายงานคอมพิวเตอร์ เช่น อินเตอร์เน็ต (cyberspace) สื่ออิเล็กทรอนิคส์ซึ่งมีการติดต่อสื่อสารออนไลน์เกิดขึ้น Collin English Dictionary ได้ให้ความหมายไว้ว่าหมายถึง ศาสตร์ที่เกี่ยวอิเล็กทรอนิคส์และคอมพิวเตอร์ เอลิส เซลดา อาร์เดวอล (Elisenda Ardevol, 2005) ได้ให้คำจำกัดความของ cyber ในงานวิจัยของเธอเรื่อง Cyberculture : Anthropological perspective of the internet. ว่า ไซเบอร์เป็นคำเสริมหน้า (prefix) ที่อ้างอิงถึงกิจกรรมและความเคลื่อนไหวทางสังคมที่เกิดขึ้นโดยผ่านอินเตอร์เน็ต เช่น กิจกรรมทางสังคมต่างๆ ศูนย์แลกเปลี่ยนข้อมูลข่าวสารทางอินเตอร์เน็ต (cybercafé) หรือ ศิลปะไซเบอร์ เป็นต้น

คอมพิวเตอร์

คอมพิวเตอร์ (computer) คือ เครื่องมือหรืออุปกรณ์อิเล็กทรอนิกส์ ที่มีความสามารถในการคำนวณอัตโนมัติตามคำสั่ง ส่วนที่ใช้ประมวลผลเรียกว่าหน่วยประมวลผล ชุดของคำสั่งที่ระบุขั้นตอนการคำนวณเรียกว่าโปรแกรมคอมพิวเตอร์ ผลลัพธ์ที่ได้ออกมานั้นอาจเป็นได้ทั้ง ตัวเลข ข้อความ รูปภาพ เสียง หรืออยู่ในรูปอื่นๆ อีกมากมาย

ลักษณะทางกายภาพของคอมพิวเตอร์นั้นมีหลากหลาย มีทั้งขนาดที่ใหญ่มากจนต้องใช้ห้องทั้งห้องในการบรรจุ และขนาดเล็กจนวางได้บนฝ่ามือ การจัดแบ่งประเภทของคอมพิวเตอร์สามารถจัดแบ่งได้ตามขนาดทางกายภาพเป็นสำคัญ ซึ่งมักจะแปลผันกับประสิทธิภาพความเร็วในการประมวลผล โดยขนาดคอมพิวเตอร์ที่มีขนาดใหญ่ที่สุดเรียกว่า ซูเปอร์คอมพิวเตอร์ ใช้กับการ

คำนวณผลทางวิทยาศาสตร์ ขนาดรองลงมาเรียกว่า เมนเฟรม มักใช้ในบริษัทขนาดใหญ่ที่ต้องมีการประมวลผลธุรกรรมทางธุรกิจจำนวนมากๆ สำหรับคอมพิวเตอร์ขนาดเล็กที่ใช้ในระดับบุคคลเรียกว่า คอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์ส่วนบุคคลที่พกพาได้เรียกว่า คอมพิวเตอร์โน๊ตบุ๊ค ส่วนคอมพิวเตอร์ขนาดเล็กที่สามารถวางบนฝ่ามือได้เรียกว่า พีดีเอ อย่างไรก็ตามคอมพิวเตอร์มีใช้กันอย่างกว้างขวางมาก ซึ่งมีอุปกรณ์หลายๆ ชนิดได้นำคอมพิวเตอร์ไปใช้เป็นกลไกหลักในการทำงาน เช่น กล้องดิจิทัล เครื่องเล่นเอ็มพีสาม หรือในรถยนต์เองก็มีคอมพิวเตอร์ที่ใช้ช่วยในการตรวจสอบระบบการทำงานของเครื่องยนต์

ประสิทธิภาพของคอมพิวเตอร์โดยรวมแล้ววัดกันที่ความเร็วการประมวลผล ซึ่งตามกฎของมัวร์ (Moore's Law) คอมพิวเตอร์จะเพิ่มประสิทธิภาพเป็นเท่าทวีคูณในทุกปี

อาชญากรรม

อาชญากรรม คือ การกระทำที่ละเมิดต่อกฎหมายที่มีโทษทางอาญาอาชญากรรมในความหมายอย่างแคบ คือ พฤติกรรมที่เป็นการละเมิดต่อกฎหมายอาญาเท่านั้น โดยการพิจารณาพฤติกรรมการกระทำของบุคคลในสังคมตามข้อกำหนดของกฎหมายอาญาเท่านั้น ไม่ได้คำนึงถึงเจตนา หรือลักษณะของความผิดแต่อย่างใด นอกจากนี้ อาชญากรรมอาจมีความหมายที่แตกต่างกันในแต่ละประเด็น ดังนี้

1. อาชญากรรมในแง่กฎหมาย เป็นการกระทำที่มีความผิดและมีบทลงโทษทางอาญาเป็นหลัก โดยการกระทำความผิดทางอาญา แบ่งเป็น 2 ประเภท คือ

1.1 อาชญากรรมที่มีความชั่วร้ายในตัวเอง (Mala inse)

1.2 อาชญากรรมที่ไม่มีความชั่วร้ายในตัวเอง (Mala prohibita)

2. อาชญากรรมในแง่สังคมวิทยา เป็นการกระทำที่ส่งผลต่อสังคมส่วนรวม และสังคมมุ่งจะลงโทษผู้ที่มีพฤติกรรมดังกล่าว

3. อาชญากรรมในแง่อาชญาวิทยา เป็นการกระทำความผิดในทางอาญา มีสาเหตุในการกระทำความผิดที่แตกต่างกัน ขึ้นอยู่กับปัจจัยที่เป็นตัวกำหนด โดยการกระทำดังกล่าวก่อให้เกิดความเสียหาย และจะต้องมีมาตรการในการปฏิบัติต่อผู้กระทำผิดที่เหมาะสม

นอกจากนี้อาชญากรรมอาจมีความหมายที่แตกต่างกัน อาทิ อาชญากรรม คือ การกระทำที่ละเมิดกฎหมายอาญา การกระทำใดๆ ไม่ว่าจะน่าประณามน่าลงโทษมากสักเพียงใด หรือไม่ว่าจะเป็นการผิดศีลธรรมมากเพียงใดก็ไม่ถือว่าเป็นอาชญากรรม ถ้าไม่มีบทบัญญัติของกฎหมายห้ามไว้

อาชญากรรมคือ การกระทำ หรือ ละเว้นการกระทำใดๆ ซึ่งกฎหมายมหาชนได้บัญญัติห้ามไว้เพื่อคุ้มครองประโยชน์สาธารณะ และถ้าผู้ใดฝ่าฝืนไม่ปฏิบัติตามจะถูกลงโทษโดยวิธีดำเนินกระบวนพิจารณาทางศาล

อาชญากรรม คือ การกระทำโดยมีเจตนาละเมิดกฎหมายอาญา หรือละเว้นไม่กระทำในสิ่งที่กฎหมายอาญาบังคับให้กระทำ (ทั้ง Statutory และ case law) โดยไม่มีข้อแก้ตัวที่สมเหตุสมผล ซึ่งทำให้รัฐต้องดำเนินการลงโทษในฐานะที่เป็นความผิด

สรุปได้ว่า อาชญากรรมในความหมายอย่างกว้าง หมายถึง พฤติกรรมที่มีการกระทำผิด โดยผู้กระทำผิดมีเจตนาในการกระทำดังกล่าว โดยเป็นการกระทำความผิดที่มีลักษณะร้ายแรง มีความรุนแรงและเป็นอันตรายต่อสังคม ซึ่งก่อให้เกิดผลกระทบจำนวนมหาศาลต่อสังคม อันเป็นการกระทำที่มีการละเมิดต่อกฎหมายบ้านเมือง ผู้กระทำผิดจะต้องได้รับโทษทั้งที่ไม่เป็นทางการจากสมาชิกในสังคม อาทิ การตำหนิ ติเตียน การไม่คบหาสมาคมด้วย และการได้รับโทษที่เป็นทางการจากข้อ กำหนดของกฎหมายบ้านเมือง โดยผู้กระทำผิดจะต้องถูกลงโทษโดยผ่านกระบวนการยุติธรรมเป็นสำคัญ

อาชญากรรมทางคอมพิวเตอร์

มีผู้ให้ความหมายไว้ 2 ประการ ได้แก่

1. การกระทำใดๆ ก็ตาม ที่เกี่ยวกับการใช้คอมพิวเตอร์ อันทำให้เหยื่อได้รับความเสียหาย และทำให้ผู้กระทำได้รับผลตอบแทน

2. การกระทำผิดกฎหมายใดๆ ซึ่งจะต้องใช้ความรู้เกี่ยวข้องกับคอมพิวเตอร์ มาประกอบการกระผิด และต้องใช้ผู้มีความรู้ทางคอมพิวเตอร์ ในการสืบสวน ติดตาม รวบรวมหลักฐาน เพื่อการดำเนินคดี จับกุม

อาชญากรทางคอมพิวเตอร์

ผู้กระทำผิดกฎหมายโดยใช้เทคโนโลยีคอมพิวเตอร์เป็นส่วนสำคัญ เป็นการกระทำใดๆ ที่เกี่ยวกับการใช้การเข้าถึงข้อมูล โดยที่ผู้กระทำไม่ได้รับอนุญาต การลักลอบแก้ไข ทำลาย คัดลอกข้อมูล ทำให้คอมพิวเตอร์ทำงานผิดพลาด แม้ไม่ถึงกับเป็นการกระทำที่ผิดกฎหมาย แต่เป็นการกระทำที่ผิดระเบียบกฎเกณฑ์ จรรยาบรรณของการใช้คอมพิวเตอร์นั้นๆ

ส่วนในเรื่องของการพัฒนาบุคลากร ก็ได้มีคำจำกัดความไว้ดังนี้

การพัฒนาบุคลากร

กระบวนการที่มุ่งจะเปลี่ยนแปลงวิธีการทำงาน ความรู้ความสามารถ ทักษะและทัศนคติของบุคลากรให้เป็นไปทางที่ดีขึ้นเพื่อให้บุคลากรที่ได้รับการพัฒนาแล้วนั้นปฏิบัติงานได้ผลตามวัตถุประสงค์ของหน่วยงานอย่างมีประสิทธิภาพ

การฝึกอบรม

มีผู้ให้คำนิยามความหมายของการฝึกอบรมไว้อย่างมากมาย ขึ้นอยู่กับว่ามองการฝึกอบรมจากแนวคิด (Approach) ใด เช่น

เมื่อมองการฝึกอบรม ในฐานะที่เป็นแนวทางในการพัฒนาข้าราชการตามนโยบายของรัฐ "การฝึกอบรม หมายถึง กระบวนการต่าง ๆ ที่ใช้เพื่อช่วยให้ข้าราชการมีความรู้ ทักษะ และทัศนคติที่จำเป็นในการปฏิบัติงาน ในหน้าที่ และเพื่อให้เกิด ความร่วมมือกันระหว่างข้าราชการในการปฏิบัติงานร่วมกันในองค์การ" หรือ

ในระยะหลัง เรามักจะมองการฝึกอบรมในเชิงของกระบวนการเปลี่ยนแปลงพฤติกรรมอันสืบเนื่องมาจากเรียนรู้ การฝึก อบรมจึงหมายถึง " กระบวนการเปลี่ยนแปลงพฤติกรรมอย่างมีระบบ เพื่อให้บุคคลมีความรู้ ความเข้าใจ มีความสามารถที่จำเป็น และมีทัศนคติที่ดีสำหรับการปฏิบัติงานอย่างใดอย่างหนึ่งของหน่วยงานหรือองค์การนั้น

การฝึกอบรม คือ " กระบวนการในอันที่จะทำให้ผู้เข้ารับการฝึกอบรมเกิดความรู้ ความเข้าใจ ทัศนคติ และความชำนาญ ในเรื่องหนึ่งเรื่องใด และเปลี่ยนพฤติกรรมไปตามวัตถุประสงค์ที่กำหนดไว้จะเห็นได้ว่า ความหมายของการฝึกอบรมมีมากมาย ขึ้นอยู่กับว่าจะพิจารณาจากแนวคิด (Approach) ใดที่เกี่ยวกับการฝึกอบรม ทั้งนี้ มีแนวคิดและทฤษฎีต่างๆ ที่เกี่ยวกับการฝึกอบรม ดังต่อไปนี้

ตารางที่ 2 – 1 เปรียบเทียบความแตกต่างระหว่างการศึกษา การพัฒนาบุคคล และการฝึกอบรม

หัวข้อในการเปรียบเทียบ	การศึกษา	การพัฒนาบุคคล	การฝึกอบรม
1. .เป้าหมาย	- เลือกอาชีพ - ปรับตัวให้เข้ากับสังคมและสภาพแวดล้อม	- เสริมสร้างคุณภาพและความก้าวหน้าของบุคคล	- เพิ่มประสิทธิภาพในการปฏิบัติงาน
2. เนื้อหา	- กว้าง	- ตรงกับศักยภาพและงานในอนาคต	- ตรงกับงานที่กำลังปฏิบัติ หรือกำลังจะได้รับมอบหมายให้ปฏิบัติ
3. ตามความต้องการของ	- บุคคล	- หน่วยงานและบุคคล	- งาน
4. ระยะเวลาที่ใช้	- ยาวและสามารถทำได้เรื่อยๆ ไม่สิ้นสุด	- ใช้เวลาตลอดอายุงาน - มองในระยะยาว	- ใช้ระยะเวลาจำกัด
5. วัย	- วัยเรียน	-วัยทำงาน	- วัยทำงาน
6. ความเสี่ยง (ที่จะบรรลุวัตถุประสงค์)	- ปานกลาง	- สูง	-ต่ำ
7. การประเมินผล ดูจาก	- การปฏิบัติงานในอนาคต	- เกือบจะทำการประเมินไม่ได้เพราะมีตัวแปรจากสภาพแวดล้อมจำนวนมากยากแก่การควบคุม	- จากพฤติกรรมในการปฏิบัติงานในหน้าที่

ที่มา : สถาบันประมวลข้อมูลเพื่อการศึกษาและการพัฒนา มหาวิทยาลัยธรรมศาสตร์

เท่าที่กล่าวมาแล้วทั้งหมดในส่วนของการศึกษา การพัฒนาบุคคลและการฝึกอบรม อาจสรุปความแตกต่างของทั้ง 3 คำ อย่างสั้นๆ ได้ดังนี้

การศึกษา (Education) เน้นที่ตัวบุคคล (Individual Oriented)

การฝึกอบรม (Training) เน้นถึงการทำให้สามารถทำงานที่ต้องการได้ (Job Oriented)

การพัฒนา (Development) เน้นที่องค์การ (Organizational Oriented) เพื่อให้ตรงกับนโยบาย เป้าหมาย ขององค์การที่สังกัด

ผู้บังคับใช้กฎหมายนอกจากจะต้องมีความรู้ ทักษะ และประสบการณ์ในงานที่ทำแล้ว สิ่งที่สำคัญมากอีกอย่างหนึ่งคือต่างมีคุณธรรมจริยธรรมและความซื่อสัตย์สุจริต

คำจำกัดความของคุณธรรมจริยธรรม

ตามพจนานุกรมฉบับราชบัณฑิตยสถาน ให้ความหมายหรือนิยามไว้ว่า

“คุณ” หมายความว่า ความดีที่มีประจำอยู่ “ธรรม” หมายความว่า คุณความดี ความถูกต้อง

“คุณธรรม” หมายความว่า สภาพคุณงามความดี

“จริยะ” หมายความว่า ความประพฤติ กริยาที่ควรประพฤติ

“ธรรมจริยา” หมายความว่า การประพฤติเป็นธรรม การประพฤติถูกธรรม

“จริยธรรมา” หมายความว่า ธรรมที่เป็นข้อประพฤติปฏิบัติ

คำจำกัดความของความยุติธรรม

ตามพจนานุกรมฉบับบัณฑิตยสถานให้คำนิยามคำว่า “ยุติธรรม” ว่าคือ ความเที่ยงธรรม ความชอบธรรม ความชอบด้วยเหตุผล และ คำว่า “เที่ยงธรรม” มีความหมายว่า “ตั้งตรงด้วยความเป็นธรรม” พระราชดำรัสและพระบรมราโชวาทของพระบาทสมเด็จพระเจ้าอยู่หัวที่ได้พระราชทานแก่นักกฎหมายในโอกาสต่างๆ ในเรื่องความยุติธรรม มีดังนี้

“กฎหมายมิใช่ตัวความยุติธรรม หากเป็นเพียงบทบัญญัติหรือปัจจัยที่ตราไว้เพื่อรักษาความยุติธรรม ผู้ใดก็ตามแม้ไม่รู้กฎหมาย แต่ถ้าประพฤติปฏิบัติด้วยความสุจริตแล้วควรจะได้รับความคุ้มครองจากกฎหมายเต็มที่ ตรงกันข้าม คนที่รู้กฎหมายแต่ใช้กฎหมายไปในทางทุจริต ควรต้องถือว่าทุจริต และกฎหมายไม่ควรคุ้มครองจนเกินเลยไป เพราะฉะนั้นไม่สมควรจะถือว่าการรักษาความยุติธรรมในแผ่นดินมีวงกว้างอยู่เพียงแต่ขอบเขตของกฎหมาย จำเป็นต้องขยายออกไปให้ถึง ศีลธรรมจรรยา ตลอดจนเหตุและผลความเป็นจริงด้วย”

พระบรมราโชวาทในพิธีพระราชทานประกาศนียบัตร แก่ผู้สอบไล่ได้ตามหลักสูตรของสำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา เมื่อวันที่ 19 กรกฎาคม 2520 ว่า “กฎหมายทั้งปวงจะธำรงความยุติธรรมและถูกต้อง เที่ยงตรง หรือจะธำรงความศักดิ์สิทธิ์และประสิทธิภาพเต็มเปี่ยมอยู่ได้หรือไม่เพียงไรนั้น ขึ้นอยู่กับการใช้ คือถ้าใช้ให้ถูกวัตถุประสงค์หรือเจตนารมณ์ของ

กฎหมายนั้นๆ จริงแล้ว ก็จะทรงความศักดิ์สิทธิ์และประสิทธิภาพอันสมบูรณ์ไว้ได้ แต่ถ้าหากนำไปใช้ผิดวัตถุประสงค์และเจตนารมณ์ โดยการพลิกแพลงบิดพลิ้วให้ผันผวนไปด้วยความหลงผิดด้วยอคติ หรือด้วยเจตนาอันไม่สุจริตต่างๆ กฎหมายก็เสื่อมความศักดิ์สิทธิ์และประสิทธิภาพลงทันทีและกลับกลายเป็นพิษเป็นภัยแก่ประชาชนอย่างใหญ่หลวง ผู้ที่ต้องการจะใช้กฎหมายสร้างสรรค์ความผาสุขสงบและความเป็นปึกแผ่นก้าวหน้าของประชาชนและบ้านเมืองจึงจำเป็นอย่างยิ่งที่จะต้องรักษาวัตถุประสงค์อันแท้จริงของกฎหมายแต่ละฉบับไว้ให้แน่วแน่เสมอไป อย่างไม่มีข้อแม้ประการใดๆ พร้อมทั้งต้องรักษาอุดมคติ จรรยา ความสุจริต และมโนธรรมของนักกฎหมายไว้โดยรอบคอบ เคร่งครัดเสมอด้วยรักษาชีวิตของตนเอง กฎหมายไทยจึงจะทรงคุณค่าอันสมบูรณ์บริบูรณ์”

การสืบสวนสอบสวนคดีความผิดเกี่ยวกับคอมพิวเตอร์นั้นมีลักษณะที่แตกต่างจากการสอบสวนคดีอาญาทั่วไป เนื่องจากมีความสลับซับซ้อนในการกระทำความผิด โดยผู้กระทำผิดเป็นผู้มีความรู้เชี่ยวชาญในการใช้คอมพิวเตอร์ หรือระบบอิเล็กทรอนิกส์ต่างๆ แต่นำมาใช้ในการกระทำผิดเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น นอกจากนี้การกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ส่วนมากเกิดขึ้นในหลายท้องที่ต่อเนื่องเกี่ยวพันกัน ทั้งในและต่างประเทศ รวมทั้งการกระทำในรูปแบบองค์กรอาชญากรรมข้ามชาติ มีการแบ่งหน้าที่กันทำในแต่ละประเทศ โดยอาศัยคอมพิวเตอร์ระบบเครือข่ายในการติดต่อสื่อสารเชื่อมโยงกัน

ดังนั้นในการดำเนินคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ เจ้าหน้าที่ผู้บังคับใช้กฎหมาย จึงต้องผู้มีความรู้ความเชี่ยวชาญในเรื่องคอมพิวเตอร์และระบบอิเล็กทรอนิกส์ รวมทั้งระบบเครือข่ายอินเตอร์เน็ต รวมทั้งต้องรู้และเข้าใจถึงคำศัพท์ คำนิยาม ข้อหาความผิด องค์ประกอบของความผิด บทลงโทษของแต่ละข้อหา วิธีการ ได้มาซึ่งพยานหลักฐาน การตรวจค้น ยึด เก็บรักษาการตรวจพิสูจน์ การสืบสวนสอบสวน การรวบรวมพยานหลักฐาน การดำเนินคดีในชั้นพนักงานอัยการ และในชั้นศาล กฎหมายต่างๆ ที่เกี่ยวข้อง เพื่อให้เกิดประสิทธิภาพในการจับกุมผู้กระทำผิดมาลงโทษตามกฎหมาย

กฎหมายที่เกี่ยวข้อง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

เป็นกฎหมายที่มีแนวคิดในการคุ้มครองมิให้ บุคคลใดกระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ รวมทั้งมิให้มีการกระทำใดๆ ที่เป็นการเข้าระบบ หรือล่วงรู้ข้อมูล แก้ไข ทำลายข้อมูลคอมพิวเตอร์ของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อ

เผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จปลอม หรือมีลักษณะลามกอนาจาร เป็นต้น อันจะก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน

โดยกฎหมายได้กำหนดคำนิยามไว้ในมาตรา 3 และหมวดที่ 1 ว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ ตั้งแต่มาตรา 5-17 หมวด 2 พนักงานเจ้าหน้าที่ โดยกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ อำนาจและวิธีปฏิบัติในการสืบสวนสอบสวน ตามมาตรา 18 – 25 และยังมีมาตราที่เกี่ยวข้องกับผู้ให้บริการบุคคลที่ต้องปฏิบัติตามคำสั่งใน มาตรา 26 – 27

คำนิยามที่สำคัญและควรรู้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

1. ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

2. ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ความผิดต่างๆ และบทลงโทษตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

ตารางที่ 2 – 2 ความผิดเกี่ยวกับการกระทำต่อคอมพิวเตอร์

ความผิดเกี่ยวกับคอมพิวเตอร์ (กระทำต่อคอมพิวเตอร์)			
ฐานความผิด	รูปแบบการกระทำความผิด	โทษจำคุก	โทษปรับ
มาตรา 5 เข้าถึงคอมพิวเตอร์โดยมิชอบ	1. สปายแวร์ (Spyware) การสอดแนมข้อมูลส่วนตัว 2. สนิฟเฟอร์ (Sniffer) การแอบดักฟัง	ไม่เกิน 6 เดือน	ไม่เกิน 10,000.- บาท
มาตรา 6 ล่วงรู้มาตรการป้องกันการเข้าถึง		ไม่เกิน 1 ปี	ไม่เกิน 20,000.- บาท
มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ		ไม่เกิน 2 ปี	ไม่เกิน 40,000.- บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์		ไม่เกิน 3 ปี	ไม่เกิน 100,000.- บาท
มาตรา 9 ทำให้เสียหาย ทำลาย แก้ไขเปลี่ยนแปลง	การใช้ชุดคำสั่งในทางมิชอบ(Malicious Code) เช่น Viruses, Worms, Trojan Horses	ไม่เกิน 5 ปี	ไม่เกิน 100,000.- บาท
มาตรา 10 ทำให้ระบบไม่สามารถทำงานได้ตามปกติ		ไม่เกิน 5 ปี	ไม่เกิน 100,000.- บาท
มาตรา 13 การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด	การโฟสต์หรือนำเข้าข้อมูลคอมพิวเตอร์	ไม่เกิน 1 ปี	ไม่เกิน 20,000.- บาท

ตารางที่ 2 – 3 ความผิดเกี่ยวกับการใช้คอมพิวเตอร์กระทำความผิด

ความผิดเกี่ยวกับคอมพิวเตอร์ (ใช้คอมพิวเตอร์กระทำความผิด)			
ฐานความผิด	รูปแบบการกระทำความผิด	โทษจำคุก	โทษปรับ
มาตรา 11 สแปมเมล์	สแปม (Spamming)	ไม่มี	ไม่เกิน 100,000.- บาท
มาตรา 14 การปลอมแปลงข้อมูลคอมพิวเตอร์/ เผยแพร่เนื้อหาอันไม่เหมาะสม	การโพสต์หรือนำเข้าข้อมูลคอมพิวเตอร์	ไม่เกิน 5 ปี	ไม่เกิน 100,000.- บาท
มาตรา 15 ความรับผิดของผู้ให้บริการ		ไม่เกิน 5 ปี	ไม่เกิน 100,000.- บาท
มาตรา 16 การเผยแพร่ภาพจากการตัดต่อ/ ดัดแปลง	การตัดต่อภาพ	ไม่เกิน 5 ปี	ไม่เกิน 100,000.- บาท

ตารางที่ 2 – 4 ความผิดเกี่ยวกับคอมพิวเตอร์กระทำนอกราชอาณาจักรไทย

ความผิดเกี่ยวกับคอมพิวเตอร์ (กระทำผิดนอกราชอาณาจักรไทย)			
ฐานความผิด	รูปแบบการกระทำความผิด	โทษจำคุก	โทษปรับ
มาตรา 17 กระทำความผิดนอกราชอาณาจักรต้องรับโทษภายในราชอาณาจักร	ทำความผิดเกี่ยวนอกราชอาณาจักร		

ตารางที่ 2 – 5 อำนาจหน้าที่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

อำนาจหน้าที่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550	
มาตรา	คำอธิบาย
มาตรา 18	อำนาจของพนักงานเจ้าหน้าที่
มาตรา 19	ข้อจำกัด/ การตรวจสอบการใช้อำนาจของพนักงานเจ้าหน้าที่
มาตรา 20	การใช้อำนาจในการ block เว็บไซต์ที่มีเนื้อหากระทบต่อความมั่นคงหรือขัดต่อความสงบเรียบร้อย
มาตรา 21	การเผยแพร่/ จำหน่ายชุดคำสั่งไม่พึงประสงค์
มาตรา 22	ห้ามมิให้พนักงานเผยแพร่ข้อมูลที่ได้มาตาม มาตรา 18
มาตรา 23	พนักงานเจ้าหน้าที่ประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูล
มาตรา 24	ความรับผิดของผู้ล่วงรู้ข้อมูลที่พนักงานเจ้าหน้าที่ได้มาตาม มาตรา 18
มาตรา 25	ห้ามมิให้รับฟังพยานหลักฐานที่ได้มาโดยมิชอบ
มาตรา 26 – 27	หน้าที่ผู้ให้บริการในการเก็บข้อมูลจราจรทางคอมพิวเตอร์และความรับผิดหากไม่ปฏิบัติตามหน้าที่
มาตรา 28	การแต่งตั้งพนักงานเจ้าหน้าที่
มาตรา 29	การรับคำร้องทุกข์กล่าวโทษ จับ ควบคุม และ การกำหนดระเบียบ/แนวทางและวิธีปฏิบัติ
มาตรา 30	การปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่

หมายเหตุ

1. Phishing คือ การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับ อี-เมล์ เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูล ส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือ ข้อมูลส่วนบุคคลอื่นๆ

2. Eavesdropping เช่น Sniffer คือ การลักลอบดักข้อมูลของการติดต่อสื่อสาร

3. Data Diddling คือ การลักลอบปลอมแปลงข้อมูล

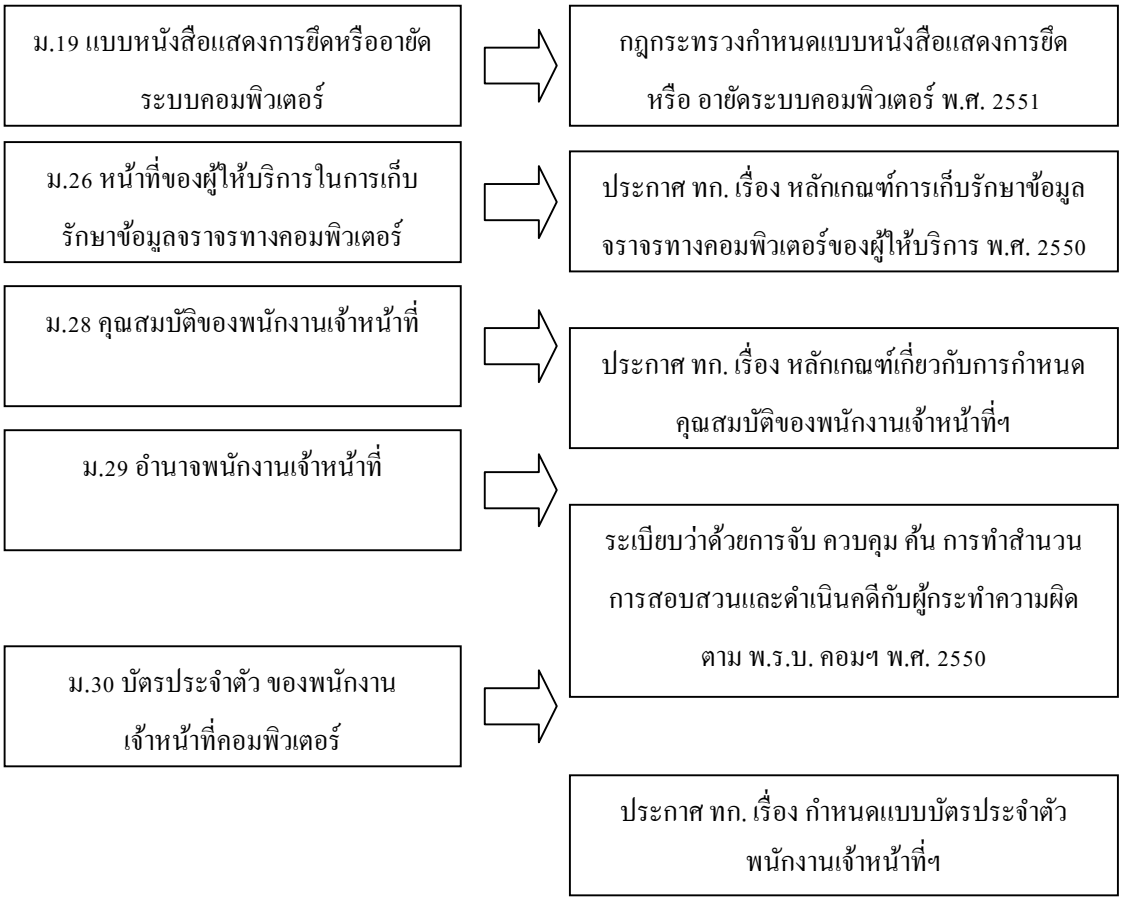
4. Spoofing คือ การหลอกลวงด้วยการปลอมแปลงให้เข้าใจผิดว่าเป็นผู้อื่น

5. Pharming คือ การขโมยข้อมูลสำคัญเพื่อผลประโยชน์ ไม่ได้ใช้วิธีการหลอกลวงแต่ด้วยวิธีการโจมตี กับส่วนที่เกี่ยวข้องกับการเข้าถึงบริการ เช่น DNS หรือBrowser

6. Denial of Service คือ การโจมตีสภาพความพร้อมใช้งานของระบบ

7. การเผยแพร่โปรแกรมไม่พึงประสงค์ (Malicious Code) เช่น Viruses/ Worms

แผนภาพที่ 2 – 1 รูปแบบและฐานความผิดทางอาชญากรรมทางคอมพิวเตอร์ กฎหมายลำดับรองภายใต้ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550



พระราชบัญญัติฉบับนี้ให้ใช้บังคับเมื่อพ้นกำหนดสามสิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป (2 มาตรา) กฎหมายฉบับนี้ประกาศในราชกิจฉานุเบกษา เล่ม 124 ตอนที่ 27ก วันที่ 18 มิถุนายน 2550 กฎหมายฉบับนี้จึงมีผลใช้บังคับตั้งแต่วันที่ 18 กรกฎาคม 2550 เป็นต้นไป ฉะนั้น การจะดำเนินคดีกับการกระทำผิดตามพระราชบัญญัติฉบับนี้ที่เกิดขึ้นก่อนวันที่ 18 กรกฎาคม 2550 จึงไม่อาจกระทำได้

2. ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาเป็นกฎหมายที่เกี่ยวข้องกับความผิดเกี่ยวกับคอมพิวเตอร์ ในกรณีที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และการกระทำความผิดดังกล่าวเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญาด้วย หรือในกรณีที่การกระทำไม่เป็นความผิดตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 แต่หากการกระทำดังกล่าวเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา จึงจะต้องนำประมวลกฎหมายอาญามาใช้บังคับด้วยเช่นกัน

และเนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายที่มีโทษทางอาญา จึงต้องนำประมวลกฎหมายอาญามาใช้บังคับด้วย ไม่ว่าจะเป็นเรื่องบทลงโทษ และการลงโทษผู้กระทำความผิด หลักในเรื่องเจตนา ตัวการ ผู้ใช้ และผู้สนับสนุน ความผิดที่ถือว่าเกิดขึ้นในและนอกราชอาณาจักร เป็นต้น ฯลฯ

นอกจากนี้ ในปี พ.ศ.2547 การใช้เอกสาร วัตถุอื่นใดหรือข้อมูล ที่จัดทำขึ้นในลักษณะบัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต บัตรสมาร์ทการ์ด หรือบัตรอื่นใด ในลักษณะคล้ายกัน โดยมีวัตถุประสงค์เพื่อประโยชน์ในการชำระค่าสินค้า บริการ หรือหนี้อื่น หรือเพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์อย่างหนึ่งอย่างใด กำลังเพิ่มปริมาณและประเภทการใช้งานอย่างแพร่หลาย และปรากฏว่าได้มีการกระทำความผิดเกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้อันส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง จึงมีการกำหนดความผิดอาญาสำหรับการกระทำความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์ดังกล่าวเพิ่มเติมให้ครอบคลุมการกระทำความผิดในรูปแบบต่างๆ และให้มีอัตราโทษเหมาะสมกับความร้ายแรงของการกระทำความผิด จึงมีการตราพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ.2547 ขึ้นใช้บังคับ และเป็นบทบัญญัติที่มีความเชื่อมโยงกับคำว่า “มาตรการในการป้องกันการเข้าถึงโดยเฉพาะ” ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 อีกด้วย

3. ประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายวิธีพิจารณาความอาญาเป็นกฎหมายบัญญัติที่มีความสำคัญที่ผู้บังคับใช้กฎหมายต้องศึกษาทำความเข้าใจเพื่อให้การสืบสวนสอบสวน และการดำเนินการต่างๆ เป็นไปในขอบเขตอำนาจ และถูกต้องชอบด้วยกฎหมาย

3.1 หลักทั่วไปในมาตรา 1–15

3.2 อำนาจพนักงานสอบสวนและอำนาจสืบสวนสอบสวน มาตรา 16-21

3.3 ความผิดที่มีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักร มาตรา 20

3.4 หมายเรียกและหมายอาญา มาตรา 52 – 70

3.5 การจับ ขัง ค้น และปล่อยชั่วคราว มาตรา 77 – 119 ทวิ

3.6 หลักทั่วไปในการสอบสวน มาตรา 120 – 129

3.7 การสอบสวนสามัญ มาตรา 130 – 147

3.8 หลักทั่วในการรับฟังพยานหลักฐาน มาตรา 226 – 227/1

3.9 พยานบุคคล มาตรา 232 – 237 ตรี

3.10 พยานเอกสาร มาตรา 238 – 240

3.11 พยานวัตถุ มาตรา 241 – 242

3.12 ผู้เชี่ยวชาญ มาตรา 243 – 244/1

4. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มีแนวคิดเพื่อรองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ เช่นการให้ความเท่าเทียมกันของข้อมูลอิเล็กทรอนิกส์ และเอกสารที่เป็นกระดาษ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 7 การรองรับวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ ฯลฯ หรือ วิธีการใช้ลายมือชื่ออิเล็กทรอนิกส์ ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 9 ตลอดจากการรับฟังพยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิกส์ เช่น การห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมาย ทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใด เพียงเพราะเหตุว่า เป็นข้อมูลอิเล็กทรอนิกส์ ... ในการชั่งน้ำหนักพยานหลักฐานว่าข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้น ให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้างเก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่ง

ข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง... ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 มาตรา 11

พระราชบัญญัติฉบับนี้ให้ใช้บังคับเพื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป (มาตรา2) กฎหมายฉบับนี้ประกาศราชกิจจานุเบกษา เล่ม 118 ตอนที่ 112 ก วันที่ 4 ธันวาคม 2544 มีผลบังคับใช้ตั้งแต่วันที่ 3 เมษายน 2545 ฉะนั้นการดำเนินคดีความผิดตามพระราชบัญญัติฉบับนี้ที่เหตุเกิดขึ้นก่อนวันที่กฎหมายมีผลบังคับใช้จึงไม่อาจกระทำได้เช่นกัน

5. พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547

พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มีส่วนเกี่ยวข้องกับความผิดเกี่ยวกับคอมพิวเตอร์ อยู่ในหมวดที่ 3 การสืบสวนและสอบสวนคดี

“มาตรา 25 ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใด ซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือส่งทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษ ซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดี ผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาพิจารณาถึงผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบกับเหตุผลและความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดที่เป็นคดีพิเศษ

2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวันโดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งสื่อสารตามคำสั่งดังกล่าวจะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลงไป อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนคดีพิเศษได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลข่าวสารที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดที่เป็นคดีพิเศษซึ่งได้รับอนุญาตตามวรรคหนึ่ง และให้ใช้ประโยชน์ในการ

สืบสวนหรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีพิเศษดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่ กคพ.กำหนด”

ซึ่งมาตรา 25 เป็นเรื่องการได้มาซึ่งข้อมูลข่าวสารที่ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่คดีพิเศษ ซึ่งเป็นเรื่องที่เกี่ยวข้องกับคอมพิวเตอร์ และนอกจากนั้น ได้มีกฎกระทรวงว่าด้วยการกำหนดคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ (ฉบับที่ 2) พ.ศ.2555 กำหนดให้คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เป็นคดีพิเศษเพิ่มเติมตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ พ.ศ.2547

6. พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556

เนื่องจากปัจจุบันประเทศไทยมีปัญหาเกี่ยวกับการประกอบอาชญากรรมที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติซึ่งส่งผลกระทบต่อความสงบเรียบร้อยและความมั่นคงของประเทศเป็นอย่างมาก แต่ปรากฏว่ากฎหมายที่มีอยู่ในปัจจุบันยังไม่สามารถใช้บังคับเพื่อดำเนินคดีกับการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติได้อย่างมีประสิทธิภาพ ประกอบกับประเทศไทยได้ลงนามในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร จึงสมควรกำหนดลักษณะความผิดให้ครอบคลุมการกระทำดังกล่าว รวมทั้งกำหนดวิธีการสืบสวน สอบสวนการกระทำความผิดดังกล่าวนั้นด้วย

คดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ผู้กระทำผิดเป็นได้ทั้งบุคคลธรรมดาทั่วไปและอาจทำในรูปแบบองค์กรอาชญากรรมข้ามชาติ ซึ่งในกรณีนี้เป็นการยากในการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน ซึ่งมีอยู่ทั้งในและต่างประเทศ ในพระราชบัญญัตินี้ได้บัญญัติวิธีการดำเนินการของเจ้าหน้าที่ผู้บังคับใช้กฎหมายไว้ คือ

มาตรา 17 ในกรณีที่มีเหตุอันควรเชื่อว่า เอกสารหรือข้อมูลข่าวสารซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือ สื่อทางเทคโนโลยีใด ถูกใช้หรืออาจถูกใช้ เพื่อให้ได้รับประโยชน์จากการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พนักงานสอบสวนซึ่งได้รับอนุมัติจากอัยการสูงสุด ผู้บัญชาการตำรวจแห่งชาติ หรือผู้ซึ่งได้รับมอบหมาย แล้วแต่กรณี อาจยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญาเพื่อมีคำสั่งอนุญาตให้ได้มาซึ่งเอกสารหรือข้อมูลข่าวสารดังกล่าวก็ได้

การอนุญาตตามวรรคหนึ่ง ให้พิจารณาผลกระทบต่อสิทธิส่วนบุคคลหรือสิทธิอื่นใดประกอบเหตุผล และความจำเป็นดังต่อไปนี้

1. มีเหตุอันควรเชื่อว่ามีการกระทำความผิดหรือจะมีการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

2. มีเหตุอันควรเชื่อว่าจะได้ข้อมูลข่าวสารเกี่ยวกับการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติจากการเข้าถึงข้อมูลข่าวสารดังกล่าว

3. ไม่อาจใช้วิธีการอื่นใดที่เหมาะสมหรือมีประสิทธิภาพมากกว่าได้

การอนุญาตตามวรรคหนึ่ง ให้อธิบดีผู้พิพากษาศาลอาญาสั่งอนุญาตได้คราวละไม่เกินเก้าสิบวัน โดยกำหนดเงื่อนไขใดๆ ก็ได้ และให้ผู้ที่เกี่ยวข้องกับข้อมูลข่าวสารในสิ่งที่สื่อสารตามคำสั่งดังกล่าว จะต้องให้ความร่วมมือเพื่อให้เป็นไปตามความในมาตรานี้ ภายหลังที่มีคำสั่งอนุญาต หากปรากฏข้อเท็จจริงว่าเหตุผลความจำเป็นไม่เป็นไปตามที่ระบุหรือพฤติการณ์เปลี่ยนแปลง อธิบดีผู้พิพากษาศาลอาญาอาจเปลี่ยนแปลงคำสั่งอนุญาตหรือขยายระยะเวลาอนุญาตได้ตามที่เห็นสมควร

เมื่อพนักงานสอบสวนได้ดำเนินการตามที่ได้รับอนุญาตแล้ว ให้รายงานการดำเนินการให้อธิบดีผู้พิพากษาศาลอาญาทราบ

บรรดาข้อมูลที่ได้มาตามวรรคหนึ่ง ให้เก็บรักษาเฉพาะข้อมูลข่าวสารเกี่ยวกับการกระทำความผิด ซึ่งได้รับอนุญาตตามวรรคหนึ่งและให้ใช้ประโยชน์ในการสืบสวน หรือใช้เป็นพยานหลักฐานเฉพาะในการดำเนินคดีดังกล่าวเท่านั้น ส่วนข้อมูลข่าวสารอื่นให้ทำลายเสียทั้งสิ้น ทั้งนี้ ตามข้อบังคับที่อัยการสูงสุดกำหนด

มาตรา 21 พนักงานสอบสวนหรือพนักงานเจ้าหน้าที่อาจใช้เครื่องมือสื่อสารโทรคมนาคม เครื่องมืออิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใด เฉพาะในการสะกดรอยผู้ต้องสงสัยว่ากระทำความผิด หรือจะกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ เพื่อสืบสวน จับกุม แสวงหา และรวบรวมพยานหลักฐาน ทั้งนี้ตามข้อบังคับที่อัยการสูงสุดกำหนด

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ. 2556 ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 26 มิถุนายน 2556 มีผลใช้บังคับเมื่อวันที่ 24 กันยายน 2556

7. พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535

โดยปกติพฤติการณ์การกระทำความผิดเกี่ยวกับคอมพิวเตอร์มักจะไม่เกิดขึ้นภายในประเทศใดประเทศหนึ่ง แต่จะเกิดขึ้นเกี่ยวพันเชื่อมโยงกันหลายประเทศ เนื่องจากผู้กระทำความผิดส่วนใหญ่มักจะกระทำโดยผ่านการเชื่อมโยงเครือข่ายอินเตอร์เน็ต ซึ่งมีสถานที่ที่เกี่ยวข้องเกินกว่าหนึ่งสถานที่ อาทิเช่น ความผิดฐานหมิ่นประมาททางอินเตอร์เน็ต จะมีสถานที่ที่เกี่ยวข้องกับการกระทำความผิดเกินกว่าหนึ่งสถานที่ กล่าวคือ จะมีสถานที่ที่ผู้กระทำความผิดได้ลงมือกระทำ สถานที่ที่ผู้เสียหายได้รับผลจากการกระทำ สถานที่ที่เป็นที่ตั้งของผู้ให้บริการอินเตอร์เน็ต และสถานที่ที่มีการส่งผ่านข้อความหมิ่นประมาท ซึ่งสถานที่ดังกล่าวอาจอยู่ในประเทศเดียวกันหรือหลายประเทศก็ได้ ซึ่งหากมีสถานที่ที่เกี่ยวข้องกับการกระทำความผิดอยู่ในหลายประเทศ ก็จะเกิดปัญหาตามมาในเรื่องของการรวบรวมพยานหลักฐาน เนื่องจากแต่ละประเทศจะมีเขตอำนาจ

อธิปไตยเป็นของตนเอง ดังนั้น เพื่อแก้ปัญหาการรวบรวมพยานหลักฐานซึ่งอยู่ในเขตอำนาจอธิปไตยของต่างประเทศ จึงได้มีการนำเอาพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 กฎกระทรวงที่ออกตามความในพระราชบัญญัติดังกล่าว และระเบียบของผู้ประสานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 พร้อมสนธิสัญญากับประเทศต่างๆ มาใช้เป็นเครื่องมือในการรวบรวม พยานหลักฐานซึ่งอยู่ในออำนาจของต่างประเทศให้ช่วยรวบรวมพยานหลักฐานแทน ซึ่งพนักงานอัยการที่ได้รับมอบหมายให้เข้าร่วมสอบสวน หรือได้รับมอบหมายให้เป็นพนักงานสอบสวนผู้รับผิดชอบ จำเป็นต้องดำเนินการตามขั้นตอน ดังนี้

7.1 หากดำเนินการสืบสวนแล้วทราบว่า มีพยานหลักฐานสำคัญอยู่ต่างประเทศและจำเป็นต้องขอความช่วยเหลือจากต่างประเทศ ให้เสนอคำขอต่ออัยการสูงสุดซึ่งเป็นผู้ประสานงานกลางตามพระราชบัญญัติดังกล่าว (มาตรา 36 ของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535)

7.2 คำขอความช่วยเหลือจากต่างประเทศ จะต้องทำคำแปลเป็นภาษาของประเทศผู้รับคำขอหรือภาษาอังกฤษที่รับรองความถูกต้อง โดยในกรณีที่ประเทศไทยไม่ได้ทำสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญากับประเทศผู้รับคำขอ จะต้องมีข้อความแสดงว่าจะให้ความช่วยเหลือในทำนองเดียวกันเมื่อประเทศผู้รับคำขอเป็นผู้ร้องขอ และอย่างน้อยจะต้องมีรายละเอียด คือ ชื่อของหน่วยงานในไทยที่ประสงค์จะขอความช่วยเหลือ ข้อเท็จจริงโดยสรุปของการกระทำความผิด บทกฎหมายที่เกี่ยวข้องกับการกระทำความผิด เรื่องที่ขอความช่วยเหลือ วัตถุประสงค์และความจำเป็นที่ต้องขอความช่วยเหลือ รวมถึงข้อมูลอื่นๆ ที่เป็นประโยชน์กับเจ้าหน้าที่ผู้มีอำนาจของต่างประเทศ เพื่อให้การดำเนินการตามคำร้องขอเป็นอย่างมีประสิทธิภาพ (มาตรา 37 ของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 ประกอบระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 17) อาทิเช่น

7.2.1 หากประสงค์จะให้สอบปากคำพยานที่อยู่ต่างประเทศ จะต้องระบุชื่อและที่อยู่ของบุคคลซึ่งเป็นพยาน และรายการข้อซักถามที่ประสงค์จะให้สอบปากคำ (ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 6)

7.2.2 หากประสงค์จะให้ช่วยส่งเอกสารที่อยู่ในความครอบครองของหน่วยงานของรัฐ ต้องระบุรายละเอียดเกี่ยวกับเอกสาร ชื่อหน่วยงานที่ครอบครองเอกสาร และความประสงค์ที่จะให้ดำเนินการเกี่ยวกับเอกสาร (ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความ

ช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 7)

7.2.3 หากประสงค์จะให้จัดส่งเอกสารทางกฎหมาย ต้องแนบเอกสารที่จะส่ง และระบุชื่อและที่อยู่ของบุคคลที่จะให้ส่งเอกสารให้ชัดเจน (ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 8)

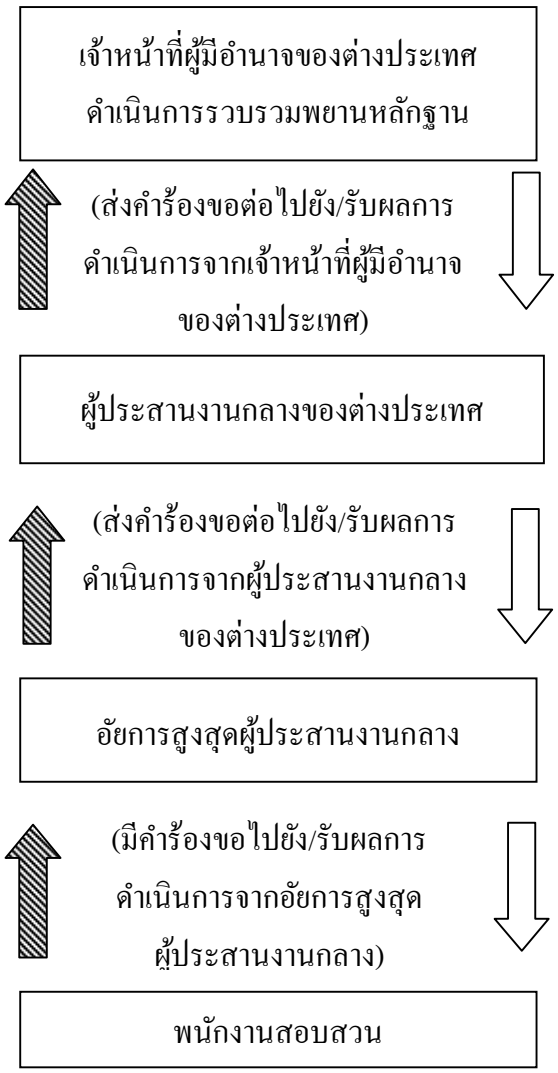
7.2.4 หากประสงค์จะให้ช่วยค้นและยึดสิ่งของซึ่งอยู่ในต่างประเทศ ต้องระบุข้อเท็จจริงหรือพยานหลักฐานอันเป็นเหตุออกหมายค้น สถานที่ที่สิ่งของนั้นอยู่ และระบุรูปพรรณของสิ่งของที่จะให้ยึด รวมทั้งความประสงค์ที่จะให้ดำเนินการกับสิ่งของ (ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 9)

7.2.5 หากประสงค์จะให้ช่วยสืบหาบุคคล ต้องระบุชื่อ รูปพรรณ และที่อยู่ของบุคคลดังกล่าว หรือสถานที่ที่มีเหตุอันควรเชื่อได้ว่าบุคคลนั้นอาศัยอยู่ รวมถึงความเกี่ยวพันของบุคคลดังกล่าวกับการสืบสวนสอบสวนในประเทศไทย (ระเบียบของผู้ประสานงานกลางว่าด้วยการให้ความช่วยเหลือและการขอความช่วยเหลือตามกฎหมายว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2537 ข้อ 11)

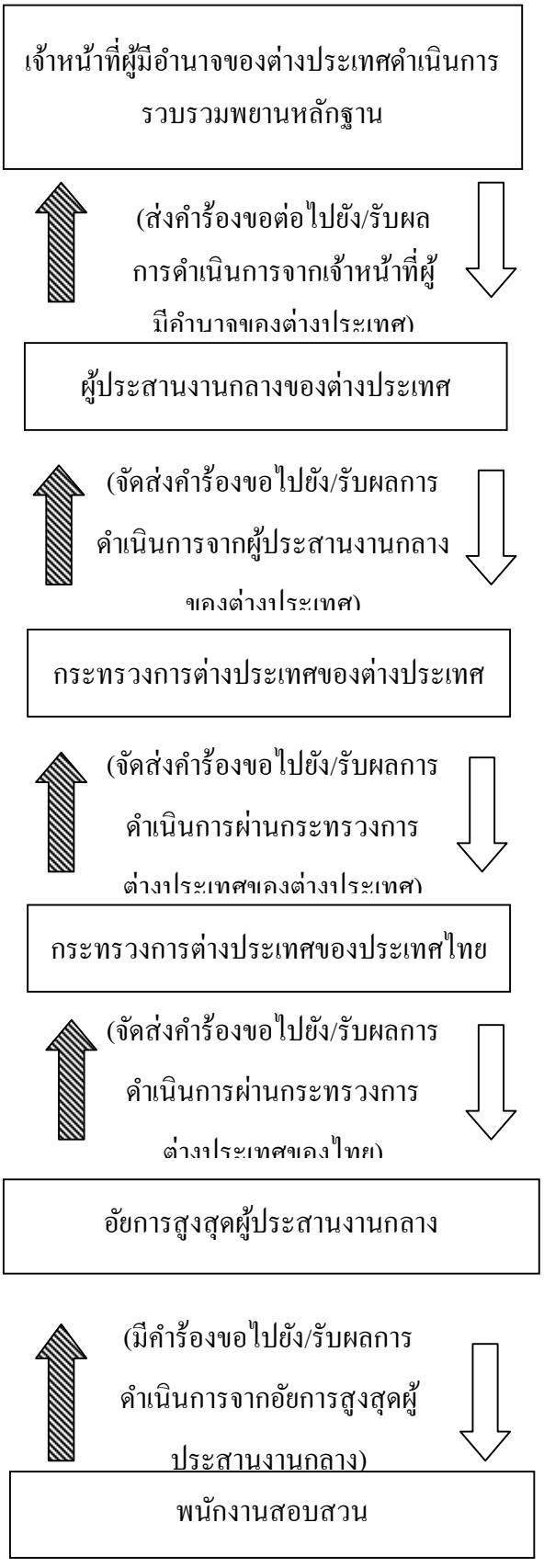
7.3 เมื่ออัยการสูงสุดผู้ประสานงานกลางได้รับคำขอแล้ว จะพิจารณาว่าควรจอความช่วยเหลือจากต่างประเทศหรือไม่โดยคำวินิจฉัยของผู้ประสานงานกลางให้ถือเป็นยุติ เว้นแต่นายกรัฐมนตรีจะมีคำสั่งเป็นอย่างอื่น ซึ่งหากอัยการสูงสุดผู้ประสานงานกลางพิจารณาแล้วเห็นว่าควรหรือไม่ควรขอความช่วยเหลือจากต่างประเทศ ก็จะแจ้งให้ผู้ขอทราบถึงข้อพิจารณาดังกล่าว (มาตรา 38 ของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535)

7.4 หากอัยการสูงสุดผู้ประสานงานกลางพิจารณาส่งคำขอความช่วยเหลือไปยังต่างประเทศขอให้ช่วยดำเนินการรวบรวมพยานหลักฐานที่อยู่ในประเทศดังกล่าว และเจ้าหน้าที่ของต่างประเทศได้ดำเนินการตามคำขอจนเป็นผลสำเร็จ พร้อมส่งพยานหลักฐานหรือเอกสารที่ได้ขอความช่วยเหลือ กลับมายังประเทศไทยอัยการสูงสุดผู้ประสานงานกลางก็จะส่งพยานหลักฐานหรือเอกสารดังกล่าวไปให้ผู้ขอนำไปเป็นพยานหลักฐานประกอบสำนวนการสอบสวนเพื่อพิจารณาดำเนินการต่อไป โดยพยานหลักฐานและเอกสารที่ได้มา ถือว่าเป็นพยานหลักฐานและเอกสารที่รับฟังได้ตามกฎหมาย (มาตรา 41 ของพระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535)

แผนภาพที่ 2 – 2 ผังการมีคำร้องขอความช่วยเหลือไปยังต่างประเทศ (กรณีมีสนธิสัญญา)



แผนภาพที่ 2 – 3 แผนผังการมีคำร้องขอความช่วยเหลือไปยังต่างประเทศ (กรณีไม่มีสนธิสัญญา)



นอกจากนี้แล้วหากผู้บังคับใช้กฎหมายได้รวบรวมพยานหลักฐานได้ปรากฏว่าผู้กระทำผิดได้หลบหนีไปต่างประเทศ ก็สามารถส่งเรื่องต่อผู้ประสานงานกลางให้ดำเนินการยื่นคำร้องขอไปยังประเทศที่รับคำร้องขอซึ่งมีหลักฐานแน่ชัดว่าผู้กระทำผิดหลบหนีไปอยู่ ณ ประเทศนั้น เพื่อให้ส่งผู้ร้ายข้ามแดนกลับมายังประเทศไทยเพื่อดำเนินคดีตามกฎหมาย ตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 ซึ่งมีข้อกำหนดหลักเกณฑ์และวิธีการปฏิบัติโดยเฉพาะ โดยสำนักงานอัยการสูงสุดเป็นผู้ดำเนินการ

หลักการพัฒนาผู้บังคับใช้กฎหมาย

ในการคัดเลือกเจ้าหน้าที่ผู้บังคับใช้กฎหมาย เพื่อให้สามารถทำงานได้อย่างประสิทธิภาพ ควรเลือกผู้ที่มีพื้นฐานความรู้ ความชำนาญ ที่เกี่ยวข้องกับคอมพิวเตอร์ เป็นผู้ที่รักการเรียนรู้อย่างต่อเนื่องตลอดเวลา เป็นผู้เสียสละ มุ่งมั่นในการทำงาน เป็นผู้มีมนุษย์สัมพันธ์ที่ดีสามารถทำงานร่วมกับผู้อื่นได้ดี

โดยการพัฒนาผู้บังคับใช้กฎหมายของหน่วยงานแต่ละแห่ง มีรูปแบบหลักสูตรเนื้อหาขึ้นอยู่กับบทบาทหน้าที่ งานที่รับผิดชอบ โดยเนื้อหาหลักสูตรประกอบด้วย

1. ฝึกอบรมด้านองค์ความรู้ในด้านกฎหมาย ระเบียบ ข้อบังคับ ต่างๆที่เกี่ยวข้องกับงาน

2. ฝึกอบรมเพื่อเสริมสร้างทักษะ เทคนิค ประสบการณ์ จากตัวอย่างคดีที่สำคัญ และต้องเรียนรู้เทคนิค โปรแกรม เทคโนโลยีใหม่ ตลอดเวลาเรียน

3. ฝึกการร่วมสืบสวนสอบสวนกับหน่วยงานอื่นๆ เพื่อให้ทำงานร่วมกันได้อย่างรวดเร็ว มีประสิทธิภาพ

4. ต้องอบรมเรื่องคุณธรรม จริยธรรม ของผู้บังคับใช้กฎหมายในการทำงาน ให้ทำงานด้วยความซื่อสัตย์ สุจริต ยุติธรรม ไม่ทุจริต รับสินบน ไม่ใช้อำนาจหน้าที่กลั่นแกล้งผู้อื่น

5. การศึกษาดูงานทั้งในและต่างประเทศ ซึ่งเป็นสิ่งจำเป็นนอกจากจะได้เรียนรู้วิทยาการใหม่ รูปแบบ แนวทางการทำงานของต่างๆ เพื่อนำมาปรับใช้ให้เหมาะสมแล้ว ยังได้แลกเปลี่ยนเรียนรู้ประสบการณ์ในการทำงานซึ่งกันและกัน สร้างช่องทางการติดต่อสื่อสารระหว่างกันรวมทั้งสร้างความสัมพันธ์ที่ดีต่อกันเพื่อประโยชน์ในการทำงานร่วมกันในอนาคต

บทที่ 3
วิธีการศึกษา

จากปัญหาที่ได้นำเสนอในบทที่ 1 ได้ไปสัมภาษณ์ผู้บริหารหน่วยงานที่ทำงานเกี่ยวข้องกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ในเรื่องของภารกิจองค์กร ขั้นตอนการทำงาน การประสาน งานกับหน่วยงานต่างๆ ปัญหาและอุปสรรคในการทำงาน จำนวนบุคลากรในองค์กรและการพัฒนา รวมทั้งแนวทางในการเตรียมพร้อมในการต่อสู้กับอาชญากรรมในอนาคต รวมทั้งข้อเสนอแนะ เพื่อเป็นข้อมูลในการศึกษาวิจัย ได้บทสรุปดังนี้

บทสัมภาษณ์ผู้บริหาร

1. พล.ต.ต.ศิริพงษ์ ติมุลา ผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.)

อำนาจหน้าที่ของหน่วยงาน มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์

กองกำกับการ 1 : การกระทำผิดที่มุ่งต่อระบบคอมพิวเตอร์เป็นเป้าหมาย

กองกำกับการ 2 : การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด

กองกำกับการ 3 : การนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์ สู่ระบบคอมพิวเตอร์ที่เป็นความผิด

กลุ่มงานสนับสนุนคดีเทคโนโลยี : ปฏิบัติการโต้ตอบในเชิงรุกโดยฉับพลันทางอินเตอร์เน็ต และสนับสนุนคดีเทคโนโลยี

ขั้นตอนการติดต่อราชการ

ถ้าเป็นการขอสำเนาบันทึกประจำวันคดี ระยะเวลาปฏิบัติ 30 นาที มีขั้นตอนดังนี้

1. ยื่นคำร้องขอคัดเสานำประจำวันต่อพนักงานสอบสวน
2. พนักงานสอบสวนมีความเห็นเสนอหัวหน้าสถานีหรือผู้รับมอบหมายพิจารณาอนุญาต
3. เมื่อหัวหน้าสถานี หรือผู้รับมอบหมาย มีความเห็นอนุญาต

4. เจ้าหน้าที่เสมียนคดีทำสำเนาประจำวันให้พนักงานสอบสวนรับรองสำเนาถูกต้องมอบให้กับผู้แจ้ง ถ้าเป็นการแจ้งความร้องทุกข์ ระยะเวลาปฏิบัติภายใน 2 ชั่วโมง (ไม่รวมระยะเวลากระบวนการสอบสวนซึ่งแล้วแต่ความซับซ้อนของคดี) มีขั้นตอนดังนี้

4.1 พบพนักงานสอบสวน เพื่อสอบถามรายละเอียดข้อเท็จจริงและสอบปากคำ

4.2 พนักงานสอบสวนมอบหลักฐานการแจ้งความร้องทุกข์

4.3 เจ้าหน้าที่เสมียนคดีประจำวันลงบันทึกประจำวัน (กรณียึดของกลาง) ภายใต้เงื่อนไขถ้าเป็นการถอนคำร้องทุกข์ ระยะเวลาปฏิบัติภายใน 2 ชั่วโมง (กรณีผู้ต้องหาไม่ถูกควบคุมตัวที่สถานีตำรวจ) ระยะเวลาปฏิบัติภายใน 3 ชั่วโมง (กรณีผู้ต้องหาถูกควบคุมตัวที่สถานีตำรวจ) มีขั้นตอนดังนี้

4.3.1 พบพนักงานสอบสวนเจ้าของคดี

4.3.2 พนักงานสอบสวนตรวจสอบเอกสารและสำเนาการสอบสวน

4.3.3 สอบปากคำผู้ขอถอนคำร้องทุกข์

4..3.4 ลงบันทึกประจำวันและลงลายมือชื่อในสมุดบัญชียึดและรักษาทรัพย์ (กรณียึดของกลาง)

ตารางที่ 3 – 1 สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี 2556 ของ บก.ปอท.

สถิติคดีอาญา	รับคำร้องทุกข์	รับเรื่องส่ง พงส. ท้องที่	รับเลขคดีอาญา	คดีเสร็จสิ้น	คดีคงค้าง	หมายเหตุ
มกราคม	72	21	12	12	0	
กุมภาพันธ์	62	18	7	7	0	
มีนาคม	88	13	6	6	0	
เมษายน	58	5	4	4	0	
พฤษภาคม	99	12	6	5	1	
มิถุนายน	121	10	2	2	0	
กรกฎาคม	120	15	1	1	0	
สิงหาคม	120	6	0	0	0	
กันยายน	125	20	2	2	0	
ตุลาคม	129	22	3	3	0	
พฤศจิกายน	121	9	5	5	0	
ธันวาคม	97	20	0	0	0	
รวม	1,212	171	48	47	1	

ที่มา : สรุปสถิติคดีอาญาเลขคดี/ร้องทุกข์ ปี 2556 ของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ตารางที่ 3 – 2 สรุปสถิติคดีอาญา เลขคดี/ร้องทุกข์ ปี 2557 ของ บก.ปอท.

สถิติคดีอาญา	รับคำร้องทุกข์	รับเรื่องส่ง พงส. ท้องที่	รับเลขคดีอาญา	คดีเสร็จสิ้น	คดีคงค้าง	หมายเหตุ
มกราคม	64	3	0	0	0	
กุมภาพันธ์	75	2	0	0	0	
มีนาคม	90	2	13	2	11	
เมษายน	115	23	13	5	8	
พฤษภาคม	151	13	3	3	0	
มิถุนายน	198	37	19	7	12	
กรกฎาคม	167	29	13	8	5	
สิงหาคม	187	36	12	4	8	
กันยายน	222	67	9	4	5	
ตุลาคม	227	57	38	1	37	
พฤศจิกายน	226	63	15	0	15	
ธันวาคม	149	25	14	0	14	
รวม	1,871	357	149	34	115	

ที่มา : สรุปสถิติคดีอาญาเลขคดี/ร้องทุกข์ ปี 2557 ของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

ช่องทางการติดต่อคดีที่จะมาถึง ปอท. มีทุกรูปแบบไม่ว่าจะเป็นการเดินเข้ามาแจ้งความทำเป็นหนังสือมาโดยตรง จะเป็นหนังสือ Email เพียงแต่ว่าระดับชั้นไหนที่จะถือว่าเป็นการร้องทุกข์โดยสมบูรณ์อันนี้ก็เป็นอีกเรื่องหนึ่ง จะโทรศัพท์เข้ามาแจ้งหรืออย่างอื่น ส่วนการตรวจสอบตำรวจจะเรียกเข้ามาหรือ Email หรือรับแจ้งเหตุ รับแจ้งเบาะแส หรือจะมาร้องทุกข์เองมีทุกรูปแบบ

ปอท. รับสำนวนมาจาก สน. ทั่วประเทศ ร้องขอให้สืบสวน สอบสวน มีทุกรูปแบบเป็นทั้งเอกสาร Walk in พูดถึงว่าถ้าเราลงตัวเลขจริงแบบว่าอยู่ดีๆ รับเรื่องร้องทุกข์เลย ทำเป็นสำนวนเลยนี้เยอะมาก เราจึงต้องมีการสืบสวนข้อเท็จจริงก่อน

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ต้องประสานงานกับหลายหน่วยงาน ทั้งภายใน ได้แก่ สำนักงานพิสูจน์หลักฐานกลาง กองปราบ สันติบาล หน่วยงานย่อยต่างๆ รวมถึงตำรวจที่อยู่ในท้องถิ่น ตำรวจนครบาล ตำรวจภูธรภาค 1

ถึงภาค 9 และภายนอกตำรวจ เช่น กระทรวงเทคโนโลยีสารสนเทศ (ICT) สำนักงานพัฒนาธุรกรรมทางอิเลคทรอนิกส์ (สพธอ.) หรือ ETDA และComputer Emergency Response team หน่วยย่อยของ สพทอ. คือหน่วยงานที่ดูแล Case เมื่อมีงานเข้ามา กรมสอบสวนคดีพิเศษ (DSI) สำนักงานนิติวิทยาศาสตร์ สำนักงานอัยการ

ส่วน กองปราบปรามอาชญากรรมทางเศรษฐกิจก็จะอยู่ในกองบัญชาการสอบสวนกลาง ทาง ปอท. จะทำงานอยู่ในลักษณะ 2 แบบ คือ

1. เป็นเจ้าภาพหลักในการดำเนินคดีที่เกี่ยวข้องในด้านนี้โดยตรง

2. เป็นหน่วยงานสนับสนุน จะว่าไปแล้วในเรื่องความรับผิดชอบถ้าจะเป็นหน่วยงานหลักเราต้องดูจากกฎกระทรวงในเรื่องของอำนาจ ขอบเขต ของ ปอท.

สำหรับคดีแบ่งเป็น 3 ประเภท ได้แก่

1. คดีที่คนร้ายก่ออาชญากรรมต่อข้อมูลคอมพิวเตอร์หรือระบบเป็นเป้าหมาย หรือเป็นเหยื่อ

2. คดีที่คนร้ายใช้คอมพิวเตอร์เป็นเครื่องมือในการประกอบอาชญากรรม

3. จะดูที่ข้อมูลถ้าอาชญากรได้นำข้อมูลอันเลวร้ายอันปรากฏอยู่ในมาตรา 14 อนุ 1-4 ข้อมูลปลอม เป็นเท็จ อันจะทำให้ประชาชนได้รับความเสียหาย ข้อมูลที่ก่อให้เกิดความตื่นตระหนกตกใจ ข้อมูลที่กระทบกระเทือนต่อความมั่นคงของราชอาณาจักร ข้อมูลลามก งานพวกนี้จะอยู่ในขอบข่ายงานของ ปอท. และในส่วนคดีอื่นๆ เช่น ลัก วิ่งราว ชิง ปล้น หรืออาชญากรรมทางเศรษฐกิจ คดีทางภาษี คดีศุลกากร คดีละเมิดลิขสิทธิ์ คนร้ายใช้คอมพิวเตอร์หรือมีพยานหลักฐานทางอิเล็กทรอนิกส์เป็นกุญแจสำคัญในคดีอันนี้อาจจะร้องขอให้ ปอท. เป็นหน่วยงานที่จะคอยช่วยสนับสนุนงานไม่ว่าจะเป็นการเข้าไปตรวจสอบสถานที่เกิดเหตุ การตรวจพิสูจน์หลักฐาน การวิเคราะห์ข้อมูลทางอิเลคทรอนิกส์

หน่วยงานภาคเอกชนก็จะมีอยู่ 2 แบบได้แก่ 1. เขาเป็นผู้เสียหาย 2. เราร้องขอให้เขามาช่วยอาจเป็นผู้ให้บริการ อาจเป็นการใช้อำนาจตามกฎหมายหรือเป็นการประสานงาน ร้องขอผู้ให้บริการอินเทอร์เน็ต ผู้ให้บริการโทรศัพท์เคลื่อนที่ รวมถึงภาคการเงิน เช่น ธนาคาร สถาบันทางการเงินในกรณีที่ต้องติดตามเส้นทางการเงินของอาชญากร

ด้านบุคลากร

จำนวนบุคลากรในองค์กรของ มีอัตรากรอบที่รัฐบาลให้มามีทั้งหมด 198 ตำแหน่ง แต่มีคนครองในตำแหน่ง 180 คน

จำนวนบุคลากรในองค์กรของ ปอท. ณ ตอนนี้กำลังขาดแคลน เพราะว่าขอบเขตอำนาจเรารับผิดชอบทั่วราชอาณาจักรทั่วไทย แต่มีบุคลากรแค่ 180 คนเอง เราขอขยายกรอบโครงสร้างใหม่และน่าจะมีบุคลากรประมาณ 500 คนถึงจะเหมาะสม สาเหตุก็เพราะว่าปริมาณงานที่

เพิ่มมากขึ้น ในข้อเท็จจริงทำไมคดีถึงเยอะเพราะปัจจุบันมีคดีพื้นๆ เช่น หลอกขายสินค้าทางอินเทอร์เน็ต การฉ้อโกง การนำเข้าข้อมูลเท็จ การหมิ่นประมาท ซึ่งตรงนี้มาแจ้งความกันเยอะ ถ้ามองแล้วระดับท้องที่น่าจะทำได้ ส่วนคดีที่ ปอท. น่าจะทำจริงๆ น่าจะเป็นคดีที่กระทำต่อระบบ Computer ข้อมูลทาง Computer หรือใช้ข้อมูลที่สลับซับซ้อน ปัญหาคือองค์ความรู้คือ ช่องว่างระหว่างตำรวจพื้นที่กับตำรวจที่ ปอท. ซึ่งคดีทางSocial media ตำรวจท้องที่น่าจะสืบสวนได้ แต่ทุกวันนี้ยังไม่มีศักยภาพเพียงพอ จึงทำให้คดีพวกนี้มากตกที่ ปอท. จนกลายเป็นคดีที่มีมากที่สุดใน ปอท.ทั้งที่จริงแล้ว ปอท.น่าจะทำคดีที่สำคัญและใช้ความเชี่ยวชาญมากกว่านั้น เช่น การเจาะระบบ อาชญากรรมข้ามชาติ ฉ้อโกง องค์กรอาชญากรรม

วุฒิการศึกษาทั่วไปคือ ปริญญาตรี ณ ตอนนี้ยังไม่ได้กำหนดสาขาวิชา แต่ในปัจจุบันส่วนมากจะมีคุณวุฒิในด้านสังคมศาสตร์ นิติศาสตร์ รัฐศาสตร์ และก็นักเรียนนายร้อยตำรวจ

การพัฒนาบุคลกรหลักๆ คือ ความรู้เบื้องต้นเกี่ยวกับคอมพิวเตอร์และอินเทอร์เน็ต, การสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี, การตรวจพิสูจน์หลักฐานทางอิเลคทรอนิกส์ ส่วนเรื่องงานเราก็จะมีการจัดฝึกอบรมหลักสูตรมาตรฐานของ Interpol , Train the Trainer for Investigation (TTI) , Trainer for Computer Forensic (TTF) และมีการจัดฝึกอบรมภายในหน่วยงานเอง มีการส่งไปเรียนต่างประเทศ

การศึกษาดูงานต่างประเทศทาง ปอท. ก็ส่งบุคลากรไปอบรมกับ Interpol, FBI หลักๆ เป็นการเวียนกันจัด เช่น ญี่ปุ่น เกาหลี ฮ่องกงและฮ่องกงเป็นศูนย์กลางหลักในการอบรมในส่วนของ Cyber crime และ Interpol เป็นหน่วยงานที่คอยติดต่อประสานงาน เชิญประเทศสมาชิก ในการจัดงานการฝึกอบรม โดยใช้งบประมาณของ ปอท. เอง และ ปอท. ก็ได้รับการสนับสนุนจากกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) อยู่ในงบเจรจาระหว่างประเทศปีละประมาณสามล้านบาท

การฝึกอบรมของเราจะหมุนเวียนกันไปโดยเฉลี่ยละปี 3 ครั้ง/ปี ปอท. เน้นเรื่องนี้เพราะเป็นยุทธศาสตร์ ตำรวจอาเซียนเขาจะให้ประเทศสิงค์โปรเป็นผู้นำในการพัฒนาในด้านการสืบสวนสอบสวนธุรกรรมทาง Cyber เขาชู Road map ของการเพิ่มศักยภาพของผู้บังคับใช้กฎหมายเป็นหลัก เนื่องจากว่าในภูมิภาคนี้มันไม่ใช่แค่ว่าคนรู้หรือไม่รู้อย่างเดียวแต่ต้องรู้ตัวกฎหมาย Know how เทคโนโลยีต่างๆเขาต้องพยายามอัพเดทประเทศสมาชิกให้เท่ากัน

หลักการเรียนรู้ ผมได้สอนน้องมีสองแบบคือ หลักของความรู้อีกกี่ร้อยปีสิ่งที่เป็นหลักการพิสูจน์ก็ยังไม่เปลี่ยนต้องเอาตรงนี้ให้ได้ แต่ Application ใหม่ ถ้ารู้หลักการแล้วการเปลี่ยน Application ไม่มีปัญหาเพียงแต่เราไปเรียนรู้เพิ่มเติมอีก แต่หลักการคิดเป็นหลักการเดียวกัน ต่อให้เป็นเครื่อง MAX , Smartphone หลักเดียวกัน ถ้าเราเก่งหลักการแล้วการที่เราจะไปเรียนรู้เพิ่มเติมก็ง่ายขึ้น

กับมหาวิทยาลัย ไม่ติดต่อโดยตรงมีลักษณะการติดต่อประสานงานอยู่ 2 แบบ คือ เชิญเป็นที่ปรึกษาในโครงการหรือปรึกษาในด้านเทคนิค Know how หรือสิ่งที่อาชญากรเขารู้และหาแนวทางป้องกัน ส่วนมากจะเป็นด้านที่ปรึกษา

ปัญหาและอุปสรรคในการทำงาน

ด้านปริมาณบุคลากร เจ้าหน้าที่ผู้เชี่ยวชาญ ตอนนี้ ปอท. ยังมีปริมาณที่น้อย ยังไม่เพียงพอเมื่อเทียบกับปริมาณงาน และการสร้างคนให้มีความรู้ในด้านนี้ทำได้ยาก อีกอย่างเขาจะมองที่สิ่งจูงใจในการทำงาน เช่น ค่าตอบแทนเราก็ให้ได้แค่อัตราเงินเดือนราชการ เขาก็จะไปทำงานที่อื่นที่ได้เงินเดือนเยอะกว่า คนเก่งเอกชนซื้อตัวไปตั้งแต่ยังเรียนไม่จบก็มี ขณะเดียวกันแหล่งผลิตบุคลากรภายในประเทศเองก็มีน้อยด้านวิทยาศาสตร์คอมพิวเตอร์

ด้านงบประมาณ ปอท. ไม่ขาดแคลนเลย เราได้งบลงทุน งบดำเนินงาน งบบุคลากรจากทาง ICT ทั้งหมด เพราะส่วนมากงานที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ทาง ICT ก็จะส่งงานมาให้ทางนี้ทั้งหมด ดังนั้น ICT จึงต้องสนับสนุนงบประมาณมาทางนี้เยอะ

ด้านอุปกรณ์ เครื่องมือทางเทคโนโลยีที่ใช้ ก็ไม่มีปัญหา

การบริหารจัดการด้านการบริหารทรัพยากรบุคคล ในเรื่องการโยกย้าย เลื่อนขั้น เลื่อนตำแหน่ง

ปอท. มีอัตราการผลัดเปลี่ยนหมุนเวียนบุคลากรในหน่วยงานสูง คือแบบว่าพอรับการแต่งตั้ง 1-2 ปีก็มีการโยกย้าย ดังนั้นคนมาใหม่ก็ต้องมานับหนึ่งใหม่ทำให้เกิดระยะเวลาที่ต้องมีการเรียนรู้ใหม่ อันนี้มันเกิดจากโครงสร้างของตำรวจ อันนี้คือปัญหา

แบบว่าคนที่มีความเชี่ยวชาญในด้านนี้แล้วให้ปฏิบัติงานตรงนี้ตลอดแล้วมีการให้ค่าตอบแทนพิเศษ ตรงนี้ไม่มี ไม่มีแท่งของผู้เชี่ยวชาญ

ปัญหาการติดต่อประสานงานกับหน่วยงานอื่นไม่มีปัญหาอะไร หรือมีก็เป็นปัญหาของราชการเท่านั้นเอง

แนวทางการทำงานในอนาคตในการต่อสู้กับ Cyber crime

เนื่องจากเทคโนโลยี โดยเฉพาะคอมพิวเตอร์อยู่ในเกณฑ์การเจริญเติบโตตามกฎของมัวร์ ที่ว่าด้วยความเร็วของ CPU จะเป็นสองเท่าภายใน 18 – 24 เดือนเสมอ กฎตรงนี้จะบอกวิสัยทัศน์ของโลกใบนี้ บอกว่าเทคโนโลยีทางคอมพิวเตอร์จะถูกลงไปเรื่อยๆ และเล็กลงไปเรื่อยๆ จึงเข้ามาใกล้ชิดกับการดำเนินชีวิตของคนมากขึ้น เช่น อยู่ในเสื้อ เข็มขัด รองเท้า มนุษย์ทุกคนจะได้สัมผัส ได้ใช้ประโยชน์ ระบบอินเทอร์เน็ตถูกและเร็วคนก็ใช้งานกันมากขึ้น ฉะนั้นวิถีชีวิตคนเราก็จะพึ่งพาการใช้ระบบทางเทคโนโลยีมากขึ้น ฉะนั้นนอกจาก Service แล้ว ยังต้องเกี่ยวกับสังคม ก็จะมีอาชญากรรม ผู้ไม่หวังดีใช้ช่องทางนี้ทำประโยชน์ให้กับตัวเองด้านการทุจริต ฉ้อฉลต่อประชาชน

แนวโน้มอาชญากรรมด้านนี้มีปริมาณสูงแน่นอน แล้วเทรนด้านนี้จะเป็นไง ในด้าน Service ด้านการกระจาย การประเมินผลที่เรียกว่า Crime computing ที่เรียกว่า Computer มากกว่า 1 เครื่องช่วยกันที่จะทำงานนอกจากตัวเองที่ทำงานเร็วขึ้นแล้ว การ Service หรือการประเมินผลก็ยิ่งเร็วขึ้นอีก ฉะนั้นปัญหาเรื่องร่องรอยหลักฐานก็จะเกิดขึ้นในหลายๆ จุด ไม่จำกัดเฉพาะในประเทศไทย อาจมีผู้เสียหายอยู่ในประเทศไทย คนร้ายอาจใช้คอมพิวเตอร์จากต่างประเทศก็ได้ แต่คนร้ายที่นั่งอยู่โต๊ะทำงานอาจจะอยู่อีกประเทศก็ได้ จะเห็นว่าร่องรอยหลักฐานจะมีมากขึ้น ถ้าถามว่า Trend การใช้เทคโนโลยีนี้มุ่งหน้าไปทางไหน ที่เรียกว่าเป็น Lead ตัวการใช้จ่าย การทำธุรกรรมทางการเงิน การค้าขาย การชำระสินค้าและบริการทางอิเล็กทรอนิกส์ จะมีมากขึ้น และผลิตภัณฑ์ต่างๆ นานาใครที่ตกเทรน ไม่สามรถที่จะ ปรับกลยุทธ์ทางธุรกิจเข้าสู่กรอบ Mobile payment ได้ก็ถือว่าว่าตดยุคไม่ทันสมัย เช่น ที่ Samsung ประกาศวิสัยทัศน์ว่าภายในอีก 8 – 10 ปีข้างหน้า ทุกอย่างต้องเป็น Internet of everything ตัว Computer internet ไม่จำกัดแค่ตัว Smartphone, tablet รวมไปถึงเครื่องใช้ไฟฟ้าทุกอย่าง ตู้เย็น หม้อหุงข้าว เตารีด ฯลฯ จะเห็นว่าสภาพแวดล้อมทางเทคโนโลยีเราเพิ่มมากขึ้น แล้วแนวทางเตรียมรับมือกับ Cyber crime อย่างไรคงต้องมองที่ Product ในระดับประเทศต้องเปลี่ยนนโยบายทางการรักษาความปลอดภัย Cyber ระดับนโยบาย ระดับปฏิบัติงานนี้ทุกภาคส่วนของรัฐก็ต้องกระตุ้นตัวเองเพื่อรองรับต่อสิ่งใหม่ ในส่วนของ ปอท. นอกจากที่จะติดตามเทคโนโลยีและความรู้ในการป้องกันและปราบปรามอาชญากรรมอยู่เสมอแล้ว ก็ต้องรู้จักแสวงหาพาคี ที่จะต้องถ่ายออกนอกประเทศมากขึ้น ผู้ช่วยของเราต้องสร้างเครือข่ายให้มากยิ่งขึ้นทั้งภายในประเทศและต่างประเทศและจะต้องเตรียมฐานข้อมูลเพื่อการจัดการด้านการป้องกันและปราบปรามให้ดียิ่งขึ้น

ฐานข้อมูลเกี่ยวกับอาชญากรรม

ทุกอย่างครับ ไม่ว่าจะเป็นตัวบุคคล แผนธุรกรรม บัญชี Blacklist , Know how หรือรูปแบบโปรแกรมไวรัส ที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีทุกประเภท และก็พยายามผลักดันการขยายโครงสร้างของสำนักงาน และที่สำคัญอยู่ที่การป้องกันภัยของประชาชน ภาคเอกชน ภาครัฐ ให้มีภูมิคุ้มกันที่ดีด้วย โอกาสของความเสี่ยงที่จะได้รับผลร้ายจากอาชญากรรมก็จะน้อยลง เราต้องให้ความรู้แก่ประชาชน เตือนสติ ทุกแนวทางไม่ว่าจะเป็นตัวเครื่อง ตัวคน ตัวระบบ ตัวผลิตภัณฑ์ในทุกมิติ ทุกด้าน

ข้อเสนอแนะ

เราทำงานมาจนตกผลึกว่าสิ่งที่จะพิสูจน์ว่าเป็นความผิด/ถูกของคนร้าย/จำเลย พยานหลักฐานก็จะอยู่ในเครื่องของคนร้ายเอง อยู่กับระบบอินเตอร์เน็ต ฯลฯ อาจจะอยู่ที่ต้นทางคือเครื่องผู้ร้าย กลางทางคือตัวระบบผู้ให้บริการ และปลายทางเครื่องของผู้เสียหายของในประเทศ/ต่างประเทศ จุดอ่อนและข้อด้อยของเราคือโครงสร้างพื้นฐานทางอินเตอร์เน็ตของเราไม่มีระบบ

กล้องวงจรปิดที่อยู่กลางทางเราไม่สามารถเข้าไปตรวจสอบ สกัดกั้นหรือตั้งด้านตรวจสอบได้เลย ซึ่งไม่เหมือนกับต่างประเทศหรือประเทศที่เจริญแล้วที่เขามีระบบนี้ ถ้าเปรียบเทียบก็เป็นเหมือนระบบตรวจคนเข้าเมือง ประเทศอื่นมีหมดแล้วแต่ไทยยังไม่มี มีแต่กฎหมายที่บังคับให้ผู้ให้บริการเก็บข้อมูลจราจรระบบ เพื่อพิสูจน์ว่าผู้ใช้บริการเป็นใคร ซึ่งเป็นแค่กฎหมาย ในทางปฏิบัติตัวระบบตรงนี้ไม่มี รัฐไม่ได้บังคับให้เขาต้องมีเหมือนกับว่าใครจะใช้บริการต้องมีการติดกล้องวงจรปิดนะตรงนี้ไม่มี เพราะฉะนั้นข้อเสนอในเชิงนโยบายรัฐก็จะต้องมองถึงกรอบนโยบายระดับชาติ อันนี้ที่ว่า พ.ร.บ.รักษาความปลอดภัยทางไซเบอร์ เห็นด้วยว่าควรต้องมีส่วน ในทางปฏิบัติรัฐควรต้องมีหน่วยงานมาดูแลตรงส่วนนี้ จะเห็นได้ว่าบ้านเราจะเกิดอาชญากรรมด้านนี้จำนวนมากแต่จับกุมได้น้อย เพราะร่องรอยการกระทำผิดหายไป ระบบการตรวจสอบก็ไม่มี เป็นหลักการที่รัฐต้องดูข้อมูลเข้าถึงได้ถ้ามีความจำเป็น เพื่อความมั่นคงของรัฐ เช่น เรื่องยาเสพติด การก่อการร้าย

หน่วยงานนี้จะขึ้นกับ ICT ก็ได้ หน่วยนี้ไม่ต้องทำคดีแต่คอยเป็นกรรมการกลางประสาน งาน ตำรวจร้องขอดู Facebook ดูการจราจรของFacebook ที่หมิ่นสถาบัน มีข้อมูลอะไรบ้าง เขาเป็นใคร อยู่ที่ไหน อะไรประมาณนี้ Lawful Interception (คือการได้มาซึ่งข้อมูลการสื่อสารผ่านเครือข่าย ดำเนินการโดยพนักงานตามกฎหมายเพื่อวิเคราะห์หรือพิสูจน์หลักฐาน) เป็นหน่วยงานกลาง แต่จะให้ใครทำก็ขึ้นอยู่กับรัฐจะไว้ใจใครหรือหน่วยงานไหนทำโครงสร้างอย่างไร ขออย่างเดียวข้อเสนอเชิงนโยบายให้ครอบคลุม

