รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง ปัจจัยความสำเร็จของสิงคโปร์: กรณีศึกษา เพื่อประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย

จัดทำโดย นางสาวกัลยา ชินาธิวร
รหัส 11044

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูต รุ่นที่ 11 ปี 2562
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ

รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง ปัจจัยความสำเร็จของสิงคโปร์: กรณีศึกษา
เพื่อประกอบการพัฒนาแนวทางการดำเนินการตาม
นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย

จัดทำโดย นางสาวกัลยา ชินาธิวร
รหัส 11044

หลักสูตรนักบริหารการทูต รุ่นที่ 11 ปี 2562
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ
รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูตของกระทรวงการต่างประเทศ

ลงชื่อ.....

(เอกอัครราชทูต วิมล คิดชอบ)
อาจารย์ที่ปรึกษา

ลงชื่อ.....

(ศาสตราจารย์ ดร. พลภัทร บุราคม)
อาจารย์ที่ปรึกษา

ลงชื่อ.....

(รองศาสตราจารย์ ดร. รุ่งพงษ์ ชัยนาม)
อาจารย์ที่ปรึกษา

บทสรุปสำหรับผู้บริหาร

ปัจจุบันทุกประเทศกำลังก้าวเข้าสู่ยุคดิจิทัล และผลักดันนโนยายเศรษฐกิจดิจิทัลด้วยการส่งเสริมให้มีการใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัล และนวัตกรรมในทุกภาคส่วน ทั้งภาครัฐ ภาคอุตสาหกรรม ภาคเอกชน และประชาชน ซึ่งเทคโนโลยีดิจิทัลที่มีการใช้งานมากที่สุด คือการใช้อินเทอร์เน็ต จนอาจกล่าวได้ว่า ชีวิตในสังคมสารสนเทศทุกวันนี้เราทุกคนเกี่ยวข้องกับอินเทอร์เน็ตในทางใดทางหนึ่ง แม้จะไม่ใช่ “ผู้ใช้อินเทอร์เน็ต” โดยตรงก็ตาม

ในขณะที่อินเทอร์เน็ตจะนำมาซึ่งโอกาสในการขับเคลื่อนไปสู่เศรษฐกิจดิจิทัล ไม่ว่าจะเป็นการส่งเสริมการเรียนรู้ การศึกษา การสร้างธุรกิจใหม่ๆ การส่งเสริมด้านสุขภาพ และการขนส่งคมนาคม แล้ว อินเทอร์เน็ตก็ถูกใช้เป็นเครื่องมือในการก่อให้เกิดภัยคุกคามไซเบอร์ และการก่ออาชญากรรมไซเบอร์ ซึ่งเป็นภัยคุกคามที่ไร้พรหมแดน และมีผลกระทบในทุกมิติไม่ว่าจะเป็นเศรษฐกิจ สังคม และความมั่นคงของประเทศ สอดคล้องกับรายงานของ World Economic Forum ซึ่งได้จัดอันดับความเสี่ยงระดับโลก ประจำปี ค.ศ. 2019 พบว่า การฉ้อโกงและโจรกรรมข้อมูล (Data fraud and theft) ถูกจัดอยู่ในอันดับที่ 4 และ การโจมตีไซเบอร์ อยู่ในอันดับที่ 5 ของ 10 อันดับความเสี่ยงที่มีผลกระทบกับการดำรงชีวิต

ตามยุทธศาสตร์ชาติ พ.ศ. 2561–2580 ภายใต้ประเด็นยุทธศาสตร์ชาติด้านความมั่นคง ข้อ 4.2 การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง กำหนดให้มีการแก้ไขปัญหาเดิมที่มีอยู่อย่างตรงประเด็นจนหมดไปอย่างรวดเร็ว และป้องกันไม่ให้ปัญหาใหม่เกิดขึ้น ซึ่งรวมถึงปัญหาอาชญากรรมทางไซเบอร์ และการติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่ ซึ่งรวมถึง ภัยคุกคามทางไซเบอร์ นอกจากนี้ ประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน ภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ ได้ระบุถึงการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ ต่อเศรษฐกิจและสังคม และปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมตระหนักถึงการปรับปรุงเปลี่ยนแปลงโครงสร้างพื้นฐานสำคัญๆ ที่กำลังเกิดขึ้นตามนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัลและไทยแลนด์ 4.0 ของรัฐบาล ซึ่งเป็นการเปลี่ยนผ่านประเทศครั้งสำคัญ โดยจะละเลยไม่ได้กับภัยคุกคามไซเบอร์ต่างๆ ที่อาจฉุดรั้งการเปลี่ยนผ่านที่เกิดขึ้น และเมื่อพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 กระทรวงฯ จึงมีภารกิจที่ต้องดำเนินการเพื่อให้เป็นไปตามพระราชบัญญัติดังกล่าว โดยเฉพาะอย่างยิ่ง การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่จะเป็นหน่วยงานหลักในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ต่อไป

การศึกษานี้ดำเนินการวิเคราะห์ปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ช่วงปี 2014–ปัจจุบัน แล้วนำผลการวิเคราะห์มาเปรียบเทียบกับการดำเนินงานของไทย เพื่อหาแนวทางและข้อเสนอแนะในการพัฒนาการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย โดยการศึกษาจะวิเคราะห์ตามกรอบดัชนี

ตัวชี้วัดตามที่สหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยแบ่งเป็น 5 เสาหลัก ได้แก่ (1) ด้านกฎหมาย (2) ด้านเทคนิค (3) ด้านองค์กร (4) ด้านการเสริมสร้างศักยภาพ และ (5) ด้านความร่วมมือ ทั้งนี้ จากการศึกษาพบว่า ปัจจัยหลักที่ทำให้สิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ คือรัฐบาลสิงคโปร์มีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วยการใช้เทคโนโลยีดิจิทัลและนวัตกรรม จึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีการดำเนินการอย่างจริงจัง ต่อเนื่อง และเป็นระบบ และดำเนินงานร่วมมือกับทุกภาคส่วนทั้งในประเทศและระหว่างประเทศ มาตั้งแต่ ปี 2548

ในส่วนของผลการศึกษาเชิงเปรียบเทียบ ผู้เขียนเห็นว่า ประเทศไทยควรให้ความสำคัญอันดับแรกกับการพัฒนาด้านการเสริมสร้างศักยภาพ โดยเฉพาะอย่างยิ่ง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และการพัฒนาบุคลากร ผู้เชี่ยวชาญ นักเทคนิค ซึ่งเป็นปัจจัยสำคัญในการขับเคลื่อนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ และอันดับที่ 2 คือ ด้านเทคนิค โดยการจัดสรรงบประมาณในการส่งเสริมการศึกษาและวิจัย การจัดทำมาตรฐาน และการนำเทคโนโลยีทันสมัยมาใช้

ในส่วนข้อเสนอเชิงนโยบายและมิติด้านการต่างประเทศ นอกจากจะสามารถนำปัจจัยความสำเร็จและวิธีดำเนินนโยบายของสิงคโปร์ โดยเฉพาะประเด็น 5 เสาหลักมาปรับใช้แล้ว กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสามารถนำผลการศึกษานี้ใช้ประกอบการพิจารณาดำเนินการเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเพื่อให้เกิดความร่วมมือในมิติด้านการต่างประเทศอย่างเป็นรูปธรรม เห็นควรเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมขยายความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับกระทรวงสื่อสารและสารสนเทศของสิงคโปร์ ภายใต้บันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแห่งราชอาณาจักรไทยและกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับลงนามเมื่อวันที่ 31 พฤษภาคม 2559 รวมทั้งพิจารณาว่า สามารถใช้ประโยชน์จากบันทึกความเข้าใจด้านเทคโนโลยีสารสนเทศและการสื่อสาร และเทคโนโลยีดิจิทัล ที่มีกับประเทศต่างๆ เพื่อขยายความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ และพิจารณาความเป็นไปได้ในการขยายความร่วมมือทั้งในลักษณะทวิภาคีและพหุภาคีกับประเทศ กลุ่มประเทศ หรือองค์การระหว่างประเทศอื่นๆ ที่เห็นว่าจะเป็นประโยชน์ต่อประเทศไทย โดยอาจทำในลักษณะการดำเนินงานภายใต้ MoU การจัดการประชุมหรือกิจกรรมประจำปีร่วมกับพันธมิตรทั้งในประเทศและต่างประเทศ โดยเฉพาะอย่างยิ่งในกรอบของอาเซียนและเอเปค

กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคลฉบับนี้ สำเร็จลงได้ด้วยความกรุณาของอาจารย์ที่ปรึกษาทั้ง 3 ท่าน ประกอบด้วย ท่านเอกอัครราชทูต วิมล คิดชอบ ศาสตราจารย์ ดร. พลภัทร บุราคม และรองศาสตราจารย์ ดร. รุ่งพงษ์ ชัยนาม ที่ให้คำแนะนำและข้อคิดเห็นอันเป็นประโยชน์ในการปรับปรุงรายงานฉบับนี้ให้มีความสมบูรณ์มากยิ่งขึ้น

ขอขอบคุณท่านปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมที่ให้โอกาสผู้เขียนรายงานฉบับนี้ได้เข้ารับการฝึกอบรมในหลักสูตรนักบริหารการทูต รุ่นที่ 11 และขอขอบคุณท่านวิทยากร เพื่อนร่วมรุ่นจากหน่วยราชการต่างๆ ตลอดจนเจ้าหน้าที่ทุกท่านจากสถาบันการต่างประเทศเทวะวงศ์วโรปการที่ทำให้ผู้เขียนได้มีโอกาสเพิ่มพูนความรู้ ประสบการณ์ และสร้างมิตรภาพ ตลอดระยะเวลาของการฝึกอบรมดังกล่าว

สุดท้ายขอขอบคุณเจ้าหน้าที่กองการต่างประเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทุกท่านที่สนับสนุนข้อมูลและเป็นกำลังใจในการเข้าร่วมฝึกอบรมในครั้งนี้

กัลยา ชินาธิวร
สิงหาคม 2562

สารบัญ

บทสรุปสำหรับผู้บริหาร	ง
กิตติกรรมประกาศ	ฉ
สารบัญ	ช
สารบัญตาราง	ซ
สารบัญภาพ	ฌ
บทที่ 1 บทนำ	1
1.1 ภูมิหลังและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการศึกษา	4
1.3 ขอบเขตการศึกษา วิธีการดำเนินการศึกษา และระเบียบวิธีการศึกษา	4
1.4 คำถามการศึกษา	5
1.5 สมมติฐานการศึกษา	5
1.6 ประโยชน์ของการศึกษา	5
1.7 นิยามศัพท์	5
บทที่ 2 แนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้อง	8
2.1 แนวคิดทฤษฎี	8
2.2 วรรณกรรมที่เกี่ยวข้อง	11
2.3 สรุปกรอบแนวคิด	24
บทที่ 3 ผลการศึกษา	25
3.1 พัฒนาการในการดำเนินนโยบายความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์	25
3.2 การวิเคราะห์ปัจจัยความสำเร็จของสิงคโปร์	27
3.3 สภาพการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของไทย	38
3.4 ผลการศึกษาเชิงเปรียบเทียบ	42
บทที่ 4 บทสรุปและข้อเสนอแนะ	45
4.1 สรุปผลการศึกษา	45
4.2 ข้อเสนอแนะ	47
บรรณานุกรม	50
ประวัติผู้เขียน	53

สารบัญตาราง

ตารางที่ 1	สถิติภัยคุกคามของไทยในปี 2561	13
ตารางที่ 2	ตัวชี้วัด GCI ของ ITU	16
ตารางที่ 3	คะแนนและอันดับของประเทศสิงคโปร์ในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์	27
ตารางที่ 4	อันดับ GCI ของโลก 6 อันดับแรก ในปี ค.ศ. 2018	38
ตารางที่ 5	คะแนนและอันดับของประเทศไทยในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์	39
ตารางที่ 6	เปรียบเทียบคะแนนตัวชี้วัด 5 ด้าน ระหว่างสิงคโปร์และไทย	42

สารบัญภาพ

ภาพที่ 1	การบรรจบกันของเทคโนโลยี	8
ภาพที่ 2	สถิติภัยคุกคามของไทยในปี 2561 คิดเป็นร้อยละ	14
ภาพที่ 3	ระดับภัยคุกคามไซเบอร์	22
ภาพที่ 4	โครงสร้างองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์	33
ภาพที่ 5	โครงสร้างของหน่วยงานที่รับผิดชอบด้าน Cybersecurity ของไทย	41