แล้วรัฐก็จะต้องกระตุ้นที่จะสร้าง Digital Citizen ให้คนไทยเรื่องการใช้งานอินเตอร์เน็ต คอมพิวเตอร์ ก็จะต้องมีหลักสูตรหรือมีการอบรมการใช้งานอินเตอร์เน็ตที่ถูกต้อง ที่มีจริยธรรมเป็นอย่างไร ต้องอยู่ในแบบเรียน เพราะทุกวันนี้บ้านเราเหมือนกับคนป่าใส่สูทไม่รู้อะไร เช่น ประเทศที่เจริญแล้วเขาจะเลือกเสพอะไร เขาต้องทำอะไรต่อไป เช่น หนังโป๊ อย่างประเทศไทยดูหนังโป๊แล้วก็ก่ออาชญากรรมทางเพศไปข่มขืน ลองดูสถิติได้เลยว่าบ้านเขาไม่ค่อยมีการก่ออาชญากรรมทางเพศ เพราะเขาเป็นผู้ใหญ่พอจะเลือกเสพ เลือกผิด เลือกถูกได้ แต่บ้านเรานี้อยู่ที่การศึกษา

ต้องมีการเรียนด้านจริยธรรม Cyber Ethic ต้องเรียนรู้การป้องกันและก็การระวังตัวทาง Cyber ว่าเราจะต้องไม่เปิดเผยข้อมูลส่วนตัวกับคนแปลกหน้าหรือเอาข้อมูลของเราไปลงประกาศให้คนทั่วไปรู้ เช่น การถ่ายบัตรประจำตัวประชาชน หรือ สำเนาเงินฝาก ซึ่งเป็นข้อมูลส่วนตัว และก็การหาคู่ใน Facebook ก็มีมาก การถ่ายรูปไว้ขู่กรรโชกทรัพย์ เราต้องสอนให้ความรู้และยิ่งบริบททางสังคมเราตอนนี้ใกล้ชิดกับเทคโนโลยีมาก ความคิด ความอ่านถูกชี้นำ ถูกครอบงำให้หลงเชื่อง่ายผ่านโลกของ Cyber สูงมาก

เรื่องเกี่ยวกับกฎหมายอันดับแรก เจ้าหน้าที่ทุกคนจะต้องมีความรู้ในกระบวนการยุติธรรมต้องสมมาตรกัน จะต้องเข้าใจข้อเท็จจริงทางเทคโนโลยี เช่น Google ไม่มีคนมาแจ้งความว่าหาชื่อเขาใน Google แล้วด่าทุกวัน อย่างนี้เราเรียกว่าไม่เข้าใจทางเทคโนโลยี หรือ ไปแจ้งความกับ ISP ว่า ISP เป็นตัวการเป็นตัวการที่ให้การสนับสนุนเว็บโป๊หารู้ไม่ว่าเป็นเพียงแค่ท่อหรือถนนที่เป็นทางผ่านเฉยๆ อย่างนี้เราเรียกว่าต้องเข้าใจเทคโนโลยี เข้าใจบริบททางเทคโนโลยี ทั้งบริบทและข้อเท็จจริงบุคคลที่อยู่ในกระบวนการไม่ว่าจะเป็นตำรวจ อัยการ ศาล ท่านเข้าใจโลกเสมือนท่านเข้าใจพรมแดนระหว่าง Cyber และกายภาพแล้วหรือยัง ฉะนั้นถ้าดูตามสารบัญญัติที่บัญญัติตั้งแต่มาตรา 5 ถึงมาตรา 16 จะเห็นว่ากายภาพผู้ใดเข้าถึง ผู้ใดทำลาย ผู้ได้ทำให้เปลี่ยนแปลง นี่คือจะต้องเป็น Digital Way จะต้องเป็นกริยาการเกิดจาก Digital Context เท่านั้น คือ จะต้องกระทำในรูปแบบอิเล็กทรอนิกส์เท่านั้น พ.ร.บ. นี้ไม่ได้พูดถึงการกระทำทางกายภาพ เป็นการเข้าถึงแบบเทคนิค ถ้าศาลท่านไม่เข้าใจตรงนี้ว่าเข้าถึงอะไรก็จะทำให้การวินิจฉัย พยานในศาล การชั่งน้ำหนักพยานหลักฐาน หรือการวินิจฉัยผิดพลาดไป ฉะนั้นบุคลากรที่อยู่ในกระบวนการยุติธรรมจะต้องเข้าใจ รู้เท่าเทียมกัน ถ้าตำรวจรู้ดีกว่าถ้าพูดข้อเท็จจริงที่เป็นเทคนิค ถ้าอัยการเข้าใจเหมือนกัน ศาลเข้าใจเหมือนกันก็ไม่ต้องไปให้ผู้เชี่ยวชาญมาตีความหรือมาทำงานช่วย คือ การเข้าใจข้อเท็จจริงที่ตรงกัน การสื่อสารก็จะตรงกัน เราจะทำอย่างไรให้คนในกระบวนการยุติธรรมมีความรู้ที่เท่าเทียมกันทั้งระบบ ศาลก็อาจมีผู้เชี่ยวชาญด้านคอมพิวเตอร์โดยเฉพาะ อัยการก็ต้องมีผู้เชี่ยวชาญด้านนี้โดยเฉพาะ โลกเราจะแคบลงมาเป็นโลกของเทคโนโลยีทั้งหมด ตัวเราก็จะอยู่ในระบบDigital แล้วเราจะเรียกว่าอภิสัญลักษณ์ เอาทุกอย่างมาลงใน Digital เช่น DNA มาลงในข้อมูลของเลขบัตรประจำตัวประชาชน 13 หลัก จะกลายเป็น Digital ทั้งหมด

2. พันตำรวจตรี สุริยา สิงหกมล ผู้บัญชาการสำนักคดีเทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ

อำนาจหน้าที่ของหน่วยงาน

1. ปฏิบัติงานด้านการป้องกัน การปราบปราม การสืบสวน และการสอบสวนคดีพิเศษเพื่อดำเนินคดีกับผู้กระทำความผิดเกี่ยวกับเทคโนโลยีและสารสนเทศ หรือตามที่อธิบดีมอบหมาย รวมทั้งดำเนินคดีพิเศษนอกราชอาณาจักรตามที่ได้รับมอบหมาย

2. ปฏิบัติงานวิเคราะห์และพิสูจน์ความผิดที่อยู่ในความรับผิดชอบ

3. ดำเนินการรวบรวม ศึกษา จัดระบบ และวิเคราะห์ข้อมูลการข่าว วางแผนงานบริหารจัดการและประสานงานเพื่อการป้องกัน การปราบปราม การสืบสวน และการสอบสวนคดีพิเศษที่อยู่ในความรับผิดชอบ

4. ปฏิบัติงานด้านการป้องกัน การปราบปราม การสืบสวน และการสอบสวนผู้กระทำความผิดในคดีอื่นตามที่ได้รับมอบหมาย

5. ดำเนินการเกี่ยวกับการเก็บรักษาพยานหลักฐานและของกลางในคดี

6. ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

ปริมาณงานปี 2557

1. คดีพิเศษ จำนวน 6 คดี ดำเนินการแล้วเสร็จ จำนวน 2 คดี

2. เรื่องสืบสวน จำนวน 14 เรื่อง ดำเนินการแล้วเสร็จ จำนวน 1 เรื่อง

3. เรื่องตรวจสอบข้อเท็จจริง จำนวน 16 เรื่อง ดำเนินการแล้วเสร็จ จำนวน 1 เรื่อง

หน้าที่หลักของสำนักคือ ความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และเป็นคดีที่อยู่ท้ายพ.ร.บ. การสอบสวนคดีพิเศษ พ.ศ.2547 ด้วย เดิมมีลักษณะเป็นเกณฑ์ว่าอยู่ในระดับไหนถึงจะเป็นคดีพิเศษ เช่น ถ้าเป็นการฉ้อโกงประชาชนและเผยแพร่ทางอินเตอร์เน็ทมูลค่าประมาณ 50 ล้านขึ้น แต่ปัจจุบันเราไม่ได้นำเกณฑ์นั้นมาใช้แล้ว โดยให้อธิบดีใช้ดุลพินิจว่ากรณีใดบ้างสมควรเป็นกรณีพิเศษ อาจจะไม่ได้มีลักษณะเป็นผู้เสียหายจำนวนคนเข้ามาจับ แต่อาจใช้ปริมาณความเสียหายอาจจะน้อยราย 5 ราย 10 ราย แต่มูลค่าความเสียหายมาก อธิบดีก็จะใช้ดุลยพินิจตรงนี้เป็นเกณฑ์การพิจารณาให้เป็นคดีพิเศษ

การรับคดีของสำนักฯ มีสองกรณี คือ กรณีที่ไปแจ้งความที่สถานีตำรวจ จากนั้นส่งต่อมาทางนี้เพราะเห็นว่าสถานีตำรวจไม่สามารถทำคดีได้ หรือไปแจ้งที่ ปอท. (กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี) ซึ่งก็มีปัญหาอีกว่าเรื่องจะเข้าช่องทางไหน ก็เลยแยกกันไม่ออกว่าตำรวจกับกรมสอบสวนคดีพิเศษ หรือ DSI แบ่งกันตรงไหน ปัจจุบันก็ยังทำกันอย่างนี้อยู่ จึงทำให้ผู้รับบริการหรือชาวบ้านยังเกิดความสับสนว่าเรื่องอย่างนี้จะไปแจ้งเรื่องที่ใคร ตำรวจเองก็สับสน เลยเป็นเรื่องของดุลยพินิจของแต่ละคน ใครที่รับเรื่องจากประชาชนก็ต้องใช้ดุลยพินิจของตัวเองว่าเรื่องอย่างนี้เรารับได้หรือไม่หรือตำรวจเองก็มีปัญหา เช่น ตำรวจพื้นที่ กับ ตำรวจ ปอท. ทุกวันนี้ที่มีปัญหาตำรวจพื้นที่ก็ไม่รับ เขาบอกว่าเนื่องจากมีกองบังคับการปราบปรามทางเทคโนโลยีขึ้นมาโดยเฉพาะ คุณต้องไปแจ้งที่ ปอท. ทุกวันนี้ ปอท. จึงมีคดีมาก อันนี้คือเฉพาะตำรวจ กรมสอบสวนคดีพิเศษ จึงต้องปรับใหม่คือต้องให้ผู้รับบริการรู้ว่าเรื่องอย่างนี้ต้องไปแจ้งที่หน่วยไหน ก็เลยต้องกำหนดหลักเกณฑ์ขึ้นใหม่ คือว่าคดีลักษณะไหนถึงเป็นคดีพิเศษเดิมจะพูดกว้าง มีความซับซ้อน แต่ยังไม่เป็นรูปธรรม แต่ตอนนี้กำลังดำเนินการจัดทำหลักเกณฑ์ใหม่อยู่

การสอบสวนคดีหนึ่งๆ โดยเฉลี่ยเรื่องระยะเวลาจะไม่แน่นอนขึ้นอยู่กับความยากง่ายของคดีถ้าเป็นคดีที่มีผู้เจาะระบบข้อมูลที่เรารับทำก็อยู่ในเกณฑ์เฉลี่ยสองปี อันนี้ถือว่าเป็นคดีที่มีความยุ่งยาก แต่คดีที่ง่ายมากกว่านั้นก็จะใช้เวลาประมาณหนึ่งปี แต่มีคดีที่พิเศษมากๆ คือการติดตามตัวผู้ต้องหาอยู่ต่างประเทศก็จะใช้ระยะเวลาการดำเนินงานนานพอสมควร

การขอความร่วมมือระหว่างประเทศทางอาญา กำหนดให้เป็นสำนักกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ คือ ทุกคดีที่เกี่ยวกับการประสานงานระหว่าประเทศ และการส่งผู้ร้ายข้ามแดน ก็ต้องไปติดต่อกับสำนักงานกิจการต่างประเทศและคดีอาชญากรรมระหว่างประเทศ เพราะฉะนั้นจะมีเรื่องที่เกี่ยวกับสองสำนักงานละ ซึ่งถ้าเกิดปัญหาและอุปสรรคมากๆ ตรงนั้นเขาจะมีคนรวบรวมและต้องผ่านสำนักงานอัยการสูงสุดด้วย คดีที่ต้องประสานงานกับต่างประเทศเราจะกำหนดระยะเวลาไม่ได้เลย

ทางเราต้องทำงานติดต่อกับหน่วยงานทั้งภาครัฐและภาคเอกชน ทางภาครัฐก็ได้แก่ ตำรวจ อัยการ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กองพิสูจน์หลักฐาน สำนักงานตำรวจแห่งชาติ สถาบันนิติเวชวิทยาศาสตร์ และล่าสุดก็ได้ไปประสานกับทาง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ ETDA ซึ่งมีห้องตรวจพิสูจน์พยานหลักฐานทางด้าน Digital ซึ่งเราก็ได้ประสานและเอางานของเราไปให้เขาช่วยทำผลที่ได้รับก็เป็นผลดี

ในการส่งพยานไปตรวจพิสูจน์ ถ้าเป็นสำนักงานตำรวจแห่งชาติก็จะมีระเบียบภายในว่าต้องส่งกองพิสูจน์หลักฐานเป็นหลัก แต่กรมสอบสวนคดีพิเศษไม่มีหลักเกณฑ์หรือข้อกำหนดที่แน่นอนชัดเจนว่าจะส่งที่ไหน ดังนั้นดุลยพินิจของเราเองก็จะมองของเราเองเป็นหลักไว้ก่อน แล้วถ้านอกเหนือจากขีดความสามารถที่เราจะทำได้ เราก็จะดูหน่วยงานอื่นซึ่งมีความน่าเชื่อถือ สิ่งที่เราคำนึงว่าจะถูกตีในชั้นศาลเราก็เลยหาหน่วยงานที่เป็นกลางและมีความน่าเชื่อถือไม่อยู่ฝ่ายใดฝ่ายหนึ่งเข้ามาช่วย เพราะฉะนั้น สิ่งที่เราเลือกในลำดับต้นๆ คือ เลือกหน่วยงานราชการเป็นหลัก สถาบันการศึกษา และหน่วยงานภาคเอกชน

เราจะดูว่าใครทำได้ เพราะมีข้อจำกัดในแต่ละคดี บางเรื่อง เช่น การดึงข้อมูลในโทรศัพท์บางทีเราต้องใช้ผู้เชี่ยวชาญและเครื่องมือซึ่งมีหลายหน่วยงานที่ทำได้ สถาบันนิติวิทยาศาสตร์ อาจารย์ภาควิชาคอมฯ บางที่ก็ทำได้ดึงข้อมูลและนำข้อมูลมาวิเคราะห์ แต่มีอีกกรณีหนึ่งที่เราต้องการข้อมูลและผู้เชี่ยวชาญด้วย

ถ้าเป็นกรณีที่สองเป็นหลักฐานและความเชี่ยวชาญเราจึงต้องเลือกใช้อาจารย์ตามมหาวิทยาลัยที่ดูแล้วเป็นกลาง แต่เราไม่ใช้หนึ่งเดี่ยว บางรายเราใช้ ETDA ด้วย เราจึงต้องใช้ทั้งสองหน่วยงาน ถ้าเราได้รายงานทั้งสองตรงกันเราก็จะนำเสนอศาล ศาลจะเชื่อหรือไม่ก็หมดหน้าที่ของ

เราเพราะเราได้นำเสนอทั้งหมดแล้ว เพราะในสาขานี้เราหาคนอื่นไม่ได้แล้ว แต่เราก็นำมาเลือกให้มีข้อเปรียบเทียบกันสองหน่วยงาน หรือหลายหน่วยงานก็ได้แล้วแต่ความเหมาะสม

ทำให้ คดีพิเศษก็อาจใช้เวลานานหน่อยเพราะต้องการให้ได้ผล 100 % ในแต่ละ LAB จะใช้เวลาประมาณเท่าได้นั้นจะไม่แน่นอน บางครั้งอาจจะใช้เวลา 2 สัปดาห์ 1 เดือน หรือ 2 เดือน แล้วแต่กรณี ส่วนค่าใช้จ่ายทางหน่วยงานเราไม่ค่อยมีปัญหาในด้านนี้ เพราะเรามีมาตรา 31 ซึ่งเราสามารถเบิกได้ สำหรับภาครัฐเราไม่ต้องเสียเงิน เช่น ธรรมศาสตร์ จุฬาฯ กรณีที่เขามีอุปกรณ์ของเขาอยู่แล้วเราก็ไม่ต้องจ่ายเงิน แต่บางกรณีที่เขาต้องไปจ้างต่ออีกเราก็ต้องเสียและเราก็เบิกได้ตามปกติ ยกเว้นกรณีที่ไม่มีหน่วยงานไหนทำได้แล้วเราถึงต้องพึ่งหน่วยงานเอกชน เครื่องมือบางตัวที่เราจำเป็นต้องดึงไฟล์ข้อมูลออกมาหรือกู้กลับคืนมาบางครั้งอาจไม่สมบูรณ์ ไม่น่าเชื่อถือ แต่หน่วยงานเอกชนบางรายเขามีอุปกรณ์ที่ทันสมัยและน่าเชื่อถือกว่าเราก็ต้องว่าจ้างเขา แต่ยังไม่เคยถึงขนาดต้องส่งไปต่างประเทศเพื่อตรวจ

ด้านบุคลากร

1. ข้าราชการ จำนวน 44 คน แบ่งเป็นชาย จำนวน 31 คน หญิง จำนวน 13 คน
2. พนักงานราชการ จำนวน 7 คน แบ่งเป็นชาย จำนวน 4 คน หญิง จำนวน 3 คน
3. ลูกจ้าง จำนวน 6 คน แบ่งเป็นชาย จำนวน 3 คน หญิง จำนวน 3 คน

ตอนนี้เรามีบุคลากรที่เป็นพนักงานสอบสวนประมาณ 30 คน และมีลูกจ้างอีก แบ่งออกเป็น 4 ส่วน แบ่งเป็นส่วนคดี 1 – 3 และก็มีกองอำนวยการทำงานด้านธุรการ จัดทำสารบบคดี

ถ้าเราทำคดีที่พิเศษจริงๆ บุคลากร 40 – 50 คน ก็อยู่ในเกณฑ์ที่เราทำได้ แต่ถ้าใช้เกณฑ์ในปัจจุบันมีพนักงานเป็นร้อยก็ไม่พอ เพราะในปัจจุบันยังไม่มีเกณฑ์อย่างทุกวันนี้การหลอกลวงทาง Facebook การใช้เครื่องSkimmer ลักข้อมูลมีปริมาณเยอะมาก พอเราไปร่วมมือกับภาคเอกชนมูลนิธิเตือนภัยผู้หญิง ซึ่งมีปริมาณคดีเยอะมาก ต่อให้มีบุคลากรเป็นร้อย สองร้อยก็ไม่พอ เราก็เลยต้องมาเลือก Volume การรับคดีเป็นสำคัญ ถ้า Volume เราสูงและรับคดีสำคัญจริงๆ แล้วประชาชนเข้าใจตรงกับเราไม่แจ้งเรื่องไร้สาระ แจ้งเรื่องที่เป็นคดีพิเศษจริงๆ คือเขาเข้าใจว่าเรื่องที่เกิดกับเขาควรจะไปแจ้งกับหน่วยงานไหนก็จะทำให้ปริมาณงานเราน้อยลง แต่ทุกวันนี้ปริมาณงานเราเยอะถ้าเราทำเกณฑ์สูง ประมาณสัก 40 – 45 คนก็จะทำงานได้

โดยการขอบุคลากรเพิ่ม เราจะเลือกจากสำนักงานคดีพิเศษ คือ เหมือนกับการย้ายสำนัก ย้ายแผนก ก็ทำเรื่องเสนอผู้บริหารในการขอย้ายแผนก และเรื่องการเลือกคน เลือกคนที่มีพื้นฐานความรู้ในดี แต่ที่สำคัญเลยคือความสนใจในงานที่จะทำและความรับผิดชอบสำคัญที่สุด หลายคนที่เราส่งไปฝึกอบรม ได้ประกาศนียบัตรสูงๆ มาเลย กลับมาไม่มีความตั้งใจทำงาน กับทำให้งานเรามีประสิทธิภาพลดลงก็มี แตกต่างจากคนที่เรารับเข้ามาใหม่และมีความตั้งใจและการเรียนรู้ก็ไม่

ยาก ของเราจะต่างจากตำรวจ คือตำรวจจะมีพนักงานสอบสวนคนเดียวรับผิดชอบเมื่อแจ้งความ ตัวเองต้องตัดสินใจได้ วางแผนได้คนเดียวเลย แต่ของเรามีลักษณะเป็นทีมงาน เพราะฉะนั้นในทีมงานของเรา ประมาณ 20 คน ก็จะมีผู้เชี่ยวชาญ ชำนาญงานในลักษณะนี้จริงๆสัก 10 คน ที่เหลือก็ขอคนที่มีความตั้งใจ

ส่วนเรื่องการพัฒนาบุคลากร ผมเป็นตำรวจมานั้นไม่ค่อยได้ฝึกอบรมเท่าไหร่ แต่ที่กรมสอบสวนคดีพิเศษมีการฝึกอบรมเยอะจริงๆ มีทั้งการฝึกอบรมภายในหน่วยงานเองและการฝึกอบรมร่วมกับหน่วยงานภายนอก และมีลักษณะการอบรมร่วมกันระหว่างสองหน่วยงาน ส่วนมากก็ก็อบรมร่วมกับทาง ICT สำนักงานตำรวจแห่งชาติ และฝ่ายความมั่นคงคือทหาร ที่เกี่ยวกับการกระทำความผิดด้านคอมพิวเตอร์ และในปัจจุบันก็มีภาคการธนาคารแห่งประเทศไทย เขาก็จะจัดการฝึกอบรมเป็นห้องใหญ่รวมหลายหน่วยงาน โดยธนาคารแห่งประเทศไทยเป็นเจ้าภาพและเชิญหน่วยงานต่างๆ ที่เกี่ยวข้องเข้าร่วมสัมมนา ส่วนการศึกษาดูงานต่างประเทศนั้นก็มีบ้างแต่มีจำนวนน้อย ส่วนมากผู้ที่ได้ไปก็จะเป็นระดับผู้บริหาร ในปี 59 เราก็ได้กันส่วนงบประมาณให้ระดับปฏิบัติการได้มีโอกาสไปดูงานในส่วนของศูนย์ต่อต้านที่เกี่ยวกับ Cyber crime เป็นหลัก

หลักสูตรการพัฒนาบุคลากร

1. โครงการพัฒนาบุคลากรด้านการตรวจพิสูจน์อิเล็กทรอนิกส์ คอมพิวเตอร์ และการสื่อสาร
2. โครงการจัดการสถานที่เกิดเหตุในคดีอาชญากรรมทางคอมพิวเตอร์
3. โครงการระบบสารสนเทศในองค์กรด้านความมั่นคง
4. โครงการสัมมนาทางวิชาการด้านไอซีทีเพื่อบริหารงานภาครัฐ
5. โครงการสัมมนาทางวิชาการยกระดับความมั่นคงปลอดภัยของเว็บไซต์ให้ได้มาตรฐาน

หน่วยงานของเราปีหนึ่งน่าจะได้รับการอบรมประมาณสองหลักสูตรต่อคนต่อปี มีการสลับกันเข้าอบรม ทั้งอบรมหน่วยงานภายในและร่วมกับหน่วยงานภายนอก

ต้องมีการพัฒนาเพิ่มเติมอยู่เรื่อยๆ เพราะบางส่วนจะอยู่ที่ตัวบุคคล การสอนงานระหว่างผู้ร่วมงานก็ยังน้อยไปเท่าที่ได้สัมผัสมา บางคนก็มีความรู้ ความเชี่ยวชาญสูงแต่ปิดตัวเองคือหน่วยงานอื่นเขาจะออกปฏิบัติงานเป็นทีม ลงพื้นที่ออกไปต่างจังหวัด แต่ส่วนสำนักงานของเราเป็นคดีในทางเทคนิคและมีความเป็นตัวเองสูงเก่งทำงานบนโต๊ะ ไม่มีลักษณะการทำงานที่เป็นทีมและออกไปข้างนอก การที่จะสัมพันธ์ในลักษณะเป็นทีมมีน้อย ผมก็มีแนวทางที่จะปรับระบบการทำงานให้เป็นทีมมากขึ้น

ผู้เชี่ยวชาญของเรายังมีไม่เพียงพอ เท่าที่เรามีผู้เชี่ยวชาญตอนนี้น่าจะมีสัก 5% ที่เชี่ยวชาญจริงๆ ซึ่งอาจจะไม่ได้จบมาทางนี้โดยตรงแต่เป็นการสั่งสมประสบการณ์และความ

เชี่ยวชาญจากหน้างาน ทำให้เขาสามารถเป็นระดับชำนาญการได้ และคนที่จบด้านคอมพิวเตอร์แต่ไม่มีความรู้ด้านกฎหมาย ของเราหลายคนจะมีทักษะที่แตกต่างกัน เพราะฉะนั้นฝ่ายสืบสวนจะต้องหาประเด็นว่าเป็นเรื่องอะไร และสามารถทำได้ไหมตรงนี้ทางผู้เชี่ยวชาญของเราก็จะสามารถตอบได้ว่าจะเก็บกู้ขึ้นได้ซึ่งตอนนี้ก็จะเป็นการเติมเต็มในคณะทำงานที่มีการติดต่อประสานกัน และทุกคนก็จะมองออกว่าเป็นประเด็นเรื่องอะไร แต่ยังไม่สามารถทำงานเองได้แต่จะมีฝ่ายเทคนิคคอยช่วย

ด้านงบประมาณและอุปกรณ์ด้านเทคโนโลยีเราไม่มีปัญหาอะไรครับ เรามีความพร้อมในระดับหนึ่งเลยครับ

การบริหารจัดการสำนักงาน การบริหารงานบุคคล การโยกย้าย การเลื่อนตำแหน่งที่สูงขึ้น

เป็นเรื่องขวัญและกำลังใจ คือ ไม่ให้สิทธิ ผบ.ในการแต่งตั้งเราก็ไม่สามารถดูแลปกครองผู้ใต้บังคับบัญชาได้เต็มที่และบางคนก็เกินกำลังเรา เช่น คนที่จะขึ้นไปในระดับ 9 – 10 บางท่านมีความตั้งใจและเชี่ยวชาญจริง แต่พอไม่ได้ขึ้นก็ทำให้ไม่มีกำลังใจ และทำให้ผู้ปฏิบัติงานตามลำดับชั้นลงมามองว่าไม่มีความก้าวหน้า และบางคนเราฝึกฝนอบรมให้มีความเชี่ยวชาญแล้วขอย้ายไปหน่วยงานอื่นก็มี เพราะต้นทุนในการฝึกอบรมก็ต้องใช้งบประมาณสูง

การติดต่อประสานงานกับหน่วยงานอื่นส่วนใหญ่ไม่ค่อยมีปัญหา เขาก็ให้ความร่วมมือเป็นอย่างดี

แนวทางในอนาคตเกี่ยวกับการต่อสู้กับ Cyber crime

ทางนี้ได้วางแนวทางไว้เกี่ยวกับจำนวนการรับคดี ต้องมีความชัดเจน และเป็นคดีพิเศษและสำคัญจริงๆ ประมาณนี้บุคลากรที่เรามีอยู่ก็สารมารถรับมือได้ ถ้ากำหนดการรับคดีได้เราก็สามารถกำหนดและวางตัวผู้รับผิดชอบได้และจะทำให้การทำงานมีประสิทธิภาพมากยิ่งขึ้น

ด้านความร่วมมือกับหน่วยงานอื่น ถ้าเป็นภาครัฐก็จะไม่มีปัญหา เพราะเราได้มีการประชุม สัมมนา ฝึกอบรมร่วมกัน และมีการพบปะกันอยู่บ่อยๆ ส่วนภาคเอกชนถ้าเป็นเรื่องภัยคุกคามทางอินเตอร์เน็ทจะไม่เกี่ยวกับหน่วยงานราชการอย่างเดียว ทุกวันนี้จะเกี่ยวข้องกับภาคเอกชนหลายกลุ่มหลายเครือข่าย ซึ่งสามารถให้ข้อมูลเกี่ยวกับการกระทำผิด ทำให้มีฐานข้อมูลจำนวนมาก ก็เลยเอาข้อมูลของเขามามาลงเป็นตัวฐานข้อมูล ในอนาคตเราก็เลยต้องจับมือร่วมกันทำงานกับหน่วยงานอื่นและสามารถลดเวลาการทำงานของเรามากขึ้น ประสานความร่วมมือให้มากขึ้น การทับซ้อนการทำ งานจะทำให้เราเห็นอะไรมากขึ้น

การหลอกลวงในการร่วมลงทุน ตั้งกองทุนและก็กำลังฮิตมากเลย เหมือนแชร์ลูกโซ่ เรื่องตรงนี้ตองมีการป้องกันให้ดี กับธนาคารแห่งประเทศไทย ซึ่งปัจจุบันเรายังไม่ได้จับมือกับหน่วยงานเหล่านี้เท่าที่ควร คือ อยู่ดีๆ คุณเปิดเว็บไซต์ขึ้นมาแล้วบอกว่าได้รับผลตอบแทน 100% ถ้า

สมมติว่าธนาคารแห่งประเทศไทยกำหนดไว้ชัดมันต้องโชว์ต้องมีใบขออนุญาต มีข้อมูลสำคัญของบริษัท ใครเป็นกรรมการ ทุนจดทะเบียน ที่อยู่ที่ติดต่อได้ ให้ประชาชนตรวจสอบความถูกต้องก่อนตัดสินใจ ก็จะทำให้การกระทำผิดทางเทคโนโลยี ทางคอมพิวเตอร์มีน้อยลงมากเลย การลงข้อมูลทางอินเตอร์เน็ตเราไม่เห็นตัว เช่น เห็นรูปบริษัทอย่างโก้หรูเลยแต่ไม่สามารถเช็คข้อมูลที่เกี่ยวกับบริษัทไม่ได้เลย อย่างนี้ต้องมีหน่วยงานที่รับผิดชอบคอยให้ข้อมูลข่าวสาร เพื่อประโยชน์ของผู้บริโภคว่ามีใบอนุญาตเปิดบริษัทไว้ชัดเจน อย่างการซื้อ-ขายสินค้างทางอินเตอร์เน็ต ถ้าเราตรวจสอบบริษัท ตรวจสอบสินค้า ตรวจสอบทุกอย่างได้อย่างถูกต้อง การทำธุรกรรมก็ถือว่ามีความยุติธรรม

ทางสำนักงานต้องการพัฒนาเรื่องระบบฐานข้อมูล ซึ่งเป็นเรื่องที่มีความสำคัญมากอย่างที่ได้เรียนไปแล้ว เช่นเรื่องของSkimmer ที่ทำเป็นองค์กรอาชญากรรม เราต้องเริ่มจากการทำฐานข้อมูลเราก็จะได้รู้ว่าผู้กระทำผิดเหล่านั้นเป็นใคร ทำมาในรูปแบบได เครือข่ายมากขนาดไหน

การพัฒนาคนเน้นการอบรมเชิงวิชาการ ทฤษฎี ภาคปฏิบัติ ร่วมกับการพัฒนาเครือข่าย คือ รูปแบบการฝึกอบรมของข้าราชการทุกหน่วยงานมาทำ Workshop ร่วมกัน เราก็จะได้เครือข่ายของผู้ปฏิบัติงานร่วมกันทุกหน่วยงาน

แต่กรมสอบสวนคดีพิเศษ ยังไม่มีการอบรมร่วมกับหน่วยงานอื่นและยังไม่มีการตั้งงบประมาณในส่วนนี้ด้วย

ข้อเสนอแนะเกี่ยวกับผู้บังคับใช้กฎหมายที่ทำคดีเกี่ยวกับ Cyber crime

1. พนักงานสอบสวนจะต้องมีความรู้ในด้านของ Cyber crime อาจจะต้องมีการพัฒนาถึงขั้นการจัดทำคู่มือการสอบสวน การดำเนินคดีด้าน Cyber crime นี้โดยเฉพาะให้กับตำรวจที่ประจำอยู่ตามสถานีตำรวจ อย่างหน่วยงานของกรมสอบสวนคดีพิเศษ ยังมีการพัฒนาอยู่เรื่อยๆ และของเราก็มีคู่มือการดำเนินงานอยู่แล้ว ต้องเพิ่มทักษะ ทำคู่มือในการปฏิบัติงาน และในเชิงป้องกันก็มีการรณรงค์ด้วยการทำแผ่นพับชี้แจงข้อมูลข่าวสาร

2. ต้องมีการสร้างคู่มือการป้องกันโดยละเอียด และการเปิดเผยข้อมูลของผู้ประกอบธุรกิจทางอินเตอร์เน็ตและการรณรงค์เผยแพร่ข้อมูลข่าวสารให้ผู้บริโภครับทราบข้อมูล

3. นายสุรศักดิ์ ศรีรัตน์ตระกูล อธิบดีอัยการ สำนักงานการสอบสวน สำนักงานอัยการสูงสุด

อำนาจหน้าที่ของหน่วยงาน

1. รับผิดชอบการสอบสวนและการดำเนินการอื่น ตามกฎหมายว่าด้วยการป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติที่กำหนดให้เป็นอำนาจและหน้าที่ของอัยการสูงสุดหรือผู้รักษาการแทน

2. รับผิดชอบการสอบสวนในความผิดที่มีโทษตามกฎหมายไทย ซึ่งได้กระทำลงนอกราชอาณาจักร ตามประมวลกฎหมายวิธีพิจารณาความอาญา ที่กำหนดให้เป็นอำนาจและหน้าที่ของอัยการสูงสุดหรือผู้รักษาการแทน

3. รับผิดชอบการร่วมสอบสวนตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษฯลฯ ประกาศ คณะกรรมการอัยการ เรื่อง การแบ่งหน่วยงาน และการกำหนดอำนาจ

ขั้นตอนการปฏิบัติงาน

กรณีความผิดตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักร ที่อัยการสูงสุดหรือผู้รักษาการแทนเป็นพนักงานสอบสวนผู้รับผิดชอบฯ ตาม ป.วิ.อาญา มาตรา 20

1. การส่งเรื่องให้อัยการสูงสุด เพื่อขอให้อัยการสูงสุด พิจารณาดำเนินการตาม ป.วิ.อาญา มาตรา 20

1.1 กรณีหน่วยงานราชการที่มีหน้าที่สอบสวนได้รับคำร้องทุกข์ หรือคำกล่าวโทษ ได้แก่ หน่วยงานในสำนักงานตำรวจแห่งชาติ และ กรมสอบสวนคดีพิเศษ ส่งเรื่องไปยังสำนักงานอัยการสูงสุด

1.2 กรณีตัวความหรือผู้แทน หรือผู้ได้รับมอบหมาย ไปร้องทุกข์ต่ออัยการสูงสุด

2. สำนักงานอัยการสูงสุด หรืออัยการสูงสุด ส่งเรื่องให้สำนักงานการสอบสวนพิจารณาเสนอความเห็นในการดำเนินการตาม ป.วิ.อาญา มาตรา 20 โดยอาจแบ่งได้เป็น 2 กรณี

2.1 กรณีเห็นว่าไม่เป็นคดีที่ความผิดตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักร ตาม ป.วิ.อาญา มาตรา 20 พนักงานอัยการ สำนักงานการสอบสวน เสนอความเห็นต่ออัยการสูงสุด ให้หน่วยงานที่มีหน้าที่สอบสวน ที่ส่งเรื่องมารับเรื่องคืนไปดำเนินการสอบสวนตามอำนาจหน้าที่ที่กำหนดไว้ใน ป.วิ.อาญา

2.2 กรณีเห็นว่าเป็นคดีที่ความผิดตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักร ตาม ป.วิ.อาญา มาตรา 20 พนักงานอัยการ สำนักงานการสอบสวน เสนอความเห็นต่ออัยการสูงสุด ให้มอบหมายหน้าที่พนักงานสอบสวนผู้รับผิดชอบ ให้พนักงานอัยการหรือพนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวนแทน โดยกรณีที่อัยการสูงสุดหรือผู้รักษาการแทน มอบหมายให้พนักงานสอบสวนคนใดเป็นผู้รับผิดชอบทำการสอบสวน อัยการสูงสุดหรือผู้รักษาการแทน จะมอบหมายให้พนักงานอัยการคนใดทำการสอบสวน ร่วมกับพนักงานสอบสวนก็ได้

3. สำนักงานการสอบสวน เสนอความเห็นต่ออัยการสูงสุด เพื่อพิจารณาสั่ง

4. สำนักงานการสอบสวน แจ้งคำสั่งอัยการสูงสุด ไปยังหน่วยงานที่เกี่ยวข้องได้แก่ หน่วยงานที่มีหน้าที่สอบสวน และส่งเรื่องไปยังสำนักงานอัยการ ของสำนักงานอัยการสูงสุด และหน่วยงานที่เป็นผู้รับผิดชอบทำการสอบสวนแทนอัยการสูงสุด (หากเป็นคนละหน่วยงาน กับ

หน่วยงานผู้ส่งเรื่องฯ) พร้อมทั้งแจ้งรายชื่อพนักงานอัยการผู้เข้าร่วมการสอบสวน (หากมอบหมายให้อัยการเข้าร่วมการสอบสวน)

4.1 กรณีหน่วยงานที่รับผิดชอบการสอบสวน อยู่ในเขตกรุงเทพมหานคร สำนักงานการสอบสวนจะมอบหมายพนักงานอัยการในสำนักงานอัยการการสอบสวน เข้าร่วมการสอบสวน หรือ

4.2 กรณีหน่วยงานที่รับผิดชอบการสอบสวน อยู่ในส่วนภูมิภาค สำนักงานการสอบสวนแจ้งให้สำนักงานอัยการส่วนภูมิภาค ทราบคำสั่งอัยการสูงสุด และแจ้งรายชื่อพนักงานอัยการผู้เข้าร่วมการสอบสวน

5. กรณีที่อัยการสูงสุด มอบหมายให้พนักงานอัยการทำการสอบสวนฝ่ายเดียว สำนักงานการสอบสวนจะมอบหมายพนักงานอัยการ หรือคณะพนักงานอัยการทำการสอบสวนตาม ป.วิ. อาญา เช่น คดีคนไทยถูกกล่าวหาว่าลักทรัพย์นายจ้าง ที่ประเทศเวียดนาม หรือ คดีนายโยฮันเนสฯ ผู้ต้องหา ถูกกล่าวหาว่ากระทำผิดในข้อหาฟอกเงิน

6. รายงานผลการดำเนินการและผลการสอบสวนต่ออัยการสูงสุดตามระเบียบสำนักงานอัยการสูงสุดว่าด้วยการดำเนินคดีอาญาของพนักงานอัยการ พ.ศ.2547 ข้อ 28

ด้านบุคลากร

จำนวนบุคลากรทั้งหมดในองค์กร 69 คน แบ่งเป็น พนักงานอัยการ 28 คน เจ้าหน้าที่ธุรการ 21 คน พนักงานราชการ 1 คน และพนักงานจ้างเหมา 19 คน

วุฒิการศึกษา พนักงานอัยการ วุฒิการศึกษาขั้นต่ำ ปริญญาตรีนิติศาสตร์บัณฑิต และเนติบัณฑิตไทย โดยพนักงานอัยการหลาย จบการศึกษาปริญญาตรีนิติศาสตร์มหาบัณฑิต

อัตรากำลังที่เหมาะสม ขึ้นอยู่กับปริมาณงาน โดยกรอบอัตรากำลังที่กำหนดไว้ คือ พนักงานอัยการ 39 คน อัตรากำลังขาดแคลน ทั้งพนักงานอัยการและเจ้าหน้าที่ธุรการ โดยมีสาเหตุ

1. คดีความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราช อาณาจักรไทย ตาม ป.วิ. อาญา มาตรา 20 และคดีความผิด ตาม พ.ร.บ.การสอบสวนคดีพิเศษ พ.ศ.2547 มีปริมาณมากขึ้น

2. คดีเกี่ยวกับองค์กรอาชญากรรมข้ามชาติ อันมีลักษณะตาม พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 มีปริมาณเพิ่มมากขึ้น และหากคดีเริ่มต้นที่อัยการสูงสุด จะต้องใช้พนักงานอัยการและเจ้าหน้าที่ผู้มีความเชี่ยวชาญเฉพาะด้านจำนวนมาก

แนวทางการพัฒนาบุคลากร

มีการฝึกอบรมภาคทฤษฎี/ปฏิบัติ ในหน่วยงานดังนี้

1. หลักสูตรเกี่ยวกับการดำเนินคดีความผิดคดีความผิดซึ่งมีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย ตาม ป.วิ.อาญา มาตรา 20

2. หลักสูตรการเข้าร่วมชันสูตรพลิกศพ การทำสำนวนการชันสูตรพลิกศพ การคุ้มครองสิทธิเด็ก

ศึกษาดูงานในประเทศ/ต่างประเทศ การศึกษาดูงานในต่างประเทศที่พนักงานอัยการมีอำนาจในการสอบสวน เช่น ญี่ปุ่น

การฝึกอบรมร่วมกับหน่วยงานอื่น

1. อบรมหลักสูตรเพิ่มประสิทธิภาพเจ้าพนักงาน ตามพระราชบัญญัติป้องกันและปราบ ปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556

2. การส่งพนักงานอัยการและเจ้าหน้าที่ ไปร่วมอบรมสัมมนาในหลักสูตรที่หน่วยงานภายนอกจัดทำขึ้นโดยเฉลี่ยบุคลากรได้รับการอบรมจำนวน 1 ครั้งต่อปี/ต่อคน แต่คาดหวังว่าควรจะเป็น 3 ครั้งต่อปี/ต่อคน

ปัญหาและอุปสรรคในการทำงาน

1. ด้านกำลังคน (เจ้าหน้าที่/ผู้เชี่ยวชาญ) พนักงานอัยการยังขาดทักษะในการสืบสวนสอบสวน โดยเฉพาะกรณีคดีความผิดที่ต้องใช้องค์ความรู้ทางเทคโนโลยี

2. ด้านงบประมาณ สำนักงานการสอบสวน ยังไม่ได้รับงบประมาณการทำงานที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ โดยเฉพาะคดีที่ตั้งต้นที่พนักงานอัยการ รวมทั้งงบประมาณในการทำงาน ประสานงานกับหน่วยงานอื่น

3. ด้านอุปกรณ์/เทคโนโลยีใหม่ๆ สำนักงานการสอบสวน ยังไม่มีอุปกรณ์ เครื่องมือในการทำงาน ตลอดจนเทคโนโลยีสมัยใหม่ที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ

4. การบริหารจัดการสำนักงาน/ทรัพยากรบุคคล การโยกย้าย การเลื่อนตำแหน่งบุคลากร ยังมีปริมาณไม่เพียงพอต่อการทำงานอย่างประสิทธิภาพ คนที่มีความรู้ความเชี่ยวชาญที่ต้องย้ายไปอยู่หน่วยอื่นหรือได้เลื่อนตำแหน่ง คนใหม่มาทดแทนต้องใช้เวลาเรียนรู้งาน

5. การติดต่อประสานงานกับหน่วยงานอื่น การประสานงานระหว่างหน่วยงานราชการ และภาคเอกชนที่ครอบครองพยานหลักฐานยังมีขั้นตอนยุ่งยากล่าช้า , การประสานงานขอความร่วมมือทางอาญาระหว่างประเทศ มีขั้นตอนที่เป็นทางการ หลายขั้นตอนในแต่ละหน่วยงาน ขาดความสะดวกรวดเร็วและมีประสิทธิภาพ ประกอบกับความร่วมมือระหว่างประเทศ ยังไม่ครอบคลุมประเทศที่เกี่ยวข้องกับการกระทำความผิด หรือครอบครองพยานหลักฐานที่ต้องใช้ในการดำเนินคดี

6. พนักงานสอบสวน (เจ้าหน้าที่ตำรวจ) ส่วนมากยังไม่เข้าใจและบางส่วนยังไม่ยอมปฏิบัติตาม ป.วิ.อาญา มาตรา 20

แนวทางการทำงานในอนาคตในการต่อสู้กับ Cyber Crime

1. สำนักงานการสอบสวนได้ให้ความรู้ พัฒนาศักยภาพของเจ้าหน้าที่ผู้ปฏิบัติงาน ในด้านการป้องกัน และปราบปราม รวมถึงการดำเนินคดี

2. สำนักงานการสอบสวนได้ประสานความร่วมมือในระดับต่างๆ ได้แก่ ระหว่างภาครัฐ กับภาครัฐ ระหว่างภาครัฐ กับเอกชน และความร่วมมือระหว่างประเทศ เพื่อให้สามารถป้องกันความเสียหาย ปราบปรามการกระทำความผิด และการดำเนินคดีกับคนร้าย หรือองค์กรอาชญากรรม ได้อย่างมีประสิทธิภาพ และรวดเร็ว

ข้อเสนอแนะ

1. ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ ภายในประเทศที่มีหน้าที่ป้องกันและปราบปราม รวมถึงการดำเนินคดี เพื่อใช้อำนาจหน้าที่ตามกฎหมายต่างๆ ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

2. ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ กับภาคเอกชน เพื่อให้เจ้าหน้าที่ของรัฐสามารถเข้าถึงข้อมูลต่างๆ เช่น ข้อมูลการเงิน ข้อมูลการสื่อสารทางโทรศัพท์ หรือเครือข่ายอินเทอร์เน็ต ได้อย่างมีประสิทธิภาพ และรวดเร็ว

3. ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ กับประเทศอื่นๆ เพื่อความร่วมมือในการใช้อำนาจรัฐ

4. ควรมอบหมายหน่วยงานใดหน่วยงานหนึ่ง ให้เป็นผู้รวบรวมข้อมูลการดำเนินคดี และเป็นผู้ประสานงานในคดีความผิดเกี่ยวกับคอมพิวเตอร์ เป็นการเฉพาะ

5. ควรมีการบูรณาการระหว่างหน่วยงานภายในสำนักงานอัยการสูงสุด เพื่อแก้ไขปัญหาข้อขัดข้อง และเพิ่มประสิทธิภาพในการดำเนินคดีทั้งกระบวนการ ได้แก่ สำนักงานการสอบสวน สำนักงานคดีอัยการสูงสุด และสำนักงานอัยการที่มีหน้าที่สั่งคดี

6. ควรให้ความสำคัญกับการดำเนินคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ เป็นการเฉพาะอย่างเร่งด่วน เพราะปัจจุบันอาชญากรใช้ช่องทางการสื่อสาร และอุปกรณ์เทคโนโลยีที่ทันสมัย ในการกระทำความผิดเป็นจำนวนมาก สร้างความเสียหายแก่ประชาชน และสังคมอย่างหนัก

4. นายสมชาย คูวิจิตรสุวรรณ อธิบดีอัยการ สำนักงานคดีเศรษฐกิจและทรัพยากร

อำนาจหน้าที่ของหน่วยงาน

สำนักงานคดีเศรษฐกิจและทรัพยากร เป็นส่วนราชการในสำนักงานอัยการสูงสุด มีอำนาจหน้าที่รับผิดชอบการดำเนินคดี ทั้งปวงอันเกี่ยวกับเศรษฐกิจและทรัพยากร ตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของพนักงานอัยการหรือสำนักงานอัยการสูงสุด ซึ่งอยู่ ในอำนาจพิจารณาพิพากษาของศาลอาญา ศาลอาญากรุงเทพใต้ ศาลอาญาธนบุรี ศาลจังหวัดตลิ่งชัน และศาลจังหวัด พระโขนง มีอำนาจหน้าที่รับผิดชอบการดำเนินคดีทั้งปวงอันเกี่ยวกับเศรษฐกิจและทรัพยากร ตามคำสั่ง กรมอัยการที่ 19/2534 ลงวันที่ 18 กุมภาพันธ์ 2538 ได้แก่ ความผิดเกี่ยวกับการเงินและการธนาคาร และความผิดเกี่ยวกับการค้าและการพาณิชย์ ความผิดเกี่ยวกับคดีเศรษฐกิจและทรัพยากรปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือได้รับมอบหมาย

ขั้นตอนการปฏิบัติงาน

เมื่อได้รับสำนวนการสอบสวนจากพนักงานสอบสวน พนักงานอัยการเจ้าของสำนวนจะดำเนินการตรวจสอบสำนวนดังกล่าวว่ามีพยานบุคคลและพยานเอกสารเพียงพอที่รับฟังได้หรือไม่ว่าผู้ต้องหาได้กระทำความผิดตามข้อกล่าวหา หากพยานหลักฐานยังไม่เพียงพอพนักงานอัยการจะดำเนินการสั่งให้พนักงานสอบสวนทำการสอบสวนเพิ่มเติม แต่หากพยานหลักฐานที่พนักงานสอบสวนรวบรวมมาเพียงพอ ครบถ้วนสมบูรณ์ที่จะพอรับฟังได้ว่าผู้ต้องหากระทำความผิดตามข้อกล่าวหาจริง พนักงานอัยการจะดำเนินการฟ้องคดีผู้ต้องหาต่อศาลต่อไป

การทำงานเกี่ยวข้องใกล้ชิดกับหน่วยงานใดบ้าง

1. หน่วยงานในสังกัดสำนักงานตำรวจแห่งชาติ เช่น สถานีตำรวจนครบาล ในกรุงเทพมหานคร กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

2. ธนาคารพานิชย์ต่างๆ

ด้านบุคลากร

จำนวนบุคลากรทั้งหมดในองค์กร 78 คน ชาย 33 หญิง 45 คน

ในส่วนอัตรากำลังของพนักงานอัยการที่มีความรู้ความเชี่ยวชาญในการดำเนินคดีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ มีประมาณ 7- 8 คน ยังขาดแคลนอยู่ ควรมีพนักงานอัยการที่มีความเชี่ยวชาญในเรื่องอาชญากรรมทางคอมพิวเตอร์ในทุกสำนักงานคดีเศรษฐกิจและทรัพยากรและมีในปริมาณที่เพียงพอที่จะทดแทน ในกรณีที่พนักงานอัยการผู้เชี่ยวชาญในเรื่องดังกล่าว จะต้องมีการโยกย้ายไปดำรงตำแหน่งในต่างจังหวัด อัตรากำลังที่จะเพียงพอต่อการทำงานในส่วนที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ประมาณ 14 – 15 คน

แนวทางการพัฒนาบุคลากร

มีการอบรมภายในสำนักงานและส่งไปอบรมข้างนอกด้วย หลักสูตรที่อบรม เช่น การเพิ่มศักยภาพการดำเนินคดีและสร้างเครือข่ายความร่วมมือในการดำเนินคดีอาชญากรรมที่เกี่ยวกับเทคโนโลยีสารสนเทศเฉลี่ยแล้วบุคลากรได้รับการอบรมจำนวน 1 ครั้งต่อปี/ต่อคน

ปัญหาและอุปสรรคในการทำงาน

1. ขาดอัยการผู้เชี่ยวชาญด้านอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ รวมทั้งเจ้าหน้าที่ที่คอยสนับสนุน เช่น นิติกร เป็นต้น และเมื่อมีการโยกย้ายพนักงานอัยการไปแล้วไม่มีคนมาทดแทน

2. ขาดงบประมาณในการพัฒนา ขาดอุปกรณ์และเทคโนโลยีใหม่ๆ ระบบการติดต่อสื่อสาร อินเตอร์เน็ทที่ใช้ในการทำงาน

ปัญหาและอุปสรรคในการดำเนินคดีเกียวกับอาชญากรรมทางคอมพิวเตอร์

1. ปัญหาเกี่ยวกับกับรวบรวมพยานหลักฐาน

1.1 พยานเอกสารที่จำเป็นต่อการพิจารณาและสืบพยานในบางเรื่องอาจอยู่ในความดูแลของหน่วยงานหรือองค์กรที่อยู่ต่างประเทศ ดังนั้น การได้มาซึ่งพยานเอกสารดังกล่าว โดยปกติจะต้องใช้วิธีแบบเป็นทางการ (ผ่านทางหน่วยงานของทางราชการ) ซึ่งจะต้องใช้ระยะเวลาในการได้มาซึ่งเอกสาร ทำให้ในบางคดีซึ่งถูกจำกัดด้วยระยะเวลาในการดำเนินคดีที่มีอยู่อย่างจำกัด ไม่สามารถที่จะได้มาซึ่งเอกสารดังกล่าวมาภายในเวลาที่กำหนดเป็นเหตุให้ไม่สามารถนำเอกสารดังกล่าวมาพิจารณาและสืบพยานในชั้นศาลได้

1.2 การกระทำความผิดในลักษณะดังกล่าว อาจเกิดปัญหาในการรวบรวมเอกสารในกรณีที่ธนาคารหรือสถาบันการเงิน ได้มีการทำลายเอกสารที่จำเป็นต้องใช้ประกอบการพิจารณาและสืบพยานไปแล้ว เนื่องจากระยะเวลาในการสืบสวนสอบสวนอาจนานเกินกำหนดระยะเวลาในการรักษาเอกสารดังกล่าว

2. ปัญหาด้านบุคลากรที่เกี่ยวข้องในการดำเนินคดี

เนื่องจากการดำเนินคดีที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ มีรูปแบบของการกระทำความผิดที่มีความสลับซับซ้อนมากกว่าคดีทั่วๆ ไป เนื่องจากผู้กระทำความผิดจะใช้เทคโนโลยีหรือรูปแบบการกระทำความผิดผ่านทางระบบคอมพิวเตอร์ ดังนั้น เพื่อที่จะเข้าใจรูปแบบของการกระทำความผิด และนำมาซึ่งการจับกุมตัวผู้กระทำความผิดได้อย่างถูกต้อง จึงจำเป็นต้องใช้บุคลากรไม่ว่าจะเป็น พนักงานสอบสวน และพนักงานอัยการ ที่มีความรู้ความเชี่ยวชาญในเรื่องดังกล่าวด้วย แต่เนื่องจากในปัจจุบันนี้ พนักงานสอบสวนผู้มีความเชี่ยวชาญในเรื่องดังกล่าวก็มีจำนวนไม่เพียงพอ ทำให้การรวบรวมพยานหลักฐานต่างๆ อาจทำได้อย่างไม่ครบถ้วน นอกจากนี้

พนักงานอัยการผู้มีความเชี่ยวชาญในเรื่องดังกล่าวก็มีอยู่อย่างจำกัด ทำให้อาจเกิดปัญหาในการพิจารณาและดำเนินคดีในความผิดดังกล่าวได้อย่างไม่สมบูรณ์เต็มที่

3. ปัญหาในการนำตัวผู้กระความผิดมาลงโทษ

ปัญหานี้เกิดขึ้นในกรณีของการกระทำความผิดผ่าน Social Media กระทำความผิดในลักษณะดังกล่าว เมื่อพิจารณาจากสำนวนการสอบสวนแล้วจะพบว่าผู้ต้องหาที่ถูกกล่าวหาว่ากระทำความผิดและถูกดำเนินคดีโดยส่วนใหญ่นั้น อาจจะไม่ใช่ตัวการในการกระทำความผิดที่แท้จริง โดยส่วนใหญ่ผู้ต้องหา ที่ถูกดำเนินคดีจะเป็นเจ้าของบัญชีธนาคารที่มีการรับโอนเงินที่ผู้เสียหายถูกหลอกมา โดยผู้ต้องหาเหล่านี้ อาจกระทำการโดยรู้เท่าไม่ถึงการณ์ โดยการรับจ้างเปิดบัญชี หรือเปิดบัญชีให้กับคนร้ายเนื่องจากถูกหลอกลวง ซึ่งเท่ากับว่าบุคคลเหล่านั้นอาจไม่มีส่วนรู้เห็นในการกระทำความผิดดังกล่าว และทำให้บุคคลที่เป็นตัวการ ในการลงข้อมูลใน Social Media หลอกลวงผู้เสียหายนั้น ไม่ถูกนำตัวมาลงโทษได้ ดังนั้นสมควรที่สถาบันการเงิน ต้องตรวจสอบและเคร่งครัดในการเปิดบัญชีให้กับ ผู้ขอเปิดบัญชีมากยิ่งขึ้น และควรมีข้อกำหนด ในสัญญาเปิดบัญชีแสดงคำเตือนว่าการรับจ้างเปิดบัญชีมีความผิดทางอาญา เป็นต้น นอกจากนี้ปัญหาดังกล่าวส่วนหนึ่งอาจเกิดจาก Social Media ที่ผู้หลอกลวงใช้เป็นเครื่องมือในการหลอกลวงผู้เสียหาย อย่างเช่น เฟสบุ๊ค (Facebook) หรือ อีเมล์ (Email) นั้น เป็นผู้ให้บริการที่อยู่ต่างประเทศ ดังนั้นในการขอข้อมูลหรือเอกสารอื่นๆ ที่จำเป็นต่อการดำเนินคดี จะต้องมีการดำเนินการในลักษณะของการขอความร่วมมือในระดับประเทศ เช่น การใช้พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 ซึ่งส่งผลให้เกิดความล่าช้า หรือในบางกรณีอาจไม่ได้รับความร่วมมือด้วยเช่นกัน

แนวทางการทำงานในอนาคตในการต่อสู้กับ Cyber Crime

1. มีการอบรมบุคลากรในสำนักงานให้มีความเชี่ยวชาญ และพร้อมที่รับมือการกระทำความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ซึ่งมีการเปลี่ยนรูปแบบการกระทำความผิดไปเรื่อยๆ

2. พยายามหาบุคลากรที่มีความเชี่ยวชาญมาเสริมศักยภาพในการทำงานให้มีประสิทธิภาพเพิ่มมาก

5. นายวันชัย รุจนวงศ์ อธิบดีอัยการ สำนักงานต่างประเทศ สำนักงานอัยการสูงสุด

สำนักงานต่างประเทศ มีอำนาจและหน้าที่รับผิดชอบงานความร่วมมือระหว่างประเทศในเรื่องทางอาญา งานดำเนินคดีส่งผู้ร้ายข้ามแดน งานสอบสวนคดีความผิดนอกราชอาณาจักร งานโอนตัวนักโทษ งานต่อต้านการค้ามนุษย์ งานดำเนินการเรื่องการลักพาเด็กข้ามชาติ งานต่อต้านองค์กรอาชญากรรมข้ามชาติและงานติดต่อประสานงานกับองค์กรระหว่างประเทศหรือหน่วยงานต่างประเทศเกี่ยวกับเรื่องที่อยู่ในอำนาจและหน้าที่ของสำนักงานอัยการสูงสุด

ปัญหาอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

1. เป็นผลมาจากความก้าวหน้าของเทคโนโลยี

2. มีความเร็วสูงมาก

3. ไม่จำกัดสถานที่และเวลาอยู่คนละที่ก็สามารถติดต่อกันได้ตลอดเวลา เพราะฉะนั้นจึงเป็นปัญหา ในขณะเดียวกันธุรกิจหรือกิจการต่างๆ ก็ต้องการคุณลักษณะของความเร็วจากการไม่จำกัดพรมแดน

4. มีต้นทุน ค่าใช้จ่ายที่ต่ำมาก เพราะต้นทุนคือ ค่าอินเตอร์เน็ตเท่านั้น ไม่เหมือนเมื่อก่อนที่ต้องเดินทาง มีการส่งจดหมาย จึงทำให้ต้นทุนสูงมาก ทีนี้ในทุกวงการก็พยายามที่จะใช้ประโยชน์จากเทคโนโลยีนี้ แต่เมื่อได้ประโยชน์แล้วก็มีคนเข้ามาหาประโยชน์ด้วยการก่ออาชญากรรมโดยใช้เทคโนโลยีนี้ด้วยเหมือนกัน แต่ว่าเรื่องของการป้องกันและการปราบปรามยังติดปัญหาอยู่มากเพราะ

4.1 เรื่องของอำนาจอธิปไตย

4.2 ระบบกฎหมายและตัวกฎหมายที่ไม่สอดคล้องกัน

4.3 ระดับความก้าวหน้าของการพัฒนามาตรการทั้งทางกฎหมายและที่มิใช่กฎหมาย การที่จะจัดการกับเทคโนโลยีรุ่นใหม่ๆ ก็มีความก้าวหน้าไม่เท่ากัน

4.4 ความไม่ไว้ใจซึ่งกันและกัน

4.5 การไม่รู้จักกัน ไม่รู้ว่าใคร

4.6 การเอาระบบเดิมไปจับกับเทคโนโลยีใหม่ เช่นการขอความร่วมมือที่ต้องผ่านหลายหน่วยงานทำให้เกิดความล่าช้า ที่เราเรียกกันว่าระบบราชการ

4.7 ระบบการพิจารณาคดีที่ยังยึดหลักการแบบเดิมคือต้องมีประจักษ์พยาน มีพยานหลักฐานชัดเจน ถูกต้องตามกฎหมาย

4.8 ความล่าช้าในการสืบสวน สอบสวน การรวบรวมพยานหลักฐาน

ซึ่งทั้งหมดถือเป็นช่องว่าง เกิดประเด็นอยู่สองส่วน คือ

1. ภาครัฐต้องพัฒนากระบวนการป้องกันและปราบปรามอาชญากรรม

2. ภาคเอกชนจะต้องหาวิธีการป้องกันตัวเองด้วย เช่น กระบวนการของธนาคารที่ทำการฝาก – ถอนโดยการใช้ระบบอิเลคทรอนิคส์ก็จะต้องหามาตรการรักษาความปลอดภัยข้อมูลของตัวเอง จะมาคอยพึ่งรัฐอย่างเดียวก็คงไม่ได้

ในเรื่องของความร่วมมือระหว่างประเทศทางอาญา การขอข้อมูล เอกสาร พยานหลักฐานต่างๆ ในต่างประเทศ อาจทำได้โดยความร่วมมือย่างไม่เป็นทางการ คือ ความร่วมมือระหว่างหน่วย งานโดยตรง เช่น ตำรวจไทยกับตำรวจต่างประเทศ หรือกับหน่วยงานอื่นๆที่เกี่ยวข้อง

กับคดี เขาสามารถประสานงานกันได้โดยตรง คือ ความร่วมมือที่จะมาผ่านสำนักงานอัยการสูงสุดที่เราทำอยู่นี้ คือ ความร่วมมืออย่างเป็นทางการ ถ้าถามว่าสองอันนี้อันไหนสำคัญกว่า คือ ความร่วมมืออย่างไม่เป็นทางการ เฉพาะกับคดีที่มีความเร็วขนาดนี้ เช่น มีการโอนเงิน มีการโกงกัน จากนี่ไปนี่ถ้าจะมัวรอส่งอัยการ กว่าจะถามไปอีก 3 เดือน 6 เดือนกว่าจะรู้ แต่ถ้ารู้จักหน่วยงานที่เขาทำงานด้านนี้โดยตรง ให้เขาช่วยเช็คให้ว่าใครเป็นคนถอนเงินออกไป หรือช่วยไปดูว่ามีใครมากดเงินไปจากตู้นั้น ก็สามารถมาตรวจเช็คได้ทันที นี่คือความร่วมมืออย่างไม่เป็นทางการ สรุปแล้วความร่วมมืออย่างเป็นทางการจะใช้ก็ต่อเมื่อคุณจะเอาพยานหลักฐานนั้นไปใช้อ้างเป็นพยานในศาล ถ้าใช้ในการสืบสวนสอบสวนก็สามารถใช้ระบบความร่วมมืออย่างไม่เป็นทางการโดยไม่ต้องผ่านสำนักงานอัยการ ความร่วมมือสองอย่างมีความแตกต่างกัน

พยานหลักฐานที่ได้อย่างไม่เป็นทางการจะเข้ามาในสำนวนได้ เพราะการสอบสวนให้รู้ว่าเกิดอะไรขึ้น ในการสอบสวนจะรู้ว่าอะไรผิดหรือไม่ผิด พยานหลักฐานที่ได้จากไม่เป็นทางการครอบ คลุมทุกอย่าง เป็นความร่วมมือส่วนตัวก็ได้ จากหน่วยงานก็ได้ สามารถทำได้หมดและไม่มีรูปแบบจะใช้โทรศัพท์หรือ อีเมล์ก็ได้ แต่ปัญหาอยู่ที่ว่าอีกฝ่ายที่จะให้ความร่วมมือเขารู้จักคุณหรือเปล่า แต่ถ้ารู้จักก็จะให้ความร่วมมือ ข้อมูลที่ได้นี้สามารถนำมาเข้าสำนวนได้ โดยทำคำร้องขอเป็นทางการไปอีกครั้งเพื่อให้ทางรัฐบาลรับรองความถูกต้องของพยานหลักฐาน สรุปคือในเบื้องต้นเพื่อความรวดเร็วในการสืบสวนสอบสวน ควรใช้ความร่วมมือแบบไม่เป็นทางการ หลังจากนั้นก็ใช้ความร่วมมืออย่างเป็นทางการส่งตามไปเพื่อให้ได้พยานหลักฐานที่ชอบด้วยกฎหมาย

เรื่องของความร่วมมือและการส่งผู้ร้ายข้ามแดนก็ยังต้องดำเนินการตามระบบ เพียงแต่ต้องมาแยกว่าความร่วมมือแบ่งเป็นสองส่วน สามระดับ ความร่วมมือเบื้องต้นสอบถามข้อมูลกันทันที แต่ละประเทศอาจจะต้องจัดเจ้าหน้าที่ที่รับผิดชอบโดยเฉพาะเพื่อจะได้รู้เป็น Focal point ไม่ใช่ว่าใครก็ได้โทรไปหรือส่งอีเมล์ไป เพราะไม่รู้หรอกว่าใครเป็นใครจะเป็นผู้ร้ายหรือเปล่าก็ไม่รู้มาหลอกถาม และต้องลดระดับความลับของข้อมูลว่าระดับไหนที่จะเปิดเผยหรือให้ข้อมูลกันได้ เพราะว่าเดิมในแต่ละประเทศจะหวงข้อมูลเพราะยังไม่มีหลักเกณฑ์ว่าอะไรที่จะเปิดเผยหรือให้ข้อมูลกันได้ ระยะกลาง พอได้ข้อมูลเบื้องต้นมาแล้วระยะกลางก็ช่วยส่งเอกสารที่เกี่ยวข้องตามมา อันนี้เป็นประโยชน์ที่จะใช้เป็นพยานหลักฐาน ขออย่างเป็นทางการเพื่อให้รัฐบาลประเทศที่เราร้องขอไปรับรองว่าเป็นเอกสารที่ถูกต้องแท้จริง แต่ความเข้าใจของการเจ้าหน้าที่ของไทยตอนนี้คือนึกว่ามีช่องทางเดียว คือความร่วมมืออย่างเป็นทางการ ที่สำนักงานต่างประเทศมีอัตรากำลังทั้งพนักงานอัยการและธุรการประมาณ 60 กว่าคน ณ ตอนนี้ก็เพียงพอ แต่ก็รับงานที่หนักพอสมควร ผมเชื่อว่าปริมาณงานจะค่อยๆ เพิ่มขึ้นเรื่อยๆ ส่วนอัตรากำลังที่เหมาะสมยังบอกไม่ได้ ขึ้นอยู่ว่ามี

ความสามารถในการสอบสวนคดี Cyber crime มากน้อยขนาดไหน คดีอาชญากรรม Cyber crime เพิ่มขึ้นแน่นอน แต่การดำเนินคดียังน้อยเพราะความสามารถในการสืบสวนสอบสวนยังน้อย

การพัฒนาบุคลากรเพื่อเตรียมรับมือกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่สำนักงานต่างประเทศ ไม่เคยจัด แต่ส่งคนไปอบรมกับหน่วยงานอื่นเป็นผู้จัด

ปัญหาที่สำคัญในการทำงานอย่างหนึ่งคือ การประสานงานขึ้นอยู่ว่าเจ้าหน้าที่ที่รับเรื่องในต่างประเทศจะทำให้เราช้าหรือไว และเรื่องการแปลภาษา บางประเทศให้แปลเป็นภาษาท้องถิ่นหรือภาษาที่เราไม่ชำนาญ ก็จะทำให้คดีล่าช้าและไม่สามารถตรวจสอบว่าแปลถูกต้องหรือไม่

ส่วนระบบอินเทอร์เน็ตในสำนักงานยังไม่ค่อยสมบูรณ์ มีหลุดบ้างเป็นครั้งคราว ซึ่งเป็นเรื่องที่ต้องปรับปรุงแก้ไข การบริหารจัดการในสำนักงาน ของเรายังไม่มีการย้ายเข้าออกจำนวนมาก คนใหม่ย้ายเข้ามา คนเก่าที่อยู่เดิมก็คอยสอนงานให้ ไม่นานก็สามารถปฏิบัติงานได้เลย

แนวทางการทำงานในการต่อสู้กับ Cyber crime ในอนาคต ต้องมีการเตรียมบุคลากรมีการพัฒนาฝึกอบรมให้มีความรู้ความสามารถ ความเชี่ยวชาญทางด้านอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ และการใช้ความรู้ในด้านการติดต่อประสานงาน

6. นาย ธนิต ประภาตนันท์ ผู้อำนวยการสำนักงานป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

มีการแบ่งส่วนงานออกเป็น 7 กลุ่มงาน ได้แก่

1. กลุ่มงานเทคนิคและเฝ้าระวัง (กทฝ.) มีอำนาจหน้าที่

1.1 งานรับเรื่องร้องเรียนทางเทคโนโลยีสารสนเทศ

1.2 งานตอบปัญหาและชี้แนะในเบื้องต้น

1.3 ตรวจสอบข้อมูลข่าวสารและรับแจ้งเบาะแสบนเครือข่ายเทคโนโลยีสารสนเทศ

1.4 เฝ้าระวังและติดตามอาชญากรรมทางเทคโนโลยีสารสนเทศ

1.5 วิเคราะห์ข้อมูลอาชญากรรมทางเครือข่ายเทคโนโลยีสารสนเทศ

1.6 ดูแล รับผิดชอบ บริหารจัดการงานศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center : CSOC

1.7 รายงานผลการดำเนินงานตามข้อ 1.6 ต่อผู้บริหารทุก 15 วัน

1.8 รายงานผู้บังคับบัญชาและผู้บริหารอย่างทันท่วงที กรณีได้รับข้อมูลข่าวสารหรือเบาะแสเกี่ยวกับการกระทำความผิดทางเทคโนโลยีสารสนเทศในประเด็นที่สื่อมวลชนสนใจหรือได้รับความสนใจจากกระแสสังคม เพื่อให้การบริหารงานจัดการเป็นไปอย่างรวดเร็ว เท่าทันต่อสถานการณ์ที่เกิดขึ้น โดยมิให้เกิดความเสียหายกับกระทรวง

1.9 ประสานงานกับผู้ให้บริการอินเทอร์เน็ตเพื่อขอความร่วมมือในเบื้องต้น กรณีจำเป็นเร่งด่วน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับกระทรวงหรือสังคมส่วนรวม

1.10 เป็นศูนย์กลางในการประสาน รวบรวมสถิติ และรายงานผลการระงับการแพร่หลายซึ่งข้อมูล คอมพิวเตอร์ที่ไม่เหมาะสม

1.11 ปฏิบัติงานอื่นตามที่มอบหมาย (เป็นกรณีชั่วคราวเฉพาะกิจ) ดังนี้

1.11.1 เป็นวิทยากรบรรยายให้ความรู้แก่หน่วยงานตามที่ร้องขอ

1.11.2 เข้าร่วมการประชุมชี้แจงต่อคณะกรรมาธิการที่เกี่ยวข้องกับทางด้านเทคนิค

2. กลุ่มงานสืบสวนทางเทคโนโลยีสารสนเทศ (กสท.) มีอำนาจหน้าที่

2.1 ปฏิบัติการ บริหารจัดการบูรณาการการทำงานด้านการสืบสวนด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ

2.2 วิเคราะห์ จัดทำแผน/นโยบาย/แนวทาง/กระบวนการสืบสวนการกระทำความผิดทางเทคโนโลยีสารสนเทศและการสื่อสาร

2.3 ปฏิบัติงานหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือได้รับมอบหมาย

2.4 สนับสนุนภารกิจศูนย์ปฏิบัติการต่อสู้เพื่อเอาชนะยาเสพติด

2.5 ปฏิบัติงานอื่นตามที่มอบหมาย (เป็นกรณีชั่วคราวเฉพาะกิจ) ดังนี้

2.5.1 ตรวจสอบข้อมูล ข่าวสารและรับแจ้งเบาะแสบนเครือข่ายเทคโนโลยีสารสนเทศ ด้านที่ขัดต่อศีลธรรมอันดีของประชาชน

2.5.2 เฝ้าระวัง วิเคราะห์ และติดตามการกระทำความผิดทางเทคโนโลยีสารสนเทศ ด้านที่ขัดต่อศีลธรรมอันดีของประชาชน

3. กลุ่มงานวิเคราะห์และพิสูจน์หลักฐานการกระทำความผิดทางเทคโนโลยีสารสนเทศ (กวผ.) มีอำนาจหน้าที่

3.1 รวบรวม จัดเก็บ ตรวจสอบ วิเคราะห์ และพิสูจน์หลักฐานอิเล็กทรอนิกส์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3.2 ให้การสนับสนุนด้านวิชาการ ให้คำปรึกษา แนะนำ บรรยาย ตอบข้อหารือเกี่ยวกับกระบวนการตรวจพิสูจน์หลักฐานอิเล็กทรอนิกส์ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3.3 พัฒนาองค์ความรู้และทักษะการตรวจพิสูจน์หลักฐานอิเล็กทรอนิกส์สู่มาตรฐานสากล

3.4 ปฏิบัติงานหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือได้รับมอบหมาย

4. กลุ่มงานส่งเสริมและสนับสนุน (กสส.) มีอำนาจหน้าที่

4.1 ปฏิบัติงานด้านนโยบายและยุทธศาสตร์

4.2 จัดทำแผนการประเมินและควบคุม

4.3 สนับสนุนการบริหารจัดการของ สป.ทก.

4.4 บริหารจัดการงบประมาณ

4.5 ให้ข้อเสนอแนะ/ความเห็นทางด้าน พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

4.6 สนับสนุนและประสานความร่วมมือระหว่างหน่วยงาน

4.7 สร้างความตระหนักรู้ภาคประชาชน

4.8 สร้างเครือข่ายความร่วมมือการดำเนินงานกับหน่วยงานอื่นที่เกี่ยวข้องหรือได้รับมอบหมาย

5. กลุ่มประสานงานด้านกฎหมายเทคโนโลยีสารสนเทศ (กปก.) มีอำนาจหน้าที่

5.1 ส่งเสริม พัฒนา ศึกษา วิเคราะห์และปรับปรุงกฎหมายที่เกี่ยวข้อง

5.2 บริการให้คำปรึกษา วิเคราะห์ และรับคำร้องทุกข์กล่าวโทษและดำเนินการตามกระบวนการทางกฎหมายที่เกี่ยวข้อง

5.3 ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นให้สอดคล้องตามกระบวนการของกฎหมาย

5.4 กลั่นกรองและวิเคราะห์และยุติการเผยแพร่ข้อมูลที่ไม่เหมาะสม

5.5 ปฏิบัติงานอื่นตามที่มอบหมาย (เป็นกรณีชั่วคราวเฉพาะกิจ) ดังนี้

5.5.1 เป็นวิทยากรบรรยายให้ความรู้แก่หน่วยงานตามที่ร้องขอ

5.5.2 บริหารจัดการงานที่เกี่ยวข้องกับพนักงานเจ้าหน้าที่ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

5.5.3 ตรวจสอบข้อมูล ข่าวสารและรับแจ้งเบาะแสบนเครือข่ายเทคโนโลยีสารสนเทศ ด้านความมั่นคง

5.5.4 เฝ้าระวัง วิเคราะห์ และติดตามการกระทำความผิดทางเทคโนโลยีสารสนเทศ ด้านความมั่นคง

6. กลุ่มงานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (กมท.) มีอำนาจหน้าที่

6.1 วิเคราะห์ ตรวจสอบ เฝ้าระวัง กำกับและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ

6.2 กำกับและประสานภารกิจ Government CERT ทั้งในและต่างประเทศ

6.3 ศึกษา วิเคราะห์ จัดทำ และเสนอแผนแม่บทด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ

7. กลุ่มงานประสานความมั่นคง (กปม.) มีอำนาจหน้าที่

7.1 ประสานงานกับหน่วยงานด้านความมั่นคงทั้งในและต่างประเทศ

7.2 ส่งเสริมภาพลักษณ์ประเทศไทยในด้านเทคโนโลยีสารสนเทศและการสื่อสาร

7.3 บูรณาการด้านความมั่นคง

7.4 ปฏิบัติงานอื่นด้านความมั่นคงตามที่ได้รับมอบหมาย

อำนาจหน้าที่ ความรับผิดชอบเพิ่มเติม ของ ผอ.กลุ่มงาน และหัวหน้าฝ่าย

1. ดูแล รับผิดชอบ กำกับตัวชี้วัดแผนงาน/โครงการให้เป็นไปตามเป้าหมาย

2. จัดทำแผนการดำเนินงานโครงการ และบริหารจัดการโครงการให้ดำเนินการเป็นไปตามเป้าหมาย และเสร็จภายในกำหนดระยะเวลา

3. ควบคุม ดูแล เร่งรัดการจัดซื้อจัดจ้าง และตรวจรับงานให้เป็นไปตามระเบียบ และภายในกำหนดระยะเวลา

4. ควบคุม ดูแล และกำกับตัวชี้วัดการปฏิบัติราชการของผู้ใต้บังคับบัญชาในสังกัด

5. จัดทำแผนการควบคุมภายใน ระดับกลุ่มงาน

6. สนับสนุนงานบริหารจัดการของ ปท. อื่นๆ ที่เกี่ยวข้อง

7. ปฏิบัติงานอื่นๆ ตามที่ ผอ.ปท. มอบหมาย

งานหลักที่ทำ

1. ปิดเว็บไซด์ ส่วนมากจะเป็นเว็บที่หมิ่นสถาบันพระมหากษัตริย์กับเว็บลามกอนาจาร ขั้นตอนคือยื่นคำร้องต่อศาล เมื่อศาลมีคำสั่งแล้ว ส่งหนังสือไปยังผู้ให้บริการ (Internet Service Provider) ปิดเว็ปไซด์ โดยส่งคำสั่งศาลให้ทางE-mail และก็มีหนังสือตามไป เมื่อได้รับคำสั่ง แล้ว ก็มีการดำเนินการปิดภายใน 4-5 ชั่วโมงไม่เกิน 6 ชั่วโมง จากนั้นท้ายที่สุดเราก็จะส่งเอา URL ของเว็บไซด์ต่างๆพร้อมทั้งคำสั่งส่งไปยัง ปอท. เพื่อดำเนินคดีตามกฎหมายต่อไป คือไปสอบสวนหาผู้กระทำความผิด เพื่อดำเนินคดีฟ้องศาล สอบสวนและส่งอัยการ ดำเนินคดีจับกุมผู้กระทำความผิด

2. ทำงานร่วมกับเจ้าหน้าที่ตำรวจที่ขอความร่วมมือมา

3. ตรวจพิสูจน์วัตถุพยานคอมพิวเตอร์

4. รับเรื่องราวร้องทุกข์ โดยให้ผู้เสียหายไปแจ้งความก่อน จากนั้นจะตรวจสอบข้อมูลให้ตามอำนาจหน้าที่ แต่ก็มีข้อจำกัด บางทีมีความเสียหายมันเกิดขึ้น หลักฐาน ข้อมูล ต้นกำเนิดแหล่งผู้กระทำความผิดอยู่ต่างประเทศ อันนี้ก็ไม่สามารถจะให้ข้อมูลได้เลย เช่น facebook , Youtube ในปัจจุบันมีข้อจำกัดแบบนี้ด้วย และก็เรื่องการเข้ารหัส ว่าถ้าเกิด http เข้ารหัสเนี่ย เราปิดไม่ได้ และก็ไม่สามารถที่จะไปตรวจสอบเขาได้ด้วย นอกจากว่าเขามี server หรือ ผู้ให้บริการเว็บไซด์ เขามีแหล่งข้อมูล แหล่งเก็บข้อมูลอยู่ต่างประเทศ อเมริกาเป็นหลัก นอกเหนืออำนาจของเรา เราก็ทำอะไรไม่ได้ เรื่องนี้มันเป็นปัญหาอยู่ทุกวันนี้ ก็พยายามหาอุปกรณ์เทคโนโลยีที่ทันสมัยแก้ปัญหา

ประกาศ คสช. เมื่อวันที่ 26 สิงหาคม 2557 อันนี้เป็นลักษณะที่พิเศษอยู่อย่างหนึ่งที่แตกต่างจาก พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 คือ ให้ปิดกั้นในกรณีที่ปรากฏข้อมูลต่างๆที่เป็นเว็บหมิ่น หรือเป็นการยุยงส่งเสริมให้เกิดการแตกแยกกัน สามารถปิดกั้นได้เลย ไม่ต้องยื่นคำร้องต่อศาล สอบสวนเพิ่มเท่านั้นเอง

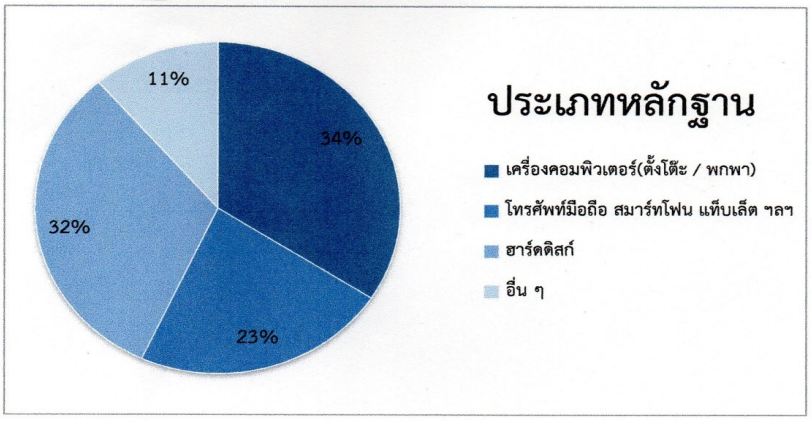
แต่ก็มีปัญหาตามมาอีก พอใช้ประกาศนี้ พอเราแจ้งขอความร่วมมือไปต่างประเทศเพื่อขอการปิดกั้น เรื่องคดีหมิ่นใน facebook เราปิดไม่ได้อย่างนี้ ทำไง ก็ต้องขอความร่วมมือจากเค้า ให้เค้าปิด ก็ต้องยื่นศาล เ เค้าต้องการคำสั่งศาล เอาคำสั่งศาลที่ว่าผิดกฎหมายไหม ก็ต้องดำเนินการตาม พรบ.คอม เพื่อว่าเมื่อได้คำสั่งศาล แล้วเนื้อหาการกระทำความผิด ขอความร่วมมือเค้า เพื่อให้เค้าปิดกั้น ก็ยังทำได้อยู่ในระดับหนึ่ง แต่ก็ไม่ได้หมายความว่าเค้าจะปิดกั้นให้เราเสมอไปนะครับ เพราะบางทีนี่เค้ามองว่าเป็นเรื่องปกติธรรมดา เว้นแต่เรื่องจำเป็นจริงๆ แล้วอาจจะมีประชาชนและสาธารณชนมีการ report รายงานไปทางเค้าเยอะ แล้วก็เค้าจะมีนักกฎหมายที่อ่านภาษาไทยเป็น จ้างคนไทยซึ่งเป็นนักกฎหมายระหว่างประเทศทำนองนั้น ช่วยแปลด้วย เค้าก็จะปิดให้เป็นบางเรื่องบางราว จะปิดให้ไม่เกิน 5 เปอร์เซนต์ เป็นการขอความร่วมมือในลักษณะของการระงับความเผยแพร่โดยให้ทางนั้นลบออกจากระบบเท่านั้นเอง

นอกจากนั้นเรามีภารกิจป้องกันปราบปราม ไม่ใช่เป็นการระงับการเผยแพร่อย่างเดียว เราก็ต้องส่งเสริม สนับสนุนลักษณะที่ว่า ในเชิงนโยบาย ในการที่เรียกว่าสร้างความตระหนักรู้ในเครือข่าย ไม่ว่าจะเป็นนักศึกษา ประชาชน สมาคม องค์กรต่างๆ อาจารย์นิสิตนักศึกษา ให้รู้ถึงตระหนักถึงการที่ว่าเราใช้คอมพิวเตอร์นะครับ ใช้ให้ถูกต้องเหมาะสม โดยที่เรียกว่าไม่ไปดำเนินการใช้คอมพิวเตอร์เป็นเครื่องมือดำเนินการกระทำความผิดตาม พ.ร.บ.จาก พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เช่น การไป forward ไปส่งข้อมูลพวกนี้ และก็ไม่ให้เด็กมีโอกาสเปิดดูข้อมูลที่ไม่เหมาะสม เช่นการพนัน ภาพโป๊ เราก็ต้องสร้างเสริมความตระหนักให้เยาวชน พ่อแม่ผู้ปกครอง ซึ่งอาจจะทำเป็นซอฟแวร์ขึ้นมา เพื่อปกป้องสกัดกั้น ลงโปรแกรมอย่าให้

ลูกหลานรู้แล้วกัน เพื่อจะได้เปิดไม่ได้ คือสร้างซอฟแวร์ขึ้นมาเพื่อการสกัดกั้นการเข้าถึงโปรแกรมเค้าเรียกว่าโปรแกรม housekeeper แล้วก็มีอีกหลายอย่าง การอบรม สัมมนา ประชาชน ผู้ใหญ่บ้านต่างๆ ให้รู้ถึง ตระหนักถึง เกี่ยวกับเรื่อง การใช้คอมพิวเตอร์ให้ถูกต้องเหมาะสมและไม่เป็นการทำผิดตามกฎหมาย และอีกอย่างคือให้ตระหนักถึงสถาบันของชาติ เช่น พระมหากษัตริย์เป็นคุณูปการของประเทศชาติอย่างไร เพื่อให้เกิดความจงรักภักดี เกิดความสามัคคีกับคนในชาติ อันนี้ก็เป็นภารกิจที่เราตระหนักในช่วงนี้

แผนภาพที่ 3 – 1 สถิติหลักฐานทางเทคโนโลยีที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้รับในปี 2557

เดือน	จำนวนเคส	จำนวนหลักฐาน				
		เครื่องคอมพิวเตอร์ (ตั้งโต๊ะ / พกพา)	โทรศัพท์มือถือ สมาร์ทโฟน แท็บเล็ต ฯลฯ	ฮาร์ดดิสก์	อื่น ๆ	รวม
ม.ค.	1	1				1
ก.พ.	0					0
มี.ค.	1	2			3	5
เม.ย.	1		3			3
พ.ค.	6	1	2	2	2	7
มิ.ย.	1			1		1
ก.ค.	3	3		1		4
ส.ค.	0					0
ก.ย.	1	1		1		2
ต.ค.	3	2	1	2		5
พ.ย.	3	3		3		6
ธ.ค.	3	2	4	4		10
	23	15	10	14	5	44

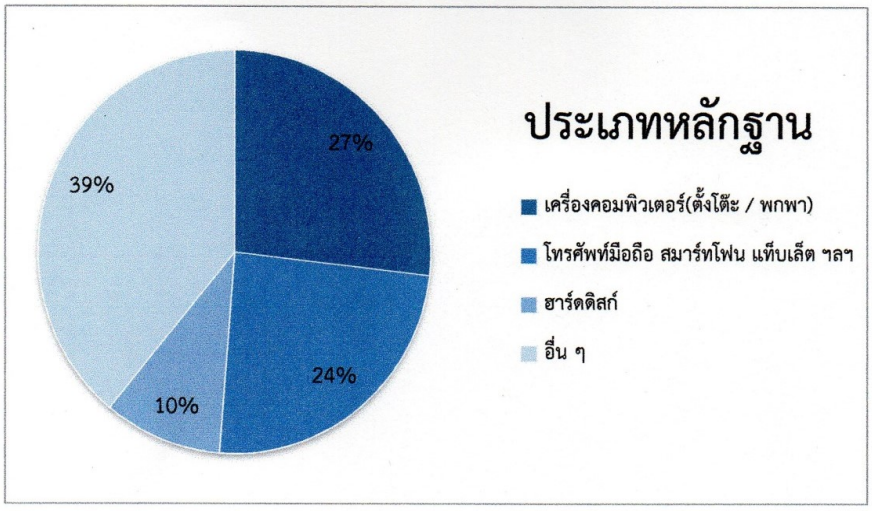


ข้อมูลอัพเดทเมื่อ 4 เมษายน 2558

ที่มา : ปริมาณงานคดีปี 2557 สถิติหลักฐานทางเทคโนโลยีปี 2557 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แผนภาพที่ 3 – 2 สถิติหลักฐานทางเทคโนโลยีที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้รับในปี2558