บทที่ 1
บทนำ

1.1 ภูมิหลังและความสำคัญของปัญหา

ปัจจุบันโลกกำลังเข้าสู่ยุคเปลี่ยนผ่านไปสู่ยุคดิจิทัล ความก้าวหน้าทางเทคโนโลยีดิจิทัลเป็นไปอย่างรวดเร็วและมีการใช้งานอย่างกว้างขว้าง ทั้งในชีวิตประจำวัน การให้บริการในทุกภาคส่วนและการดำเนินการ/ประกอบการธุรกิจ สำหรับประชาชนในทุกเพศทุกวัย สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union หรือ ITU) ซึ่งเป็นทบวงการชำนัญพิเศษภายใต้สหประชาชาติได้รายงานว่าสิ้นปี 2561 จำนวนประชากรโลกร้อยละ 51.2 หรือคิดเป็นจำนวน 3.9 พันล้านคน มีการใช้งานอินเทอร์เน็ต ทั้งนี้ ITU คาดว่า ภายในปี 2566 จำนวนผู้เข้าถึงอินเทอร์เน็ตจะเพิ่มเป็นร้อยละ 70 สอดคล้องกับผลสำรวจของสำนักงานสถิติแห่งชาติ ปี 2561 (ช่วงไตรมาส 1) จากประชากรผู้มีอายุ 6 ปีขึ้นไป พบว่ามีผู้ใช้งานอินเทอร์เน็ต 36.5 ล้านคน คิดเป็นร้อยละ 56.8 ของประชากร 63.3 ล้านคน เปรียบเทียบกับผลการสำรวจปี 2557 ซึ่งมีจำนวน 21.8 ล้านคน หรือร้อยละ 34.9 นอกจากนี้ จากผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทยปี 2561 โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ ยังพบว่า ประเทศไทยขยับสู่สังคมดิจิทัลเต็มรูปแบบแล้ว เมื่อค่าเฉลี่ยการใช้งานอินเตอร์เน็ตคนไทยหนักหน่วงมากยิ่งขึ้น มีการเติบโตเพิ่มขึ้นมากกว่าปีที่ผ่านมาถึง 3 เท่าตัว

อย่างไรก็ตาม ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตมาพร้อมกับความท้าทายและภัยคุกคามทางไซเบอร์ซึ่งมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ข้อมูลที่ไม่เป็นจริง การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างหน้าเว็บไซด์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ และปัจเจกบุคคล มีข้อมูลรายงานว่า บริษัท Norton ซึ่งเป็นผู้ผลิตซอฟต์แวร์สำหรับฆ่าไวรัสที่อยู่บนโลกออนไลน์พบว่า ในปี ค.ศ. 2017 มีผู้ได้รับผลกระทบจากอาชญากรรมไซเบอร์ถึง 978 ล้านคน ใน 20 ประเทศ (www.todayonline.com วันที่ 6 มิถุนายน 2562) นอกจากนี้ ยังมีรายงานระบุว่า แพลตฟอร์มสื่อสังคมออนไลน์ได้ตกเป็นเป้าหมายของกิจกรรมที่เป็นอันตราย และบัญชีสื่อสังคมออนไลน์กว่า 1.3 พันล้านบัญชีได้ถูกโจรกรรมไปตั้งแต่ปี 2556 โดย ITU ได้คาดการณ์ว่า ค่าใช้จ่ายสำหรับโครงการที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในปี 2562 ทั่วโลก มีจำนวนประมาณ 2 ล้านล้านเหรียญสหรัฐอเมริกา

ในส่วนของประเทศไทย จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย ปี 2561 รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต หรือ ThaiCERT) พบว่าความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์อันดับ 1 ของประเทศไทย ซึ่งมีจำนวน 1,102 เรื่อง คิดเป็นสัดส่วนร้อยละ 43.3 จากภัยคุกคามทั้งหมด 2,520 เรื่อง จากภัยคุกคามจำแนกเป็น 9 ประเภท ตามมาด้วยภัยคุกคามอันดับ 2 คือ

การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) คิดเป็นร้อยละ 36.86 โดยไทยมีการแจ้งเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มากเป็นอันดับที่ 5 รองจากเยอรมันนี สหราชอาณาจักร ออสเตรเลีย และสหรัฐอเมริกา ตามลำดับ ดังนั้น การเฝ้าระวัง การป้องกันและรับมือกับภัยคุกคามจึงต้องอาศัยความรวดเร็ว ทันเหตุการณ์ เทคโนโลยีที่ทันสมัย และการทำงานที่มีระบบและมีประสิทธิภาพ เพราะมีผลกระทบต่อการขาดความเชื่อมั่นในการใช้งานเทคโนโลยีดิจิทัลในมิติต่างๆ รวมถึงความสูญเสียและความเสียหายที่จะเกิดขึ้น

จากสภาพปัญหาดังกล่าว ทั่วโลกต่างตระหนักถึงภัยคุกคามทางไซเบอร์ซึ่งทวีความรุนแรงขึ้นตามจำนวนผู้ใช้งานอินเทอร์เน็ต มีความซับซ้อน และมีผลกระทบในวงกว้างมากขึ้นทุกๆ ปี ทั้งยังควบคุมได้ยากเนื่องจากเป็นการสื่อสารไร้พรหมแดน ปัญหาของภัยคุกคามมีสาเหตุสำคัญมาจากการขาดระบบการบริหารจัดการเครือข่ายที่ดี ความไม่พร้อมของระบบเทคโนโลยี การขาดแคลนบุคลากรที่มีความเชี่ยวชาญด้านเทคโนโลยีสื่อสารและด้านความมั่นคงปลอดภัยไซเบอร์ ทำให้แต่ละประเทศรวมทั้งสหประชาชาติและองค์การระหว่างประเทศต่างๆ ที่เกี่ยวข้องต่างหามาตรการและกำหนดแนวนโยบายในการสร้างความมั่นคงปลอดภัยไซเบอร์ รวมทั้งมีความร่วมมือในการป้องกันภัยคุกคามทางไซเบอร์ โดย ITU ได้ทำการศึกษาและจัดทำดัชนีตัวชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อวัดระดับความสามารถในการจัดการเรื่องดังกล่าวในประเทศสมาชิก ITU ทั้งหมด 193 ประเทศ รวมทั้งประเทศไทย และได้จัดทำแบบสอบถามให้ประเทศสมาชิกตอบแบบสอบถามและนำมาวิเคราะห์ร่วมกับข้อมูลอื่นๆ ประกอบ เพื่อจัดอันดับประเทศที่มีการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง โดยจัดทำเป็นรายงานทุกปี เริ่มตั้งแต่ ปี 2556 ซึ่งผลปรากฏว่าในภูมิภาคเอเชียและแปซิฟิก ประเทศสิงคโปร์จะได้คะแนนสูงสุด เป็นอันดับ 1 ในทุกปี และได้คะแนนติด 10 อันดับแรกของโลกทุกปีเช่นกัน โดยในปี 2560 สิงคโปร์เป็นอันดับ 1 ของโลก และเป็นอันดับ 6 ในปี 2561 ในขณะที่ประเทศไทยอยู่อันดับที่ 22 ในปี 2560 และอันดับที่ 35 ในปี 2561

รัฐบาลไทยได้กำหนดนโยบายไทยแลนด์ 4.0 ซึ่งขับเคลื่อนเศรษฐกิจและสังคมด้วยนวัตกรรมและการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัลในทุกภาคส่วน และตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศไทย ก็ได้กำหนดกรอบยุทธศาสตร์การพัฒนาไว้ 6 ด้าน โดยยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล ซึ่งมุ่งเน้นการมีกฎหมาย กฎระเบียบ กติกาและมาตรฐานที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมและทำธุรกรรมออนไลน์ต่างๆ รวมถึงสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัล นอกจากนี้ ตามพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560 มาตรา 6 นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมมีเป้าหมายและแนวทางอย่างน้อย ดังนี้ (4) การส่งเสริมให้เกิดมาตรฐานหรือกฎเกณฑ์ในการใช้งานเทคโนโลยีดิจิทัลให้สอดคล้องกันเพื่อให้การทำงานระหว่างระบบสามารถทำงานเชื่อมโยงกันได้อย่างมีความมั่นคงปลอดภัย อยู่ในสภาพพร้อมใช้งาน รวมตลอดทั้งทำให้ระบบหรือการให้บริการมีความน่าเชื่อถือ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมตระหนักถึงการปรับปรุงเปลี่ยนแปลงโครงสร้างพื้นฐานสำคัญๆ ที่กำลังเกิดขึ้นตามนโยบายการขับเคลื่อนเศรษฐกิจดิจิทัลและไทยแลนด์ 4.0 ของรัฐบาล ซึ่งเป็นการเปลี่ยนผ่านประเทศครั้งสำคัญ อันหมายถึง การเคลื่อนย้ายจากสังคมหนึ่งไปอีก

สังคมหนึ่งด้วยการเข้าถึงข้อมูลและการบริการต่างๆ ด้วยระบบดิจิทัลและนวัตกรรม โดยจะยิ่งละเลยไม่ได้กับภัยคุกคามไซเบอร์ต่างๆ ที่อาจฉุดรั้งการเปลี่ยนผ่านที่เกิดขึ้น กระทรวงฯ จึงได้ดำเนินการในการเสนอร่างกฎหมาย โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุมคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบภายในประเทศ

ในมิติด้านการต่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ลงนามในบันทึกความเข้าใจที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศและการสื่อสาร และเทคโนโลยีดิจิทัล กับประเทศต่างๆ รวมทั้งประเทศสิงคโปร์ซึ่งได้มีการลงนามในบันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในปัจจุบัน) แห่งราชอาณาจักรไทย และกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Memorandum of Understanding between the Ministry of Information and Communication Technology of the Kingdom of Thailand and the Ministry of Communications and Information of the Republic of Singapore for Cooperation in the Field of Information and Communication Technology) เมื่อวันที่ 31 พฤษภาคม 2559 บันทึกความเข้าใจฉบับดังกล่าว มีวัตถุประสงค์เพื่อพัฒนาความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสารระหว่างกันโดยมีขอบเขตความร่วมมือในสาขาต่างๆ ซึ่งสอดคล้องกับนโยบายของรัฐบาลและกระทรวงฯ ได้แก่ การแบ่งปันประสบการณ์และความรู้ด้านการพัฒนารัฐบาลอิเล็กทรอนิกส์ การแลกเปลี่ยนทัศนะเกี่ยวกับความรู้และการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์ การแลกเปลี่ยนทัศนะและความร่วมมือในการยกระดับระบบนิเวศน์ด้วยธุรกิจเกิดใหม่ด้านเทคโนโลยีดิจิทัล การจัดหรือการอำนวยความสะดวกการฝึกอบรมและโปรแกรมการพัฒนาความสามารถ การแลกเปลี่ยนประสบการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และความร่วมมือในสาขาอื่นๆ ที่อยู่ในความสนใจของคู่ภาคี ทั้งนี้ ทั้งสองฝ่ายอาจกำหนดขอบเขตความร่วมมือเกี่ยวกับการแลกเปลี่ยนข้อมูลและประสบการณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อย่างไรก็ตาม หลังจากมีการลงนามบันทึกความเข้าใจดังกล่าวแล้ว ทั้งสองฝ่ายยังมิได้มีการดำเนินการตามกรอบความร่วมมืออย่างเป็นรูปธรรม

การศึกษาปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ จะเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้องของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และประเทศไทยในการนำมาเป็นข้อมูลสนับสนุนการดำเนินนโยบายของไทยด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนเป็นโอกาสในการขยายความร่วมมือกับประเทศสิงคโปร์และประเทศที่ 3 อื่นๆ ในเรื่องความมั่นคงปลอดภัยไซเบอร์ต่อไป

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษา วิเคราะห์ และประเมิน ปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์มาตลอดระยะเวลา 5 ปีที่ผ่านมา (ช่วงปี 2014–ปัจจุบัน)

1.2.2 เพื่อนำผลการศึกษามาเป็นข้อเสนอแนะในการพัฒนาแนวทางในการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

1.3 ขอบเขตการศึกษา วิธีการดำเนินการศึกษา และระเบียบวิธีการศึกษา

1.3.1 ขอบเขตการศึกษา

การศึกษานี้ดำเนินการวิเคราะห์ปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ช่วงปี 2014–ปัจจุบัน แล้วนำผลการวิเคราะห์มาเปรียบเทียบกับการดำเนินงานของไทย เพื่อหาแนวทางและข้อเสนอแนะในการพัฒนาการการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย

1.3.2 วิธีการดำเนินการศึกษา

การศึกษาจะวิเคราะห์ตามกรอบดัชนีตัวชี้วัดตามที่สหภาพโทรคมนาคมระหว่างประเทศจัดทำ ซึ่งเป็นที่ยอมรับทั่วโลก โดยแบ่งเป็น 5 เสาหลัก ดังนี้

1) ด้านกฎหมาย (legal measures) โดยวิเคราะห์จากกรอบกฎหมายที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

2) ด้านเทคนิค (technical measures) โดยวิเคราะห์จากกรอบงานทางเทคนิคที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

3) ด้านองค์กร (organizational measures) โดยวิเคราะห์จากสถาบัน องค์กรที่ประสานงานเชิงนโยบาย และวิเคราะห์จากยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ

4) ด้านการเสริมสร้างศักยภาพ (capacity building) โดยวิเคราะห์จากการศึกษาวิจัยและการพัฒนา (R&D) การฝึกอบรม การรับรองหน่วยงานภาครัฐและหน่วยงานระดับมืออาชีพที่ส่งเสริมการพัฒนาศักยภาพ

5) ด้านความร่วมมือ (cooperation) โดยวิเคราะห์จากหุ้นส่วนพันธมิตร กรอบความร่วมมือ และเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง

1.3.3 ระเบียบวิธีศึกษา

1) ใช้ระเบียบวิธีแบบพรรณาเชิงวิเคราะห์ (Descriptive Analysis) โดยการทบทวนและวิเคราะห์ข้อมูลวรรณกรรมที่เกี่ยวข้องกับขอบเขตการศึกษาในหัวข้อ ทั้งหนังสือ เว็บไซต์ พระราชบัญญัติ แผนนโยบายและยุทธศาสตร์ ข้อมูลสถิติ รายงาน และเอกสารวิชาการ

2) รวบรวมข้อมูลทุติยภูมิที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานที่เกี่ยวข้อง เช่น สหภาพโทรคมนาคมระหว่างประเทศ ThaiCERT สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ Cyber Security Agency of Singapore และ InfoComm Media Development Authority (IMDA) แห่งสิงคโปร์ เป็นต้น

1.4 คำถามการศึกษา

อะไรคือปัจจัย และมีการดำเนินการอย่างไร ที่ทำให้สิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และจะสามารถนำปัจจัยความสำเร็จและวิธีดำเนินนโยบายของสิงคโปร์มาปรับใช้เพื่อการพัฒนาแนวทางการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยได้หรือไม่ อย่างไร

1.5 สมมติฐานการศึกษา

การให้ความสำคัญกับความร่วมมือในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจังทั้งในระดับประเทศ ระดับภูมิภาค และระดับโลก ของสิงคโปร์ เป็นปัจจัยความสำเร็จซึ่งน่าจะสามารถนำมาปรับใช้ในการพัฒนาการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยให้ประสบความสำเร็จอย่างมีประสิทธิภาพได้

1.6 ประโยชน์ของการศึกษา

1.6.1 เป็นข้อมูลสำหรับเจ้าหน้าที่และหน่วยงานที่เกี่ยวข้องของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตลอดจนผู้บริหารกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อใช้ประกอบการพิจารณาจัดทำแผนปฏิบัติการณ์เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสนอคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ ตามที่กำหนดไว้ในมาตรา 9 (3) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.6.2 เป็นข้อมูลในการกำหนดขอบเขตความร่วมมือเกี่ยวกับการแลกเปลี่ยนข้อมูลและประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับประเทศสิงคโปร์ภายใต้บันทึกความเข้าใจซึ่งได้มีการลงนามเมื่อวันที่ 31 พฤษภาคม 2559 ได้อย่างเป็นรูปธรรม

1.6.3 เพื่อใช้ประโยชน์ในการขยายความร่วมมือทางวิชาการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กับประเทศอื่นๆ โดยเฉพาะประเทศที่ประสบความสำเร็จในการดำเนินการในเรื่องดังกล่าวและเป็นประเทศที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ลงนามในบันทึกความเข้าใจระหว่างกันแล้ว เช่น ประเทศออสเตรเลีย

1.7 นิยามศัพท์

“ดิจิทัล” หมายความว่า เทคโนโลยีที่ใช้วิธีการนำสัญญลักษณ์ศูนย์และหนึ่งหรือสัญญลักษณ์อื่นมาทดแทนค่าสิ่งทั้งปวง เพื่อใช้สร้าง หรือก่อให้เกิดระบบต่างๆ เพื่อให้มนุษย์ใช้ประโยชน์

“ดิจิทัลเพื่อเศรษฐกิจและสังคม” หมายความว่า ระบบเศรษฐกิจและสังคมที่มีการติดต่อสื่อสาร การผลิต การอุปโภคบริโภค การใช้สอย การจำหน่ายจ่ายแจก การพาณิชย์อิเล็กทรอนิกส์ การทำธุรกรรมทางอิเล็กทรอนิกส์ การคมนาคมขนส่ง การโลจิสติกส์ การศึกษา การเกษตรกรรม การอุตสาหกรรม การสาธารณสุข การเงินการลงทุน การภาษีอากร การบริหารจัดการข้อมูล และเนื้อหาหรือกิจกรรมทางเศรษฐกิจและสังคมอื่นใด หรือการใดๆ ที่มีกระบวนการ

หรือการดำเนินงานทางดิจิทัลหรือทางอิเล็กทรอนิกส์ ทั้งในกิจการกระจายเสียง กิจการโทรทัศน์ กิจการวิทยุคมนาคม กิจการโทรคมนาคม กิจการสื่อสารดาวเทียม และการบริหารคลื่นความถี่ โดยอาศัยโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งเทคโนโลยีที่มีการหลอมรวม หรือเทคโนโลยีอื่นใดในทำนองเดียวกันหรือคล้ายคลึงกัน

“อินเทอร์เน็ต” หมายความว่า เครือข่ายคอมพิวเตอร์ที่มีขนาดใหญ่ มีการเชื่อมต่อระหว่างเครือข่ายหลายๆ เครือข่ายทั่วโลก โดยใช้ภาษาที่ใช้สื่อสารกันระหว่างคอมพิวเตอร์ที่เรียกว่า โพร์โทคอล ผู้ใช้เครือข่ายนี้สามารถสื่อสารถึงกันได้ในหลายๆ ทาง เช่น ไปรษณีย์อิเล็กทรอนิกส์ หรืออีเมล์ และสามารถสืบค้นข้อมูลและข่าวสารต่างๆ รวมทั้งคัดลอกแฟ้มข้อมูลและโปรแกรมมาใช้ได้

“ออนไลน์” หมายความว่า ติดต่อสื่อสารกับคอมพิวเตอร์โดยตรง และพร้อมใช้งาน

“แพลตฟอร์ม” หมายความว่า สภาวะแวดล้อมที่ประกอบด้วยฮาร์ตแวร์และซอฟต์แวร์ของระบบคอมพิวเตอร์ระบบหนึ่ง

“ไซเบอร์” หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่งคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพวิเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“การอภิบาลอินเทอร์เน็ต” หมายความว่า การที่รัฐบาลภาคเอกชน และภาคประชาสังคมพัฒนาและประยุกต์ใช้หลักการ บรรทัดฐาน หลักเกณฑ์ ขั้นตอนการตัดสินใจ และโครงการร่วมกันตามบทบาทของตน เพื่อกำหนดลักษณะวิวัฒนาการและการใช้ประโยชน์ของอินเทอร์เน็ต

“แฮกเกอร์” (Hacker) หมายความว่า คือ ผู้ที่มีความรู้ความเข้าใจในระบบคอมพิวเตอร์อย่างสูงมาก ไม่ว่าจะเป็นเรื่องเครือข่าย ระบบปฏิบัติการ จนสามารถเข้าใจว่าระบบมีช่องโหว่ตรงไหน หรือสามารถไปค้นหาช่องโหว่ได้จากตรงไหนบ้าง เมื่อก่อนภาพลักษณ์ของแฮกเกอร์จะเป็นพวกมิจฉาชีพ ขโมยข้อมูล หรือ ทำลายให้เสียหาย แต่ปัจจุบัน คำว่า แฮกเกอร์ หมายถึง ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย ที่คอยใช้ความสามารถช่วยตรวจตราระบบ และแจ้งเจ้าของระบบว่ามีช่องโหว่ตรงไหนบ้าง อาจพูดง่ายๆว่าเป็นแฮกเกอร์ที่มีจริยธรรมนั่นเอง ในต่างประเทศมีวิชาที่สอนถึงการเป็น Ethical Hacker หรือ แฮกเกอร์แบบมีจริยธรรม ซึ่งแฮกเกอร์แบบนี้เรียกอีกอย่างว่า White Hat Hacker ก็ได้ ส่วนพวกที่มีความประพฤติไม่ดีจะถูกเรียกว่า Cracker หรือ Black Hat Hacker ซึ่งก็คือ มีความสามารถเหมือนแฮกเกอร์ทุกประการ เพียงแต่พฤติกรรมของ Cracker นั้นจะเป็นการกระทำที่ขาดจริยธรรม เช่น ขโมยข้อมูลหรือเข้าไปทำลายระบบคอมพิวเตอร์ให้ทำงานไม่ได้ เป็นต้น

“ระบบคลาวด์คอมพิวติงค์” (Clound computing) หมายถึงการใช้ซอฟต์แวร์ ระบบและทรัพยากรของเครื่องคอมพิวเตอร์ของผู้ให้บริการ ผ่านอินเทอร์เน็ต โดยสามารถเลือกกำลังการประมวลผล เลือกจำนวนทรัพยากร ได้ตามความต้องการในการใช้งาน และให้เราสามารถเข้าถึงข้อมูลบนคลาวด์จากที่ไหนก็ได้ มีทั้งแบบไม่มีค่าใช้จ่ายและแบบมีค่าใช้จ่ายในการใช้บริการ

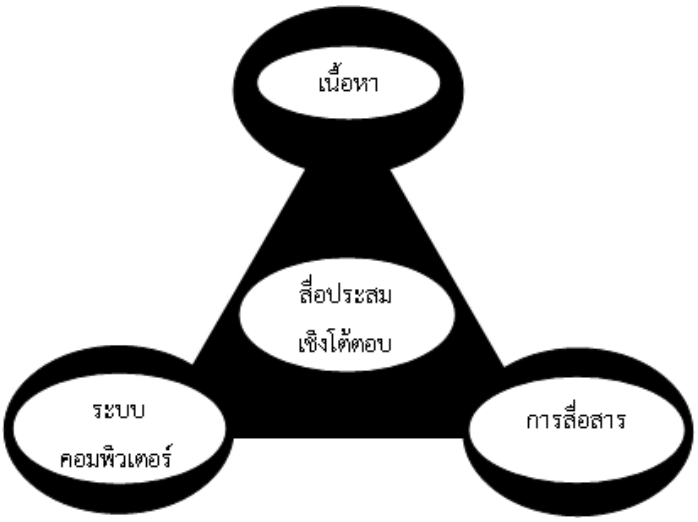
“อินเทอร์เน็ตทุกสรรพสิ่ง” (Internet of Things หรือ IoT) หมายถึง การที่อุปกรณ์ต่างๆ สิ่งต่างๆ ได้ถูกเชื่อมโยงทุกสิ่งทุกอย่างสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเทอร์เน็ต เช่น การเปิด–ปิด อุปกรณ์เครื่องใช้ไฟฟ้า (การสั่งการเปิดไฟฟ้าภายในบ้านด้วยการเชื่อมต่ออุปกรณ์ควบคุม เช่น มือถือ ผ่านทางอินเทอร์เน็ต) รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องมือทางการเกษตร อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่างๆ ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น

บทที่ 2
แนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

2.1 แนวคิดทฤษฎี

2.1.1 แนวคิดเศรษฐกิจดิจิทัล (Digital Economy)