เดือน	จำนวนเคส	จำนวนหลักฐาน				
		เครื่องคอมพิวเตอร์ (ตั้งโต๊ะ / พกพา)	โทรศัพท์มือถือ สมาร์ทโฟน แท็บเล็ต ฯลฯ	ฮาร์ดดิสก์	อื่น ๆ	รวม
ม.ค.	2	3	4	1	1	9
ก.พ.	5	7	2	1	14	24
มี.ค.	4	1	4	2	1	8
เม.ย.						0
พ.ค.						0
มิ.ย.						0
ก.ค.						0
ส.ค.						0
ก.ย.						0
ต.ค.						0
พ.ย.						0
ธ.ค.						0
	11	11	10	4	16	41



ข้อมูลอัพเดทเมื่อ 4 เมษายน 2558

ที่มา : ปริมาณงานคดีปี 2558 สถิติหลักฐานทางเทคโนโลยีปี2558/กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ทำงานเกี่ยวข้องใกล้ชิดกับ

1. กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี
2. กรมสอบสวนคดีพิเศษ
3. สำนักงานอัยการสูงสุด
4. ผู้ให้บริการ
5. กระทรวงต่างประเทศ
6. หน่วยงานด้านความมั่นคง/กองทัพ

ด้านบุคลากร

ทุกกลุ่มงานมีรวมประมาณ 30 คน ถ้าเป็นนักวิชาการคอมพิวเตอร์ ก็จบพวกวิทยาศาสตร์คอม, วิศวกรรมคอมพิวเตอร์, สารสนเทศรวมทั้งกลุ่มมีอัตรากำลัง 50 คนน่าจะเหมาะสม ที่ต้องการอัตรากำลังเพิ่ม เพราะว่าเทคโนโลยีต่างๆมันเปลี่ยนแปลงไป เราก็ต้องมีความเท่าทัน พอมีความเท่าทันแล้วเทคโนโลยีก็ต้องเพิ่มขึ้น คนที่จะต้องมารับรองใช้อุปกรณ์พวกนี้ก็ต้องเพิ่มขึ้นตามคนและเครื่องมือต้องสอดคล้องกันทั้งสองอย่าง คนมากแต่เครื่องมือน้อย ไม่ได้ มันต้อง Balanceกัน เพราะที่นี่รับผิดชอบทั้งประเทศ

มีเจ้าหน้าที่เพียง 3 – 4 คน นี่คือคนเฝ้าระวัง ส่วนด้าน Forensic ที่นี่มีแค่ 2 คน ต้องเป็นผู้เชี่ยวชาญถึงระดับที่ออกรายงานได้ และก็ต้องไปเป็นพยานศาลอีกด้วย ตอนนี้มีมาฝึกงานช่วยอีก 1 คน

แนวการพัฒนาบุคลากร

1. การพัฒนาตอนนี้ก็มี อบรมในประเทศ เกี่ยวกับเรื่อง การเป็นพนักงานเกี่ยวกับการสืบสวน สอบสวน การเป็นพนักงาน Forensics ที่เราต้องการให้ใกล้เคียงกับตำรวจ และอีกอันก็คือเรื่องด้านเทคนิคเกี่ยวกับว่า เกี่ยวกับพวกการระบบเครือข่าย การเจาะระบบ นี่สำคัญ Forensics เข้ามาพิสูจน์หาบุคคล หาร่องรอยการกระทำความผิด แต่ว่านี่สำคัญ แต่เราหาคนมาฝึกสอนยาก แต่ตอนนี้ เริ่มพัฒนา หาคนเป็นอาจารย์มาได้ปีหนึ่งก็ประมาณ 1 – 2 หลักสูตร แต่ที่อื่นถ้ามีหลักสูตรเหมือนกัน แต่ใกล้เคียง เช่นภาคเอกชนจัดขึ้นมา เราก็ส่งคนไปร่วม

2. การศึกษาดูงานในประเทศและต่างประเทศ โดยตัวเองไม่มี มีแต่คนอื่นเชิญไป ถ้ามีงบสนับสนุนเราก็ไป ผู้บริหารก็มี แต่ถ้าผู้บริหารไม่ไปก็ให้ระดับผู้ปฏิบัติงานไปจะได้เพิ่มความรู้และทักษะ เช่น ประเทศ เกาหลี ญี่ปุ่น อินโด มาเลย์ อเมริกา ไปดูการประสานงาน การอบรม เพื่อรู้ถึงปัญหาอาชญากรรมข้ามชาติ เพื่อแลกเปลี่ยนข้อมูลกันพวกอาชญากรรมข้ามชาติ ให้รู้ถึงปัญหาและให้เตรียมพร้อมไว้ว่าคุณจะแก้ปัญหายังไง หรือออกกฎหมายรองรับยังไง การฝึกอบรมประมาณปีหนึ่งก็ 2 – 3 ครั้ง ไม่เกิน 3 ครั้ง/คน

ปัญหาและอุปสรรคในการทำงาน

1. ด้านกำลังคนขององค์กร มีน้อยไป

2. ด้านงบประมาณและอุปกรณ์ ยังต้องคงต้องการอุปกรณ์ที่สำคัญจำเป็นอยู่ซึ่งมีราคาสูงมาก

3. ปัญหาด้านการโยกย้ายจากที่อื่นมารับตำแหน่งในกระทรวง การสร้างขวัญกำลังใจค่าตอบแทนพิเศษ

4. การติดต่อประสานงานอื่น กับหน่วยงานอื่น ทั้งภาครัฐและเอกชน ไม่ว่าจะเป็นตำรวจ อัยการ ศาล ได้รับการประสานงานติดต่ออย่างดี

แนวการทำงานในอนาคต การต่อสู้กับ Cyber crime

รอการปรับเปลี่ยนโครงสร้างใหม่ที่จะเป็นกระทรวง Digital และ กฎหมายที่จะออกใหม่ซึ่งมีความสำคัญประมาณ 3 ฉบับ คือ

1. กฎหมาย พ.ร.บ.คอมพิวเตอร์ 2550 ที่มีการแก้ไขใหม่

2. กฎหมายเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์

3. กฎหมายเกี่ยวกับพ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล ป้องกันข้อมูลส่วนบุคคล

และคิดว่าเมื่อกฎหมายทั้ง 3 ฉบับนี้ออกแล้วจะทำให้ระบบในประเทศไทย โครงสร้างด้านไซเบอร์มีประสิทธิภาพและทัดเทียมกับนานาอารยประเทศ

ข้อเสนอแนะ

1. เน้นความสำคัญอันที่สุดคือ เรื่องเกี่ยวกับสถาบันเบื้องสูง เป็นเรื่องสำคัญที่เราจะต้องดูแลปกป้อง ไม่ให้ใครมาล่วงละเมิด เพราะว่าเป็นสิ่งยึดเหนี่ยวให้ประชาชน ถ้าหากว่า เราสามารถดูแล มีอุปกรณ์เทคโนโลยีที่ทันสมัยและก็สร้างความตระหนักรู้ เข้าใจ ในบทบาทของสถาบันเบื้องสูงได้ ตั้งแต่พวกเด็กและเยาวชน ซึ่งรุ่นใหม่นี่ไม่เคยรู้จักกันหรอกว่าบทบาทพระราชกรณียกิจของในหลวงเราเป็นอย่างไร ถ้าหากว่าได้เข้าใจ วิธีการในประชาสัมพันธ์ให้เห็น สร้างความตระหนักถึงสิ่งที่เป็นคุณูปการของประเทศชาติด้านสถาบัน มันก็จะเกิดความเป็นอันหนึ่งอันเดียวกัน ความร่วมเย็นเป็นสุขในสังคม ซึ่งแตกต่างจากประเทศอื่นๆทั่วโลก

2. ต้องมีเทคโนโลยีที่ให้การสนับสนุนในการปกป้องไม่ให้ใครมาล่วงละเมิดสถาบัน เช่น 1.เทคโนโลยีปิดกั้น 2.เทคโนโลยีในการรวบรวมข้อมูลต่างๆที่มีการล่วงละเมิดและก็มีการชี้แจงให้ข้อมูลประชาสัมพันธ์กลับไปยังแหล่งข้อมูลที่เข้าใจผิดคลาดเคลื่อน หมดแล้วก็รวมมาคนไหนมีซอฟแวร์มีอุปกรณ์ที่รวมดึงเข้ามา ใครที่เข้าใจผิดมา ใครดูถูกรัฐบาล ใครดูถูกสถาบัน เสร็จแล้วเราก็ชี้แจงพิมพ์ข้อมูลมาพิจารณาวิเคราะห์ที่สามารถเจียนไปแล้ว สื่อสารไปแล้วเค้าจะเข้าใจ เค้าจะตระหนัก เค้าจะรู้ถึงบทบาทที่เค้าทำไปแล้วเป็นผลร้ายต่อสังคม สื่อให้เค้าเข้าใจ เราก็ต้องมีกลุ่มคนที่

ใช้วิธีการเชิงรุกสารพัดกับเค้าโดยอุปกรณ์กับเครื่องมืออีกลักษณะหนึ่ง ไม่ใช่แต่เพียงปิดกั้นเฉยๆ การปิดกั้นไม่ใช่การแก้ปัญหา การแก้ปัญหาคือการหาอุปกรณ์ ก็ต้องใช้เทคโนโลยี ก็คือซอฟแวร์และฮาร์ดแวร์ เพื่อเสริมสร้างประชาสัมพันธ์โต้ตอบ ซึ่งตรงนี้ยังขาดไป โต้ตอบให้เค้าได้ตระหนักรู้ถึงประเด็น ถึงข้อเท็จจริง สิ่งที่เค้าจะได้รับตามมา ทั้งผลดีผลเสียเป็นอย่างไร ให้เค้าใช้วิจารณญาณของเค้าเอง เราแค่ให้ข้อมูลที่ถูกต้อง คิดว่าสิ่งเหล่านี้ก็จะผ่อนคลายและลดลงหมดไปในสังคม

3. ให้ออกกฎหมายที่ทันสมัยเหมือนอย่างนานาอารยประเทศ คือ Lawful interseption เป็นกฎหมายเกี่ยวกับจัดระเบียบข้อมูล จะเป็นกฎหมายที่ให้อำนาจของรัฐเข้าไปสืบเสาะ แสวงหาดักข้อมูลอะไรต่างๆได้ ให้อำนาจรัฐปกป้องเจ้าหน้าที่ของรัฐ ทำให้การทำงานเรามีประสิทธิภาพมากขึ้น เพราะทุกวันนี้เรายังไม่มี

4. เพิ่มค่าตอบแทนให้กับเจ้าหน้าที่เพื่อเป็นขวัญกำลังใจในการทำงาน

7. พล.ต.ต.ธวัชชัย เมฆประเสริฐสุข ผู้บังคับการกองพิสูจน์หลักฐาน และ พ.ต.อ.อนุชิต บุญญะปฏิภาค กลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง

กลุ่มงานนี้ มีหน้าที่และความรับผิดชอบเกี่ยวกับงานตรวจพิสูจน์พยานหลักฐานและของกลางในคดีที่เกี่ยวกับคอมพิวเตอร์และเทคโนโลยี โดยปฏิบัติหน้าที่ดังนี้

1. ปฏิบัติงานธุรการ งานสารบรรณ สถิติผลการปฏิบัติงานของกลุ่มงาน

2. ตรวจพิสูจน์ข้อมูลดิจิตอลที่บันทึกในหน่วยบันทึกข้อมูลหรือหน่วยความจำคอมพิวเตอร์

3. ตรวจพิสูจน์คอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์

4. ตรวจพิสูจน์การตัดต่อสื่อบันทึกเสียงและวีดีทัศน์

5. ตรวจพิสูจน์เปรียบเทียบร่องรอยบนแผ่นซีดี

6. ดำเนินการจัดทำรายงานการตรวจพิสูจน์ รับ-ส่งของกลาง เก็บรักษาของกลางและสำเนารายงานการตรวจพิสูจน์

7. งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

ขณะนี้มีบุคลากรจำนวน 7 คนและอยู่ในระหว่างการฝึกงานอีก 3 คน จบการศึกษาด้านวิทยาศาสตรบัณฑิต รับงานตรวจพิสูจน์พยานหลักฐานจากสถานีตำรวจนครบาลและในภูมิภาคระดับผู้ชำนาญการ เป็นผู้ตรวจและลงนามในรายงาน โดยในรายงานเราจะลงแค่ ยศ – ชื่อ ผู้ตรวจพิสูจน์ รับผิดชอบทุกอย่างตั้งแต่เริ่มต้นจนถึงกระบวนการขึ้นศาล การรายงาน เรื่องอายุโดยเฉลี่ยอยู่ที่ประมาณ 30 ปีเศษ

ตอนนี้ทางสำนักงานก็ยังขาดแคลนอัตรากำลังอยู่ ถ้าจะทำงานให้มีประสิทธิภาพน่าจะมีสัก 9 คน จึงจะเหมาะสม สาเหตุก็คือเราถูกจำกัดอัตรากำลังของภาครัฐ แต่พอได้มาก็ยังต้องถูกกระจายกำลังให้หน่วยงานอื่นอีก ตอนนี้ที่ศูนย์พิสูจน์หลักฐานก็จะมี 10 ศูนย์ทั่วประเทศ ศูนย์ใหญ่มีอยู่สามที่ คือ ลำปาง นครราชสีมา และสามจังหวัดชายแดนภาคใต้ มีผู้บังคับการเป็นผู้บัญชา ส่วนที่ลำปางกำลังฝึกงานอยู่ 1 คน และสามจังหวัดชายแดนใต้ก็มีเฉพาะโครงสร้างของสำนักงานแต่ยังไม่มีผู้ปฏิบัติงาน ส่วนนครราชสีมามีผู้ปฏิบัติงานอยู่คนเดียวและกำลังฝึกงานอยู่ 1 คน ส่วนการฝึกอบรมก็มีอยู่ 3 ขั้นตอน คือภาคทฤษฎี ฝึกภาคปฏิบัติอีกอย่างน้อย 1 ปี และต้องทำงานตรวจพิสูจน์อย่างน้อย 100 เรื่อง และมีการทดสอบประมวลผลความรู้ต่อคณะกรรมการชุดตรวจอาชญากรรมทางคอมพิวเตอร์เป็นผู้ประเมิน (คณะกรรมการของ สพฐ.) ผลการทดสอบต้องไม่น้อยกว่า 80 % ถึงจะสามารถเป็นผู้ชำนาญการในการตรวจพิสูจน์ เซ็นรับรองรายงานได้

ในตอนนี้เราทำงานใกล้ชิดกับ เช่น กองบังคับการสนับสนุนทางเทคโนโลยี, ปอท., ETDA (สำนักงานพัฒนาธุรกรรมทางอิเล็คทรอนิคส์) เพราะเขาให้ความช่วยเหลือเราอยู่ตลอด ส่วนกระทรวงเทคโนโลยีและการสื่อสาร ไม่ค่อยมี

การติดต่อกับหน่วยงานภาคเอกชน ก็มีการติดต่อประสานงานอยู่บ้าง เช่น การติดต่อขอซื้อเครื่องมือ และการฝึกอบรม เขาก็จะส่งเจ้าหน้าที่ วิทยากรมาคอยแนะนำจากต่างประเทศมาให้ความรู้แก่เรา และเมื่อมีการอบรมที่ไหน เมื่อไหร่เขาก็จะแจ้งมาถ้ามีค่าใช้จ่ายเราก็ทำตามขั้นตอนไป ไม่มีค่าใช้จ่ายเราก็ไปร่วมได้เลย

นอกจากมีเจ้าหน้าที่มาอบรมการใช้เครื่องมือให้ ยังมีเจ้าหน้าที่จากต่างประเทศที่เราประสานงานด้วยมาให้ข้อมูล สมัยก่อน ATA ของสหรัฐอเมริกาเขาให้การสนับสนุนเครื่องมือเราจำนวนมากและเป็นเครื่องมือที่มีความทันสมัยที่สุดในประเทศเพราะเขาซื้อใหม่ๆ เขาเอามาให้เราเลยเราไม่ต้องทำตัดซื้อจัดจ้างเลย และเขาก็ยังให้เจ้าหน้าที่มาแนะนำวิธีการใช้เครื่องมือและอุปกรณ์มาสอนเพิ่มเติมให้อยู่เรื่อยๆ ก็ถือเป็นหน่วยงานภายนอก แต่ส่วนมากจะเป็นการติดต่อส่วนตัวแล้วค่อยรายงานผู้บังคับบัญชา

แนวทางการพัฒนาบุคลากรโดยภาพรวม

มีการฝึกอบรมอยู่ตลอด การสัมมนาเชิงปฏิบัติการ ความรู้ต่างๆ ก็มีหลายแห่งที่เปิดฝึกอบรมเราก็ไปฝึกอบรมร่วมกับเขา เราเป็นหน่วยงานใหม่ เราก็พยายามเปิดตัว มีอะไรก็ส่งมาให้บ้างทางเราบ้างเพื่อเป็นข้อมูลใหม่ๆ จะได้รู้ จะได้ทราบข้อมูลข่าวสาร การฝึกอบรมมีทั้งในประเทศและต่างประเทศ มีการฝึกอบรมร่วมกับหน่วยงานอื่นๆ

ส่วนมากเป็นหลักสูตรที่เกี่ยวกับ Digital Forensic ปริมาณการฝึกอบรมทั้งในประเทศและต่างประเทศประมาณ 5 – 6 ครั้ง/คน/ปี ส่วนมากเป็นหลักสูตรสั้นๆ 3 – 5 วัน ส่วนเรื่อง

งบประมาณถ้าเป็นงบประมาณต่างประเทศเราไม่มีงบประมาณเลย แต่จะได้รับการสนับสนุนจากหน่วยงานที่จัดการฝึกอบรมที่เชิญเราไปอบรม เช่น อเมริกา จีน ออสเตรเลีย บุคลากรของเราต้องมีการตื่นตัวอยู่ตลอดเวลา เพราะว่าสถานการณ์โลก เทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา เราต้องทำความเข้าใจกับเครื่องใหม่ๆอยู่ตลอด

การดูงานต่างประเทศโดยส่วนมากเขาจะใช้ภาษาอังกฤษเราก็เลยไม่ต้องใช้ล่ามเพราะเจ้าหน้าที่เราใช้ภาษาอังกฤษสื่อสารได้ดีกันทุกคน สำหรับการศึกษาดูงานก็จะมีเป็นช่วงๆ เวลาไปก็จะมีการหมุนเวียนกันไปแล้วแต่หลักสูตร เช่นหลักสูตรเกี่ยวกับระดับปฏิบัติการ หลักสูตรเกี่ยวกับผู้บริหาร ก็ดูตามสมควร

ด้านงบประมาณ งบประมาณเราก็ยังมีน้อยไป ในเรื่องการของบประมาณนั้นเราขอไปเท่าไหร่เขาก็จะให้เราเท่านั้น แต่เราต้องไปนำเสนอให้ได้ว่าเอาไปใช้ดำเนินการอะไรบ้าง เรายังต้องการเพิ่มอีก เนื่องจากปริมาณงานเพิ่มขึ้นมาโดยตลอด เพื่อรองรับคดีในอนาคต

การบริหารงานบุคคล การโยกย้าย การเลื่อนตำแหน่ง

ขึ้นอยู่กับความพึงพอใจ ขวัญกำลังใจ เขาก็จะอยู่ได้นาน อย่างนักวิทยาศาสตร์ นักพิสูจน์หลักฐานจะไปที่อื่นยาก เพราะว่าหน่วยงานที่จะทำงานแนวนี้ไม่ค่อยมี เช่น ของตำรวจนี้ไปไม่ได้อยู่แล้ว นอกจากจะไปศึกษาเพิ่มให้มีวุฒิการศึกษาด้านกฎหมายหรืออย่างอื่น แต่โดยภาพรวมแล้วก็จะไม่ให้ไป เพราะเรามีหลักเกณฑ์ว่าคุณจะต้องอยู่นี้กี่ปี ไม่งั้นหายหมด ต่อไปคุณจะไปสมัครกองคดีคุณก็ไปไม่ได้เพราะคุณไม่มีวุฒิทางกองคดีเพราะเขาก็กำหนดคุณสมบัติของเจ้าหน้าที่อยู่แล้วก่อนหน้านี้ก็มีการไปเรียนเพิ่มและก็โอนย้ายไปหมด แต่คนที่จะมาปฏิบัติหน้าที่แทนก็ไม่มี

สิ่งที่ต้องการคือแรงจูงใจ อย่างเช่น กรณีไปฝึกอบรมมาได้ประกาศนียบัตร ก็ต้องให้เงินเพิ่มเดือนละ 500 หรือ 1000 ส่วนเรื่องการโยกย้าย การเลื่อนตำแหน่ง ก็ไม่มีปัญหาอะไร และก็ไม่ค่อยโยกย้ายไปไหน เพราะคุณสมบัติที่ตรงตามความต้องการอยู่แล้ว แต่น่าจะมีการขอค่าตอบแทนเพิ่มขึ้นอีก

การติดต่อประสานงานกับหน่วยงานอื่น ไม่มีปัญหาอะไร

แนวทางการทำงานในอนาคตในการต่อสู้กับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

1. ต้องการอัตรากำลังคนคนเพิ่ม และฝึกคนให้ทำงานได้เร็วขึ้น

2. หาเครื่องมืออุปกรณ์การตรวจที่ทันสมัย และมีจำนวนมากขึ้น เพื่อช่วยในการทำงาน

3. ของบประมาณเป็นค่าตอบแทนการทำงานนอกเวลา เพื่อให้เจ้าหน้าที่ปฏิบัติงานได้ 24 ชั่วโมง

4. สร้างเครือข่ายความร่วมมือกับหน่วยงานต่างๆ ในต่างประเทศ เช่น สหรัฐอเมริกา ออสเตรเลีย เพื่อแลกเปลี่ยนประสบการณ์และแสวงหาเทคโนโลยีใหม่กับต่างประเทศ

ข้อเสนอแนะ

1. ควรหาหน่วยงานภาครัฐเป็นเจ้าภาพในการบูรณการทำงาน ฝึกอบรมร่วมกันของหน่วยงานที่เกี่ยวข้อง มีการแลกเปลี่ยนข้อมูล ข่าวสาร ไม่ต่างคนต่างทำ

2. เร่งสร้างผู้ตรวจพิสูจน์ที่เชี่ยวชาญ ให้เพียงพอกับปริมาณคดี

3. สร้างขวัญกำลังใจ ค่าตอบแทน และสวัสดิการให้เหมาะสม

4. จัดหาอาคารสถานที่ที่กว้างขวางกว่าที่เป็นอยู่ และจัดหา อุปกรณ์การทำงานที่ทันสมัยมีประสิทธิภาพ

8. คุณอมรรัตน์ เล็กพิชัย หัวหน้ากลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์ สถาบันนิติวิทยาศาสตร์

กลุ่มงานนี้ตั้งอย่างเป็นทางการเมื่อวันที่ 1 ต.ค.57 มีเจ้าหน้าที่รวม 3 คน มีหน้าที่คือ การตรวจพิสูจน์พยานหลักฐานทางอิเลคทรอนิกส์ ประเภทคอมพิวเตอร์ โทรศัพท์มือถือ อุปกรณ์จัดเก็บบันทึกข้อมูล จากหน่วยงานที่ร้องขอให้มีการตรวจพิสูจน์

โดยรับงานจากหน่วยงานรัฐ ส่วนมากรับงานจากกรมสอบสวนคดีพิเศษ ตำรวจ และจากหน่วยงานภายในจากคดีที่ทำเอง เช่น คดีเกี่ยวกับชีวิตที่เจ้าหน้าที่สถาบันฯ ไปเก็บพยานหลักฐานได้ จากการไปตรวจที่เกิดเหตุเอง ไม่คิดค่าใช้จ่ายในการตรวจพิสูจน์

ขั้นตอนการปฏิบัติงาน

เริ่มจากเมื่อได้รับของกลางมาแล้ว สถาบันเราจะมีระบบ มีห้องสำหรับรับวัตถุพยานแล้วจะให้เลขบาร์โค๊ด แล้วเขาก็จะจัดส่งมาที่ห้องLab พอมาถึงห้อง Lab จะมีการลงรับและบันทึกในสมุดรับว่าได้รับวัตถุพยานมาเมื่อไหร่ วันไหน และก็ทำการจ่ายงานให้กับเจ้าหน้าที่แต่ละคนในการตรวจพิสูจน์ โดยที่เรากำหนดตาม KPI ว่าจะต้องทำให้เสร็จและรายงานผลการตรวจพิสูจน์ภายในไม่เกิน 30 วัน

การรายงานก่อนเวลาก็มีและเกินเวลาก็มีบ้าง แล้วแต่งานว่ายากหรือง่ายข้อมูลมากน้อยขนาดไหน ส่วนที่เกินก็อย่าง เช่น 1 งานเรารับวัตถุพยานคอมพิวเตอร์มาจำนวน 10 เครื่อง เราก็จะทยอยเอาเรื่องที่สำคัญมากก่อนแล้วค่อยๆ ทำส่วนที่สำคัญรองลงไปตามลำดับ

เราก็ต้องคุยกับผู้ส่งพยานหลักฐานว่าประเด็นที่คุณอยากได้คืออะไรที่สำคัญที่สุด เราก็จะดำเนินการในส่วนนั้นก่อน ช้าหรือเร็วขึ้นอยู่กับข้อมูล ทำงานเกี่ยวข้องกับ กรมสอบสวนคดีพิเศษ ตำรวจ กรมราชทัณฑ์ ปปส. สำนักงานอัยการสูงสุด

ปริมาณงาน ตั้งแต่ตุลาคม 2557 ถึงปัจจุบัน (เดือนกุมภาพันธ์ 58) มีอยู่ 2 Case และมีวัตถุพยานอยู่ 19 เครื่อง รับเรื่องจากกรมสอบสวนคดีพิเศษ ส่งผลและรายงานเรียบร้อยแล้ว 1 Case

และมีวัตถุพยานอยู่ 14 เครื่อง เพราะทั้ง 2 Case เราเพิ่งรับงานในเดือนธันวาคม 2557 ส่วนที่เหลืออยู่ระหว่างการดำเนินงานอยู่ต้องปรึกษาอาจารย์จากมหาวิทยาลัยมหิดลเพราะเป็นงานที่เกี่ยวกับภาพ

ส่วนงานที่สถาบันเก็บมาจากที่เกิดเหตุส่วนใหญ่จะเป็นงานที่แบบว่าการฆ่าตัวตายแล้วมีโทรศัพท์อยู่ข้างศพ เราก็จะนำมาตรวจสอบว่าเขาได้ติดต่อกับใครบ้างก่อนเกิดเหตุ มีลงรับเอกสารเหมือนงานทั่วไป แต่จะไม่นานมากเพราะดึงข้อมูลจากโทรศัพท์ ก็ไม่มีประเด็นมากและเป็นงานเร่งด่วนด้วย เช่น บางคดีเก็บโทรศัพท์จากเรือนจำเขาจะส่งมาบางคดี ส่วนมากก็จะเป็นข้อมูลว่าผู้ต้องหาได้ติดต่อกับใคร ภาพถ่าย เล่น Line แต่ละเครื่องก็ต้องดูข้อมูลเยอะเหมือนกัน กรมราชทัณฑ์ก็จะสนใจว่าเครื่องนี้มีการใช้งานในช่วงที่อยู่ในคุกหรือเปล่า ดึงข้อมูลแล้วก็จะส่งไปเรือนจำ

งานของกรมราชทัณฑ์ เมื่อก่อนจะมีอยู่ 4 แห่ง ในช่วงปี 2555-2557 ที่ส่งเข้ามาให้เราตรวจพิสูจน์ แต่ปัจจุบันเขาแยกเป็นโครงการของกระทรวง และกรมสอบสวนคดีพิเศษรับงานตรงนี้ไปแล้ว เพราะช่วงนั้นยังไม่ได้จัดตั้งเป็นกลุ่มงานแต่เป็นกลุ่มงานตรวจสอบสถานที่เกิดเหตุเป็นงานที่อยู่ในกลุ่มนี้

การจัดทำรายงานผลการตรวจพิสูจน์ มีการตรวจงานอยู่ 2 ระดับ คือ การลงนามในหนังสือรายงานร่วมกัน 2 คน โดยใช้ตำแหน่งคือผู้รับรองรายงานผลการพิสูจน์ ตำแหน่งช่างภาพการแพทย์ (ถ่ายภาพในที่เกิดเหตุ ถ่ายภาพศพ) และนิติวิทยาศาสตร์

ถ้าโดยตำแหน่งไม่แน่ใจว่าทำได้ไหม แต่ด้วยความรู้ ความสามารถ เขาก็มีคุณสมบัติพอที่จะทำได้เพราะเขาไปเรียนปริญญาโททางด้านเทคโนโลยีสารสนเทศ (MIS) ส่วนอีกคนก็เรียนปริญญาโททางด้าน computer forensic ก็ยังรอปรับตำแหน่งให้ตรงกับตำแหน่งที่ปฏิบัติงานอยู่ แต่ยังทำไม่ได้

ส่วนมาตรฐาน ISO ของสถาบันนิติวิทยาศาสตร์ ตอนนี้ยังไม่ได้ แต่เรากำลังจะทำ ISO 17025 (ISO/IEC 17025 คือ มาตรฐานสากลซึ่งเป็นการประเมินความสามารถทางวิชาการของห้องปฏิบัติการ ISO/IEC 17025 ครอบคลุมทุกด้านของการบริหารจัดการห้องปฏิบัติการ ตั้งแต่การเตรียมตัวอย่างถึงความชำนาญในการวิเคราะห์ทดสอบ ถึงการเก็บบันทึกและการรายงานผล มาตรฐานนี้เน้นองค์ประกอบหลายด้านแต่ไม่ได้จำกัดเฉพะแค่ด้านเหล่านี้ ซึ่งได้แก่ระบบคุณภาพของห้องปฏิบัติการ การควบคุมเอกสาร การปฏิบัติการแก้ไขและป้องกัน สถานที่และภาวะแวดล้อม เครื่องมือ การประมาณค่าความไม่แน่นอน หลักฐานความสอบกลับได้ การสุ่มตัวอย่างและอื่นๆ

เรื่องบุคลากร ตอนนี้เราอยากได้บุคลากรเพิ่มอีกอย่างน้อย 3 คน รวมเป็น 6 คน คุณสมบัติจบการศึกษาด้านวิทยาศาสตร์บัณฑิต นิติวิทยาศาสตร์

สาเหตุอาจมาจากที่หน่วยงานของเราเพิ่งจะจัดตั้งใหม่ ยังไม่มีการเพิ่มกรอบอัตรากำลังจากทางกระทรวง ก็เลยต้องเกลี่ยมาช่วยงานก่อน

ด้านการพัฒนาบุคลากร

จัดการฝึกอบรมสัมมนาทั้งภายในหน่วยงานและภายนอกหน่วยงาน ส่วนมากจะเป็นการอบรมเกี่ยวกับคอมพิวเตอร์ การใช้โปรแกรม การเก็บรวบรวมพยานหลักฐานในที่เกิดเหตุว่าเก็บอย่างไรให้ถูกวิธี เทคนิคในการตรวจพิสูจน์ อบรมทั้งกลุ่มงาน อบรมที่ ICT ,EDDA จัดบ้างก็มี เรื่องโปรแกรม STK เรื่องการตรวจพิสูจน์หลักฐานทางมือถือ ในหนึ่งปีจะมีการอบรม สัมมนา 3-4 หลักสูตร

ส่วนการศึกษาดูงานไม่ค่อยมีนะเรื่องการศึกษาดูงานในประเทศและต่างประเทศ อยากไปฝึกอบรมศึกษาดูงานในต่างประเทศ เช่น ที่ Homeland Security ประเทศสหรัฐอเมริกา ที่เขาเปิด Lab ทางด้านนี้โดยเฉพาะ เพื่อเป็นการเพิ่มพูนความรู้ และประสบการณ์ให้มีมากขึ้น

การบริหารทรัพยากรบุคคล การโยกย้าย การเลื่อนขั้น/ตำแหน่งยังไม่มีปัญหาอะไร เพราะมีบุคลากรอยู่เท่านี้เอง การประสานงานกับหน่วยงานที่เกี่ยวข้องก็เป็นไปด้วยดี ส่วนมากจะเจอกันในการอบรมสัมมนาร่วมกันมากกว่าแล้วก็หยิบ Case มาคุยกัน ก็ไม่มีปัญหาอะไร

ด้านงบประมาณ

ยังไม่ค่อยมีปัญหาเท่าไหร่ อาจเป็นเพราะว่าหน่วยงานของเราเพิ่งเริ่มการจัดตั้งใหม่ รวมถึงอุปกรณ์ทางด้านเทคโนโลยีต่างๆ ก็ยังไม่เพียงพอ เช่น เครื่องมือตรวจพิสูจน์หลักฐานที่ใช้ดึงข้อมูลจากโทรศัพท์มือ โปรแกรมที่ใช้ในการทำงานต้องมีการปรับปรุงให้ทันสมัยตลอดเวลา ทำให้มีค่าใช้จ่าย มีสัญญาปีต่อปีค่าใช้จ่ายก็ประมาณ 20% ของราคาเครื่อง อุปกรณ์ทั้งชุดที่มีการซื้อ-ขายกัน การupdateในแต่ละปีเขาก็จะเพิ่ม Soft ware ใหม่ๆ ที่เกิดขึ้นมาให้กับเราด้วย

แนวทางการการทำงานในอนาคตด้านการต่อสู้กับ Cyber crime

สำหรับในตอนนี้ก็จะเตรียมความพร้อมในด้านบุคลากร เรื่องเพิ่มจำนวนบุคลากรคงจะยากหน่อย ก็เลยของบประมาณในการนำบุคลากรเข้ารับการฝึกอบรม เพิ่มความรู้ ทักษะในการปฏิบัติงาน และที่ต้องให้ความสำคัญเป็นอย่างมากก็ คือ เครื่องมือที่มีความจำเป็นต่อการปฏิบัติงาน เพื่อให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี

ต้องการฝึกอบรมประเภทที่เกี่ยวกับการตรวจพิสูจน์ ขั้นตอนการตรวจพิสูจน์ การศึกษาดูงานจนกระทั่ง การติดต่อประสานงานกับหน่วยงานที่เขาตรวจพิสูจน์ทางด้านนี้ ส่วนด้านการทำงานเป็นทีมก็เคยมีกระทรวง ICT เขาจัดขึ้น โดยจำลองเหตุการณ์ขึ้นมาแล้วก็เชิญหน่วยงานที่ดำเนินการด้านนี้เข้าร่วมก็มีหลายหน่วยงานเหมือนกัน ก็มี ปอท. ปปง. อัยการ ฯลฯ แต่ก็มีการจัดในปริมาณที่น้อยมากมีจัดปีละครั้ง เพราะไม่มีเจ้าภาพ ไม่มีงบประมาณ และแต่ละหน่วยงานก็มีงบประมาณของแต่ละหน่วยงานเองซึ่งก็ยังไม่เพียงพอ จะไปเป็นเจ้าภาพกลางก็จะยิ่งแย่เลย

การเตรียมพร้อมด้านอุปกรณ์นี้อยากให้มีการ upgrade Soft ware Hardware ใหม่ๆ ที่สามารถรองรับเทคโนโลยีใหม่ๆ Version ใหม่ที่ออกมา

การสร้างเครือข่ายในการแนะนำ แลกเปลี่ยนข้อมูล ก็อยู่ตรงที่ว่าเวลาเรามีปัญหา เราจะต้องปรึกษาใครหรือว่าหน่วยงานไหนเคยทำ Case นี้มาก่อน เวลาเรามีปัญหาเราจะได้ปรึกษาหรือสอบถามข้อมูลได้

ข้อเสนอแนะ

1. ต้องการให้บูรณการหามาตรฐานการทำงานขึ้นมา มีการทำงานร่วมกัน มีมาตรฐานการตรวจพิสูจน์ มาตรฐานด้านบุคลากร คือ จำเป็นไหมที่เราจะต้องไปขึ้นทะเบียนเป็นผู้เชี่ยวชาญของต่างประเทศ เพราะเราจะต้องใช้งบประมาณจำนวนมาก เราสามารถตั้งเป็นไทย Standard มาตรฐานผู้ตรวจพิสูจน์ คือ มาตรฐานที่ศาลจะรับฟังได้ว่าคนนี้ได้รับการขึ้นทะเบียนของประเทศไทย และเรื่องความน่าเชื่อถือ

2. รัฐควรมีมาตรการ การสื่อสารเผยแพร่วิธีการกระทำความผิดในรูปแบบใหม่ๆ ให้ประชาชนทราบถึงภัยอาชญากรรมใหม่ๆ

3. ให้รัฐจัดหาอุปกรณ์ตรวจจับภาพและบันทึกภาพเหตุการณ์ (กล้องCCTV) ที่มีคุณภาพ ประสิทธิภาพและติดตั้งในทิศทางที่เหมาะสมเวลาตรวจจะได้มีประโยชน์ในการตรวจพิสูจน์ และ Cyber crime เป็นเรื่องที่พิสูจน์ได้ยากมาก เพราะเราไม่รู้จักตัวตนผู้กระทำความผิดเลยตัวตนอยู่ที่ไหน

9. นายดล บุนนาค ผู้พิพากษารองหัวหน้าศาลจังหวัดนนทบุรี

การศึกษาจบปริญญาตรี นิติศาสตร์ จากจุฬาลงกรณ์มหาวิทยาลัย ปริญญาโทที่สหรัฐ อเมริกา 2 ใบ และปริญญาเอกที่มหาวิทยาลัยมหิดล สาขาอาชญาวิทยา

มีส่วนเกี่ยวข้องโดยเป็นผู้แทนศาลในการชี้แจงในชั้นกฤษฎีกาและชั้นสภาคือ พรบ. ว่าด้วยความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ พ.ศ.2550 และเป็นกรรมการยกร่างกฎหมายฉบับปัจจุบันที่จะออกใช้บังคับแทนฉบับ พ.ศ.2550

แนวทางการพัฒนาของเจ้าหน้าที่บังคับใช้กฎหมาย

เพื่อให้การปฏิบัติงานเป็นไปอย่างประสิทธิภาพ รวดเร็ว เป็นที่น่าเชื่อถือของประชาชน เนื่องจากเชื่อว่าปริมาณคดีจะต้องเพิ่มมากขึ้นแน่นอน แต่เห็นว่าเจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญในด้านนี้ยังมีไม่เพียงพอ จึงควรสร้างความตระหนักรู้ รู้จักภัยจากเทคโนโลยีเหล่านี้ว่ามีรูปแบบภัย ลักษณะ พฤติการณ์ในการกระทำผิด ก่อให้เกิดความเสียหายอย่างไรบ้าง เพื่อให้คนที่ไม่ทราบได้ทราบถึงความสำคัญเพื่อเตรียมพร้อมรับมือ และใช้ความระมัดระวังไม่ให้เป็นเหยื่อ โดยเผยแพร่ให้เจ้าหน้าที่และประชาชนทั่วไปทราบ แต่สำหรับผู้ปฏิบัติงานจริงเช่นตำรวจที่จะไปสืบสวน สอบสวน

อัยการที่จะสั่งฟ้องคดี รวมถึงผู้พิพากษาที่จะพิจารณาพิพากษาคดี จะต้องมีความรู้ความเชี่ยวชาญในเรื่องนี้เป็นพิเศษ ไม่ว่าจะปฏิบัติงานอยู่ในส่วนกลางหรือส่วนภูมิภาค

ในส่วนของศาลมีการอบรมหลายระดับ ตั้งแต่ผู้ช่วย หัวหน้าศาล หัวหน้าคณะ รองหัวหน้าศาล ศาลอุธรณ์ ศาลฎีกา หัวหน้าคณะศาลอุธรณ์ เป็นต้น จะอบรมก่อนเลื่อนสู่ตำแหน่ง ในส่วนอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ ก็มีการอบรมบ้างแต่ไม่ได้ลงลึก

ในด้านกฎหมายควรมีการใช้กฎหมายในส่วนของวิธีพิจารณาคดีที่เกี่ยวข้องกับอาชญากรรมประเภทนี้โดยเฉพาะ เช่น ในส่วนที่เกี่ยวข้องกับการสืบสวนสอบสวน การใช้วิธีการและเครื่องมือพิเศษ การรับฟังพยานหลักฐาน โดยเฉพาะพยานหลักฐานดิจิตอล พยานหลักฐานที่เป็นข้อมูลทางอิเล็กทรอนิคส์ การนำเสนอพยานหลักฐาน เสนอรูปแบบไหน แล้วเวลาศาลชั่งน้ำหนักใช้เหมือนธรรมดาได้ไหม

และตอนนี้อยู่ในระหว่างการแก้ไข พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ให้ทันต่อสถานการณ์ ลักษณะการกระทำความผิดใหม่ๆ ที่เกิดขึ้นในปัจจุบัน แต่ไม่มีการแก้ไขเพิ่มเติมในส่วนที่เกี่ยวข้องกับการดำเนินกระบวนพิจารณา

และควรมีหน่วยปฏิบัติการเฉพาะกิจ หรือองค์กรที่มีรูปแบบการรวมตัวของเจ้าหน้าที่ที่เกี่ยวข้องหลายๆ ฝ่ายมาปฏิบัติการร่วมกันในการปราบปรามอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ และทำงายด้านความมั่นคงของประเทศ โครงสร้างองค์กรจะเป็นกึ่งๆ บริษัท และมีความเป็นอิสระ แต่คนทำงานจะต้องดึงมาจากข้าราชการกลุ่มตำรวจ อัยการ ศาล ไปนั่งทำงานร่วมมือกัน มานั่งด้วยกัน ไม่ใช่ต่างคนต่างอยู่แล้ว อาจจะมาทำงานคนละ 1 ปี หรือเป็นคราวๆ เวียนกันเข้ามา

ที่หน่วยปฏิบัติการพิเศษ นี้ควรเป็นทั้งศูนย์การติดต่อประสานงานทั้งในและจากต่างประเทศเป็นที่เก็บรวบรวมข้อมูล และมีหน่วยปฏิบัติการในสืบสวนสอบสวน ตรวจค้นจับกุมมีห้องปฏิบัติการตรวจพิสูจน์พยานหลักฐานทางเทคโนโลยี รวมทั้งบุคลากรที่เชี่ยวชาญด้านเทคโนโลยีคอยสนับสนุน ทำงานแบบครบวงจร ควรดึงเอกชนเข้ามาร่วมทำงานด้วย ส่วนบุคลากรก็คัดผู้ที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์ มีเงินเดือน และสวัสดิการที่ดี

ควรมีการสอนกฎหมายที่เกี่ยวข้อง การสืบสวนสอบสวน การตรวจพิสูจน์พยานหลักฐานดิจิตอล (Forensic) ให้แก่นักศึกษาในสถาบันการศึกษาในคณะที่เรียนเกี่ยวข้องกับคอมพิวเตอร์และเทคโนโลยี เพื่อจะได้มีความรู้พื้นฐานจบออกมา อบรมเพิ่มเติมจากหน่วยงานบังคับใช้กฎหมายที่ทำงานก็จะสามารถทำงานได้เร็วขึ้น

ข้อเสนอแนะอื่นๆ

1. การศึกษาการให้ความรู้ต่อสังคม เรื่องพิษภัยของอาชญากรรม และต้องสอนเด็กในห้องเรียน ให้รู้จักอินเตอร์เน็ต มารยาทการใช้อย่างเหมาะสมและโดยชอบด้วยกกหมายและเรียนรู้พิษภัยที่เกิดจากอินเตอร์เน็ต

2. ส่วนของผู้ปฏิบัติงานทั้งหมด ตำรวจ อัยการ ศาล จัดฝึกอบรมร่วมกัน เป็นหลักสูตรต่างๆ ให้ตระหนักรู้และให้สามารถปฏิบัติหน้าที่ให้เกี่ยวข้องได้ มีหน่วยงานเฉพาะขึ้นมาดูแลในเรื่องนี้อย่างจริงจัง

3. มาตรฐานในการตรวจพิสูจน์พยานหลักฐาน (Forensic) เป็นเรื่องสำคัญเป็นเรื่องใหม่ที่ต้องทำ เพื่อให้ศาลใช้เป็นเครื่องเป็นมาตรวัดได้ว่า พยานชิ้นนี้ปฏิบัติตามมาตรฐานมีหลักฐานน่าเชื่อถือ การทำจะต้องรวมกัน ระหว่าง อาจารย์มหาวิทยาลัย ตำรวจ อัยการ ศาล และทนายความมานั่งรวมกันทำมาตรฐานว่า มาตรฐานนี้ทุกฝ่ายเห็นด้วย และประกาศออกมา ถ้าหน่วยงานอื่นชอบก็ทำตาม รับเป็นมาตรฐาน แต่ตอนนี้รวมกันไม่ติด ไม่มีใครเป็นเจ้าภาพ รวมทั้งมาตรฐานของผู้เชี่ยวชาญด้วยว่ามีคุณสมบัติอย่างไรบ้าง