คำว่า “เศรษฐกิจดิจิทัล” ถูกกล่าวถึงครั้งแรกในประเทศญี่ปุ่นโดยอาจารย์ชาวญี่ปุ่นและนักเศรษฐศาสตร์การวิจัยในช่วงเศรษฐกิจญี่ปุ่นถดถอยในช่วงปี ค.ศ. 1990 แต่หนังสือ “The Digital Economy” เขียนโดย Don Tapscott[1] ซึ่งได้พิมพ์ออกจำหน่ายมาตั้งแต่ปี ค.ศ. 1995 ได้นำเสนอแนวความคิดเกี่ยวกับเศรษฐกิจดิจิทัลว่า ในอดีต ข้อมูลจะส่งต่อกันผ่านสิ่งที่จับต้องได้ เช่น เงินสด รายงาน การประชุมตัวต่อตัว ดูรูปภาพ โทรศัพท์พูดคุยกัน หรือใบปลิวโฆษณา แต่ทุกวันนี้ข้อมูลต่างๆ อยู่ในรูปดิจิทัล จัดเก็บอยู่ในเครื่องคอมพิวเตอร์แล้วส่งผ่านกันด้วยความเร็วแสง โลกเศรษฐกิจยุคใหม่ ยังถูกเรียกอีกชื่อหนึ่งว่า เศษรฐกิจแห่งองค์ความรู้ โดยการเพิ่มมูลค่าเข้าไปในสิ่งต่างๆ ด้วยสมองมากว่าพละกำลัง เกษตรกรจะต้องเปลี่ยนเป็นแรงงานที่มีความรู้มากยิ่งขึ้น เครื่องจักรในฟาร์มถูกควบคุมด้วยเครื่องสมองกล สินค้าหลายอย่างมีวงจรอัจฉริยะเก็บอยู่ในตัวเอง Tapscott ยังได้แสดงให้เห็นถึงโครงสร้างเศรษฐกิจที่แปรเปลี่ยนไปด้วยระบบประมวลผล (ฮาร์ดแวร์ ซอฟต์แวร์ บริการ) การสื่อสาร (เคเบิล ดาวเทียม ระบบไร้สาย) และเนื้อหาสาระ (ความบันเทิง สื่อสิ่งพิมพ์ ผู้ให้บริการข้อมูล) ซึ่งแสดงเอาไว้ในภาพที่ 1



ภาพที่ 1 การบรรจบกันของเทคโนโลยี
ที่มา: เศรษฐกิจดิจิทัล. แปลและเรียบเรียงโดย พรศักดิ์ อุรัจฉัทชัยรัตน์

[1]Tapscott. เศรษฐกิจดิจิทัล. แปลและเรียบเรียงโดย พรศักดิ์ อุรัจฉัทชัยรัตน์. กรุงเทพมหานคร: แมคกรอ–ฮิล อินเตอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2558

แนวคิดสำคัญสำหรับเศรษฐกิจดิจิทัลคือ ตั้งอยู่บนเศรษฐกิจแห่งนวัตกรรม วิกิพีเดีย ได้อธิบายความหมายของนวัตกรรมว่า หมายถึงการทำสิ่งต่างๆ ด้วยวิธีใหม่ๆ และยังอาจหมายถึง การเปลี่ยนแปลงทางความคิด การผลิต กระบวนการ หรือองค์กร ไม่ว่าการเปลี่ยนนั้นจะเกิดขึ้นจาก การปฏิวัติ การเปลี่ยนอย่างถอนรากถอนโคน หรือการพัฒนาต่อยอด ทั้งนี้ มักมีการแยกแยะ ความแตกต่างอย่างชัดเจน ระหว่างการประดิษฐ์คิดค้น ความคิดริเริ่ม และนวัตกรรม อันหมายถึง ความคิดริเริ่มที่นำมาประยุกต์ใช้อย่างสัมฤทธิ์ผล (Mckeown, 2008) และในหลายสาขา เชื่อกันว่า การที่สิ่งใดสิ่งหนึ่งจะเป็นนวัตกรรมได้นั้น จะต้องมีความแปลกใหม่อย่างเห็นได้ชัด และไม่เป็นแค่เพียง การเปลี่ยนแปลงครั้งสำคัญ เป็นต้นว่า ในด้านศิลปะ เศรษฐศาสตร์ เศรษฐกิจ และนโยบายของรัฐ ในเชิงเศรษฐศาสตร์นั้น การเปลี่ยนแปลงนั้นจะต้องเพิ่มมูลค่า มูลค่าของลูกค้า หรือมูลค่าของผู้ผลิต เป้าหมายของนวัตกรรมคือการเปลี่ยนแปลงในเชิงบวก เพื่อทำให้สิ่งต่างๆเกิดเปลี่ยนแปลงในทางที่ดีขึ้น นวัตกรรมก่อให้ได้ผลิตผลเพิ่มขึ้น และเป็นที่มาสำคัญของความมั่งคั่งทางเศรษฐกิจ

Eric Schmidt ประธานบริหาร กูเกิล ได้กล่าวคำนิยมในหนังสือ The Digital Economy ฉบับฉลองครบรอบ 20 ปี ตอนหนึ่งว่า การปฏิวัติดิจิทัลถือเป็นเหตุการณ์ครั้งสำคัญที่ทำให้ เศรษฐกิจทั่วโลกเกิดการเปลี่ยนสภาพ ไม่ว่าจะเป็นประสิทธิผลหรือประสิทธิภาพ ก่อให้เกิด แบบจำลองธุรกิจใหม่ๆ ขึ้นมา รวมถึงภาครัฐเองก็เปลี่ยนวิธีให้บริการประชาชนของตน

ท่ามกลางความเปลี่ยนแปลงทั้งมวล อินเทอร์เน็ต คือระบบเครือข่ายคอมพิวเตอร์ ขนาดใหญ่ที่ทำให้เครื่องคอมพิวเตอร์สื่อสารถึงกันได้ มีพัฒนาการอย่างต่อเนื่อง ช่วงกลางยุคที่ 90 เว็บไซด์ถือกำเนิดขึ้นเพื่อนำเสนอข้อมูลผ่านทางหน้าจอ และเมื่อมาถึงปลายยุค 90 เริ่มเข้าสู่ยุค เศรษฐกิจดิจิทัล ซึ่งมีการค้าขายผ่านทางอินเทอร์เน็ต หรือ e–commerce และปี ค.ศ. 2005 เมื่อ บริษัทควอลคอมม์และ BlackBerry ได้นำ Mobile Internet เข้าสู่ตลาด ตามมาด้วยแอปเปิล และ ซัมซุง ทำให้คนหลายร้อยล้านคนมีการใช้อินเทอร์เน็ตผ่านโทรศัพท์มือถือ จนกระทั่งปี ค.ศ. 2010 สื่อ สังคมออนไลน์ ก็เข้ามาเป็นส่วนหนึ่งของชีวิตผู้คน เริ่มต้นจาก myspace ติดตามด้วย Facebook และ Twitter อาจกล่าวได้ว่า อินเทอร์เน็ตได้ถูกใช้งานจนเป็นปัจจัยพื้นฐานสำหรับทุกคน เป็นแหล่งที่ เราเข้าถึงโอกาสทางธุรกิจและสังคมได้อย่างไม่เคยมีมาก่อน

จากเว็บไซด์ https:// translate.google.com/ ได้วิเคราะห์ว่า ในระบบเศรษฐกิจใหม่นี้ ระบบเครือข่ายและโครงสร้างพื้นฐานการสื่อสารเป็นแพลตฟอร์มระดับโลกที่ผู้คนและองค์กรกำหนด กลยุทธ์โต้ตอบสื่อสารทำงานและค้นหาข้อมูล และอีกไม่นานเศรษฐกิจดิจิทัลได้ถูกกำหนดให้เป็นสาขา เศรษฐศาสตร์ที่ศึกษา ศูนย์ต้นทุนสินค้าไม่มีตัวตน เหนือขอบสุทธิ และเป็นที่ยอมรับกันอย่างกว้างขวางว่า การเติบโตของเศรษฐกิจดิจิทัลมีผลกระทบอย่างกว้างขว้างต่อเศรษฐกิจโดยรวม ทั้งยังมีการพยายาม จัดหมวดหมู่ขนาดของผลกระทบต่อภาพดั่งเดิมหลายครั้ง

อย่างไรก็ตาม แม้ว่าเศรษฐกิจดิจิทัลจะสร้างโอกาสใหม่ๆ แต่ยังมีความท้าทายและ ภัยคุกคามที่เราทุกคนต้องเผชิญ ไม่ว่าจะเป็น การสูญเสียความเป็นส่วนตัว การสูญเสียสิทธิขั้นพื้นฐาน ความไม่มั่นคงในการจ้างงาน ความไม่เท่าเทียมกันของรายได้ และความขัดแย้งของการเคลื่อนย้าย แรงงานจำนวนมหาศาล

2.1.2 แนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)

ในช่วงที่หลายประเทศกำลังเปลี่ยนผ่านเข้าสู่ยุคดิจิทัลหรือก้าวเข้าสู่ระบบเศรษฐกิจดิจิทัล ทุกคนล้วนเกี่ยวข้องกับอินเทอร์เน็ตในทางหนึ่งทางใด แม้จะไม่ใช่ผู้ใช้อินเทอร์เน็ตโดยตรงก็ตาม มีคำศัพท์ที่เกี่ยวเนื่องกับคำว่าอิเทอร์เน็ตหลายคำ และสามารถใช้ทดแทนกันได้ ซึ่งแต่ละคำอธิบายถึงปรากฏการณ์ของอินเทอร์เน็ต มีแนวโน้มที่เรามักใช้ “อี” ข้างหน้าคำว่า “คอมเมิร์ซ” และเติมคำว่า “ไซเบอร์” ต่อท้ายคำว่า “อาชญากรรม” และ “ความมั่นคง” เติมคำว่า “ดิจิทัล” ต่อท้ายช่องว่างด้านการพัฒนา และเติมคำว่า “เสมือน” ต่อท้ายสกุลเงิน ในกรณีที่เป็นเงินออนไลน์

โจวาน เคอร์บาลิจา[2] ได้กล่าวว่า ในแง่นิรุกติศาสตร์ คำว่า “ไซเบอร์” สามารถสืบย้อนกลับไปถึงสมัยกรีกโบราณ โดยมีความหมายว่า “การปกครอง” ในปี ค.ศ. 1984 วิลเลียม กิบสัน (William Gibson) ได้คิดค้นคำว่า “ไซเบอร์สเปซ” (cyberspace) ในนิยายวิทยาศาสตร์ เป็นสาเหตุให้มีการใช้คำว่าไซเบอร์สเปซมากขึ้นพร้อมๆ กับการเติบโตของอินเทอร์เน็ต ช่วงปลายทศวรรษ 1990 คำไหนที่เกี่ยวข้องกับอินเทอร์เน็ตมักถูกเติมคำว่าไซเบอร์นำหน้า เช่น ชุมชนไซเบอร์ (cybercommunity) กฎหมายไซเบอร์ (cyberlaw) และอาชญากรรมไซเบอร์ (cybercrime) เป็นต้น ช่วงต้นทศวรรษ 2000 คำว่าไซเบอร์ค่อยๆ หายไปจากการใช้ในวงกว้างเหลืออยู่เฉพาะในคำศัพท์เกี่ยวกับการรักษาความปลอดภัยเท่านั้น

โจวาน เคอร์บาลิจา ได้นำเสนอแนวคิดระหว่าง “เก่า–จริง” (old–real) กับ “ใหม่–ไซเบอร์” (new–cyber) ที่เป็นแนวทางในการพิจารณาประเด็นต่างเกี่ยวกับการอภิบาลอินเทอร์เน็ต กล่าวคือ “เก่า–จริง” ถือว่าอินเทอร์เน็ตไม่ได้ทำให้เกิดสิ่งใหม่ใดๆ ต่อประเด็นการอภิบาล เป็นเพียงเครื่องมือใหม่อีกชนิด ไม่แตกต่างจากเครื่องมือที่เคยมีมา เช่น ภาพถ่าย โทรศัพท์ และวิทยุ ยกตัวอย่าง เช่น ในการอภิปรายเกี่ยวกับกฎหมาย ตามแนวทางนี้ถือว่ากฎหมายที่มีอยู่สามารถนำมาใช้กับอินเทอร์เน็ตได้โดยปรับปรุงเนื้อหาเพียงเล็กน้อย ในแง่เศรษฐกิจ แนวทางนี้ถือว่าไม่มีความแตกต่างระหว่างพาณิชยกรรมทั่วไปกับพาณิชย์กรรมอิเล็กทรอนิกส์ เป็นเหตุให้ไม่จำเป็นต้องกำหนดระเบียบเป็นการเฉพาะสำหรับพาณิชย์อิเล็กทรอนิกส์

ในขณะที่แนวทาง “ใหม่–ไซเบอร์” แย้งว่า อินเทอร์เน็ตเป็นระบบสื่อสารซึ่งแตกต่างจากระบบที่เคยมีมาทั้งหมด แนวคิดพื้นฐานของแนวทางไซเบอร์คืออินเทอร์เน็ตลดความเชื่อมโยงระหว่างความจริงทางสังคมกับการเมืองออกจากรัฐอธิปไตย (ที่แยกจากกันในเชิงภูมิศาสตร์) ไซเบอร์สเปซแตกต่างจากพื้นที่จริงและจำเป็นต้องมีรูปแบบการกำกับบดูแลที่แตกต่างไปในแง่กฎหมายสำนักคิดในแนวไซเบอร์เห็นว่ากฎหมายเดิมที่มีอยู่เกี่ยวกับอำนาจศาลอาชญากรรมคอมพิวเตอร์และสัญญาต่างๆ ไม่สามารถนำมาใช้กับอินเทอร์เน็ต และต้องมีการกำหนดกฎหมายขึ้นมาใหม่ ขณะที่แนวทาง “เก่า–จริง” เริ่มมีความสำคัญขึ้นเรื่อยๆ ทั้งในส่วนของการกำกับดูแลกำหนดนโยบาย

ความปลอดภัยไม่ได้

เป็นปัญหาหลักในช่วงที่มีการพัฒนาอินเทอร์เน็ตในเบื้องต้น เนื่องจากในช่วงดังกล่าว อินเทอร์เน็ตยังเป็นเครือข่ายแบบปิดของสถาบันวิจัย เมื่ออินเทอร์เน็ตขยายตัวครอบคลุม

---

[2] เคอร์บาลิจา โจวาน. เปิดประตูสู่การอภิบาลอินเทอร์เน็ต. แปลโดย พิภพ อุดมอิทธิพงศ์. กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2558.