10. นายปริญญา หอมอเนก ประธานและผู้ก่อตั้ง, ACIS Professional Center Co.,Ltd.(ACIS)

เป็นสถาบันให้บริการด้านการฝึกอบรม (Training Center) และเป็นที่ปรึกษางานเกี่ยว กับระบบเทคโนโลยีสารสนเทศ (Information Technology) ความมั่นคงปลอดภัยสารสนเทศ (Information Security) และการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) แบบครบวงจร ซึ่งครอบคลุมทั้งด้านบุคลากร (People) กระบวนการปฏิบัติ (Process) และเทคโนโลยี (Technology)

โดยมีเป้าหมายเพื่อเพิ่มประสิทธิภาพและประสิทธิผลของการบริหารจัดการทั้งในด้านธุรกิจและระบบเทคโนโลยีสารสนเทศเพื่อให้สามารถบรรลุเป้าหมายขององค์กร และสร้างความความเชื่อมั่นต่อผู้ใช้บริการทั้งในและนอกองค์กร ตลอดจนเพิ่มขีดความสามารถหรือสร้างความแตกต่างในการแข่งขันทางธุรกิจ การให้บริการของ ACIS ดำเนินการโดยผู้เชี่ยวชาญที่มีความรู้ความสามารถ และมีประสบการณ์ในการฝึกอบรมและให้คำปรึกษาแก่หน่วยงานทั้งภาครัฐและเอกชน ที่ ACIS เราให้ความสำคัญกับการพัฒนาบุคลากร

โดยสนับสนุนให้ทีมงานของเราค้นคว้าหาความรู้เพิ่มเติมอย่างต่อเนื่องและสอบประกาศนียบัตรเพื่อรับรองความรู้ความสามารถจากสถาบันที่ได้รับการยอมรับในระดับสากล อาทิ CISSP, SSCP, CSSLP, CISA, CISM, CGEIT, CRISC, CBCI, CFE, IRCA: ISMS Lead Auditor, IRCA: ITSMS & BCMS Provisional Auditor, SANS GIAC GPEN & GXPN, ITIL

Expert, ITIL Foundation, COBIT 5 Certified Trainer เป็นต้น นอกจากนี้ ACIS ยังร่วมมือกับสถาบันและองค์กรในระดับสากลในด้านการจัดฝึกอบรมหลักสูตรที่เป็นมาตรฐานสากลหลากหลายหลักสูตร เช่น ISC2, Business Continuity Institute, TUV NORD, IT preneurและ EC-Council เป็นต้น

นอกจากนั้น ยังได้เป็นที่ปรึกษาของหน่วยงานราชการหลายแห่ง ร่วมให้คำปรึกษาแนะนำกรณีมีเรื่องที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งในด้านความมั่นคงและอาชญากรรม รวมทั้งสอนหนังสือและบรรยายให้แก่หน่วยงานภาครัฐและเอกชนจำนวนมาก ACIS เปิดอย่างเป็นทางการ 13 ปี ที่ไม่เป็นทางการ 15 ปี มีจำนวนพนักงานทั้งสิ้น 71 ท่านคน พนักงานที่นี่ส่วนมากจบปริญญาโทด้านไอทีคอมพิวเตอร์รับตั้งแต่จบปริญญาตรี แล้วค่อยๆ ฝึกจนเก่งใช้เวลา ประมาณ 2 – 3 ปี แต่เดี๋ยวนี้มันไม่ค่อยทันก็ต้องรับคนที่ทำงานเป็นมาเลย แต่พวกนี้ค่าตัวค่อนข้างจะแพงแต่ความรักองค์กรจะต่ำกว่าคนที่อยู่กับเรามานาน

เงินเดือนจะเริ่มต้นประมาณ 2 – 3 หมื่น จนไปถึงแสนขึ้นถ้าบริษัทมีกำไร ก็ให้โบนัสเฉลี่ยประมาณ 2 – 3 เดือน ถ้าทำงานดี เฉลี่ยประมาณ 4 – 5 เดือน มีรางวัลพิเศษให้เรียน อยากเรียนอะไรก็ให้เรียน ถ้าสอบผ่านประกาศนียบัตรได้ ให้เงินเพิ่มตัวละ 5 พันบาทต่อเดือน บุคลากรของ ACIS สามารถที่จะเป็นอาจารย์สอนได้เลย

การพัฒนาบุคลากรในองค์กร คนที่จบมาใหม่ๆ ยังทำงานไม่ได้ใช้ระบบให้พี่พี่เลี้ยงคอยดูแล สอนงานและส่งไปทำงานร่วมกับคนอื่น เรียนรู้จากคนที่เก่งก่อน จากนั้นเราก็จะให้เดี่ยวและเราก็จะดูจากหน่วยก้าน ถ้าจะให้สอนก็จะให้เริ่มจากคลาสเล็กๆ ก่อน วิชาง่ายๆ ก่อน ห้องละ 5 – 10 คน วิชาง่ายๆ ถ้าหลุดจากตรงนั้นได้ก็ให้สอนวิชาที่ยากขึ้น

ส่วนปัญหาการลาออกก็มีบ้าง เนื่องจากคนที่นี่เก่งต้องการเงินเดือนสูง ถ้าไม่ให้เขาก็ออกเพราะว่าบริษัทคู่แข่งรับทันที แต่ส่วนมากจะเข้าใจทำงานด้วยกันชี้ให้เห็นเส้นทางความก้าวหน้าในอาชีพ

แนวโน้มในอนาคตจะอยู่ในยุคของที่เรียกว่า Internet of Things คือ ทุกอย่างเชื่อมต่อ Internet หมดเลย นาฬิกา โทรศัพท์มือถือ เครื่องใช้ไฟฟ้า อะไรทุกอย่างเชื่อมต่อ Internet หมดเลย และมันก็จะมีแรง 4 แรงเข้ามา เรียกว่า SMIC S หมายถึง Social network, Social Media , M หมายถึง Mobile , I หมายถึง Information , C หมายถึง Cloud ข้อมูลจะถูกนำมาวิเคราะห์เพื่อทำการตลาดขายสินค้าและบริการ มีการขายข้อมูล คอมพิวเตอร์จะมีราคาถูกขึ้น ไวขึ้น เสถียรมากขึ้น อาชญากรรมจะเกิดมากขึ้น เด็กรุ่นใหม่มีเครื่องมือในการกระทำความผิด เพราะมีขายอย่างแพร่หลาย ภัยถึงตัวมากขึ้นและเร็วขึ้น คนร้ายเจาะจงมาที่ตัวคนได้เพราะมีข้อมูล

ปัญหาคือ เจ้าหน้าที่ผู้บังคับใช้กฎหมายที่เชี่ยวชาญด้านนี้มีน้อย ส่วนมากยังมีทักษะในด้านคอมพิวเตอร์ต่ำอยู่ ควรเร่งรัดพัฒนาให้ผู้บังคับใช้กฎหมายมีความรู้และทักษะด้านเทคโนโลยีให้มากขึ้น ควรจัดตั้งหน่วยงานพิเศษของรัฐที่มีความเป็นอิสระในการทำงาน กำหนดคุณสมบัติของ

เจ้าหน้าที่ ที่มีความรู้ความเชี่ยวชาญด้าน IT ให้มีอัตราเงินเดือนที่สูง เพื่อป้องกันสมองไหลก้าวหน้าในการป้องกันและปราบปรามการกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ ควรจัดทำมาตรฐานผู้เชี่ยวชาญด้าน IT

11. ผศ.ดร.สุรทศ ไตรติลานันท์ ผู้ช่วยศาสตราจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ปริญญาเอกด้าน Information Security จาก Information Security Institute, Queensland University of Technology, Australia

ปี 2553-2557 : หัวหน้าโครงการพัฒนานวัตกรรมและการเรียนรู้ทางด้านนิติวิศวกรรมคอมพิวเตอร์ (Digital Forensic Innovation and Training Center: DFIT), ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

2554-ปัจจุบัน : รองประธานหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต (คอมพิวเตอร์), ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

2555-ปัจจุบัน : ผู้ช่วยศาสตราจารย์, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

2557-ปัจจุบัน : อาจารย์พิเศษ, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

2555-2556 : อาจารย์พิเศษ, ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร

ที่ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล ที่มหาวิทยาลัยมีคณะที่สอนหลักสูตรที่เกี่ยวคอมพิวเตอร์ คือ คณะวิศวกรรมศาสตร์, วิทยาศาสตร์ หลักสูตรปริญญาตรี, ปริญญาโท หัวข้อวิชาหลัก Network Security and Digital Forensics ระยะเวลาในการศึกษา 2 ปี เมื่อจบการศึกษาแล้วสามารถทำงานที่เกี่ยวข้องด้าน Network Security Engineering, Network Security Analyst, Security Auditor, Computer Consultant, Digital Forensic Examiner, Digital Forensic Analyst, Digital Evidence Investigator, Fraud Detector แต่ละปีมีนักศึกษาจบประมาณ 10 คน แบ่งเป็น ชาย 7 คน หญิง 3 คน

ทางมหาวิทยาลัยได้ให้ความช่วยเหลือทางภาครัฐในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องคอมพิวเตอร์ โดยในช่วง 2-3 ปีที่ผ่านมา ได้มีการให้คำปรึกษากับหน่วยงานราชการ รวมถึงการเปิดหลักสูตรจัดการอบรมเน้นภาคปฏิบัติให้กับหน่วยงานราชการที่เกี่ยวข้องกับงานด้านการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องคอมพิวเตอร์ เช่น กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานตำรวจแห่งชาติ ตำรวจกองปราบปรามด้านเทคโนโลยี

สารสนเทศ (ปอท.) กรมสอบสวนคดีพิเศษ สถาบันนิติวิทยาศาสตร์ ปปง. สำนักงานอัยการ และศาล เป็นต้น

คอมพิวเตอร์เป็นสาขาวิชาที่ไม่หยุดนิ่ง มีการพัฒนาเทคโนโลยีไปข้างหน้าอย่างรวดเร็ว รูปแบบอาชญากรรมที่แฮกเกอร์ใช้ในการโจมตี ก็ได้มีการพัฒนารูปแบบ เพื่อให้หลีกเลี่ยงการป้องกันและตรวจจับได้ ดังนั้นเจ้าหน้าที่ผู้ปฏิบัติงานของรัฐฯ ยังไงก็ต้องเป็นฝ่ายวิ่งไล่ตามเทคนิคต่างๆ ของผู้โจมตี พร้อมทั้งไล่ตามปิดช่องโหว่ต่างๆ เหล่านั้น ดังนั้นจึงมีความจำเป็นอย่างมากที่เจ้าหน้าที่ของรัฐฯ จะต้องหมั่นเพิ่มพูนทักษะความรู้และฝึกปฏิบัติตนเองอย่างสม่ำเสมอ เพื่อไม่ให้คนร้ายนั้นทิ้งช่องว่างระยะห่างขององค์ความรู้และทักษะออกห่างไปเรื่อยๆ ทางมหาวิทยาลัยมีการเตรียมความพร้อมในการรับมือ โดยมีการพัฒนาทักษะให้กับอาจารย์ผู้สอน เพื่อให้สามารถนำมาถ่ายทอดต่อให้กับนักศึกษา ให้มีความรู้ที่ทันสมัยและเท่าเทียมกับโลกภายนอกให้มากที่สุด

นักศึกษาอาจมีความสนใจที่ต่างกันในแต่ละรุ่น รวมทั้งความสนใจต่องานทางด้านความมั่นคงปลอดภัยของนักศึกษาแต่ละรุ่นนั้นมีไม่เท่ากัน ส่วนในเรื่องค่านิยมต่องานในภาครัฐฯ นั้น ที่ผ่านมาก็มีอัตราส่วนของ นศ.ที่สนใจในแต่ละรุ่นแตกต่างกันเช่นกัน แต่โดยเฉลี่ยจะอยู่ที่ประมาณ 20% ที่สนใจทำงานภาครัฐ อาจเกิดจากสาเหตุที่เวลามีงานทางด้าน job fair ที่จัดขึ้นในมหาวิทยาลัย บริษัทที่เข้ามาจะมีแต่ในส่วนของภาคเอกชนเท่านั้น

ข้อเสนอแนะต่อภาครัฐและประชาชนทั่วไป

ควรมีการประชาสัมพันธ์เชิงรุกให้มากกว่านี้ และควรมีเป้าหมายและทิศทางในด้านการสร้างบุคลากรและการป้องกัน รวมทั้งเผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายคอมพิวเตอร์ เพื่อสร้างความรู้และความเข้าใจให้กับประชาชนให้มากกว่าที่เป็นอยู่นี้

12. นายเรืองไกร รังสิพล ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ โครงสร้างพื้นฐานบริษัทในเครือ ทรู คอร์ปอเรชั่น จำกัด (มหาชน)

ทรู เป็นผู้ให้บริการตาม มาตรา 26 ของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีเฉพาะรายและเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับแต่การใช้บริการสิ้นสุด หากผู้ให้บริการไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

การประสานงานขอข้อมูลมายังหน่วยงานที่รับผิดชอบคือ สำนักกฎหมายและหลักเกณฑ์การกำกับดูแล (Law and Regulation Office) โดยวิธีการขอ

1. ต้องทำเป็นหนังสือโดยผู้มีอำนาจขอ พร้อมแสดงเหตุแห่งการขอข้อมูลนั้นตามที่กฎหมายกำหนด

2. ขอบเขตของข้อมูลที่ต้องการ วัน เวลา ไอพีแอดเดรส หรือ หมายเลขโทรศัพท์เคลื่อนที่ ทั้งนี้ย้อนหลังไม่เกินหกเดือน

3. ข้อมูลที่ส่งมอบ ข้อมูลบ่งชี้บุคคลผู้ใช้บริการตามขอบเขตที่กำหนด เช่นบ้านเลขที่ หมายเลขโทรศัพท์ หรือชื่อผู้ใช้ที่ลงทะเบียนไว้ เป็นต้น

ผู้ขอต้องเป็นพนักงานเจ้าหน้าที่ตามของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ถ้าเป็นคดีอาญาประเภทอื่นๆ พนักงานสอบสวนตาม ป.วิอาญา

เมื่อได้รับคำขอจะใช้ระยะเวลาดำเนินงานประมาณ 2 สัปดาห์ ถึง 1 เดือน เราต้องประสานงานกับหน่วยงานภายในของเราที่มีหน้าที่เก็บข้อมูล คลังข้อมูลเราต้องทำเรื่องเบิกจากคลังมา

หน่วยงานนี้จะเป็นนักกฎหมายทำหน้าที่ประสานงานกับเจ้าหน้าที่ของรัฐ กลั่นกรองความชอบด้วยกฎหมายตามคำขอ แต่เวลาไปขอข้อมูลจริงต้องไปขอกับเจ้าหน้าที่ปกติ ซึ่งไม่ได้มีหน้าที่นี้ ไม่มีใครมีข้อมูลนี้ ก็จะขอเป็นคราวๆ ไป ฉะนั้นคนที่มีหน้าที่ประจำคือคนที่ประสานเท่านั้น ที่เหลือคือคนทำงานปกติ

ปัญหาหลักที่พบคือเจ้าหน้าที่ของรัฐไม่ค่อยปฏิบัติตามขั้นตอนตามกฎหมาย บางครั้งรีบปิดคดี ต้องการความรวดเร็ว ความสะดวก คือ ถ้าพบ รับเรื่องเขาก็ส่งมาเลยถ้าเป็นคดีเร่งด่วนเขาก็ตามให้ แต่บางประเภทไม่มีอะไรมาเลยก็จะมีปัญหา

สิ่งที่ให้ได้ ถ้าเป็นข้อมูลทาง พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ เราก็ให้ได้ทั้งหมด ชื่อผู้ใช้ สถานที่ ชื่อระบบต้น หมายเลข IT หมายเลขโทรศัพท์ ข้อมูลที่บงชี้บุคคลเราสามารถให้ได้เลย

ความต่างของข้อมูลของโทรศัพท์กับข้อมูลทางอินเตอร์เน็ต ต่างกันตรงที่ว่าข้อมูลทางโทรศัพท์จะง่ายกว่าข้อมูลทางคอมพิวเตอร์ โทรศัพท์จะแค่บอกว่า นาย ก. โทรหาใคร เมื่อไหร่ เวลาไหน นานเท่าไหร่บ้างเก็บทุกครั้งที่โทร แต่ถ้าเป็นข้อมูลทางคอมพิวเตอร์เราจะเก็บว่าเขาเข้ามาใช้ระบบเมื่อไหร่ และเลิกใช้เมื่อไหร่ แต่ในระหว่างช่วงเวลาที่เขาใช้ติดต่อใครนั้นมันมากเราจะเก็บข้อมูลไม่ได้

ข้อมูลนี้จะต้องเก็บไว้ 90 วัน แล้วหลังจาก 90 วัน ในทางปฏิบัติเราใช้ตามพื้นที่จัดเก็บถ้าจะหมดเราก็จะเคลียร์พื้นที่แต่ส่วนมากน่าจะเกิน 90 วัน พอพื้นที่จะหมดก็จะทยอยไล่เคลียร์พื้นที่ออกเพื่อจะได้เก็บข้อมูลใหม่ๆ แต่ถ้ามีการขอเกิน 90 วัน ทางนิติกรเขาก็จะไม่หาให้ แต่ถ้าเป็นกรณีพิเศษเขาก็อาจจะไปค้นดูเผื่ออาจจะยังไม่ลบข้อมูลเพราะถ้าเลย 90 วัน นิติกรเราไม่มีหน้าที่จะต้องค้นหาข้อมูลให้แล้ว เพราะจะต้องเสียเวลาในการสืบค้นข้อมูลมาก

ปัญหานอกจากผู้ขอไม่ทำตามระเบียบแล้วก็มีการขอข้อมูลมาไม่ครบถ้วน คือ ไม่ระบุช่วงเวลาที่แน่ชัดเพราะเราต้องการรายละเอียดตรงส่วนนี้มาก อย่างเช่นบอกช่วงเวลากลางวัน อันนี้เป็นปัญหาที่กว้างมาก

หลักของจราจรคอมพิวเตอร์ง่ายนิดเดียวว่าเบอร์ IP Address ที่ใช้นี้เป็นเบอร์ใครต้องมาพร้อมเบอร์ IP กับเวลาการเกิดเหตุ ไม่ได้ไปเก็บว่าการกระทำที่ทำให้เกิดเหตุมันมาจาก IP Address อะไร ความจริงต้องไปพิสูจน์ต้นทางเพื่อให้ได้หลักฐานนี้ก่อน บางครั้งเห็นแต่เหตุแล้วมาขอ ถ้ากรณีเราไม่ใช่ผู้เสียหายนะ หลักฐานสำคัญเยอะๆ ที่จริงไม่ได้อยู่ที่เราแต่จะอยู่ที่ผู้เสียหายก็ต้อง Forensics ที่นั่นเยอะๆ

การติดต่อสามารถติดต่อไปที่สำนักงานใหญ่ของ True cooperation ได้แล้วเราก็จะประสานไปที่บริษัทในเครือที่มีหน้าที่รับผิดชอบโดยตรง

ในอนาคตบริษัทตรงจุดนี้มีการเตรียมพร้อมเพื่อรองรับปริมาณข้อมูลต่างๆ ในอนาคต คือ การประมาณการเติบโตของข้อมูล ถ้าข้อมูลตามหน้าที่เดิม ในวันข้างหน้าจะต้องเตรียมการเพื่อรองรับปริมาณผู้ใช้ อันนี้เราเตรียมอยู่ทุกปี การล่าช้าเพราะว่าบางทีระบบมันใหญ่ การค้นหาจะใช้เวลานานและต้องปรับปรุงระบบให้เร็วขึ้น พอมีเรื่องขอมาก็จะใช้เวลาไม่นาน คือ คนอาจจะไม่จำเป็นต้องเพิ่ม แต่จะเป็นการปรับปรุงระบบการจัดเก็บทั้งหลายให้มีประสิทธิภาพมากขึ้น ที่จะสามารถทำให้การสืบค้นได้รวดเร็ว ถูกต้องและแม่นยำได้มากยิ่งขึ้น

เราเรียกที่เก็บข้อมูลตรงนี้ว่า Stores ต้องคำนวณทั้งปีว่าขยายเท่าไหร่ และตอนนี้ก็ขยายขึ้นทุกปี ปีละเกิน 50 % คือการเพิ่มขึ้นของข้อมูลไม่สอดคล้องกับค่าบริการที่เราเก็บเหมือนใช้ฟรี แต่ต้นทุนแฝงมีเยอะ

ตัวที่เก็บข้อมูลตัวนี้ จริงแล้วมันจะเสียทางกายภาพ แต่ระบบเก็บข้อมูลเราจะมีตัวป้องกันระบบความล้มเหลวอยู่แล้ว และเรามีที่เก็บไว้สองที่ อุปกรณ์ที่เก็บมีสองที่เพราะสำรองการสูญหายของข้อมูล

บุคคลนอกจะมาเจาะระบบ (Hack) ข้อมูลตรงนี้ไม่ได้ครับ เพราะเป็นระบบที่ควบคุมการเข้าถึงอย่างเคร่งครัดและมีคนเข้าถึงได้ไม่กี่คน แล้วระบบก็จะบันทึกด้วยว่าใครเข้ามาดึง-ใช้ข้อมูลตรงนี้

ก็จะมีไม่กี่คนที่สามารถเข้ามาสืบค้นหาข้อมูลในนี้ ก็จะเป็นวิศวกรที่ดูแลระบบเท่านั้น แล้วแต่ว่าเวลาจะดู ทบทวนการเข้าก็จะดูว่าต้นเรื่องมาจากที่ไหนถึงจะสืบค้นกันได้ อยู่ดีๆ จะเข้าไปดูมันดูไม่ได้เขาไล่ออกทันทีเลย เพราะมันเป็นข้อมูลลับของลูกค้า ตำแหน่งนี้คือ ตำแหน่งเจ้าหน้าที่บริหารงานทั่วไปแต่มีหน้าที่คอยดูแลระบบ บริหารระบบ ส่วนมากจบสาขาวิศวกรรมคอมพิวเตอร์ จบวิทยาศาสตร์คอมพิวเตอร์ ส่วนตำแหน่งนิติกรก็จะรับคนที่จบนิติศาสตร์มีความรู้ด้านกฎหมาย

คนที่ทำหน้าที่ดึงข้อมูลเขาจะแปลข้อมูลมาให้เลย พออ่านข้อมูลมาเป็นตัวเลขเขาก็จะแปลเป็นข้อความมาพร้อมเลย เวลาตอบผลการแปลไม่ใช่ข้อมูลดิบ

อ่านและแปลข้อมูลเป็นภาษา ที่ไม่ใช่ภาษาเครื่อง เพราะฉะนั้นงานก็จะมาช้าอยู่ตรงนี้ ทั้งดึงข้อมูล และแปลข้อมูล การแปลข้อมูลก็ไม่ยาก แต่ก็ระวังการแปลผิด

ในความเห็นของผม รัฐควรจำนำข้อมูลดิบตรงนี้ไปแล้วไปแปลเองเพื่อให้ได้ข้อมูลที่ถูกต้อง

เรามีการตรวจว่าข้อมูลจากต้นทางจริงไหมนั้นมีผู้ตรวจ แต่เรื่องการแปลผิดแปลถูกผมว่าไม่ใช่หน้าที่เขา เขามีหน้าที่ในการดึงข้อมูลดิบออกมาให้ ส่วนเรื่องการแปลนั้นเป็นเรื่องของคนขอต้องไปจัดการกันเอง เพราะเขาไม่รู้ด้วยซ้ำว่าข้อมูลที่ขอมานั้นเอาไปทำอะไร เพราะเอกสารที่ขอมาก็มีแค่คำขอ บอกแค่ขอข้อมูลตรงนี้หน่อย

ลักษณะของแปลผิด ผมว่าที่สำคัญ คือ ระบุผู้ใช้ผิด เพราะข้อมูลนี้เป็นข้อมูลบ่งชี้บุคคล ถ้าเวลาผิดอาจจะเปลี่ยนคนก็ได้ บางระบบผมยกตัวอย่างตั้งเวลาสากลถ้าเป็นเมืองไทยต้อง +7 ชม. การดูข้อมูลต้องมีการ +7 ชม. ก่อนค่อยไปเก็บข้อมูล ข้อมูลที่อยู่ในตัวหนังสือบอกเวลาบ่ายโมงพอเรารู้แล้วว่าจริงๆ แล้วเวลานี้จะเป็น 8 โมงหรือ 2 ทุ่ม เพราะต้องบวกเข้าไปอีก 7 ชม. เพราะฉะนั้นอย่างนี้พอแปลแล้วมันจะผิดเลย ถ้าไปดูแล้วเราไม่รู้เรื่องของเวลาแล้วพอดูข้อมูลเราก็คิดว่ามันถูก

เราไปเป็นพยานศาล ส่วนมากจะเป็นนิติกร คือ เจ้าหน้าที่น้อยที่จะไปขึ้นศาลเอง วิศวกรจะไม่ขึ้นศาลเลย ไปยืนยันว่าเราเก็บข้อมูลตามปกติที่เราทำกันอยู่แล้ว เราไม่มีการโกรธเคืองหรือเก็บข้อมูลใครเป็นพิเศษ กระบวนการเก็บและดึงข้อมูลเป็นอย่างนี้ วันเวลาตามนี้ แต่ไม่มีใครเอาข้อมูลดิบไปสืบ

ส่วนกลุ่มงานด้านโทรศัพท์อยู่อีกที่หนึ่งครับ การทำงานก็จะมีลักษณะเหมือนกัน

ต่อไปเป็นกรณีที่ บริษัท ทรูฯ เป็นผู้เสียหาย ถ้าตามกฎหมายส่วนมาก คือ การเข้าถึงโดยมิชอบ การเปลี่ยนแปลงแก้ไขข้อมูลโดยมิชอบ การใช้บัตรอิเลคทรอนิกส์โดยมิชอบ ในความผิดตาม ป.อาญา ส่วนมากคือ การเอา User คนอื่นมาใช้บัตรอิเล็กทรอนิกส์ อันนี้คือความผิดที่เกี่ยวข้องกับทางคอมพิวเตอร์ การฉ้อโกง ก็รวมอยู่ตรงนี้ตาม พ.ร.บ.คอมพิวเตอร์ฯ ที่เกี่ยวกับอิเลคทรอนิกส์จะมีอยู่ 3-4 ฐานทางอาญา

การเข้าถึงข้อมูลโดยมิชอบคือการเข้ามาเจาะระบบข้อมูลของบริษัท เข้ามาเปลี่ยนแปลงข้อมูลของบริษัท การใช้บัญชีบัตรอิเลคทรอนิกส์ของคนอื่นมาใช้โดยมิชอบเช่น ไปได้ User Password ของคนอื่นมาแล้วนำไปใช้พอคีย์เข้าไปก็ผิดฐานนี้เลย เพราะ User Password เป็นบัตรอิเล็กทรอนิกส์ ก็จะรวมกันมาอยู่ 3 ข้อหานี้แหละ

ความเสียหายที่เกิดขึ้น ถ้าเป็นคดีใหญ่ก็จะเป็นทำให้เสียทรัพย์เกี่ยวกับบัตรเติมเงิน ส่วนเรื่องการเจาะระบบข้อมูลไม่ค่อยบ่อยครับ

เมื่อเกิดเหตุก็ดำเนินการทำตามขั้นตอนคือ การไปแจ้งความร้องทุกข์หรือฟ้องคดี มีแบบฟ้องคดีเองหรือเปล่า ทำตามขั้นตอนตามปกติ คดีหลักๆ ก็จะเป็นคดีการเจาะระบบข้อมูล ที่เหลือก็เป็นคดีเล็กๆ ไม่ได้เยอะมากมาย

หน่วยที่ดูแลรักษาความปลอดภัยของบริษัท ความมั่นคงปลอดภัยสารสนเทศและเครือข่าย

หน่วยงานนี้มีหน้าที่ดูแลความปลอดภัยในระบบสารสนเทศทั้งหมดของบริษัทแล้ว ผู้ปฏิบัติงานจำนวน 6 คน ทุกคนก็จบวิศวคอมฯ ภารกิจหลัก เขาทำในเชิงป้องกันมากกว่า เราจะมี 3 ส่วนที่ 1. คือ การทดสอบทดสอบความแรงของระบบ ระบบของเราน่าจะมีอยู่สักประมาณ 20,000 ระบบ ทุกปีเราต้องเช็คทั้งหมดเลย ว่ามันมีข้อบกพร่อง อะไรที่ให้คนเจาะระบบเข้ามาได้หรือเปล่า เราก็ตีระฆังนี่คือ กรณีที่ 1 ส่วนที่ 2 คือ ทดสอบการก่อนให้บริการ เวลาเรามีระบบอะไรใหม่ๆ ก็จะไปแจ้งให้ทำการทดสอบก่อน ว่าระบบนี้มันเจาะได้หรือไม่ได้ แล้วก็ไปแก้ไขให้เรียบร้อย แล้วค่อยเปิดให้บริการ ส่วนที่ 3 คือ ซุ่มตรวจสอบ จุดที่เราล่อแหลมสู่อินเตอร์เน็ต น่าจะมีอยู่ประมาณ 300 กว่าจุด ที่คนสามารถเข้าถึงได้ เพราะเราเปิดให้ใช้บริการอยู่ ไอ้ 300 กว่า เราจะเจาะระบบเองกันแทบจะทุกวัน ว่าเราซุ่มตรวจสอบจุดล่อแหลมที่บุคคลภายนอกเข้าถึงได้ ที่ให้บริการอยู่ก็ได้ครับ อันนี้คือภารกิจหลักของทีม

และยังมีอีกหน่วยงานหนึ่งเรียกว่า หน่วยงานความมั่นคง

ถ้ามีเรื่องหรือมีคดี ที่เกี่ยวกับข้อง ถ้าเราดูแล้วอันนี้บริษัทเราได้รับความเสียหายหรือถูกละเมิด หน่วยงานนั้นก็จะดำเนินการก่อนหรือบางครั้งก็ทำงานร่วมกัน

เฉพาะหน่วยงานความมั่นคง มีบุคลากร ไม่ถึง 10 คนส่วนใหญ่เขาจะประสานงานให้พนักงานสอบสวน มาทำคดีครับ

แนวนโยบาย แนวทางป้องกันขององค์กรคือ 1. ป้องกันตัวเองให้ดีที่สุด 2.ถ้าเสียหายก็ดำเนินคดีจนถึงที่สุดเหมือนกัน เป็นการป้องปรามคือ ถ้าทางนี้ทำดี งานมันจะไหลมาน้อยมาก

ในเรื่องของ Security งบประมาณเป็นเรื่องรอง ทักษะเป็นเรื่องใหญ่คือ ถ้าไม่มีทักษะลงทุนไปก็ไม่ปลอดภัย เพราะฉะนั้นจะเห็นว่างานที่เราทำส่วนใหญ่จะอาศัยพื้นฐานเกี่ยวกับทักษะของคนเป็นหลัก คนไม่เยอะ แต่งาน 10,000 - 20,000 ขึ้น เราทำกัน 2 – 3 เดือนก็เสร็จ ทำทุกปี ซึ่งมันต้องมีเครื่องมือถ้าใช้เป็นมันไม่ได้จะแพงมาก

ด้านการพัฒนาบุคลากร การฝึกอบรมถ้าอบรมในประเทศ เราแทบจะไม่ค่อยได้อบรมเลย ถ้ามีก็จะอบรมต่างประเทศ ก็จะส่งผู้ปฏิบัติงานไปเรียนแล้วก็มา สร้างระบบจำลอง ฝึกฝนกันเอง

ในการทำงานกับภาครัฐ ทางบริษัท ให้การร่วมมือสนับสนุนอย่างดีมาโดยตลอด ไม่ว่าจะเป็นฝ่ายไหนมาขอความร่วมมืออย่างดี เช่น เป็นวิทยากรบรรยาย อำนวยการศึกษาดูงานที่บริษัท

ถ้าทางบริษัท มีคดีที่ได้รับความเสียหายมาก เราก็จะไปที่ กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ ปอท. เพราะว่าที่นั่น เขาจะมีความรู้ความสามารถในด้านนี้มากกว่า

เวลามีคดีเกี่ยวกับเรื่องข้อมูลจราจรคอมพิวเตอร์อะไร อย่างนี้ทางนี้จะมีความเชี่ยวชาญชำนาญกว่าเพราะเป็นคดีที่มีความซับซ้อนกว่า

ในระยะ 2 ปี คดีอาญาที่มีส่วนเกี่ยวข้องกับ อิเล็กทรอนิกส์ ผมว่าเพิ่มขึ้นอีกหลายเท่าตัวมากเลย เรื่องอิเล็กทรอนิกส์ มันเป็นส่วนหนึ่งของการกระทำ ความผิด เป็นเครื่องมือในการกระทำความผิดอื่น ถ้าเกิดว่าผู้บังคับใช้กฎหมายไม่เข้าใจความสัมพันธ์ การกระทำอิเล็กทรอนิกส์กับการกระทำอาญา ผมว่าลำบาก หลักฐานที่เขาโฆษณาฉ้อโกงอยู่บนอิเล็กทรอนิกส์อย่างนี้

ถ้าถามทางวิชาการเขาว่ากระบวนทัศน์มันเปลี่ยน ในการมองปัญหา เป็นอีกแบบหนึ่งเลย จริงๆ อันนี้น่าจะทำทั้งกระบวนการเลย

อันนี้ต้องทำไปถึงศาลด้วย วิธีการดำเนินพิจารณาคดีในชั้นศาลก็ต้องเปลี่ยน เพราะมันไม่มีประจักพยานแล้ว มันเป็นร่องรอยทางอิเลคทรอนิกส์เท่านั้นเอง ที่เราตามเราตามร่องรอยทางอิเลคทรอนิคส์ ซึ่งมันจะเป็นตัวบ่งชี้เท่านั้นเองว่าใครเป็นผู้กระทำความผิด มันไม่ใช่เหมือนคดีฆ่าหรือคดีชกต่อยกันที่มันจะต้องประจักพยาน มันไม่มี

เพราะเดิมทีที่เราทำคดีนั้น เขายังลบ ลบร่อยรอย แล้วอย่างข้อมูลอิเลคทรอนิคส์ เวลาพิจารณาด้วยเหตุผลทางธรรมชาติ มันไม่ได้ เพราะมันต้องมีความรู้เรื่องนั้นด้วยเวลาเราดูพยานหลักฐานมันต้องประกอบพยานหลักฐาน กับความรู้ของผู้อ่านพยานหลักฐานด้วย มันทำให้ลำบากตรงนี้ครับ

สมมุติ ผู้เชี่ยวชาญคนอีกคนบอกอ่านแบบนี้ อีกคนบอกคุณรู้ได้ไงว่าอ่านแบบนี้ถูก มันต้องอ่านแบบนี้ กลายเป็นว่าตกลงพยานหลักฐานไม่น่าเชื่อถือ

การรวบรวมพยานหลักฐานมันก็ยากอยู่แล้ว พอมาพิสูจน์ความผิดจำเลย ยิ่งยากหนักความน่าเชื่อถือ คดีอาญาด้วย

ข้อเสนอแนะ ต่อภาครัฐ

1. รัฐต้องเปลี่ยนมุมมองในการจัดเก็บพยานหลักฐาน คือ ทุกวันนี้รัฐให้เป็นภาระของเอกชน 100% เลย ซึ่งผมว่าวิธีคิดแบบไม่ทำให้เกิดประสิทธิผล

คือตอนนี้รัฐมองว่าเป็นหน้าที่ของเอกชนอย่างเดียว แต่จริงๆ ประโยชน์มันเกิดขึ้นกับรัฐ แต่ก็คือประชาชนทั้งหมด แต่ว่าผู้ให้บริการเอกชนจริงๆแทบจะไม่มีส่วนได้ส่วนเสียอะไร มีแต่

ส่วนเสีย และถ้าจัดเก็บไม่ดี ที่เสียหายก็ไม่ใช่เอกชน แต่เป็นรัฐทั้งหมดที่เสียหาย ประชาชนทั้งหมดเสียหาย ควรให้รัฐมีส่วนรับผิดชอบ คือรัฐอาจจะเป็นผู้เก็บ คือ ผมว่าทุกวันนี้เก็บมากเก็บน้อยและมีข้อโต้แย้ง เพราะเอกชนไม่สามารถรับภาระนี้ได้ทั้งหมด

อีกประการหนึ่งก็คือเห็นว่ามันเป็นภาระความรับผิดชอบร่วมกัน ทั้ง 3 ฝ่าย คือ ประชาชนผู้ใช้บริการ ผู้ให้บริการ แล้วก็รัฐ จริงๆประชาชนควรจะมีส่วนรับผิดชอบในส่วนนี้ด้วย คือผมว่าต้องมีการสร้างความเข้าใจ ให้ประชาชนเข้าใจว่าจริงๆถ้าคุณที่มาก ที่ค่าบริการที่คุณจ่ายส่วนหนึ่งต้องใช้เก็บข้อมูลหลักฐานเพื่อคุ้มครองคุณในอนาคตด้วย เพราะว่าทุกวันนี้เวลาเราพูดถึงเราจะพูดถึง ค่าบริการทำไมมันถูก มันแพง ลดลงกว่านี้ได้ไหม ใช้ฟรีไปเลย ผมว่าถ้าร่วมกัน 3 ฝ่าย เรื่องนี้ข้อมูลหลักฐานไม่เป็นปัญหา แต่ทุกวันนี้ถ้ามันเป็นปัญหา ผมก็ให้บริการอย่างเดียวนิมันจะเป็นปัญหาของทั้งหมดในระยะยาว

เพราะว่าหลักฐานตัวที่เก็บ มันใช้คุ้มครองผู้ใช้ในอนาคต ถ้าเขาตกเป็นผู้เสียหาย

รัฐควรมีช่องทางประชาสัมพันธ์ให้เขา ถ้าประชาชนเขามีปัญหา เขาจะต้องทำอย่างไรบ้าง ซึ่งปัจจุบันนี้ เหมือนกับผู้เสียหายจะต้องไปถามเอง ไปค้นเอง ไปหาเอง โดยที่เขาไม่รู้ ขั้นตอนต้องการการติดต่อ คือถ้ารัฐจะทำดิจิตอลอีโคโนมี ควรจะทำศูนย์ช่วยเหลือประชาชนทางดิจิตอลให้หน่อย คือถ้าประชาชนไม่รู้อะไรก็โทรมาถาม

ควรพูดให้ประชาชนรู้สึกตระหนักตัวเอง ในทางเป็นจริงมันไม่ได้ทำได้ง่าย มาดูข่าวเรื่องทั่วๆไปแล้วคิดว่าตัวเองจะกลับไประวังมันไม่ใช่เรื่องที่เกิดขึ้นได้ง่าย แต่เอาเป็นว่ากรรีที่เขาเกิดข้อปัญหา เกิดข้อสงสัย เกิดความเสียหาย ให้มีคนทางราชการประสานงานและเขาจะต้องได้รับความช่วยเหลือยังไง อย่างน้อยตรงนี้จะต้องมีการเก็บสถิติหลักเลยว่า เป็นศูนย์แรกที่รับเรื่องจะได้สถิติที่สามารถเอามาทำอะไรได้อีกมาก เอามาวิเคราะห์ทำอะไรได้อีก

สร้างความตระหนัก ในทางอินเตอร์เน็ต แล้วเกี่ยวกับเด็ก คิดว่าควรจะเป็น มีวิชาสอนเกี่ยวกับการใช้ระบบ ผมมีประเด็น คือ ทุกวันนี้เวลาเด็กกระทำผิด ผมว่าเขาไม่รับรู้ถึงความเสียหายผลของการกระทำของเขามันเกิดความเสียหาย แล้วเด็กจะไม่ค่อยกลัว จึงอาจจะต้องเพิ่มในส่วนนั้นเข้าไป แต่ในทางที่เขาอยากจะทำนั้นอีกส่วนที่อาจจะทำให้เขาตกเป็นผู้เสียหายได้ เราก็ต้องให้ความรู้ว่า เป็นช่องทางที่ทำให้อื่นติดต่อเขาได้โดยตรง ต้องระมัดระวังอะไรอย่างนี้ ถ้ามีข้อมูลลักษณะไหนที่ควรต้องระวัง

ให้เห็นผล ให้ระมัดระวัง เห็นผลของการกระทำ ทำอย่างนี้เสียหาย ต้องติดคุกอะไร แค่กดนิดเดียวติดคุกเลย ถูกล่อลวง มี 2 มุม คือเด็กที่เป็นผู้กระทำ และเด็กที่เป็นผู้ถูกเสียหายนั้น อายุจะลดลง ช่วงนี้อายุจะลดลงเรื่อยๆ เด็กหาย เพราะเด็กเขาเรียนรู้ เด็กเรียนรู้ที่จะไปหลอกคนอื่น คือมันอยู่หน้าเครื่อง มันจะไม่รู้สึกถึงความเดือดร้อนของคน

ในการแชร์ อย่างเช่นข่าวลือหรืออะไรก็ตาม ในการแชร์แล้วคนอื่นได้รับความเสียหาย ไม่ตรวจสอบข้อมูลก่อน แล้วก็การส่งข้อมูล พวกนี้มันใช้ได้เร็วไป สังคมมันยังไม่เรียนรู้ ทุกคนใช้ทีเสรีภาพเต็มที่เลย ความยับยั้งชังใจมันต่างกัน

ด้านบุคลากร เฉพาะ ที่จบวิศวะกร ประมากประมาณ 1000 คน

เฉพาะ วิศวะกรคอมฯ ประมาณ 500 – 600 คน ระบบมันเยอะนะ ระบบเป็นหมื่นๆ บริการเยอะ แต่ละคนก็มีหน้าที่ในหลายๆ เรื่อง เครือข่าย สารข้อมูล ระบบ

ค่าตอบแทน ขั้นต่ำเลย ปริญญาตรี เริ่มที่ประมาณ 20,000 บาทมีโบนัส ค่าล่วงเวลารูปแบบอื่นๆ

เรื่องความก้าวหน้าทางวิชาชีพ เด็กเข้ามาแล้วรู้ชัดเจน ว่าเขาจะไปเติบโตยังไง

แผนพัฒนาบุคคล IDP

ที่นี่จะมี 2 สาย สายบริหารกับสายผู้ชำนาญการ ระดับมันเท่ากัน แต่ว่าสายผู้ชำนาญการก็ไม่ต้องบริหารคน ก็ทำให้เชี่ยวชาญไป

การพัฒนาบุคลากรและการฝึกอบรม

เรามีโปรแกรมการพัฒนาภายใน มีศูนย์ฝึกอบรม แล้วจริงๆอะไรที่เป็นเรื่องพื้นฐานทั่วไปที่ต้องอบรม เขามีโปรแกรมทั้งปีเลยครับ และไปสามารถสมัครลงเรียนได้เลย และจริงๆมีภาคบังคับด้วยนะครับ ว่าแต่ล่ะปีต้องเรียนอะไร

แต่ถ้าพูดถึงโดยเฉพาะของอาชีพอันนี้ต้องหาเองครับ หัวหน้าก็ต้องหาเองว่าอันไหน แต่ก็มีงบประมาณให้

ถ้าอย่างเรื่อง Security ต้องไปอบรมที่ต่างประเทศ

การที่ฝึกคนให้เป็นเรื่อง Security ด้วยวิธีการฝึกอบรมได้ผล อยู่ที่ทักษะ อยู่ที่ตัวบุคคลจริงๆคนที่เขาทำเรื่องพวกนี้ได้ จริงๆคือ เพราะเขาวิศวกรปกตินะ แต่ว่าเขาเป็นคนใฝ่รู้และค้นคว้าอะไรใหม่ๆ เพราะสิ่งที่เขาทำเป็นสิ่งที่ไม่มีใครทำมาก่อนเสมอ เป็นคนอีกแบบหนึ่งนะ อบรมก็ไม่เป็น ต้องแบบใฝ่รู้ ค้นคว้า และก็มีทักษะ คนมีทักษะด้านนี้คนที่จะเป็นแฮกเกอร์ได้

บทที่ 4
ผลการศึกษา

ในบทที่แล้วได้มีการสัมภาษณ์ผู้บริหารและผู้เชี่ยวชาญจากหน่วยงานต่างๆ ที่ทำงานเกี่ยวกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ และจากศึกษาข้อมูลสถิติภัยคุกคามของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พบว่ามีภัยคุกคามเพิ่มมากขึ้นทุกปี