ผู้ใช้งาน 2 พันล้านคนทั่วโลก และเมื่ออินเทอร์เน็ตกลายเป็นเครื่องมือเชิงพาณิชย์ที่สำคัญมากยิ่งขึ้น คำถามเกี่ยวกับความปลอดภัยเริ่มเป็นประเด็นสำคัญ เนื่องจากการออกแบบสถาปัตยกรรมอินเทอร์เน็ตในเบื้องต้นไม่ได้คำนึงถึงความปลอดภัย การเพิ่มระบบรักษาความปลอดภัยเข้ามาจึงจำเป็นต้องอาศัยการเปลี่ยนแปลงโครงสร้างพื้นฐานของอินเทอร์เน็ต

ปัญหาความมั่นคงไซเบอร์อาจแบ่งได้ตามหลักเกณฑ์ดังนี้

1) จำแนกตามปฏิบัติการ ซึ่งอาจรวมถึงการดักจับข้อมูล การแทรกแซงข้อมูล การเข้าถึงอย่างผิดกฎหมาย การทำให้ข้อมูลเพี้ยน (data corruption) การก่อวินาศกรรม การขัดขวางการบริการ และการโจรกรรมอัตลักษณ์ (identity theft)

2) จำแนกตามคนร้าย คนร้ายในกรณีนี้มักประกอบด้วยแฮกเกอร์ อาชญากรไซเบอร์ (cybercriminals) นักรบไซเบอร์ (cyberwarriors) และผู้ก่อการร้ายไซเบอร์ (cyberterrorists)

3) จำแนกตามเป้าหมาย ซึ่งอาจมีความหลากหลาย ตั้งแต่ปัจเจกบุคคล บริษัทเอกชน และหน่วยงานสาธารณะ ไปจนถึงโครงสร้างพื้นฐานที่สำคัญ รัฐบาล และทรัพย์สินของกองทัพ

ความมั่นคงปลอดภัยไซเบอร์ เป็นประเด็นสำคัญที่เพิ่งเริ่มต้น ยังมีความสับสนในเชิงแนวคิดและคำศัพท์อยู่บ้าง คำศัพท์บางคำถูกใช้อภิปรายโดยยังไม่มีความชัดเจนในเชิงนโยบาย ไม่ว่าจะเป็นการจราจลไซเบอร์ (cyber–riots) การก่อการร้ายไซเบอร์ (cyberterrorism) การก่อวินาศกรรมไซเบอร์ (cybersabotage) ฯลฯ เช่น ผู้ก่อการร้ายไซเบอร์มักใช้เครื่องมือแบบเดียวกับอาชญากรไซเบอร์ แต่มีเป้าหมายที่ต่างกัน ในขณะที่อาชญากรไซเบอร์มีแรงจูงใจเป็นผลประโยชน์ด้านการเงิน ผู้ก่อการร้ายไซเบอร์มักมีเป้าหมายที่จะสร้างความปั่นป่วนและวุ่นวายครั้งใหญ่ในที่สาธารณะ

อย่างไรก็ตาม เป็นที่แน่ชัดว่า ทุกประเทศต่างตระหนักถึงภัยจากอาชญากรรมไซเบอร์ ซึ่งนอกจากจะมีความซับซ้อนเพิ่มขึ้นตามความก้าวหน้าทางเทคโนโลยี ยังเป็นภัยคุกคามที่แพร่ขยายได้รวดเร็วและไร้พรมแดน จากรายงานของ World Economic Forum ได้จัดอันดับความเสี่ยงระดับโลกประจำปี ค.ศ. 2019 (The Global Risks Report 2019) พบว่า การฉ้อโกงและโจรกรรมข้อมูล (Data fraud and theft) ถูกจัดอยู่ในอันดับที่ 4 และ การโจมตีไซเบอร์ (cyber–attack) อยู่ในอันดับที่ 5 ของ 10 อันดับความเสี่ยงที่มีผลกระทบกับการดำรงชีวิต และมีความเสี่ยงสูงที่จะจู่โจมทำลายโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศมากขึ้น ทำให้ประเทศต่างๆ หามาตรการในการป้องกันและรับมือกับภัยคุกคามไซเบอร์ รวมทั้งเสริมสร้างความร่วมมือกับหุ้นส่วนพันธมิตรทั้งในประเทศและระหว่างประเทศเพื่อป้องกัน รับมือ ฟื้นฟูความเสียหาย และแก้ไขปัญหาดังกล่าว

2.2 วรรณกรรมที่เกี่ยวข้อง

2.2.1 ประเภทของภัยคุกคามไซเบอร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) จัดตั้งขึ้นในปี 2543 (ชื่อเดิม ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย) โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ภายใต้สังกัดของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยี มีภาระหน้าที่หลักเพื่อ

ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

ในฐานะที่เป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/ Forum of Incident Response and Security Teams) ไทยเซิร์ต จึงมีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้ กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง ในปัจจุบันภารกิจของไทยเซิร์ตถูกโอนย้ายมาสังกัดอยู่ภายใต้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. และเปลี่ยนชื่อเป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย

จากเว็บไซต์ของไทยเซิร์ต ได้แบ่งประเภทภัยคุกคามออกเป็น 9 ประเภท ได้แก่

1) Abusive content (เนื้อหาที่ไม่เหมาะสม) หมายถึง การใช้หรือเผยแพร่ข้อมูลที่ไม่เป็นจริง หรือไม่ เหมาะสม เพื่อทำลายความน่าเชื่อถือ ก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามกอนาจาร หมิ่นประมาท รวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (Spam)

2) Availability (การโจมตีสภาพความพร้อมใช้งานของระบบ) หมายถึง การโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการ จนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ เช่น การโจมตีประเภท DDoS (Distributed Denial of Service) นอกจากนี้ยังรวมถึงการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า เป็นต้น

3) Fraud (ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) หมายถึง การฉ้อฉล ฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ เช่น การสร้างหน้าเว็บไซต์ปลอม (Phishing) ที่หลอกขโมยรหัสผ่านสำหรับล็อกอินจากผู้ใช้ การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ให้กับตนเอง

4) Information gathering (ความพยายามรวบรวมข้อมูลของระบบ) หมายถึง การพยายามรวบรวมข้อมูลจุดอ่อนของระบบ ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูล เกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้ง หรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User account) ที่มีอยู่บนระบบ รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social engineering)

5) Information security (การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต) หมายถึง การที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized

access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) รวมถึงนำข้อมูลที่รั่วไหลออกไปเผยแพร่ (Data leakage)

6) Intrusion attempts (ความพยายามบุกรุกเข้าระบบ) หมายถึง ความพยายามที่จะบุกรุกหรือเจาะเข้าระบบ ทั้งผ่านช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE–Common Vulnerabilities and Exposures) หรือผ่านช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบนี้ รวมถึงความพยายามจะบุกรุกหรือเจาะระบบด้วยวิธีการสุ่ม/เดาข้อมูล หรือ วิธีการทดสอบรหัสผ่านทุกค่า (Brute force)

7) Intrusions (การบุกรุกหรือเจาะระบบได้สำเร็จ) หมายถึง การที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้สำเร็จ ซึ่งผู้ประสงค์ร้ายสามารถควบคุมเครื่องและระบบ รวมไปถึงการปรับเปลี่ยนหน้าเว็บ (Web defacement)

8) Malicious code (โปรแกรมไม่พึงประสงค์) หมายถึง โปรแกรมหรือชุดคำสั่งที่ถูกพัฒนาขึ้นด้วยความประสงค์ร้าย เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบ เช่น Virus, Worm, Trojan หรือ Spyware

9) Other (อื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น) หมายถึง ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงประเภทใหม่ หรือ ไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น

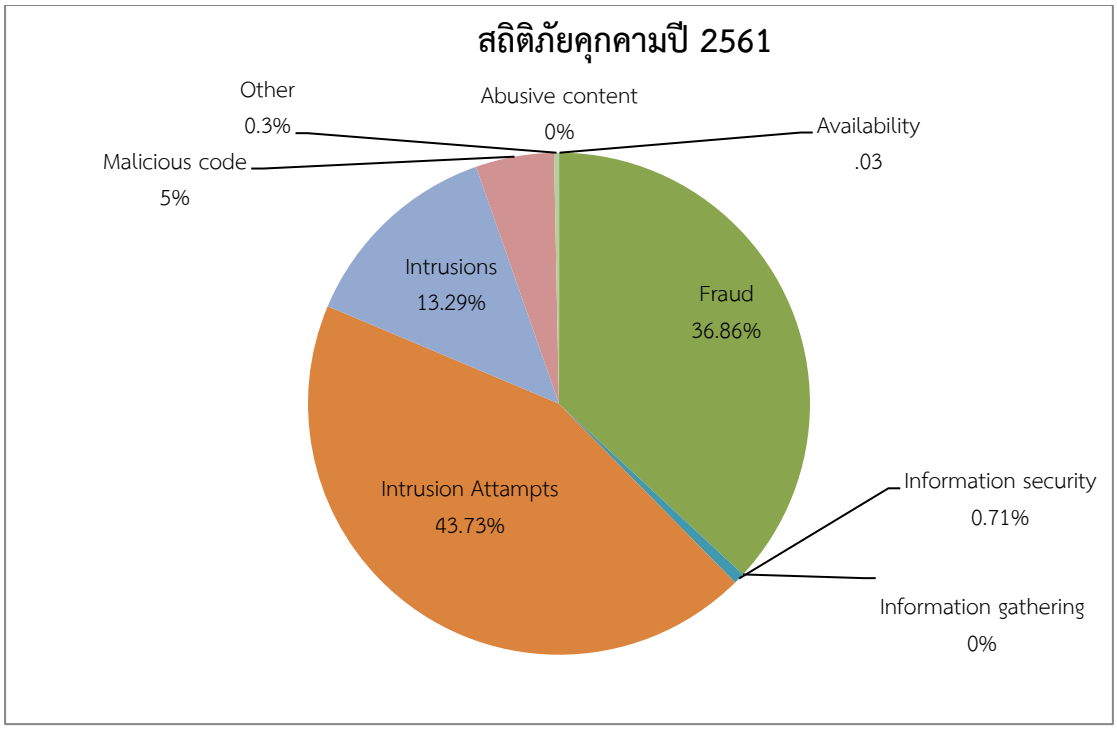
จากรายงานสถิติภัยคุกคาม ประจำปี พ.ศ. 2561 ตั้งแต่เดือนมกราคม–เดือนธันวาคม ที่ไทยเซิร์ต ได้รายงาน พบว่า มีจำนวนทั้งสิ้น 2,520 เรื่อง รายละเอียดแย่งตามประเภทได้ตามตารางที่ 1 ดังนี้

ตารางที่ 1 สถิติภัยคุกคามของไทยในปี 2561

ประเภทภัยคุกคาม	รวม
Abusive content	1
Availability	0
Fraud	929
Information gathering	0
Information security	18
Intrusion attempts	1,102
Intrusions	335
Malicious code	127
Others	8
รวม	**2,520**

ที่มา: ข้อมูลจากเว็บไซต์ ThaiCERT (https: thaicert.or.th)

ซึ่งหากคิดเป็นร้อยละของแต่ละประเภทของภัยคุกคาม ภัยคุกคามประเภท Intrusion attempts มีจำนวนสูงสุดคิดเป็นร้อยละ 43.73 อันดับที่ 2 คือ Fraud คิดเป็นร้อยละ 36.86 ตามภาพที่ 2



ภาพที่ 2 สถิติภัยคุกคามของไทยในปี 2561 คิดเป็นร้อยละ
ที่มา: ข้อมูลจากเว็บไซต์ ThaiCERT (https: thaicert.or.th)

จากการทบทวนวรรณกรรมที่เกี่ยวข้องพบว่า ประเภทของภัยคุกคามของแต่ละหน่วยงาน แต่ละประเทศ มีความแตกต่างกันในการเรียกชื่อประเภทของแต่ละภัยคุกคาม และมีการเรียกชื่อภัยคุกคามใหม่ๆ ที่เกิดขึ้นอยู่เสมอ Mark Hachman ได้สรุปผลการประชุมในงาน RSA Conference 2017 จัดขึ้นที่ซานฟรานซิสโก เมื่อวันที่ 16 กุมภาพันธ์ ปี ค.ศ. 2017 โดยมีการแปลเป็นภาษาไทยผ่านเว็บไซต์ http://www.csoonline.com/article/3170832/security/what-happens-if-your-thermostat-is-hacked-researchers-name-the-top-7-security-threats.html สรุปได้ว่าผู้เชี่ยวชาญจาก SANS Institute ได้ทำการจัดอันดับภัยคุกคามที่อันตรายที่สุดในโลก 7 รายการ ดังนี้

1) Ransomware

Ransomware ตัวแรกถูกคิดค้นเมื่อ 20 ปีก่อน และพัฒนาจนกลายเป็นภัยร้ายแรงพร้อมเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์ เหยื่อจำเป็นต้องจ่ายเงินค่าไถ่เพื่อแลกกับกุญแจสำหรับปลดรหัส Ransomware ในปัจจุบันแพร่กระจายไปทั่วโลก

2) การโจมตีบนอินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things หรือ IoT)

วิวัฒนาการถัดมาของผลิตภัณฑ์สำหรับผู้บริโภคคืออุปกรณ์ที่เชื่อมต่อหากันได้ สิ่งของตั้งแต่กล้องถ่ายรูปสำหรับเด็กไปจนถึงแปรงสีฟันใช้ Wi–Fi ในการสื่อสารระหว่างกันและเชื่อมต่อกับอินเทอร์เน็ต สิ่งที่ตามมาคือช่องโหว่จำนวนมากที่แฮ็คเกอร์สามารถโจมตีได้

3) Ransomware บนอุปกรณ์ IoT

เป็นการรวมระหว่างภัยคุกคามอันดับ 1 และ 2 ในเว็บไซต์ได้ยกตัวอย่างว่า เมื่อปี 2016 โรงแรมแห่งหนึ่งในประเทศออสเตรียถูกเจาะเข้าระบบคีย์การ์ดอิเล็กทรอนิกส์ไม่สามารถใช้งานได้ ทำให้แขกที่มาพักติดอยู่นอกห้องไม่สามารถเข้าไปได้

4) การโจมตีอุปกรณ์ระบบควบคุมของโรงงาน

ในปี ค.ศ. 2015 และ ค.ศ. 2016 มีผู้บุกรุกเข้าระบบและได้โจมตีและล่มระบบของสถานีจ่ายไฟฟ้าในประเทศยูเครน ทั้งเมืองเกือบเข้าสู่ภาวะไร้พลังงาน แต่พนักงานทราบเหตุเร็ว จึงได้ทำการสับเบรกเกอร์และฟื้นฟูระบบกลับคืนมา จากรายงาน พบว่าการโจมตีระบบโครงสร้างพื้นฐานสำคัญของประเทศมีความซับซ้อนและรับมือได้ยากขึ้นเรื่อยๆ

5) ระบบสุ่มตัวเลขเปราะบางเกินไป

การสุ่มตัวเลขถือว่าเป็นพื้นฐานสำคัญของการเข้ารหัสข้อมูล และอัลกอริธึมด้านความมั่นคงปลอดภัยหลายประเภท แต่ระบบสุ่มตัวเลขที่ใช้อยู่ในปัจจุบันไม่ใช่การ “สุ่ม” จริงๆ ทำให้การเข้ารหัสข้อมูลยังคงมีความเสี่ยงต่อการถูกทำลายได้ง่าย ถ้าแฮ็คเกอร์สามารถจับรูปแบบบางอย่างได้ปัญหานี้เป็นปัญหาสำหรับผู้ผลิตอุปกรณ์ต่างๆ ที่ต้องหามาตรการควบคุมเพิ่มเติม และในความเป็นจริงระบบที่ “มั่นคงปลอดภัย” ในชีวิตจริงอาจเปราะบางกว่าที่คิด

6) เชื่อมั่นใน Web Services มากเกินไป

แอพพลิเคชันและซอฟต์แวร์ในปัจจุบันมักเชื่อมต่อหรือทำงานร่วมกับบริการจากบุคคลที่สามมากขึ้น เช่น ระบบ Cloud Computing ซึ่งไม่มีหลักประกันที่มั่นใจได้ว่า บริการจากบุคคลที่สาม เหล่านั้นจะไม่ยุ่งเกี่ยวหรือทำอันตรายต่อข้อมูลของเรา

7) ภัยคุกคามบนฐานข้อมูล NoSQL

ปัญหาสำคัญสำหรับนักพัฒนาระบบ เนื่องจากฐานข้อมูล NoSQL ซึ่งเป็นเทคโนโลยีฐานข้อมูลที่ถูกออกแบบมาสำหรับงานเฉพาะและเป็นระบบฐานข้อมูลสำหรับงานที่ต้องรองรับข้อมูลขนาดใหญ่ๆ รองรับการขยายระบบได้ง่าย แต่มีข้อเสียคือความมั่นคงปลอดภัยยังไม่ดีเท่าที่ควร ส่งผลให้ข้อมูลที่อยู่ในฐานข้อมูลมีความเสี่ยงต่อภัยคุกคามรูปแบบต่างๆ

2.2.2 การจัดทำตัวชี้วัดในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

จากรายงานการจัดอันดับประเทศที่มีการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) ประจำปี ค.ศ. 2017 และ 2018 ที่จัดทำโดยสหภาพโทรคมนาคมระหว่างประเทศ (ITU) พบว่า ITU ได้จัดทำกรอบตัวชี้วัดแบ่งเป็น 5 เสาหลัก ได้แก่

1) ด้านกฎหมาย (legal) โดยวิเคราะห์จากกรอบกฎหมายที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

2) ด้านเทคนิค (technical) โดยวิเคราะห์จากกรอบงานทางเทคนิคที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

3) ด้านองค์กร (organizational) โดยวิเคราะห์จากสถาบัน องค์กร ที่ประสานงานเชิงนโยบาย และวิเคราะห์จากยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ

4) ด้านการเสริมสร้างศักยภาพ (capacity building) โดยวิเคราะห์จากการศึกษาวิจัยและการพัฒนา (R&D) การฝึกอบรม การรับรองหน่วยงานภาครัฐและหน่วยงานระดับมืออาชีพที่ส่งเสริมการพัฒนาศักยภาพ

5) ด้านความร่วมมือ (cooperation) โดยวิเคราะห์จากหุ้นส่วนพันธมิตร กรอบความร่วมมือ และเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง

โดยจะมีตัวชี้วัดย่อยรวมทั้งสิ้น 25 ตัว ตามตารางที่ 2 แบ่งตามน้ำหนักแต่ละตัวชี้วัด ดังนี้

ตารางที่ 2 ตัวชี้วัด GCI ของ ITU

No.	Indicators	Weighing
1.	Legal Measures	0.2
1.1	Cybercriminal Legislation	0.079
1.2	Cybersecurity Regulation	0.079
1.3	Containment/curbing of spam legislation	0.042
2.	Technical Measures	0.2
2.1	National, Government, Sectorial of CERT/CIRT/CSIRT	0.065
2.2	Cybersecurity Standards Implementation Framework for Organizations	0.035
2.3	Standardization Body	0.030
2.4	Technical mechanisms and capabilities deployed to address spam	0.024
2.5	Use of cloud for cybersecurity purpose	0.019
2.6	Child Online Protection mechanisms	0.027
3.	Organizational Measures	0.2
3.1	Strategy	0.092
3.2	Responsible Agency	0.063
3.3	Cybersecurity Metrics	0.045
4.	Capacity Building	0.2
4.1	Public Awareness Campaigns	0.036
4.2	Cybersecurity Standards and Certification for Professionals	0.027
4.3	Cybersecurity Professional Training Courses	0.032
4.4	National Education Programs and Academic Curriculums	0.032

No.	Indicators	Weighing
4.5	Cybersecurity Research & Development Programs	0.026
4.6	Incentive Mechanisms	0.024
4.7	Home Grown Cybersecurity Industry	0.023
5.	Cooperation	0.2
5.1	Bilateral Agreements	0.038
5.2	Multilateral Agreements	0.038
5.3	Participation of international fora/associations	0.036
5.4	Public–private partnership	0.034
5.5	Interagency/intra–agency partnerships	0.026
5.6	Cybersecurity best practices	0.028
	Total	**1**

ที่มา: Global Cybersecurity Index (GCI) 2018

2.2.3 การดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์

กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) ได้ประกาศใช้เมื่อวันที่ 2 มีนาคม ปี ค.ศ. 2018 ซึ่งเป็นกรอบกฎหมายในการควบคุมการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ โดยมีเป้าหมายหลัก 4 ประการ ได้แก่

1) เสริมสร้างการป้องกันโครงสร้างพื้นฐานและข้อมูลที่สำคัญ (CII) จากการโจมตีทางไซเบอร์

2) อนุญาตให้หน่วยงาน Cyber Security Agency (CSA) ป้องกันและตอบสนองต่อภัยคุกคามและเหตุการณ์ที่เกิดขึ้นในโลกไซเบอร์ โดยกฎหมายฉบับนี้ได้ให้อำนาจผู้บัญชาการของ CSA ในการตรวจสอบภัยคุกคามและเหตุการณ์ในโลกไซเบอร์เพื่อกำหนดผลกระทบของพวกเขาและป้องกันไม่ให้เกิดอันตรายเพิ่มเติมหรือเหตุการณ์ความมั่นคงปลอดภัยในโลกไซเบอร์เกิดขึ้น

3) กำหนดกรอบสำหรับการแบ่งปันข้อมูลด้านความปลอดภัยไซเบอร์

4) กำหนดกรอบในการออกใบอนุญาตสำหรับผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย CAS ใช้วิธีแบบ light–touch (การอนุญาตให้หน่วยงานผู้ขอรับอนุญาตใช้สิทธิ)

นอกจากนี้ สิงคโปร์ยังมีกฎหมายอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น Personal Data Protection Act 2012 รวมทั้งกฎระเบียบหรือแนวทางปฏิบัติจากหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญบางหน่วย เช่น “Telecommunication Cybersecurity Code of Practice” ของ Infocomm Media Development Authority (IMDA) เพื่อเตรียมความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของภาคโทรคมนาคม อีกตัวอย่าง ได้แก่ “Technology Risk Management Guidelines” ของ Monetary Authority of Singapore ซึ่งมีวัตถุประสงค์เพื่อปรับปรุงการจัดการความเสี่ยงของภาคการเงิน (ThaiCERT, 2018)

ในส่วนขององค์กรที่รับผิดชอบในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์อยู่ภายใต้การควบคุมของคณะรัฐมนตรี ได้แก่

1) Ministry of Communication and Information

(1) Info–Communications Media Development Authority ซึ่งมีหน่วยงาน Personal Data Protection Commission ร่วมดำเนินงานด้วย

(2) Cyber Security Agency มี SingCERT

21) Prime Minister's Office

(1) The National Security Coordination Secretariat

(2) The Smart Nation and Digital Government Group ซึ่งจะมีหน่วยงาน The Government Technology Agency of Singapore อยู่ภายใต้

จากรายงาน Singapore Cyber Landscape 2017 (Cyber Security Agency of Singapore, 2018) ได้ระบุถึงกลยุทธ์ในการสร้างความยืดหยุ่นให้แก่ระบบนิเวศน์ด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ ได้แก่

1) เพิ่มศักยภาพการเตรียมการในการรับมือกับภัยคุมคามไซเบอร์
2) เสริมสร้างความร่วมมือระหว่างประเทศ
3) พัฒนากำลังคนให้มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์
4) ส่งเสริมการวิจัยและพัฒนา (R&D)
5) สร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ให้กับทุกภาคส่วน

2.2.4 แนวทางการส่งเสริมความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน

การประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers' Meeting–TELMIN) ภายใต้กรอบการประชุมดังกล่าว มีการประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Senior Officials' Meeting–TELSOM) และมีการจัดตั้งกรอบการประชุม ASEAN Network Security Action Council (ANSAC) ที่ดำเนินการเกี่ยวกับด้านความมั่นคงปลอดภัยทางสารสนเทศในอาเซียนด้วย