ตารางที่ 4 – 1 สถิติภัยคุกคามปี 2554

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content							12	8	6	7	39	5	77
Availability							1	2	2	0	1	0	6
Fraud							44	38	56	69	66	36	309
Information gathering							28	13	18	14	12	8	93
Information security							0	0	0	0	0	0	0
Intrusion Attempts							9	20	19	19	16	11	94
Intrusion							0	0	0	0	0	0	0
Malicious code							6	10	14	7	18	8	63
Other							0	0	0	1	0	3	4
รวม							100	91	115	117	152	71	646

ตารางที่ 4 – 2 สถิติภัยคุกคามปี 2555

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	1	0	0	0	1	0	0	0	0	3
Availability	0	1	0	0	0	0	0	0	1	0	0	0	2
Fraud	16	37	32	42	32	32	51	54	74	49	48	67	534
Information gathering	4	5	10	8	8	5	5	10	5	0	1	1	62
Information security	0	1	0	0	0	0	0	0	0	0	1	0	2
Intrusion Attempts	3	3	13	8	8	6	7	10	8	2	2	5	75
Intrusion	1	1	1	1	0	3	1	0	0	0	1	4	13
Malicious code	3	6	9	12	7	4	7	3	8	8	10	5	82
Other	4	5	3	2	1	2	2	0	0	0	0	0	19
รวม	31	59	69	74	56	52	73	78	96	59	63	82	792

ตารางที่ 4 – 3 สถิติภัยคุกคามปี 2556

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	2	3	1	1	2	0	0	0	1	2	0	13
Availability	1	0	0	0	0	0	0	8	0	1	0	0	10
Fraud	36	48	49	56	78	56	110	53	53	54	59	42	694
Information gathering	3	0	0	0	0	2	0	0	0	3	0	0	8
Information security	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion Attempts	56	23	17	23	16	11	24	16	24	46	24	36	316
Intrusion	6	3	50	61	115	94	67	63	89	46	27	10	631
Malicious code	1	4	6	4	3	11	9	7	5	6	5	12	73
Other	0	0	0	0	0	0	0	0	0	0	0	0	0
รวม	104	80	125	145	213	176	210	147	171	157	117	100	1745

ตารางที่ 4 – 4 สถิติภัยคุกคามปี 2557

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	8
Availability	0	0	2	2	0	0	1	3	0	0	0	0	8
Fraud	59	68	69	72	145	85	94	66	98	88	101	65	1010
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	29
Information security	0	1	0	0	0	2	0	0	1	0	0	0	4
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	74	503
Intrusion	9	150	77	33	55	50	69	47	86	32	35	68	711
Malicious code	3	7	129	125	102	226	304	161	263	98	132	185	1735
Other	0	0	0	0	0	0	0	0	0	0	0	0	0
รวม	112	257	315	291	352	393	514	319	482	265	316	392	4008

ตารางที่ 4 – 5 สถิติภัยคุกคามปี 2558

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	2	0	0	0	0								2
Availability	0	0	0	0	0								0
Fraud	75	83	100	90	155								503
Information gathering	0	0	0	0	0								0
Information security	0	0	1	0	0								1
Intrusion Attempts	83	89	65	27	60								324
Intrusion	69	76	88	12	78								323
Malicious code	104	83	174	143	140								644
Other	0	0	0	0	0								0
รวม	333	331	428	272	433								1797

ตารางที่ 4 – 6 ประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดย eCSIRT

ประเภทภัยคุกคาม	คำอธิบาย
1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)
2 โปรแกรมไม่พึงประสงค์ (Malicious Code)	ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ
3 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
4 ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆ ของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
5 การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

ตารางที่ 4 – 6 ประเภทภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดย eCSIRT (ต่อ)

6 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
7 การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้
8 การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ
9 ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุก คามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

โดยจะพบว่าในเรื่องของการฉ้อโกง (Fraud) มีปริมาณมากขึ้นทุกปี ชี้ให้เห็นถึงจำนวนงานที่ผู้บังคับใช้กฎหมายจะต้องสืบสวนสอบสวนหาตัวผู้กระทำผิดมาลงโทษตามกฎหมาย แต่บุคลากรในงานนี้ไม่มีเพิ่มมากขึ้นเท่าจำนวนคดี มองให้เห็นปัญหาที่เกิดขึ้นในปัจจุบันและในอนาคต หากไม่มีการเพิ่มและพัฒนาผู้บังคับใช้กฎหมายให้มีศักยภาพในการดำเนินคดี

ผลการศึกษา

1. จำนวนเจ้าหน้าที่สืบสวน พนักงานสอบสวน ที่มีความรู้ความเชี่ยวชาญในอาชญากรรมประเภทนี้ยังมีน้อยมากสำหรับประเทศไทย ผู้มีความรู้ความชำนาญส่วนมากจะอยู่ในกรุงเทพมหานคร ในต่างจังหวัดเมื่อเกิดเหตุขึ้น การดำเนินคดีจะมีปัญหามากมาย พนักงานสอบสวนไม่รู้ว่าจะเริ่มต้นสอบสวนอย่างไร การเก็บ การตรวจยึดพยานหลักฐานทำไม่ถูกต้องตามมาตรฐาน การรวบรวมพยานหลักฐานที่สำคัญในสำนวนคดี การขอข้อมูลจากผู้ให้บริการ การส่งวัตถุพยานไปตรวจพิสูจน์ บางครั้งไม่ทราบว่าต้องการข้อมูลอะไรอยู่ตรงไหน เนื่องจากข้อมูลในเครื่องคอมพิวเตอร์มีจำนวนมาก จึงต้องเอาเฉพาะส่วนที่เกี่ยวข้องกับคดีเท่านั้น

2. จำนวนผู้เชี่ยวชาญในการตรวจพิสูจน์พยานหลักฐานดิจิตอล มีไม่เพียงพอ ผู้เชี่ยวชาญกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติมีประมาณ 4 คน,ของสถาบันนิติวิทยาศาสตร์ มี 3 คน และจากกลุ่มงานวิเคราะห์และพิสูจน์หลักฐานการกระทำผิดทางเทคโนโลยี กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มีจำนวน 2 คน เท่านั้นนอกจากนั้นก็อาจขอช่วยเหลือจากอาจารย์ที่มีความเชี่ยวชาญจากทางมหาวิทยาลัย เพื่อให้ช่วยตรวจพิสูจน์ หาข้อมูล พยานหลักฐานจากคอมพิวเตอร์ smartphone อุปกรณ์ต่างๆ ที่สามารถเก็บข้อมูล

นอกจากนั้น ยังมีปัญหาในเรื่องมาตรฐานของผู้เชี่ยวชาญว่าต้องมีคุณสมบัติอย่างไรบ้าง ถึงจะเป็นที่ยอมรับของศาล เนื่องจากเท่าที่ศึกษาวิจัยมาความรู้และประสบการณ์ของผู้ตรวจพิสูจน์ในการทำงานไม่เท่ากัน รวมทั้งการฝึกอบรม รวมทั้งเรื่องมาตรฐานในการตรวจพิสูจน์หลักฐานว่าได้มาตรฐานสากลหรือไม่อย่างไรในขั้นตอนการดำเนินงานในการตรวจพิสูจน์ การรายงานผลการตรวจพิสูจน์ และเรื่องสำคัญอีกเรื่องหนึ่งคือ Chain of custody นอกจากนั้นพบว่าห้องปฏิบัติการคับแคบไม่มีที่เก็บวัตถุพยานที่เหมาะสมได้มาตรฐานอาจทำให้ผู้อื่นสามารถเข้าถึงวัตถุพยานไปทำลายหรือเพิ่มเติมข้อมูลได้ ทำให้ขาดความน่าเชื่อถือ

ปัญหาในการดำเนินคดีชั้นพนักงานอัยการ

1. ปัจจุบันพนักงานสอบสวนมักทำสำนวนการสอบสวนคดีเกี่ยวกับเทคโนโลยีไปตามรูปแบบการสอบสวนแบบเดิม คือเมื่อมีการร้องทุกข์กล่าวโทษ พนักงานสอบสวนก็จะสอบปากคำผู้เสียหาย แล้วไปดำเนินการขอศาลออกหมายจับผู้ต้องหาโดยไม่ได้มีการสอบสวนเชิงลึกก่อน ประเด็นที่เกิดปัญหาในปัจจุบันคือ เมื่อพนักงานสอบสวนได้หมายจับจึงรีบเร่งไปทำการจับกุมตัวผู้ต้องหาทั้งที่พยานหลักฐานทางดิจิตอล หรือพยานหลักฐานทางเอกสารยังไม่ได้รวบรวม ปัญหาคือบางคดีเช่นความผิดเกี่ยวกับการหลอกขายสินค้าทางอินเตอร์เน็ต ซึ่งเป็นความผิดฐาน

ฉ้อโกงประชาชน และ นำข้อมูลเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น มีอัตราโทษจำคุกไม่เกินห้าปี ซึ่งสามารถขออำนาจศาลฝากขังผู้ต้องหาได้เพียง 4 ครั้ง ครั้งละไม่เกิน 12 วัน รวม 48 วัน แต่เนื่องจากพนักงานสอบสวนไม่ได้มีการสอบสวนเชิงลึกก่อนทำการจับกุม ทำให้ระยะเวลาในการรวบรวมพยานหลักฐานไม่เพียงพอที่จะทำการตรวจสอบข้อเท็จจริงในการกระทำผิด เช่น การตรวจสอบไปยังผู้ดูแลระบบเว็บไซต์ที่คนร้ายนำข้อมูลเท็จไปโฆษณาในเว็บไซต์ว่าใครเป็นผู้นำข้อมูลเท็จเข้าสู่เว็บไซต์ โดยใช้หมายเลขไอพีแอดเดรสใด และนำเข้าข้อมูลเมื่อวันเวลาใด ซึ่งองค์ประกอบสำคัญในการดำเนินคดีกับผู้กระทำความผิดในข้อหา นำข้อมูลเท็จเข้าสู่ระบบคอมพิวเตอร์ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น อีกทั้งบางคดีพยานหลักฐานสำคัญอยู่ในความครอบครองของหน่วยงานในต่างประเทศ การนำพยานหลักฐานดังกล่าวมาใช้ในการดำเนินคดีในประเทศจึงจำเป็นต้องปฏิบัติตามพระราชบัญญัติความร่วมมือในการดำเนินคดีทางอาญา พ.ศ.2535 ทำให้ในการดำเนินคดีขาดพยานหลักฐานทางดิจิตอลและพยานเอกสารสำคัญในการพิสูจน์การกระทำความผิดของผู้ต้องหาในบางคดีจึงทำให้ไม่สามารถฟ้องผู้ต้องหาได้ภายในเวลาที่ศาลอนุญาตฝากขัง ทำให้ต้องปล่อยตัวผู้ต้องหาไปและเป็นเหตุให้ผู้ต้องหาไหวตัวออกไปทำลายพยานหลักฐานทางดิจิตอลและพยานเอกสารสำคัญ จนสูญสิ้น

2. ด้านการขอความร่วมมือในการสอบสวนในคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ ในคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ ที่ใช้ระบบเครือข่ายอินเทอร์เน็ต เป็นเครื่องมือในการกระทำความผิด การสอบสวนรวบรวมพยานหลักฐาน เพื่อระบุตัวผู้กระทำความผิด จะต้องใช้ข้อมูลหรือพยานหลักฐานจากผู้ให้บริการต่างๆ ในระบบอินเทอร์เน็ต และคดีเป็นจำนวนมากที่คนร้ายอาศัยเครือข่ายที่อยู่ประเทศหนึ่งในการลงมือกระทำความผิดต่อบุคคล ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่อยู่อีกประเทศหนึ่ง การสอบสวนรวบรวมพยานหลักฐานจึงต้องอาศัยความร่วมมือระหว่างประเทศในเรื่องทางอาญา ซึ่งจะต้องกระทำอย่างเร่งด่วน เพื่อให้ทันกับการนำข้อมูลดังกล่าวไปใช้สืบหาตัวผู้กระทำผิดต่อไป แต่ในทางปฏิบัติแล้วการดำเนินการตามกฎหมายและสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา มักไม่ได้รับความร่วมมือจากประเทศต่างๆ หรือการสอบสวนที่ขอความร่วมมือจากต่างประเทศ มักเกิดความล่าช้า และไม่มีสภาพบังคับ หรือแนวทางแก้ไขเพิ่มเติม ทำให้เป็นอุปสรรคต่อการสอบสวนคดี โดยเฉพาะอย่างยิ่งกรณีที่มีกำหนดเวลาจำกัด ในเรื่องต่างๆ เช่น การใช้ IP Address เป็นพยานหลักฐานในคดี ซึ่งจะต้องรวบรวมโดยด่วน เพื่อให้ทันต่อระยะเวลาในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Computer Traffic Data) จากแหล่งต่างๆ จึงควรพิจารณาวิธีการสอบสวนในแนวทางอื่นเพิ่มเติม และหาแนวทางแก้ไขปัญหาโดยสร้างเครือข่ายความร่วมมืออย่างเป็นระบบ ให้ทันต่อการสืบสวนสอบสวนดำเนินคดีอย่างมีประสิทธิภาพด้วย

3. การนำตัวผู้กระทำความผิดที่เป็นตัวการที่แท้จริงมาลงโทษ ปัญหานี้เกิดขึ้นในกรณีของการกระทำความผิดผ่าน Social Media กระทำความผิดในลักษณะดังกล่าว เมื่อพิจารณาจากสำนวนการสอบสวนแล้วจะพบว่าผู้ต้องหาที่ถูกกล่าวหาว่ากระทำความผิดและถูกดำเนินคดีโดยส่วนใหญ่นั้น อาจจะไม่ใช่ตัวการในการกระทำความผิดที่แท้จริง โดยส่วนใหญ่ผู้ต้องหาที่ถูกดำเนินคดีจะเป็นเจ้าของบัญชีธนาคารที่มีการับโอนเงินที่ผู้เสียหายถูกหลอกมา โดยผู้ต้องหาเหล่านี้อาจกระทำการโดยรู้เท่าไม่ถึงการณ์ โดยการรับจ้างเปิดบัญชี หรือเปิดบัญชีให้กับคนร้ายเนื่องจากถูกหลอกลวง ซึ่งเท่ากับว่าบุคคลเหล่านั้นอาจไม่มีส่วนรู้เห็นในการกระทำความผิดดังกล่าว และทำให้บุคคลที่เป็นตัวการในการลงข้อมูลใน Social Media หลอกลวงผู้เสียหายนั้น ไม่ถูกนำตัวมาลงโทษได้ ดังนั้นสมควรที่สถาบันการเงิน ต้องตรวจสอบและเคร่งครัดในการเปิดบัญชีให้กับผู้ขอเปิดบัญชีมากยิ่งขึ้น และควรมีข้อกำหนด ในสัญญาเปิดบัญชีแสดงคำเตือนว่าการรับจ้างเปิดบัญชีมีความผิดทางอาญา เป็นต้น นอกจากนี้ปัญหาดังกล่าวส่วนหนึ่งอาจเกิดจาก Social Media ที่ผู้หลอกลวงใช้เป็นเครื่องมือในการหลอกลวงผู้เสียหาย อย่างเช่น เฟสบุ๊ค (Facebook) หรือ อีเมล์ (Email) นั้น เป็นผู้ให้บริการที่อยู่ต่างประเทศ ดังนั้นในการขอข้อมูลหรือเอกสารอื่น ๆ ที่จำเป็นต่อการดำเนินคดีจะต้องมีการดำเนินการในลักษณะของการขอความร่วมมือในระดับประเทศ เช่น การใช้พระราชบัญญัติความร่วมมือระหว่างประเทศในเรื่องทางอาญา พ.ศ.2535 ซึ่งส่งผลให้เกิดความล่าช้าหรือในบางกรณีอาจไม่ได้รับความร่วมมือด้วยเช่นกัน

4. สำนักงานอัยการสูงสุดยังขาดพนักงานอัยการที่มีความเชี่ยวชาญในอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ อีกจำนวนมาก ทั้งในด้านการสืบสวนสอบสวนในกรณีที่เป็นความผิดที่มีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย และความเชี่ยวชาญในการพิจารณาสั่งสำนวนและการดำเนินคดีในชั้นศาล

5. สำนักงานการสอบสวน สำนักงานอัยการสูงสุด ยังขาดรับงบประมาณที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ โดยเฉพาะคดีที่ตั้งต้นที่พนักงานอัยการ รวมทั้งงบประมาณในการบริหารจัดการ การประสานงานกับหน่วยงานอื่น ยังขาดแคลนอุปกรณ์ เครื่องมือในการทำงานตลอดจนเทคโนโลยีสมัยใหม่ที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ

6. การติดต่อประสานงานระหว่างหน่วยงานราชการ และภาคเอกชน ที่ครอบครองพยานหลักฐานยังมีขั้นตอนยุ่งยากล่าช้า , การประสานงานขอความร่วมมือทางอาญาระหว่างประเทศมีขั้นตอนที่เป็นทางการ หลายขั้นตอนในแต่ละหน่วยงาน ขาดความสะดวกรวดเร็วและมีประสิทธิภาพ ประกอบกับความร่วมมือระหว่างประเทศ ยังไม่ครอบคลุมประเทศที่เกี่ยวข้องกับการกระทำความผิด หรือครอบครองพยานหลักฐานที่ต้องใช้ในการดำเนินคดี

สาเหตุที่อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์มีปริมาณเพิ่มมากขึ้น เนื่องจากในยุคปัจจุบันเป็นยุคของการสื่อสารอุปกรณ์ในการติดต่อสื่อสาร คอมพิวเตอร์ Smartphone มีให้เลือกหลากหลาย ราคาไม่แพง ปริมาณผู้ใช้ทวีจำนวนมากขึ้น มีการเชื่อมต่อระบบอินเตอร์เน็ทสามารถสื่อสารทางโปรแกรมสนทนาต่างๆ ทาง Line , facebook การส่งข้อความ ภาพถ่าย การทำธุรกรรมการเงิน ซื้อขายสินค้าออนไลน์ คนร้ายเป็นผู้ที่มีความรู้ความเชี่ยวชาญในการใช้คอมพิวเตอร์สามารถหลอกลวงคนได้ทีละจำนวนมากพร้อมกันได้อย่างรวดเร็ว และเสียค่าใช้จ่ายน้อยมาก มีการเชื่อมต่ออินเตอร์เน็ทได้ก็สามารถกระทำผิดได้ทุกที่ทุกเวลา ใครไม่ระมัดระวังป้องกันตัว ประมาทเลินเล่อ ไม่พิจารณาข้อมูลข่าวสารให้รอบคอบ หลงเชื่อง่าย ก็จะตกเป็นเหยื่อ ทำให้ถูกหลอกสูญเสียทรัพย์สิน หรือถูกหลอกไปข่มขืนกระทำชำเรา เป็นต้น นอกจากนั้นหากผู้ใช้ไม่มีจิตสำนึกในการลงหรือส่งต่อข้อความ ส่งต่อภาพและข้อความที่ไม่เหมาะสมก็อาจจะเป็นความผิดตามกฎหมายได้

ปัญหาในเรื่องของการขาดบุคลากรที่เชี่ยวชาญในด้านคอมพิวเตอร์ เนื่องจากเป็นการยากที่จะนำผู้บังคับใช้กฎหมายส่วนมากที่มีอยู่ในปัจจุบันมาฝึกฝนให้เชี่ยวชาญด้านคอมพิวเตอร์ เนื่องจากไม่มีความคุ้นเคยกับการใช้คอมพิวเตอร์มาก่อนและมีความสามารถเพียงใช้งานได้ในขั้นพื้นฐานเท่านั้น แต่ในการแกะรอย ติดตามหาผู้กระทำความผิด การดึงข้อมูลพยานหลักฐานที่สำคัญต่างๆ ยังไม่สามารถทำได้ ต้องใช้ผู้ที่มีความรู้ความชำนาญโดยเฉพาะที่ได้ศึกษามาโดยตรง

แต่ปัญหาที่ตามมา เนื่องจากในยุคปัจจุบันเด็กที่จบการศึกษาอยู่ในช่วง Generation Y คือ กลุ่มคนที่เกิดระหว่างปี พ.ศ.2523-2543 เป็นกลุ่มคนที่โตมาพร้อมกับคอมพิวเตอร์-อินเตอร์เน็ต และเทคโนโลยีไอที พวกนี้เป็นวัยที่จัดว่าเพิ่งเริ่มเข้าสู่วัยทำงาน มีลักษณะนิสัยชอบแสดงออก มีความเป็นตัวของตัวเองสูง ไม่ชอบอยู่ในกรอบและไม่ชอบเงื่อนไข คนกลุ่มนี้ต้องการความชัดเจนในการทำงานว่า สิ่งที่ทำมีผลต่อตนเองและต่อหน่วยงานอย่างไร อีกทั้งยังมีความสามารถในการทำงานที่เกี่ยวกับการติดต่อสื่อสาร และยังสามารถทำงานหลายๆ อย่างได้ในเวลาเดียวกัน ซึ่งจะมีทัศนคติ แนวคิด และอุปนิสัยไปในทิศทางที่แตกต่างจากคนในยุคก่อนหน้า การดำเนินชีวิตที่ไม่จำเป็นที่จะต้องอยู่กับที่เสมอไป เช่น การทำงานในออฟฟิศตั้งแต่แปดโมงเช้ายันห้าโมงเย็น ก็สามารถเปลี่ยนเป็นการไปท่องเที่ยวและใช้โทรศัพท์มือถือประสานงานหรือสั่งงานแทนได้ ซึ่งปัจจุบันเทคโนโลยี 3G และ Wifi ก็สามารถทำให้ผู้คนในยุคนี้มีชีวิตที่เคลื่อนที่ไปด้วยทำงานไปด้วยได้ ใช้ชีวิตในการทำงานและชีวิตส่วนตัวบนหลายๆ อุปกรณ์ที่มีจอภาพ ได้แก่ หน้าจอทีวี หน้าจอคอมพิวเตอร์ หน้าจอแท็บเล็ต และหน้าจอมือถือ

เด็กที่เก่งด้านคอมพิวเตอร์ เมื่อจบแล้วบริษัทภาคเอกชนจะไปเสนองานให้ทำและให้เงินเดือนสูงกว่าอัตราปริญญาตรีของทางราชการ และมีสวัสดิการ รางวัล มีความเจริญก้าวหน้าที่ชัดเจน ทำให้เด็กตัดสินใจไปทำงานภาคเอกชนจำนวนมาก เหลือมาสนใจรับราชการจำนวนน้อย

ประกอบกับการเข้ารับราชการมีระเบียบ มีขั้นตอนและการแข่งขันสูง และแต่ละปีรับจำนวนน้อย จึงเป็นส่วนหนึ่งของปัญหาในการขาดบุคลากรเมื่อได้เข้ารับราชการแล้วก็ต้องใช้เวลาฝึกอบรมเรียนรู้การทำงานระบบราชการและงานที่เกี่ยวข้อง รวมทั้งงานในหน้าที่ที่ต้องรับผิดชอบ เพื่อให้สามารถทำงานได้ตามเป้าหมายอย่างมีประสิทธิภาพ ซึ่งหากพนักงานสอบสวน พนักงานอัยการ ได้ผู้ที่มีความรู้ความเชี่ยวชาญด้านคอมพิวเตอร์ มาช่วยงานอย่างใกล้ชิดแล้วจะทำให้การได้มาซึ่งข้อมูลสำคัญ เช่น การติดต่อสื่อสารของคนร้าย การแกะรอยติดตามคนร้าย การรวบรวมพยานหลักฐานจะเป็นไปอย่างรวดเร็วมากขึ้น

แนวทางในการพัฒนาผู้บังคับใช้กฎหมาย

1. รัฐต้องหาแนวทางจูงใจให้ผู้ที่จบการศึกษาด้านคอมพิวเตอร์เข้ามารับราชการในส่วนที่เกี่ยวข้องกับกระบวนการยุติธรรม โดยเปิดรับจำนวนมากและให้อัตราเงินเดือนใกล้เคียงกับภาคเอกชน

2. จัดฝึกอบรมให้ความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสมัยใหม่ในส่วนที่เกี่ยวข้องกับการทำคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ให้กับผู้บังคับใช้กฎหมายอย่างเร่งด่วนและจำนวนมาก รวมทั้งต้องฝึกอบรมอย่างต่อเนื่อง เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา

3. สร้างผู้เชี่ยวชาญในการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ให้มีจำนวนมากขึ้น

4. การจัดฝึกอบรมร่วมกันระหว่างหน่วยงานภาครัฐที่เกี่ยวข้องทั้งหมด เพื่อให้เกิดประสิทธิภาพในการทำงานร่วมกัน การแบ่งปันข้อมูล รวมทั้งการสร้างความสัมพันธ์ที่ดี

5. จัดประชุมสัมมนาร่วมกับภาคเอกชน นักวิชาการ ผู้ให้บริการ หน่วยงานความมั่นคงอื่นๆ เพื่อแลกเปลี่ยนข้อมูลข่าวสารและข้อเสนอแนะในการทำงาน เรียนรู้วิทยาการใหม่ๆ

6. การให้โอกาสผู้ปฏิบัติงานไปศึกษาดูงาน ฝึกอบรม ประชุมในต่างประเทศ เพื่อให้รู้เท่าทันกับต่างประเทศในด้านเทคนิค วิทยาการต่างๆ รวมทั้งได้รู้จักกับเจ้าหน้าที่ในประเทศต่างๆ เพื่อประโยชน์ในการติดต่อสื่อสารในการทำงานในอนาคต

7. ให้อัตราเงินเดือนที่สูงกว่า สร้างขวัญและกำลังใจให้กับผู้ปฏิบัติงาน พร้อมทั้งกำหนดเส้นทางความก้าวหน้าในอาชีพชัดเจน

8. อบรมเรื่องคุณธรรมจริยธรรม ทำงานด้วยความซื่อสัตย์ สุจริต ไม่ทุจริตคอรัปชั่น ปฏิบัติหน้าที่ด้วยความโปร่งใส ตรวจสอบได้ และอำนวยความยุติธรรมแก่ทุกฝ่ายอย่างเสมอภาคกัน

บทที่ 5
สรุปและข้อเสนอแนะ

สรุป

จากการศึกษาวิจัยพบว่าความเจริญก้าวหน้าทางเทคโนโลยีเป็นไปอย่างรวดเร็วมาก นอกจากนั้น เครื่องใช้ไฟฟ้า คอมพิวเตอร์ Smartphone และเครื่องมือสื่อสาร อุปกรณ์อื่นๆ ที่ใช้ในการบันทึกข้อมูล การติดตาม บอกเส้นทาง กล้องวงจรปิด มีราคาถูกลง ขนาดเล็กลง แต่มีประสิทธิภาพมากขึ้น ในอนาคตอันใกล้จะเข้าสู่ยุค Internet of Things หมายถึง การที่สิ่งต่างๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเตอร์เน็ต เช่น การสั่งเปิด – ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรมอาคารบ้านเรือน เครื่องใช้ในชีวิตประจำวันต่างๆ ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น หากวันนั้นมาถึงอย่างเต็มรูปแบบจะเป็นทั้งประโยชน์อย่างมหาศาล และความเสี่ยงไปพร้อมๆ กัน เพราะหากระบบรักษาความปลอดภัยของอุปกรณ์และเครือข่ายอินเทอร์เน็ตไม่ดีพอ จะทำให้ผู้ไม่ประสงค์ดีเข้ามากระทำการที่ไม่พึงประสงค์ต่ออุปกรณ์ข้อมูลสารสนเทศหรือความเป็นส่วนตัวของบุคคลได้

นอกจากนั้นแล้วผู้ใช้คอมพิวเตอร์จะมีอายุน้อยลง แต่มีความสามารถในการใช้อุปกรณ์และโปรแกรมต่างๆ ได้อย่างคล่องแคล่ว ซึ่งหากไม่ได้รับการให้คำแนะนำชี้แนะในทางที่ถูกต้องแล้วอาจนำความรู้ความสามารถไปใช้ในทางในที่ไม่เหมาะสมก่อให้เกิดความเสียหายแก่ผู้อื่นหรือทำในสิ่งที่ผิดกฎหมายได้

จากความก้าวหน้าทางเทคโนโลยีและผู้คนทั่วโลกใช้คอมพิวเตอร์ Smartphone ติดต่อสื่อสาร ทำธุรกิจค้าขายกันตลอด 24 ชั่วโมง โดยขาดความรู้ความเข้าใจในระบบคอมพิวเตอร์ไม่รู้วิธีการใช้อย่างถูกต้อง หรือประมาทไม่ระมัดระวังการเก็บรักษาข้อมูลสำคัญหรือหลงเชื่อข้อมูลข่าวสารโดยไม่พิจารณาตรวจสอบให้รอบคอบ จะทำให้ตกเป็นเหยื่อของอาชญากรที่มุ่งร้าย ทำให้อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์จะทวีจำนวนมากขึ้น ภัยอันตรายจะกระทบถึงตัวบุคคลได้ง่ายและรวดเร็ว รูปแบบการกระทำผิดมีความหลากหลาย สลับซับซ้อน อำพรางตนไม่ให้ติดตามจับกุมได้โดยง่าย ต้องใช้เจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์โดยตรงในการแกะรอย ติดตามคนร้าย ค้นหาข้อมูล รวบรวมพยานหลักฐานต่างๆ

และการกระทำความผิดจะเป็นลักษณะข้ามชาติไร้พรมแดน รวมทั้งอาจเป็นกรณีองค์กรอาชญากรรมข้ามชาติ ซึ่งคนร้ายจะเป็นทั้งผู้ที่มีความรู้ความเชี่ยวด้านคอมพิวเตอร์ การใช้เทคโนโลยีด้านๆ มีการทำงานเป็นทีม แบ่งหน้าที่กันทำ ร่วมกันฉ้อโกงหลอกลวงทรัพย์สินของผู้เสียหายจำนวนมาก ก่อให้เกิดปัญหาแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายในด้านการสืบสวนสอบสวน การรวบรวมพยานหลักฐาน ในกรณีที่คนร้ายและพยานหลักฐานอยู่ในต่างประเทศ เกิดปัญหาความล่าช้า ในการติดต่อประสานงาน ตั้งแต่การขอความร่วมมือระหว่างประเทศในทางอาญา การส่งผู้ร้ายข้ามแดน ถึงแม้จะมีสนธิสัญญาต่อกัน หรือมีการให้คำมั่นต่างตอบแทนก็ตาม แต่ว่าในแต่ละประเทศก็ยังมีกฎหมายภายใน มีระเบียบ ขั้นตอน ในการพิจารณาดำเนินคดีของตนที่แตกต่างกันไป ซึ่งทางเราไม่สามารถไปก้าวก่ายการทำงานของเจ้าหน้าที่ในประเทศนั้นๆ ได้ นอกจากจะมีความร่วมมืออย่างไม่เป็นทางการ มีความสัมพันธ์ส่วนตัวที่ดีต่อกัน ความเชื่อใจซึ่งกันและกัน จะช่วยให้การประสานงานเป็นไปโดยง่ายขึ้น นอกจากนั้นเรื่องแปลภาษาก็เป็นปัญหาที่สำคัญมากอย่างหนึ่งคือ ค่าใช้จ่ายในการแปล ระยะเวลาที่ใช้ในการแปล และกรณีที่ต้องแปลเป็นภาษาท้องถิ่น ที่เจ้าหน้าที่เราไม่มีความเชี่ยวชาญ เช่น ภาษารัสเซีย เกาหลี อินเดียทำให้ไม่สามารถตรวจสอบได้ว่าแปลถูกต้องตามเอกสารที่ส่งไปหรือไม่อย่างไร

จากบทสัมภาษณ์ผู้บริหารของหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องพบว่าผู้บังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญในด้านกฎหมาย มีทักษะและประสบการณ์การสืบสวนสอบสวน พร้อมทั้งความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์ การใช้เทคโนโลยีสมัยใหม่ ยังมีจำนวนน้อยมาก ไม่เพียงพอที่จะต่อสู้กับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่เกิดขึ้นในปัจจุบันและแนวโน้มที่จะเกิดขึ้นในอนาคตได้อย่างมีประสิทธิภาพ เนื่องจากผู้ที่มีความรู้ความเชี่ยวชาญทางด้านคอมพิวเตอร์เลือกที่ทำงานในภาคเอกชนที่มีรายได้สูงกว่าเงินเดือนราชการมาก มีสวัสดิการผลตอบแทนที่ดี มีเส้นทางความก้าวหน้าในอาชีพที่ค่อนข้างชัดเจน เด็กรุ่นใหม่ที่เรียนจบด้านคอมพิวเตอร์ หรือวิทยาศาสตร์ เลือกที่จะทำงานกับเอกชนมากกว่าที่จะรับราชการ ระบบราชการมีตำแหน่งน้อยเข้ายาก มีการขึ้นอัตราเงินเดือนช้าและน้อยกว่าเอกชน และต้องรับภาระรับผิดชอบสำนวนคดีจำนวนมาก ขาดขวัญและกำลังใจที่ดี เส้นทางความก้าวหน้าไม่ชัดเจน การเลื่อนตำแหน่ง การโยกย้าย ทำให้กำลังเจ้าหน้าที่ขาดแคลน ต้องใช้เวลาฝึกฝนคนที่ย้ายมาอยู่ใหม่ นอกจากนั้นยังขาดงบประมาณในการจัดหาอุปกรณ์ที่มีประสิทธิภาพ และค่าใช้จ่ายที่เกี่ยวข้องในการบริหารจัดการคดี การฝึกอบรมยังไม่ทั่วถึงและน้อยเกินไปไม่ต่อเนื่อง ขาดการศึกษาดูงานทั้งในและต่างประเทศ ขาดการฝึกอบรมร่วมกันระหว่างผู้บังคับใช้กฎหมาย การสัมมนา ประชุมระหว่างภาครัฐและหน่วยงานเอกชนที่เกี่ยว การแบ่งปันข้อมูลข่าวสารระหว่างหน่วยงาน

ดังนั้นประชาชนต้องตระหนักรู้ถึงภัยร้ายต่างๆ ที่จะเกิดขึ้น ดูแลป้องกันตัวเองอย่าให้ตกเป็นเหยื่อของคนร้าย ซึ่งเมื่อเกิดการกระทำผิดแล้ว โอกาสที่จะได้รับการเยียวยาหรือ การได้ทรัพย์สินมาเป็นไปได้ยาก และต้องใช้เวลานานกว่าจะจับได้ตัวคนร้ายมาลงโทษตามกฎหมาย

ข้อเสนอแนะ

1. การให้ความรู้ต่อสังคมให้ตระหนัก เรื่องพิษภัยของอาชญากรรมที่เกิดจากอินเตอร์เน็ต และต้องสอนเด็กในโรงเรียนเรียน ให้เรียนรู้ระบบของคอมพิวเตอร์ การทำงาน การใช้อินเตอร์เน็ต รวมทั้งมารยาทการใช้อย่างเหมาะสมและโดยชอบด้วยกฎหมาย

1.1 ควรมีการประชาสัมพันธ์เชิงรุกให้มากกว่านี้ เผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายคอมพิวเตอร์ เพื่อสร้างความรู้และความเข้าใจให้กับประชาชนให้มากกว่าที่เป็นอยู่นี้ เผยแพร่วิธีการกระทำความผิดในรูปแบบใหม่ๆ และมีช่องทางให้ประชาชนสามารถติดต่อ แจ้งเหตุ ให้ข้อมูล ขอคำแนะนำได้อย่างสะดวก หลากหลายช่องทาง

1.2 การซื้อขาย การทำธุรกรรมทางการเงิน ออนไลน์ ต้องให้ข้อมูลแก่ประชาชนเกี่ยวกับบริษัทที่จดทะเบียนของผู้ซื้อและผู้ขาย รายละเอียดของสินค้า และข้อมูลสำคัญที่เกี่ยวข้องกับการทำธุรกรรมสามารถตรวจสอบติดตามหลังเกิดเหตุได้

1.3 ควบคุม ตรวจสอบ เฝ้าระวังการเผยแพร่เว็บไซต์ที่หมิ่นสถาบันพระมหากษัตริย์ เว็บไซต์ที่ขายของผิดกฎหมาย ลามกอนาจาร หรือเว็บไซต์ที่ไม่เหมาะสมขัดต่อศีลธรรมอันดี

2. การพัฒนาเจ้าหน้าที่ผู้บังคับใช้กฎหมาย

2.1 ควรเร่งรัดพัฒนาผู้บังคับใช้กฎหมายให้มีความรู้ความเชี่ยวชาญในด้านกฎหมายการสืบสวนสอบสวนและทักษะด้านคอมพิวเตอร์และเทคโนโลยีสมัยใหม่ให้มากขึ้น อบรมตำรวจตามสถานีตำรวจทั้งในกรุงเทพและต่างจังหวัดให้มีความรู้และทักษะ จนสามารถทำคดีที่เกี่ยวข้องกับคอมพิวเตอร์ได้ เพื่อลดภาระงานของกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ ปอท.

2.2 จัดฝึกอบรมการสืบสวนสอบสวนร่วมกันระหว่างผู้บังคับใช้กฎหมายที่เกี่ยวข้องทุกหน่วยงาน เพื่อฝึกการทำงานเป็นทีม การทำความรู้จักกัน การแบ่งปันข้อมูลข่าวสารซึ่งกันและกัน การสร้างเครือข่าย การสร้างจิตสำนึกในการทำงานร่วมกัน โดยถือผลสำเร็จของคดีเป็นเป้าหมาย นอกจากนั้นควรจัดประชุมสัมมนากับหน่วยงานภาคเอกชน นักวิชาการ ที่ต้องทำงานเกี่ยวข้องกับผู้บังคับใช้กฎหมายอย่างสม่ำเสมอเพื่อให้ทันต่อสถานการณ์การเปลี่ยนแปลง รูปแบบการกระทำผิด

2.3 สร้างมาตรฐานในการตรวจพิสูจน์พยานหลักฐาน (Forensic) รวมทั้งมาตรฐานของผู้เชี่ยวชาญด้วยว่ามีคุณสมบัติอย่างไรบ้าง

2.4 จัดทำคู่มือในการปฏิบัติงานของแต่ละสำนักงาน และคู่มือหรือแนวทางในการทำงานร่วมกันในคดีสำคัญ

2.5 ให้โอกาสผู้บังคับใช้กฎหมายในระดับผู้ปฏิบัติงานไปศึกษา ดูงาน ฝึกอบรม ประชุมในต่างประเทศ เพื่อให้เรียนรู้ในด้านเทคนิค วิทยาการต่างๆ รวมทั้งได้รู้จักกับเจ้าหน้าที่ในประเทศต่างๆ เพื่อประโยชน์ในการติดต่อสื่อสารสร้างเครือข่ายในการทำงานร่วมกันในอนาคต

2.6 เพิ่มอัตราเงินเดือนให้สูงขึ้น มีรางวัลรวมทั้งแรงจูงใจในการทำงาน และรู้เส้นทางความก้าวหน้าในอาชีพชัดเจน

2.7 ให้ความสำคัญกับการดำเนินคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ เป็นการเฉพาะอย่างเร่งด่วน เพราะปัจจุบันอาชญากรใช้ช่องทางการสื่อสาร และอุปกรณ์เทคโนโลยีที่ทันสมัย ในการกระทำความผิดเป็นจำนวนมาก สร้างความเสียหายแก่ประชาชน และสังคมอย่างมาก

3. การสร้างเครือข่ายการทำงาน

3.1 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ ภายในประเทศที่มีหน้าที่ป้องกัน และปราบปราม รวมถึงการดำเนินคดี เพื่อใช้อำนาจหน้าที่ตามกฎหมายต่างๆ ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

3.2 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ กับภาคเอกชน เพื่อให้เจ้าหน้าที่ของรัฐสามารถเข้าถึงข้อมูลต่างๆ เช่น ข้อมูลการเงิน ข้อมูลการสื่อสารทางโทรศัพท์ หรือเครือข่ายอินเทอร์เน็ต ได้อย่างมีประสิทธิภาพ และรวดเร็ว การทำงานร่วมกับ Thai cert รวมทั้ง ETDA

3.3 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐและเอกชนในต่างประเทศ เช่น ตำรวจสากล I 24/7 การหาแนวทางให้การขอความร่วมมือระหว่างประเทศทางอาญาและการส่งผู้ร้ายข้ามแดนให้รวดเร็วและมีประสิทธิภาพมากขึ้น

4. ควรมีการแก้กฎหมายให้ทันต่อสถานการณ์ในด้านสารบัญญัติ รูปแบบการกระทำผิด กำหนดบทลงโทษให้เหมาะสมกับความเสียหายที่เกิดขึ้น แก้ไขปรับปรุงประมวลกฎหมายวิธีพิจารณาความอาญา เกี่ยวกับการสืบสวนสอบสวน การตรวจ ค้นยึดของกลาง การรับฟังพยานหลักฐาน เป็นต้น เนื่องจากอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์มีลักษณะพิเศษกว่าอาชญากรรมอื่นๆ มีเรื่องเกี่ยวกับการใช้เทคโนโลยีต่างๆ มาเกี่ยวข้อง

5. ควรมีศาลที่มีอำนาจพิจารณาคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์โดยเฉพาะ

6. สำนักงานอัยการสูงสุดควรมีสำนักงานคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์โดยเฉพาะ เพื่อสร้างผู้เชี่ยวชาญในคดีดังกล่าว และสามารถบริหารจัดการสารบบและสถิติคดได้ รวมทั้งหน่วยงานที่เกี่ยวข้องสามารถติดต่อประสานงานได้โดยตรง

7. รัฐควรมีหน่วยปฏิบัติการเฉพาะกิจ โดยให้มีเจ้าหน้าที่ผู้บังคับใช้กฎหมายและเจ้าหน้าที่ด้านต่างๆที่เกี่ยวข้อง ผู้ตรวจพิสูจน์ ผู้เชี่ยวชาญด้านคอมพิวเตอร์ มาทำงานร่วมกันทำคดีที่สำคัญๆ เช่น คดีฉ้อโกงประชาชน แชร์ลูกโซ่ องค์กรอาชญากรรมข้ามชาติ เป็นต้น เป็นหน่วยงานที่รวบรวมข้อมูลการดำเนินคดี และศูนย์กลางการติดต่อประสานงานทั้งในและต่างประเทศในคดีความผิดเกี่ยวกับคอมพิวเตอร์เป็นการเฉพาะ โดยมีอาคารสำนักงานงานที่เหมาะสม มีห้องปฏิบัติการการตรวจพิสูจน์พยานหลักฐาน อุปกรณ์ทันสมัยมีประสิทธิภาพ และมีอัตราเงินเดือนเจ้าหน้าที่ที่เหมาะสม การบริหารจัดการมีความยืดหยุ่นคล่องตัว

8. เพิ่มหลักสูตรการเรียนรู้เกี่ยวกับคอมพิวเตอร์ วิทยาศาสตร์ เทคโนโลยีมัยใหม่ในหลักสูตรของโรงเรียนนายร้อยตำรวจ หลักสูตรฝึกอบรมของพนักงานอัยการ ผู้พิพากษา

9. เพิ่มหลักสูตรเกี่ยวกับกฎหมายเบื้องต้นที่เกี่ยวข้องคอมพิวเตอร์ การสืบสวนสอบสวน รวบพยานหลักฐานดิจิตอล ให้กับหลักสูตรที่เกี่ยวข้องกับคอมพิวเตอร์ วิทยาศาสตร์วิศวกรรมคอมพิวเตอร์

บรรณานุกรม

หนังสือ

สำนักงานอัยการสูงสุด. คู่มือพนักงานอัยการสำหรับการสอบสวนและการดำเนินคดีความผิดเกี่ยวกับคอมพิวเตอร์. กรุงเทพฯ : สำนักงานอัยการสูงสุด, 2557.

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. คู่มือและหลักการปฏิบัติเบื้องต้นในการค้นหาพยาน หลักฐานทางอินเตอร์เน็ต. กรุงเทพฯ : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2557.