ในส่วนของการประชุม ภายใต้ TELMIN และ TELSOM มีการดำเนินงานที่เกี่ยวข้องกับด้านไซเบอร์ โดยในปัจจุบันมีการดำเนินการประเด็นหลัก 2 เรื่อง ได้แก่ การจัดทำยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงปลอดภัยทางสารสนเทศ ระหว่างปี 2560–2563 (ASEAN Cybersecurity Cooperation Strategy 2016–2020) และการดำเนินการจัดตั้งศูนย์ความร่วมมืออาเซียน–ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN–Japan Cybersecurity Capacity Building Centre)

นอกจากนี้ ได้มีการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน (ASEAN ICT Master Plan) หรือ AIM เพื่อเป็นแนวทางการดำเนินความร่วมมือด้าน ICT ในภูมิภาคอาเซียน โดยแผนฉบับที่1 สิ้นสุดเมื่อปี ค.ศ. 2015 และปัจจุบันดำเนินการตามแผนฉบับที่ 2 (AIM 2020) สำหรับการดำเนินการ ระหว่างปี ค.ศ. 2016–2020

แผนแม่บท AIM 2020 ได้กำหนดวิสัยทัศน์ คือ การนำอาเซียนสู่ระบบเศรษฐกิจและสังคมที่ใช้ดิจิทัล อย่างมั่นคงปลอดภัย ยั่งยืน และสามารถปรับเปลี่ยนได้ อันจะก่อให้เกิดประชาคมอาเซียนที่ขับเคลื่อนด้วยนวัตกรรม มีความเท่าเทียมทั่วถึง และเป็นอันหนึ่งอันเดียวกัน

ประกอบด้วย 8 ยุทธศาสตร์ ดังนี้ (1) การรวมตัวและการปรับเปลี่ยนทางเศรษฐกิจ (2) การรวมตัวและการสร้างพลังของประชาชนด้วยไอซีที (3) การสร้างนวัตกรรม (4) การพัฒนาโครงสร้างพื้นฐานไอซีที (5) การพัฒนาทุนมนุษย์ (6) ไอซีทีในตลาดเดียว (7) สื่อและเนื้อหารูปแบบใหม่ และ (8) ความมั่นคงปลอดภัยทางสารสนเทศและการรับรองความปลอดภัยด้านข้อมูล

โดยยุทธศาสตร์ที่ 8 ความมั่นคงปลอดภัยทางสารสนเทศและและการรับรองความปลอดภัยด้านข้อมูล (Information Security and Assurance) จะมุ่งเน้นแนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยทางสื่อออนไลน์ที่เพิ่มสูงขึ้น ทั้งด้านเศรษฐกิจและสังคม จากซอฟต์แวร์ที่เป็นอันตราย การแฮ็ก การขโมยข้อมูล และกลโกงทางออนไลน์ ซึ่งภัยคุกคามดังกล่าวยังคงเป็นอุปสรรคในการก้าวสู่เศรษฐกิจดิจิทัลของอาเซียน ทั้งนี้ อาเซียนจะมุ่งเน้นการสร้างระบบนิเวศดิจิทัลที่มั่นคง เพื่อให้การติดต่อและแลกเปลี่ยนข้อมูลมีความปลอดภัย มั่นคง และเชื่อถือได้ โดยมีรายละเอียด ดังนี้

ข้อริเริ่ม 8.1 สร้างเสริมความมั่นคงปลอดภัยของข้อมูลในภูมิภาคอาเซียน
สร้างเศรษฐกิจดิจิทัลที่มั่นคงในภูมิภาคอาเซียน

แผนงาน	คำอธิบาย	เป้าหมาย/โครงการ
8.1.1 กำหนดหลักการป้องกันของข้อมูลในภูมิภาค	ส่งเสริมการปกป้องข้อมูลในภูมิภาคอาเซียนโดยกำหนดแนวทางในภูมิภาค	1. ศึกษาเปรียบเทียบกรอบการปกป้องข้อมูลส่วนบุคคลในอาเซียน ซึ่งจะช่วยกำหนดแนวทางปฏิบัติในปัจจุบัน จัดทำกรณีศึกษา และแบ่งแยกประเด็นในระดับต่าง ๆ เช่น ระดับท้องถิ่น ระดับประเทศ ระดับข้ามพรมแดน ระดับภูมิภาคอาเซียน 2. กำหนดแนวทางหรือกรอบการปกป้องข้อมูลส่วนบุคคลในภูมิภาคอาเซียน
8.1.2 กำหนดแนวปฏิบัติที่ดีที่สุดสำหรับความมั่นคงปลอดภัยในเครือข่ายภูมิภาค	กำหนดและจัดทำหลักการความมั่นคงปลอดภัยของเครือข่ายไอซีทีพื้นฐานเพื่อนำไปใช้ปฏิบัติในภูมิภาคอาเซียน	กำหนดแนวทางการศึกษาเพื่อความมั่นคงปลอดภัยของข้อมูลและเครือข่ายในภูมิภาคอาเซียน รวมทั้งการประมวลผลแบบคลาวด์
8.1.3 กำหนดแนวทางปฏิบัติในการฟื้นฟูโครงสร้างพื้นฐานข้อมูลสำคัญในภูมิภาค	ระบุโครงสร้างพื้นฐานข้อมูลสำคัญที่มีประเด็นกลยุทธ์และจัดหาวิธีป้องกันการโจมตีทางสื่อออนไลน์	ทำรายงานเพื่อระบุโครงสร้างพื้นฐานข้อมูลสำคัญที่มีอยู่ในปัจจุบัน และเสนอแนะแนวทางปฏิบัติที่เหมาะสมที่สุดในการปกป้องและตอบสนอง

ข้อริเริ่ม 8.2 สร้างความพร้อมด้านความมั่นคงปลอดภัยของข้อมูลในภูมิภาคอาเซียน *ปรับปรุงความร่วมมือและการตอบสนองต่อการแจ้งเหตุภัยคุกคามด้านคอมพิวเตอร์*		
แผนงาน	**คำอธิบาย**	**เป้าหมาย/โครงการ**
8.2.1 ส่งเสริมความร่วมมือในการตอบสนองต่อการแจ้งเหตุภัยคุกคามด้านคอมพิวเตอร์	ส่งเสริมความร่วมมือเพื่อสร้างเครือข่ายศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (CERT) เพื่อให้สามารถตอบสนองต่อการละเมิดความมั่นคงปลอดภัยทางสื่อออนไลน์ได้ในทันที	1. ศึกษาความเป็นไปได้ในการจัดตั้งศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (CERT) ในภูมิภาคอาเซียน และพิจารณารูปแบบการบริหารไม่ว่าโดยรัฐบาลของประเทศสมาชิกอาเซียนหรือความร่วมมือระหว่างภาครัฐ–เอกชน 2. จัดทำกรอบการรายงานเหตุการณ์ รวมถึงเทมเพลตและการตอบสนองที่เป็นมาตรฐานต่อ ‘ภัยคุกคามระดับต่าง ๆ’ และระบุประเภท 3. ส่งเสริมความร่วมมือเพื่อความมั่นคงปลอดภัยด้านคอมพิวเตอร์ระหว่างภาครัฐบาล ภาคธุรกิจ และประชาชน โดยการรณรงค์สร้างความรู้ความเข้าใจร่วมกันและการแลกเปลี่ยนสื่อต่าง ๆ

ที่มา: แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน ปี ค.ศ. 2020

2.2.5 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เสนอร่างพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งได้ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 มีทั้งหมด 83 มาตรา แบ่งเป็นบททั่วไป ได้แก่ วันบังคับใช้ นิยาม และผู้รักษาการ ประกอบด้วย 4 หมวด ดังนี้ หมวดที่ 1 คณะกรรมการ หมวดที่ 2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หมวดที่ 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ หมวดที่ 4 บทกำหนดโทษ และมีบทเฉพาะกาล หลักการสำคัญของพระราชบัญญัติคือ มุ่งที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ

พระราชบัญญัติได้กำหนดให้มีคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ และได้กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) และคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) รวมทั้ง กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีเลขาธิการคณะกรรมการ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะทำหน้าที่เป็นหน่วยงานธุรการของคณะกรรมการทั้ง 3 คณะ และมีหน้าที่สำคัญดังนี้

1) ส่งเสริม สนับสนุน งานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

2) ปฏิบัติการ ประสานงานเฝ้าระวัง แจ้งเตือน ให้ความช่วยเหลือ

3) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

5) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

6) ฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

7) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

ตามมาตรา 41–44 ได้กำหนดเกี่ยวกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

1) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

2) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

3) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

4) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

5) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

6) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน

7) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

8) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา 49 ได้กำหนดให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure หรือ CII) ได้แก่ (1) ด้านความมั่นคงของรัฐ (2) ด้านบริการภาครัฐที่สำคัญ (3) ด้านการเงินการธนาคาร (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (5) ด้านการขนส่งและโลจิสติกส์ (6) ด้านพลังงานและสาธารณูปโภค (7) ด้านสาธารณสุข และ (8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

ระดับของภัยคุกคามทางไซเบอร์ตามพระราชบัญญัตินี้แบ่งเป็น 3 ระดับ ได้แก่ (1) ภัยระดับไม่ร้ายแรง (2) ภัยระดับร้ายแรง และ (3) ภัยระดับวิกฤติ รายละเอียดตามภาพที่ 3

ภาพที่ 3 ระดับภัยคุกคามไซเบอร์
ที่มา: กองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

พระราชบัญญัตินี้ กำหนดให้มีพนักงานเจ้าหน้าที่ โดยมีหน้าที่และอำนาจเฉพาะที่กำหนดไว้ในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และในการปฏิบัติหน้าที่ต้องอยู่ภายใต้การกำกับดูแลของ กกม. และเลขาธิการ ทั้งนี้ หากเป็นการใช้อำนาจที่อาจละเมิดสิทธิ์ของประชาชน เช่น การเข้าตรวจค้น ยึด อุปกรณ์คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องจะทำได้เฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์เท่านั้น และต้องมีคำสั่งศาลก่อนเสมอ

ในส่วนของบทเฉพาะกาลมีสาระสำคัญดังนี้

1) ในวาระเริ่มแรก ให้ กมช. ประกอบด้วยประธานกรรมการและกรรมการโดยตำแหน่งและให้เลขาธิการ เป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช. ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้

2) ให้ดำเนินการเพื่อให้มี กกม. และ กบส. ภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช.

3) ให้ดำเนินการแต่งตั้งเลขาธิการตามระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ

4) ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

5) ระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ

6) ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

7) ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนด

8) เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่มีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับไปเป็นของสำนักงานตามพระราชบัญญัตินี้

2.2.6 บันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมในปัจจุบัน) แห่งราชอาณาจักรไทย และ กระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ในระหว่างการประชุม ASEAN Telecommunications & Information Technology Ministers Meeting (ASEAN TELMIN) ครั้งที่ 15 เมื่อเดือนพฤศจิกายน 2558 ณ เมืองดานัง สาธารณรัฐสังคมนิยมเวียดนาม รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (นายอุตตม สาวนายน–ในขณะนั้น) ได้หารือทวิภาคีกับรัฐมนตรีว่าการกระทรวงสื่อสารและสารสนเทศ (Ministry of Communications and Information: MCI) แห่งสาธารณรัฐสิงคโปร์ ทั้งสองฝ่ายได้หารือเกี่ยวกับการจัดทำบันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแห่งราชอาณาจักรไทยและกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสารซึ่งเสนอโดยฝ่ายสิงคโปร์ เพื่อส่งเสริมความร่วมมือด้านไอซีทีของประเทศไทยและสาธารณสิงคโปร์ และต่อมาได้มีการลงนามบันทึกความเข้าใจฯ เมื่อวันที่ 31 พฤษภาคม 2559

บันทึกความเข้าใจดังกล่าว มีวัตถุประสงค์เพื่อพัฒนาความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสารระหว่างกัน ซึ่งภายใต้วรรค 1 ขอบเขตความร่วมมือ ได้ระบุว่า ประเทศภาคีจะพยายามที่จะร่วมมือกันในสาขา ICT ตามบันทึกฉบับนี้ ด้วยวัตถุประสงค์นี้ ประเทศภาคีอาจร่วมกันกำหนดโครงการความร่วมมือ 1 โครงการหรือมากกว่า ความร่วมมือดังกล่าวอาจรวมถึง

1) การแบ่งปันประสบการณ์และความรู้ด้านการพัฒนารัฐบาลอิเล็กทรอนิกส์

2) การแลกเปลี่ยนทัศนะเกี่ยวกับความรู้และการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์

3) การแลกเปลี่ยนทัศนะและความร่วมมือในการยกระดับระบบนิเวศน์ด้วยธุรกิจเกิดใหม่ด้านเทคโนโลยีดิจิทัล