ฐานข้อมูลอิเล็กทรอนิกส์

ดวงใจ ศุภสารัมภ์. “เรื่องที่ผู้จัดโครงการฝึกอบรมควรรู้”. คู่มือการจัดฝึกอบรม. เข้าถึงได้จาก : http : www.tu.ac.th/org/ofrector/person/train/.../training.html

การพัฒนาบุคลากร. ออนไลน์เข้าถึงได้จาก http : www.hrtothai.com/PerformanceManagement

ความหมายและอาชญากรคอมพิวเตอร์. ออนไลน์เข้าถึงได้จาก https : //www.Gotoknow.org/posts/372559 อาชญากร

คำจำกัดความของคุณธรรมจริยธรรม. ออนไลน์เข้าถึงได้จากhttp:www.islamshia.net/Portal/Cultcure/Thai/.../71243.aspx/คุณธรรม

ความยุติธรรมคมชัดลึก. ออนไลน์เข้าถึงได้จาก http://www.komchadluek.net/detail/20121209/146698/มุมมองเชิงพุทธยุติธรรมแท้เทียม.html

ความหมายของไซเบอร์. กรมวิทยาศาสตร์และเทคโนโลยีกลาโหม. ออนไลน์เข้าถึงได้จาก http : www.dstd.mi.th/board/index.php?topic=887.0

คอมพิวเตอร์. ออนไลน์เข้าถึงได้จาก http://www.vcharkarn.com/vblog/59764

หนังสือคอมพิวเตอร์ เพื่องานอาชีพ 2001-0001 สำนักพิมพ์สกายบุ๊กส์ จำกัด อาชญากรรม. ออนไลน์เข้าถึงได้จาก www.l3nr.org › หน้าแรก › น.ส. ขวัญชนก สร้อยอุดม

ประวัติย่อผู้วิจัย

ชื่อ	นาง จตุพร แสงหิรัญ
วัน เดือน ปีเกิด	16 ส.ค.2505
การศึกษา	ปริญญาตรีนิติศาสตรบัณฑิต มหาวิทยาลัยธรรมศาสตร์ เนติบัณฑิต สำนักอบรมศึกษาภาคกฎหมายแห่งเนติบัณฑิตยสภา ปริญญาโทคณะวิทยาศาสตร์ สาขาจัดการความรู้ มหาวิทยาลัยเชียงใหม่
ประวัติการทำงาน โดยย่อ	รับราชการเป็นพนักงานอัยการในปี 2532 ในด้านคดีอาญา, คดีแพ่ง, คดีเยาวชน และครอบครัว โดยรับราชการในกรุงเทพฯ และ ต่างจังหวัด
ตำแหน่งปัจจุบัน	อัยการผู้เชี่ยวชาญพิเศษ สถาบันพัฒนาข้าราชการฝ่ายอัยการ สำนักงานอัยการสูงสุด

สรุปย่อ

ลักษณะวิชา การเมือง

เรื่อง การพัฒนาผู้บังคับใช้กฎหมายในการต่อสู้อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์

ผู้วิจัย นางจตุพร แสงหิรัญ หลักสูตร วปอ. รุ่น 57

ตำแหน่ง อัยการผู้เชี่ยวชาญพิเศษ

ความเป็นมาและความสำคัญของปัญหา

คอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพมากในการทำงาน มีการพัฒนาระบบการทำงานโปรแกรมรูปแบบใหม่ๆ และทันสมัยขึ้นตลอดเวลา เพื่ออำนวยความสะดวกให้แก่ผู้ใช้ ปัจจุบันคอมพิวเตอร์เป็นสิ่งที่มีความสำคัญและเป็นสิ่งจำเป็นในการใช้ชีวิตประจำวันของคนทั่วไป คนทั่วโลกใช้คอมพิวเตอร์ในติดต่อสื่อสารกันได้โดยง่ายและรวดเร็ว ใช้ในการทำธุรกิจการค้าหลากหลายรูปแบบ ซึ่งปริมาณการใช้คอมพิวเตอร์สูงขึ้นทุกปี โดยคอมพิวเตอร์ในปัจจุบันมีทั้งแบบตั้งโต๊ะ แบบพกพาเคลื่อน ที่ได้ รวมทั้งโทรศัพท์แบบพกพาที่มีการพัฒนาเทคโนโลยีจนสามารถทำงานได้เช่นเดียวกับคอมพิวเตอร์

เมื่อคอมพิวเตอร์เป็นเครื่องมือที่มีประสิทธิภาพมากในการใช้งาน จึงเป็นช่องทางให้ผู้ที่ประสงค์ร้ายใช้คอมพิวเตอร์เข้ามามีส่วนเกี่ยวข้องในการกระทำความผิด

คอมพิวเตอร์มีบทบาทหรือเกี่ยวข้องในการกระทำความผิด ดังนี้คือ

1. คอมพิวเตอร์เป็นวัตถุหรือเป้าหมายที่ถูกกระทำ (Computer as Targets) เช่นการกระทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์ โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือ มีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน

2. การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดในฐานความผิดอื่นๆ (Computer as Tools)

3. การใช้คอมพิวเตอร์เก็บข้อมูลต่างๆที่เกี่ยวข้องกับการกระทำความผิดอีกด้วย (Computer as Storage)

ด้วยระบบการทำงานของคอมพิวเตอร์และโครงข่ายการสื่อสารทางอินเตอร์เน็ตที่รวดเร็วและทันสมัยทำให้การติดต่อสื่อสารทำได้ง่าย รวดเร็ว ไร้พรมแดน คนร้ายกับผู้เสียหายอาจอยู่ห่างกันคนละซีกโลกแต่ก็ถูกหลอกลวง ถูกฉ้อโกงได้ มีลักษณะของการกระทำที่สลับซับซ้อน สามารถสร้างความเสียหายได้อย่างมากและรวดเร็ว เกิดขึ้นที่ไหนเมื่อไหร่ก็ได้ ทั้งในและนอกราชอาณาจักร กฎหมายที่มีอยู่ในปัจจุบันอาจไม่คลอบคลุมถึงรูปแบบการทำกระผิดใหม่ที่เกิดขึ้นจากการพัฒนาทางเทคโนโลยี ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อชื่อเสียง ทรัพย์สินของผู้อื่นและความมั่นคงต่อประเทศชาติ

เมื่อเกิดเหตุขึ้นแล้วยากต่อการติดตามผู้กระทำความผิดมาลงโทษได้โดยง่าย เนื่องจากไม่เห็นตัวผู้กระทำผิด ต้องใช้เวลาในการสืบสวนสอบสวนกว่าจะได้ทราบว่าคนร้ายเป็น ใครอยู่ที่ใดและมีขั้นตอนการทำงานที่สลับซับซ้อน ต้องใช้เจ้าหน้าที่ที่มีความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์มาช่วยในการติดตามคนร้าย ตรวจพิสูจน์การทำงานและหาข้อมูลพยานหลักฐานที่สำคัญในคดีที่อยู่ในคอมพิวเตอร์

ในปัจจุบันมีรูปแบบอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ หลากหลายรูปแบบที่ทำให้ผู้เสียหายต้องสูญเสียทรัพย์สิน เสื่อมเสียชื่อเสียง ได้รับความอับอาย บางรายถึงกับเสียชีวิตเช่น

1. ในเรื่องการฉ้อโกง/การหลอกลวงในรูปแบบต่างๆ
2. การส่งจดหมายอิเล็กทรอนิกส์ (e - mail) หลอกลวง
3. หมิ่นประมาท เผยแพร่ด้วยภาพหรือข้อความให้ผู้อื่นอับอายอับอาย
4. เจาะระบบคอมพิวเตอร์ผู้อื่น เข้าไปแก้ไขข้อมูล เปลี่ยนแปลงข้อมูลทางการเงินเพื่อให้ได้ทรัพย์สินแก้ไขบัญชีธนาคารเพื่อให้โอนเงินเข้าบัญชีคนร้าย
5. การขโมยข้อมูลส่วนบุคคล นำไปใช้ประโยชน์ต่างๆทำธุรกรรมทางการเงิน/แอบอ้างเป็นตัวเรา
6. การทำปลอมหน้า website ผู้อื่น
7. การพนันออนไลน์

ทุกวันนี้หากใช้คอมพิวเตอร์คลิกเข้าสู่อินเตอร์เน็ต ต้องระมัดระวังในการใช้งาน เพราะในโลกอินเตอร์เน็ตอันกว้างใหญ่ มีภัยอันตรายอย่างมัลแวร์แฝงอยู่ ซึ่งมัลแวร์มีหลายประเภท แต่มีมัลแวร์ชนิดหนึ่งที่จะมาจับเครื่องคอม และไฟล์ของเราเป็นตัวประกัน เรียกเงินค่าไถ่ จนทำให้คนทั่วโลกและไทยตื่นตัวมาก มีหนังสือราชการ ประกาศออกเตือนผู้ใช้คอม เพิ่มความระมัดระวังเป็นพิเศษ มัลแวร์ที่กำลังระบาดตอนนี้คือ Ransomware

Ransomware เป็นมัลแวร์ที่ออกแบบมาเพื่อเรียกค่าไถ่เหยื่อโดยเฉพาะโดยส่วนใหญ่เกิดจากการคลิก link อันตราย หรือไปดาวน์โหลดไฟล์ ที่แนบในอีเมล์ เพื่อเปิดเอกสาร แต่กลายเป็น

พวกมัลแวร์อันตรายโดยเมื่อคลิกลิงค์ หรือรันไฟล์มัลแวร์ที่แนบมากับอีเมล์ มัลแวร์ ransomware นี้จะสแกนไฟล์ต่างๆทั้งไฟล์ เอกสารทั่วไป , ไฟล์ภาพ , ไฟล์วีดีโอ ซึ่งเป็นไฟล์ที่เราคุ้นเคยและใช้อยู่ในชีวิตประจำวันแล้วมัลแวร์จะนำไฟล์ในคอมเราทั้งหมดนี้ไปทำการเข้ารหัส แล้วเปิดหน้าต่างเป็นข้อความขึ้นมาบนเครื่องเพื่อเรียกค่าไถ่ โดยมีข้อความปรากฏว่ากรุณาจ่ายเงินตามจำนวนเงิน ภายในระยะเวลาที่กำหนด ถ้ายอมจ่ายจะได้ตัวถอดรหัสไฟล์เพื่อมาถอดรหัสที่คนร้ายทำการเข้ารหัสไว้ ให้เหยื่อสามารถเปิดไฟล์กลับมาใช้ได้ตามเดิม หากไม่จ่ายภายในกำหนดระยะเวลาแล้ว ค่าไถ่จะขึ้นราคาแพงขึ้นอีกเท่าตัวแต่ถึงแม้จะจ่ายเงินแล้วก็ไม่แน่ว่าจะได้เอกสารข้อมูลต่างๆของเราคืนทั้งหมดหรือไม่

และนอกจากนั้นในอนาคตอันใกล้โลกจะเข้าสู่ยุค Internet of Things = IOT หรือ“อินเตอร์เน็ตในทุกสิ่ง” หมายถึงการที่สิ่งต่างๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเตอร์เน็ตทำให้มนุษย์สามารถสั่งการ ควบคุมใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเตอร์เน็ตเช่น การสั่งเปิด-ปิดอุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือเครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตรเครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือนเครื่องใช้ในชีวิตประจำวันต่างๆ ผ่านเครือข่ายอินเตอร์เน็ต เป็นต้น หากวันนั้นมาถึงอย่างเต็มรูปแบบจะเป็นทั้งประโยชน์อย่างมหาศาลและความเสี่ยงไปพร้อมๆ กัน เพราะหากระบบรักษาความปลอดภัยของอุปกรณ์และเครือข่ายอินเตอร์เน็ตไม่ดีพอ จะทำให้ผู้ไม่ประสงค์ดีเข้ามากระทำการที่ไม่พึงประสงค์ต่ออุปกรณ์ข้อมูลสารสนเทศหรือความเป็นส่วนตัวของบุคคลได้

ดังนั้นผู้บังคับใช้กฎหมายที่เกี่ยวข้อง เช่น ตำรวจ อัยการ เจ้าหน้าที่ผู้ตรวจพิสูจน์พยานหลักฐาน เป็นต้น จึงจำเป็นต้องได้รับการพัฒนาองค์ความรู้และทักษะในส่วนที่เกี่ยวข้องกับกฎหมาย ความรู้ในด้านการสืบสวนสอบสวน การตรวจค้นจับกุม การตรวจยึดของกลาง การได้มาซึ่งพยานหลักฐานที่ชอบด้วยกฎหมายในคดีที่มีคอมพิวเตอร์มาเกี่ยวข้อง และรู้ระบบขั้นตอนการทำงานของคอมพิวเตอร์และโครงข่ายการติดต่อสื่อสารทางอินเตอร์เน็ตและการใช้สื่อสังคมออนไลน์ในรูปแบบต่างๆ ที่มีอยู่ในปัจจุบัน ผู้บังคับใช้กฎหมายต้องทำงานร่วมกันอย่างรวดเร็วใกล้ชิด เพื่อยับยั้งการกระทำผิดและจับกุมผู้กระทำผิดมาลงโทษ แต่ปัจจุบันเจ้าหน้าที่ผู้บังคับใช้กฎหมายที่มีความรู้ความเชี่ยวชาญในอาชญากรรมด้านนี้มีจำนวนน้อย ไม่เพียงพอกับปริมาณคดีที่เพิ่มมากขึ้นในปัจจุบัน ทำให้การดำเนินคดีเป็นไปด้วยความล่าช้า ขาดประสิทธิภาพ การรวบรวมพยานหลักฐานต่างๆ เป็นไปได้ยาก รวมทั้งการติดตามพยานหลักฐานที่อยู่ต่างประเทศซึ่งใช้ระยะเวลานานมาก เจ้าหน้าที่ผู้ตรวจพิสูจน์หลักฐานเกี่ยวกับอาชญากรรมคอมพิวเตอร์มีน้อย ทำให้ต้องรอผลการตรวจพิสูจน์ รอข้อมูลจากผู้ให้บริการอินเตอร์เน็ต ทำให้พยานหลักฐานในสำนวนยังไม่รัดกุมเพียงพอที่จะชี้ชัดไปว่าผู้ใดกระทำผิดทำที่ไหน ด้วยวิธีใด กระบวนการยุติธรรมเป็นไปอย่างล่าช้า

ประชาชนผู้เสียหายไม่ได้รับการชดใช้เยียวยา ไม่เชื่อมั่นว่าเจ้าหน้าที่รัฐจะสามารถจับกุมลงโทษผู้กระทำผิดได้ ขาดความเชื่อมั่นศรัทธาในกระบวนการยุติธรรม จึงยอมสูญเสียทรัพย์สิน ชื่อเสียง ไม่ไปร้องทุกข์กับเจ้าหน้าที่

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาขั้นตอนการดำเนินการของเจ้าหน้าที่ผู้บังคับใช้กฎหมายในองค์กรต่างๆ ที่เกี่ยวข้อง และวิเคราะห์ปัญหาและอุปสรรคที่เกิดขึ้นในการทำงาน รวมทั้งปัญหาด้านบุคลากร งบประมาณ การบริหารจัดการคดีและองค์กร

2. เสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคต่างๆ เพื่อการพัฒนาบุคลากรผู้บังคับใช้กฎหมายในองค์กรต่างๆที่เกี่ยวข้อง ให้มีความรู้ ความเชี่ยวชาญ และมีจำนวนเพียงพอที่จะสามารถในการดำเนินคดีกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ

ขอบเขตการวิจัย

1. งานวิจัยนี้เริ่มทำในห้วงเวลาตั้งแต่เดือนพฤศจิกายน 2557 ถึงเดือนพฤษภาคม 2558

2. เน้นการวิจัยเฉพาะขั้นตอนการดำเนินคดีกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ รวมทั้งปัญหาและอุปสรรคในการทำงาน การบริหารจัดการคดี บุคลากรในองค์กรดังนี้ สำนักงานตำรวจแห่งชาติ , สำนักงานอัยการสูงสุด , กรมสอบสวนคดีพิเศษ , สถาบันนิติวิทยาศาสตร์ , กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

3. เน้นหาแนวทาง วิธีการ การพัฒนาบุคลากรผู้บังคับใช้กฎหมายที่เกี่ยวข้องในแต่ละองค์กร

ผลการศึกษา

จากศึกษาข้อมูลสถิติภัยคุกคามของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พบว่ามีภัยคุกคามเพิ่มมากขึ้นทุกปี

สถิติภัยคุกคามปี 2554

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content							12	8	6	7	39	5	77
Availability							1	2	2	0	1	0	6
Fraud							44	38	56	69	66	36	309
Information gathering							28	13	18	14	12	8	93
Information security							0	0	0	0	0	0	0
Intrusion Attempts							9	20	19	19	16	11	94
Intrusion							0	0	0	0	0	0	0
Malicious code							6	10	14	7	18	8	63
Other							0	0	0	1	0	3	4
รวม							100	91	115	117	152	71	646

สถิติภัยคุกคามปี 2555

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	1	0	0	0	1	0	0	0	0	3
Availability	0	1	0	0	0	0	0	0	1	0	0	0	2
Fraud	16	37	32	42	32	32	51	54	74	49	48	67	534
Information gathering	4	5	10	8	8	5	5	10	5	0	1	1	62
Information security	0	1	0	0	0	0	0	0	0	0	1	0	2
Intrusion Attempts	3	3	13	8	8	6	7	10	8	2	2	5	75
Intrusion	1	1	1	1	0	3	1	0	0	0	1	4	13
Malicious code	3	6	9	12	7	4	7	3	8	8	10	5	82
Other	4	5	3	2	1	2	2	0	0	0	0	0	19
รวม	31	59	69	74	56	52	73	78	96	59	63	82	792

สถิติภัยคุกคามปี 2556

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	2	3	1	1	2	0	0	0	1	2	0	13
Availability	1	0	0	0	0	0	0	8	0	1	0	0	10
Fraud	36	48	49	56	78	56	110	53	53	54	59	42	694
Information gathering	3	0	0	0	0	2	0	0	0	3	0	0	8
Information security	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion Attempts	56	23	17	23	16	11	24	16	24	46	24	36	316
Intrusion	6	3	50	61	115	94	67	63	89	46	27	10	631
Malicious code	1	4	6	4	3	11	9	7	5	6	5	12	73
Other	0	0	0	0	0	0	0	0	0	0	0	0	0
รวม	104	80	125	145	213	176	210	147	171	157	117	100	1745

สถิติภัยคุกคามปี 2557

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	1	1	0	0	0	0	3	1	1	1	0	0	8
Availability	0	0	2	2	0	0	1	3	0	0	0	0	8
Fraud	59	68	69	72	145	85	94	66	98	88	101	65	1010
Information gathering	1	2	6	8	7	0	1	1	3	0	0	0	29
Information security	0	1	0	0	0	2	0	0	1	0	0	0	4
Intrusion Attempts	39	28	32	51	43	30	42	40	30	46	48	74	503
Intrusion	9	150	77	33	55	50	69	47	86	32	35	68	711
Malicious code	3	7	129	125	102	226	304	161	263	98	132	185	1735
Other	0	0	0	0	0	0	0	0	0	0	0	0	0
รวม	112	257	315	291	352	393	514	319	482	265	316	392	4008

สถิติภัยคุกคามปี 2558

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	2	0	0	0	0								2
Availability	0	0	0	0	0								0
Fraud	75	83	100	90	155								503
Information gathering	0	0	0	0	0								0
Information security	0	0	1	0	0								1
Intrusion Attempts	83	89	65	27	60								324
Intrusion	69	76	88	12	78								323
Malicious code	104	83	174	143	140								644
Other	0	0	0	0	0								0
รวม	333	331	428	272	433								1797

โดยจะพบว่าในเรื่องของการฉ้อโกง (Fraud) มีปริมาณมากขึ้นทุกปี ชี้ให้เห็นถึงจำนวนงานที่ผู้บังคับใช้กฎหมายจะต้องสืบสวนสอบสวนหาตัวผู้กระทำผิดมาลงโทษตามกฎหมายแต่บุคลากรในงานนี้ไม่มีเพิ่มมากขึ้นเท่าจำนวนคดี มองให้เห็นปัญหาที่เกิดขึ้นในปัจจุบันและในอนาคต หากไม่มีการเพิ่มและพัฒนาผู้บังคับใช้กฎหมายให้มีศักยภาพในการดำเนินคดี

จากการศึกษาพบเห็นปัญหาในชั้นพนักงานสอบสวนและผู้ตรวจพิสูจน์พยานหลักฐาน คือ

1. จำนวนเจ้าหน้าที่สืบสวน พนักงานสอบสวน ที่มีความรู้ความเชี่ยวชาญในอาชญากรรมประเภทนี้ยังมีน้อยมากสำหรับประเทศไทย ผู้มีความรู้ความชำนาญส่วนมากจะอยู่ในกรุงเทพมหานคร ในต่างจังหวัดเมื่อเกิดเหตุขึ้น การดำเนินคดีจะมีปัญหามากมาย พนักงานสอบสวนไม่รู้ว่าจะเริ่มต้นสอบสวนอย่างไร การเก็บ การตรวจยึดพยานหลักฐานทำไม่ถูกต้องตามมาตรฐาน การรวบรวมพยานหลักฐานที่สำคัญในสำนวนคดี การขอข้อมูลจากผู้ให้บริการ การส่งวัตถุพยานไปตรวจพิสูจน์ บางครั้งไม่ทราบว่าต้องการข้อมูลอะไรอยู่ตรงไหน เนื่องจากข้อมูลในเครื่องคอมพิวเตอร์มีจำนวนมาก จึงต้องเอาเฉพาะส่วนที่เกี่ยวข้องกับคดีเท่านั้น

2. จำนวนผู้เชี่ยวชาญในการตรวจพิสูจน์พยานหลักฐานดิจิตอล มีไม่เพียงพอ ผู้เชี่ยวชาญกลุ่มงานตรวจพิสูจน์อาชญากรรมคอมพิวเตอร์ กองพิสูจน์หลักฐานกลาง สำนักงานตำรวจแห่งชาติมีประมาณ 4 คน,ของสถาบันนิติวิทยาศาสตร์ มี 3 คน และจากกลุ่มงานวิเคราะห์และพิสูจน์หลักฐานการกระทำผิดทางเทคโนโลยี กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีจำนวน 2 คน เท่านั้น

นอกจากนั้นก็อาจขอช่วยเหลือจากอาจารย์ที่มีความเชี่ยวชาญจากทางมหาวิทยาลัย เพื่อให้ช่วยตรวจพิสูจน์หาข้อมูล พยานหลักฐานจากคอมพิวเตอร์ smartphone อุปกรณ์ต่างๆที่สามารถเก็บข้อมูล

นอกจากนั้น ยังมีปัญหาในเรื่องมาตรฐานของผู้เชี่ยวชาญว่าต้องมีคุณสมบัติอย่างไรบ้าง ถึงจะเป็นที่ยอมรับของศาล เนื่องจากเท่าที่ศึกษาวิจัยมาความรู้และประสบการณ์ของผู้ตรวจพิสูจน์ในการทำงานไม่เท่ากัน รวมทั้งการฝึกอบรม รวมทั้งเรื่องมาตรฐานในการตรวจพิสูจน์หลักฐานว่าได้มาตรฐานสากลหรือไม่อย่างไรในขั้นตอนการดำเนินงานในการตรวจพิสูจน์ การรายงานผลการตรวจพิสูจน์ และเรื่องสำคัญอีกเรื่องหนึ่งคือ Chain of custody นอกจากนั้นพบว่าห้องปฏิบัติการคับแคบไม่มีที่เก็บวัตถุพยานที่เหมาะสมได้มาตรฐานอาจทำให้ผู้อื่นสามารถเข้าถึงวัตถุพยานไปทำลายหรือเพิ่มเติมข้อมูลได้ ทำให้ขาดความน่าเชื่อถือ

ปัญหาในการดำเนินคดีชั้นพนักงานอัยการ

1. พยานหลักฐานยังไม่สมบูรณ์ครบถ้วน คือเมื่อมีการร้องทุกข์กล่าวโทษ พนักงานสอบสวนก็จะสอบปากคำผู้เสียหาย แล้วไปดำเนินการขอศาลออกหมายจับผู้ต้องหาโดยไม่ได้มีการสอบสวนเชิงลึกก่อน ประเด็นที่เกิดปัญหาในปัจจุบันคือ เมื่อพนักงานสอบสวนได้หมายจับจึงรีบเร่งไปทำการจับกุมตัวผู้ต้องหาทั้งที่พยานหลักฐานทางดิจิตอล หรือพยานหลักฐานทางเอกสารยังไม่ได้รวบรวม แต่จะต้องรีบพิจารณาเพราะจะครบกำหนดระยะเวลาฝากขัง

2. ด้านการขอความร่วมมือในการสอบสวนในคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ ในคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ ที่ใช้ระบบเครือข่ายอินเทอร์เน็ต เป็นเครื่องมือในการกระทำความผิด การสอบสวนรวบรวมพยานหลักฐาน เพื่อระบุตัวผู้กระทำความผิด จะต้องใช้ข้อมูลหรือพยานหลักฐานจากผู้ให้บริการต่างๆ ในระบบอินเทอร์เน็ต และคดีเป็นจำนวนมากที่คนร้ายอาศัยเครือข่ายที่อยู่ประเทศหนึ่งในการลงมือกระทำความผิดต่อบุคคล ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่อยู่อีกประเทศหนึ่ง การสอบสวนรวบรวมพยานหลักฐานจึงต้องอาศัยความร่วมมือระหว่างประเทศในเรื่องทางอาญา ซึ่งจะต้องกระทำอย่างเร่งด่วน เพื่อให้ทันกับการนำข้อมูลดังกล่าวไปใช้สืบหาตัวผู้กระทำผิดต่อไป แต่ในทางปฏิบัติแล้วการดำเนินการตามกฎหมายและสนธิสัญญาว่าด้วยความร่วมมือระหว่างประเทศในเรื่องทางอาญา มักไม่ได้รับความร่วมมือจากประเทศต่างๆ หรือการสอบสวนที่ขอความร่วมมือจากต่างประเทศ มักเกิดความล่าช้า และไม่มีสภาพบังคับ หรือแนวทางแก้ไขเพิ่มเติม ทำให้เป็นอุปสรรคต่อการสอบสวนคดี โดยเฉพาะอย่างยิ่ง

3. การนำตัวผู้กระทำความผิดที่เป็นตัวการที่แท้จริงมาลงโทษปัญหานี้เกิดขึ้นในกรณีของการกระทำความผิดผ่าน Social Media กระทำความผิดในลักษณะดังกล่าว เมื่อพิจารณาจากสำนวนการสอบสวนแล้วจะพบว่าผู้ต้องหาที่ถูกกล่าวหาว่ากระทำความผิดและถูกดำเนินคดีโดยส่วนใหญ่นั้น อาจจะไม่ใช่ตัวการในการกระทำความผิดที่แท้จริง โดยส่วนใหญ่ผู้ต้องหาที่ถูก

ดำเนินคดีจะเป็นเจ้าของบัญชีธนาคารที่มีการรับโอนเงินที่ผู้เสียหายถูกหลอกมา โดยผู้ต้องหาเหล่านี้อาจกระทำการโดยรู้เท่าไม่ถึงการณ์ โดยการรับจ้างเปิดบัญชี หรือเปิดบัญชีให้กับคนร้าย

4. สำนักงานอัยการสูงสุดยังขาดพนักงานอัยการที่มีความเชี่ยวชาญในอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ อีกจำนวนมาก ทั้งในด้านการสืบสวนสอบสวนในกรณีที่เป็นความผิดที่มีโทษตามกฎหมายไทยได้กระทำลงนอกราชอาณาจักรไทย และความเชี่ยวชาญในการพิจารณาสั่งสำนวนและการดำเนินคดีในชั้นศาล

5. สำนักงานการสอบสวน สำนักงานอัยการสูงสุด ยังขาดรับงบประมาณที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ โดยเฉพาะคดีที่ตั้งต้นที่พนักงานอัยการ รวมทั้งงบประมาณในการบริหารจัดการ การประสานงานกับหน่วยงานอื่นยังขาดแคลนอุปกรณ์ เครื่องมือในการทำงานตลอดจนเทคโนโลยีสมัยใหม่ที่เพียงพอต่อการปฏิบัติหน้าที่อย่างประสิทธิภาพ

6. การติดต่อประสานงานระหว่างหน่วยงานราชการ และภาคเอกชน ที่ครอบครองพยานหลักฐานยังมีขั้นตอนยุ่งยากล่าช้า , การประสานงานขอความร่วมมือทางอาญาระหว่างประเทศมีขั้นตอนที่เป็นทางการ หลายขั้นตอนในแต่ละหน่วยงาน ขาดความสะดวกรวดเร็วและมีประสิทธิภาพ

สาเหตุที่อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์มีปริมาณเพิ่มมากขึ้น

1. ยุคปัจจุบันเป็นยุคของการสื่อสารอุปกรณ์ในการติดต่อสื่อสาร คอมพิวเตอร์ Smartphone มีให้เลือก หลากหลายราคาไม่แพงปริมาณผู้ใช้ทวีจำนวนมากขึ้น

2. มีความสะดวก รวดเร็ว และเสียค่าใช้จ่ายน้อย มีการเชื่อมต่อระบบอินเตอร์เน็ทสามารถสื่อสารทางโปรแกรมสนทนาต่างๆ ทาง Line , facebook การส่งข้อความ ภาพถ่าย การทำธุรกรรมการเงิน ซื้อขายสินค้าออนไลน์

3. ผู้ใช้ไม่ระมัดระวังป้องกันตัว ประมาทเลินเล่อ ไม่พิจารณาข้อมูลข่าวสารให้รอบคอบหลงเชื่อง่ายก็จะตกเป็นเหยื่อทำให้ถูกหลอกสูญเสียทรัพย์สิน หรือถูกหลอกไปข่มขืนกระทำชำเรา เป็นต้น นอกจากนั้นหากผู้ใช้ไม่มีจิตสำนึกในการลงหรือส่งต่อข้อความ ส่งต่อภาพและข้อความที่ไม่เหมาะสมก็อาจจะเป็นความผิดตามกฎหมายได้

ปัญหาในเรื่องของการขาดบุคลากรที่เชี่ยวชาญในด้านคอมพิวเตอร์ เนื่องจากเป็นการยากที่จะนำผู้บังคับใช้กฎหมายส่วนมากที่มีอยู่ในปัจจุบันมาฝึกฝนให้เชี่ยวชาญด้านคอมพิวเตอร์ เนื่องจากไม่มีความคุ้นเคยกับการใช้คอมพิวเตอร์มาก่อนและมีความสามารถเพียงใช้งานได้ในขั้นพื้นฐานเท่านั้น แต่ในการแกะรอย ติดตามหาผู้กระทำความผิด การดึงข้อมูลพยานหลักฐานที่สำคัญต่างๆ ยังไม่สามารถทำได้ ต้องใช้ผู้ที่มีความรู้ความชำนาญโดยเฉพาะที่ได้ศึกษามาโดยตรง

แต่ปัญหาที่ตามมา เนื่องจากในยุคปัจจุบันเด็กที่จบการศึกษาอยู่ในช่วง Generation Y คือกลุ่มคนที่เกิดระหว่างปี พ.ศ.2523-2543 เป็นกลุ่มคนที่โตมาพร้อมกับคอมพิวเตอร์-อินเตอร์เน็ต และเทคโนโลยีไอทีพวกนี้เป็นวัยที่จัดว่าเพิ่งเริ่มเข้าสู่วัยทำงาน มีลักษณะนิสัยชอบแสดงออกมีความเป็นตัวของตัวเองสูง ไม่ชอบอยู่ในกรอบและไม่ชอบเงื่อนไขคนกลุ่มนี้ต้องการความชัดเจนในการทำงานว่าสิ่งที่ทำมีผลต่อตนเองและต่อหน่วยงานอย่างไรอีกทั้งยังมีความสามารถในการทำงานที่เกี่ยวกับการติดต่อสื่อสารและยังสามารถทำงานหลายๆอย่างได้ในเวลาเดียวกันซึ่งจะมีทัศนคติ แนวคิด และอุปนิสัยไปในทิศทางที่แตกต่างจากคนในยุคก่อนหน้าการดำเนินชีวิตที่ไม่จำเป็นที่จะต้องอยู่กับที่เสมอไป

ภาคเอกชนเองก็จะไปเสนองานให้นักศึกษาที่จบใหม่ทำและให้เงินเดือนสูงกว่าอัตราปริญญาตรีของทางราชการ และมีสวัสดิการ รางวัล มีความเจริญก้าวหน้าที่ชัดเจน ทำให้เด็กตัดสินใจไปทำงานภาคเอกชนจำนวนมาก เหลือมาสนใจรับราชการจำนวนน้อย ประกอบกับการเข้ารับราชการมีระเบียบ มีขั้นตอนและการแข่งขันสูง และแต่ละปีรับจำนวนน้อย จึงเป็นส่วนหนึ่งของปัญหาในการขาดบุคลากร

แนวทางในการพัฒนาผู้บังคับใช้กฎหมาย

1. รัฐต้องหาแนวทางจูงใจให้ผู้ที่จบการศึกษาด้านคอมพิวเตอร์เข้ามารับราชการในส่วนที่เกี่ยวข้องกับกระบวนการยุติธรรม โดยเปิดรับจำนวนมากและให้อัตราเงินเดือนใกล้เคียงกับภาคเอกชน

2. จัดฝึกอบรมให้ความรู้เกี่ยวกับคอมพิวเตอร์และเทคโนโลยีสมัยใหม่ในส่วนที่เกี่ยวข้องกับการทำคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ให้กับผู้บังคับใช้กฎหมายอย่างเร่งด่วนและจำนวนมาก รวมทั้งต้องฝึกอบรมอย่างต่อเนื่อง เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา

3. สร้างผู้เชี่ยวชาญในการตรวจพิสูจน์พยานหลักฐานทางคอมพิวเตอร์ให้มีจำนวนมากขึ้น

4. การจัดฝึกอบรมร่วมกันระหว่างหน่วยงานภาครัฐที่เกี่ยวข้องทั้งหมด เพื่อให้เกิดประสิทธิภาพในการทำงานร่วมกัน การแบ่งปันข้อมูล รวมทั้งการสร้างความสัมพันธ์ที่ดี

5. จัดประชุมสัมมนาร่วมกับภาคเอกชน นักวิชาการ ผู้ให้บริการ หน่วยงานความมั่นคงอื่นๆ เพื่อแลกเปลี่ยนข้อมูลข่าวสารและข้อเสนอแนะในการทำงาน เรียนรู้วิทยาการใหม่ๆ

6. การให้โอกาสผู้ปฏิบัติงานไปศึกษาดูงาน ฝึกอบรม ประชุมในต่างประเทศ เพื่อให้รู้เท่าทันกับต่างประเทศในด้านเทคนิค วิทยาการต่างๆ รวมทั้งได้รู้จักกับเจ้าหน้าที่ในประเทศต่างๆ เพื่อประโยชน์ในการติดต่อสื่อสารในการทำงานในอนาคต

7. ให้อัตราเงินเดือนที่สูงกว่าสร้างขวัญและกำลังใจให้กับผู้ปฏิบัติงาน พร้อมทั้งกำหนดเส้นทางความก้าวหน้าในอาชีพชัดเจน

8. อบรมเรื่องคุณธรรมจริยธรรม ทำงานด้วยความซื่อสัตย์ สุจริต ไม่ทุจริตคอรัปชั่น ปฏิบัติหน้าที่ด้วยความโปร่งใส ตรวจสอบได้ และอำนวยความยุติธรรมแก่ทุกฝ่ายอย่างเสมอภาคกัน

ข้อเสนอแนะ

1. การให้ความรู้ต่อสังคมให้ตระหนักเรื่องพิษภัยของอาชญากรรมที่เกิดจากอินเตอร์เน็ตและต้องสอนเด็กในโรงเรียนเรียน ให้เรียนรู้ระบบของคอมพิวเตอร์ การทำงาน การใช้อินเตอร์เน็ต รวมทั้งมารยาทการใช้อย่างเหมาะสมและโดยชอบด้วยกฎหมาย

1.1 ควรมีการประชาสัมพันธ์เชิงรุกให้มากกว่านี้ เผยแพร่ข่าวสารด้านความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายคอมพิวเตอร์ เพื่อสร้างความรู้และความเข้าใจให้กับประชาชนให้มากกว่าที่เป็นอยู่นี้เผยแพร่วิธีการกระทำความผิดในรูปแบบใหม่ๆ และมีช่องทางให้ประชาชนสามารถติดต่อแจ้งเหตุ ให้ข้อมูล ขอคำแนะนำได้อย่างสะดวก หลากหลายช่องทาง

1.2 การซื้อขาย การทำธุรกรรมทางการเงิน ออนไลน์ ต้องให้ข้อมูลแก่ประชาชนเกี่ยวกับบริษัทที่จดทะเบียนของผู้ซื้อและผู้ขาย รายละเอียดของสินค้า และข้อมูลสำคัญที่เกี่ยวข้องกับการทำธุรกรรมสามารถตรวจสอบติดตามหลังเกิดเหตุได้

1.3 ควบคุม ตรวจสอบ เฝ้าระวังการเผยแพร่เว็บไซด์ที่หมิ่นสถาบันพระมหากษัตริย์ เว็บไซต์ที่ขายของผิดกฎหมายลามกอนาจารหรือเว็บไซด์ที่ไม่เหมาะสมขัดต่อศีลธรรมอันดี

2. การพัฒนาเจ้าหน้าที่ผู้บังคับใช้กฎหมาย

2.1 ควรเร่งรัดพัฒนาผู้บังคับใช้กฎหมายให้มีความรู้ความเชี่ยวชาญในด้านกฎหมายการสืบสวนสอบสวนและทักษะด้านคอมพิวเตอร์และเทคโนโลยีสมัยใหม่ให้มากขึ้น อบรมตำรวจตามสถานีตำรวจทั้งในกรุงเทพและต่างจังหวัดให้มีความรู้และทักษะ จนสามารถทำคดีที่เกี่ยวข้องกับคอมพิวเตอร์ได้ เพื่อลดภาระงานของกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ ปอท.

2.2 จัดฝึกอบรมการสืบสวนสอบสวนร่วมกันระหว่างผู้บังคับใช้กฎหมายที่เกี่ยวข้องทุกหน่วยงาน เพื่อฝึกการทำงานเป็นทีม การทำความรู้จักกัน การแบ่งปันข้อมูลข่าวสารซึ่งกันและกัน การสร้างเครือข่าย การสร้างจิตสำนึกในการทำงานร่วมกัน โดยถือผลสำเร็จของคดีเป็นเป้าหมาย นอกจากนั้นควรจัดประชุมสัมมนากับหน่วยงานภาคเอกชน นักวิชาการ ที่ต้องทำงานเกี่ยวข้องกับผู้บังคับใช้กฎหมายอย่างสม่ำเสมอเพื่อให้ทันต่อสถานการณ์การเปลี่ยนแปลง รูปแบบการกระทำผิด

2.3 สร้างมาตรฐานในการตรวจพิสูจน์พยานหลักฐาน (Forensic) รวมทั้งมาตรฐานของผู้เชี่ยวชาญด้วยว่ามีคุณสมบัติอย่างไรบ้าง

2.4 จัดทำคู่มือในการปฏิบัติงานของแต่ละสำนักงาน และคู่มือหรือแนวทางในการทำงานร่วมกันในคดีสำคัญ

2.5 ให้โอกาสผู้บังคับใช้กฎหมายในระดับผู้ปฏิบัติงานไปศึกษา ดูงาน ฝึกอบรม ประชุมในต่างประเทศ เพื่อให้เรียนรู้ในด้านเทคนิค วิทยาการต่างๆ รวมทั้งได้รู้จักกับเจ้าหน้าที่ในประเทศต่างๆ เพื่อประโยชน์ในการติดต่อสื่อสารสร้างเครือข่ายในการทำงานร่วมกันในอนาคต

2.6 เพิ่มอัตราเงินเดือนให้สูงขึ้น มีรางวัลรวมทั้งแรงจูงใจในการทำงานและรู้เส้นทางความก้าวหน้าในอาชีพชัดเจน

2.7 ให้ความสำคัญกับการดำเนินคดีอาชญากรรมเกี่ยวกับคอมพิวเตอร์ เป็นการเฉพาะอย่างเร่งด่วน เพราะปัจจุบันอาชญากรใช้ช่องทางการสื่อสาร และอุปกรณ์เทคโนโลยีที่ทันสมัย ในการกระทำความผิดเป็นจำนวนมากสร้างความเสียหายแก่ประชาชน และสังคมอย่างมาก

3. การสร้างเครือข่ายการทำงาน

3.1 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ ภายในประเทศที่มีหน้าที่ป้องกัน และปราบปราม รวมถึงการดำเนินคดี เพื่อใช้อำนาจหน้าที่ตามกฎหมายต่างๆ ที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ

3.2 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐ กับภาคเอกชน เพื่อให้เจ้าหน้าที่ของรัฐสามารถเข้าถึงข้อมูลต่างๆ เช่น ข้อมูลการเงิน ข้อมูลการสื่อสารทางโทรศัพท์ หรือเครือข่ายอินเทอร์เน็ต ได้อย่างมีประสิทธิภาพ และรวดเร็วการทำงานร่วมกับ Thai cert รวมทั้ง ETDA

3.3 ควรสร้างเครือข่ายการประสานงานระหว่างหน่วยงานภาครัฐและเอกชนในต่างประเทศ เช่นตำรวจสากลI 24/7การหาแนวทางให้การขอความร่วมมือระหว่างประเทศทางอาญาและการส่งผู้ร้ายข้ามแดนให้รวดเร็วและมีประสิทธิภาพมากขึ้น

4. ควรมีการแก้กฎหมายให้ทันต่อสถานการณ์ในด้านสารบัญญัติ รูปแบบการกระทำผิด กำหนดบทลงโทษให้เหมาะสมกับความเสียหายที่เกิดขึ้นแก้ไขปรับปรุงประมวลกฎหมายวิธีพิจารณาความอาญา เกี่ยวกับการสืบสวนสอบสวน การตรวจ ค้นยึดของกลาง การรับฟังพยานหลักฐาน เป็นต้น เนื่องจากอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์มีลักษณะพิเศษกว่าอาชญากรรมอื่นๆ มีเรื่องเกี่ยวกับการใช้เทคโนโลยีต่างๆมาเกี่ยวข้อง

5. ควรมีศาลที่มีอำนาจพิจารณาคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์โดยเฉพาะ

6. สำนักงานอัยการสูงสุดควรมีสำนักงานคดีอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์โดยเฉพาะ เพื่อสร้างผู้เชี่ยวชาญในคดีดังกล่าว และสามารถบริหารจัดการสารบบและสถิติคดได้ รวมทั้งหน่วยงานที่เกี่ยวข้องสามารถติดต่อประสานงานได้โดยตรง

7. รัฐควรมีหน่วยปฏิบัติการเฉพาะกิจ โดยให้มีเจ้าหน้าที่ผู้บังคับใช้กฎหมายและเจ้าหน้าที่ด้านต่างๆที่เกี่ยวข้อง ผู้ตรวจพิสูจน์ ผู้เชี่ยวชาญด้านคอมพิวเตอร์ มาทำงานร่วมกันทำคดีที่สำคัญๆ เช่นคดีฉ้อโกงประชาชน แชร์ลูกโซ่ องค์กรอาชญากรรมข้ามชาติ เป็นต้น เป็นหน่วยงานที่รวบรวมข้อมูลการดำเนินคดี และศูนย์กลางการติดต่อประสานงานทั้งในและต่างประเทศในคดีความผิดเกี่ยวกับคอมพิวเตอร์เป็นการเฉพาะ โดยมีอาคารสำนักงานงานที่เหมาะสมมีห้องปฏิบัติการการตรวจพิสูจน์พยานหลักฐาน อุปกรณ์ทันสมัยมีประสิทธิภาพ และมีอัตราเงินเดือนเจ้าหน้าที่ที่เหมาะสม การบริหารจัดการมีความยืดหยุ่นคล่องตัว

8. เพิ่มหลักสูตรการเรียนรู้เกี่ยวกับคอมพิวเตอร์ วิทยาศาสตร์ เทคโนโลยีมัยใหม่ในหลักสูตรของโรงเรียนนายร้อยตำรวจหลักสูตรฝึกอบรมของพนักงานอัยการ ผู้พิพากษา

9. เพิ่มหลักสูตรเกี่ยวกับกฎหมายเบื้องต้นที่เกี่ยวข้องคอมพิวเตอร์ การสืบสวนสอบสวน รวบพยานหลักฐานดิจิตอล ให้กับหลักสูตรที่เกี่ยวข้องกับคอมพิวเตอร์ วิทยาศาสตร์วิศวกรรมคอมพิวเตอร์