4) การจัดหรือการอำนวยความสะดวกการฝึกอบรมและโปรแกรมการพัฒนาความสามารถ

5) การแลกเปลี่ยนประสบการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

6) ความร่วมมือในสาขาอื่นๆ ที่อยู่ในความสนใจของประเทศภาคี

นอกจากนี้ วรรค 2 ของบันทึกความเข้าใจฯ ได้กำหนดเกี่ยวกับความตกลงโดยเฉพาะ (Specific Agreement) ดังนี้

1) เนื่องจากข้อจำกัดทางกฎหมายของทั้งสองประเทศ ดังนั้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแห่งราชอาณาจักรไทยและกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ อาจจัดทำความตกลงแยกกันเพื่อดำเนินโครงการหรือกิจกรรมภายใต้ขอบเขตของบันทึกความเข้าใจฉบับนี้

2) ความตกลงภายใต้ข้อ 1 ของวรรคนี้ อาจมีการดำเนินการในทางใดทางหนึ่งระหว่างประเทศภาคีและหน่วยงานภาครัฐของอีกประเทศภาคี และหน่วยงานภาครัฐที่เกี่ยวข้องของประเทศภาคีหรือของแต่ละบริษัทในเครือ หรือหน่วยงานภาครัฐที่เกี่ยวข้องของประเทศภาคีและหน่วยงานภาครัฐที่เกี่ยวข้องของอีกประเทศภาคีหรือแต่ละบริษัทในเครือของคู่ภาคี

ทั้งนี้ บันทึกความเข้าใจฯ มีผลใช้บังคับในวันที่ลงนามโดยประเทศภาคี และมีผลใช้บังคับเป็นระยะเวลา 36 เดือนหลังจากนั้น เว้นแต่ประเทศภาคีฝ่ายใดฝ่ายหนึ่งจะขอยุติโดยแจ้งเป็นลายลักษณ์อักษรแก่อีกฝ่ายหนึ่งล่วงหน้าเป็นเวลา 6 เดือน

2.3 สรุปกรอบแนวคิด

ปัจจุบันหลายประเทศกำลังก้าวสู่เศรษฐกิจดิจิทัล ซึ่งมีเทคโนโลยีและนวัตกรรมเป็นตัวขับเคลื่อน เทคโนโลยีดิจิทัลที่มีบทบาทสำคัญคือการใช้อินเทอร์เน็ต ซึ่งนอกจากจะมาพร้อมกับโอกาสแล้วยังมาพร้อมกับความท้าทายและภัยคุกคามซึ่งมีอยู่หลายรูปแบบ หลายประเทศจึงต้องมีการกำหนดนโยบายในเรื่องความมั่นคงปลอดภัยไซเบอร์เพื่อไม่ให้ภัยคุกคามดังกล่าวมาเป็นอุปสรรคในการเติบโตของเศรษฐกิจดิจิทัล รวมทั้งสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัล ในส่วนของประเทศไทยก็ให้ความสำคัญกับนโยบายดังกล่าวและอยู่ในช่วงเริ่มต้นของการดำเนินการ การศึกษานี้จะศึกษาปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ โดยจะพิจารณาจากตัวชี้วัดสำคัญ 5 เสาหลัก ที่เป็นส่วนประกอบสำคัญที่สหภาพโทรคมนาคมระหว่างประเทศได้กำหนดไว้และนำมาพิจารณาเปรียบเทียบกับการดำเนินงานของไทยเพื่อจัดทำเป็นข้อเสนอแนะตามที่ระบุไว้ในวัตถุประสงค์ของการศึกษา

บทที่ 3
ผลการศึกษา

3.1 พัฒนาการในการดำเนินนโยบายความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์

สิงคโปร์เป็นประเทศที่มีการติดต่อสื่อสารและมีการใช้เทคโนโลยีสารสนเทศและการใช้อินเทอร์เน็ตสูงทั้งการติดต่อสื่อสารภายในและระหว่างประเทศ และยังเป็นศูนย์กลางการค้า การเงิน และการขนส่ง โดยเฉพาะอย่างยิ่ง เมื่อประเทศสิงคโปร์ได้ประกาศนโยบาย “Smart Nation” ซึ่งมีเป้าหมายที่จะทำให้ประเทศก้าวหน้ายิ่งขึ้นด้วยเทคโนโลยีเพื่อนำไปสู่ความกินดีอยู่ดีของประชาชนอย่างมีนัยสำคัญ ทำให้การเชื่อมโยงดิจิทัลนำไปสู่การรวมเป็นหนึ่งเดียวของชุมชนได้อย่างเข้มแข็ง รวมทั้งพลังอำนาจของโครงข่าย ข้อมูล และเทคโนโลยีสารสนเทศ ที่เสริมสร้างโอกาสทางเศรษฐกิจ โดยให้ทุกภาคส่วนและประชาชนมีส่วนร่วมในการดำเนินงานร่วมกัน โดยนายกรัฐมนตรีของสิงคโปร์ Lee Hsien Loong ได้เน้นย้ำว่า ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นส่วนสำคัญยิ่งต่อระบบนิเวศน์ของ Smart Nation ของสิงคโปร์

ผลการศึกษาพบว่า รัฐบาลสิงคโปร์มีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนการพัฒนาเศรษฐกิจและสังคม จึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์มีการดำเนินการอย่างจริงจัง ต่อเนื่อง และเป็นระบบ เริ่มตั้งแต่ ปี ค.ศ. 2005 หน่วยงานกำกับดูแล Info–communications Development Authority หรือ IDA (ซึ่งปัจจุบันเปลี่ยนเป็น Info–communications and Media Development Authority หรือ IMDA) ได้จัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์ ฉบับแรก คือ Infocomm Security Masterplan 2005–2007 สาระสำคัญของแผนแม่บทเพื่อประสานงานระหว่างหน่วยงานของรัฐในเรื่องความมั่นคงปลอดภัยไซเบอร์ โดยให้ความสำคัญอันดับแรกคือการเสริมสร้างความสามารถในหน่วยงานภาครัฐในการบรรเทา และรับมือกับภัยคุกคามไซเบอร์

ปี ค.ศ. 2008 ได้ประกาศแผนแม่บทฯ ฉบับที่ 2 สำหรับปี 2008–2012 ซึ่งเป็นแผนแม่บทที่มุ่งเน้นเรื่องการรักษาความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Infrastructure Information หรือ CII) ของสิงคโปร์ ภายใต้วิสัยทัศน์การทำให้สิงคโปร์เป็นศูนย์กลางความมั่นคงปลอดภัยและไว้วางใจได้ “Secure and Trusted Hub”

ในปี ค.ศ. 2009 สิงคโปร์ได้จัดตั้งหน่วยงาน Infocomm Technology Security Authority (SITSA) ภายใต้กระทรวงกิจการภายใน (Ministry of Home Affairs) มีหน้าที่ป้องกันการถูกโจมตีทางไซเบอร์ การเตรียมความพร้อมอย่างเชี่ยวชาญ รวมทั้งการรักษาความมั่นคงปลอดภัย CII ของประเทศ จากภัยคุมคามไซเบอร์

ปี ค.ศ. 2013 ได้ประกาศใช้แผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 3 ครอบคลุมระบบนิเวศน์สารสนเทศและการสื่อสารกว้างขึ้น ทั้งภาคเอกชน และปัจเจกบุคคล ไม่เฉพาะเพียง CII เพื่อให้สิงคโปร์เป็นศูนย์กลางสารสนเทศและการสื่อสารที่มั่นใจและเข็มแข็งได้

นอกจากนี้ รัฐบาลยังได้จัดตั้งโครงการวิจัยและพัฒนาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (The National Cybersecurity R&D Programme) โดยมีวัตถุประสงค์เพื่อปรับปรุงโครงสร้างพื้นฐานความมั่นคงปลอดภัยไซเบอร์ให้มีความมั่นคงปลอดภัย ไว้วางใจได้ ความสามารถในการฟื้นตัวหลังเกิดเหตุและสามารถใช้งานได้อย่างมีประสิทธิภาพ โดยทำงานร่วมกับ National Research Foundation และ Cybersecurity Agency of Singapore

ปี ค.ศ. 2014 National Cyber Security Centre (NCBC) ได้ก่อตั้งขึ้น โดยเป็นส่วนหนึ่งของ SITSA เพื่อเฝ้าระวังสถานการณ์ไซเบอร์หรือเหตุการณ์ที่เกี่ยวเนื่องกับความมั่นคงปลอดภัยไซเบอร์อย่างมีนัยสำคัญ ของหน่วยงานต่างๆ รวมทั้งประสานงานในลักษณะข้ามองค์กรหรือหน่วยงานกับหน่วยงานหลักต่างๆ เพื่อให้ข้อมูลการตอบสนองและรับมือเหตุการณ์ไซเบอร์ในระดับชาติ

ปี ค.ศ. 2015 เป็นปีสำคัญ ที่มีการจัดตั้งหน่วยงาน Cyber Security Agency of Singapore (CSA) ภายใต้สำนักนายกรัฐมนตรี และบริหารจัดการโดยกระทรวงสารสนเทศและการสื่อสาร (Ministry of Communications and Information หรือ MCI) โดยมีการรวมหน่วยงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ได้แก่ (1) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (Singapore Computer Emergency Response Team หรือ SingCERT) และ (2) หน่วยงานจัดทำแผนแม่บทฯ จาก IDA และ SITA เข้าเป็นหน่วยงานเดียว

นอกจากนี้ ในปี ค.ศ. 2015 กระทรวงกิจการภายในยังได้ก่อตั้งหน่วยบัญชาการอาชญากรรมไซเบอร์ Cybercrime Command เป็นหน่วยงานภายใต้กรมสืบสวนอาชญากรรม (Criminal Investigation Department หรือ CID) ภายใต้สำนักงานตำรวจ หน่วยบัญชาการฯ จะทำงานอย่างใกล้ชิดกับหน่วยงานบังคับใช้กฎหมายอื่นๆ และผู้มีส่วนได้ส่วนเสียของภาคอุตสาหกรรม รวมทั้ง INTERPOL Global Complex for Innovation ตั้งอยู่ที่สิงคโปร์ เพื่อสืบสวนเกี่ยวกับอาชญากรรมไซเบอร์

สิงคโปร์ยังได้ประกาศใช้แผนปฏิบัติการต่อต้านอาชญากรรมไซเบอร์แห่งชาติ (National Cybercrimes Action Plan) เมื่อเดือนกรกฎาคม ปี ค.ศ. 2016 โดยกระทรวงกิจการภายในได้กำหนดแผนปฏิบัติที่จัดลำดับความสำคัญที่จำเป็นในการต่อสู้กับอาชญากรรมไซเบอร์ ซึ่งรวมถึง (ก) ความจำเป็นในการให้การศึกษาแก่ประชาชนว่าทำอย่างไรให้อยู่ในโลกไซเบอร์อย่างปลอดภัย (ข) การพัฒนาความสามารถในการต่อสู้กับอาชญากรรมไซเบอร์ (ค) การเสริมสร้างความแข็งแกร่งของกฎหมายที่เกี่ยวกับอาชญากรรมไซเบอร์ และ (ง) การสร้างหุ้นส่วนพันธมิตรทั้งในระดับท้องถิ่นและในระดับระหว่างประเทศ

ในปี ค.ศ. 2017 มีการแก้ไขกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์และการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse and Cybersecurity Act) โดยกำหนดให้การกระทำต่อไปนี้เป็นการกระทำผิดกฎหมายด้วย (ก) กระทำการเพื่อได้มาซึ่งข้อมูลส่วนบุคคลอย่างผิดกฎหมาย โดยมีวัตถุประสงค์ที่มิชอบด้วยกฎหมาย (ข) การมีเครื่องมือที่ใช้สำหรับเจาะข้อมูล (ซึ่งรวมถึงเครื่องมือทางกายภาพ ซอล์ฟแวร์ และรหัสผ่าน) เพื่อกระทำผิดกฎหมายผ่านไซเบอร์ และ (ค) กระทำอาชญากรรมที่ก่อให้เกิดความเสี่ยงที่เป็นอันตรายต่อสิงคโปร์ แม้จะอยู่ในต่างประเทศ

กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) มีผลบังคับใช้เมื่อวันที่ 2 มีนาคม ปี ค.ศ. 2018 ซึ่งเป็นกรอบกฎหมายสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2 การวิเคราะห์ปัจจัยความสำเร็จของสิงคโปร์

ในเวทีระหว่างประเทศได้มีความพยายามในการจัดทำกรอบในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ โดยในปี ค.ศ. 2007 สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้จัดทำ Global Cybersecurity Agenda ขึ้น เพื่อให้ประเทศสมาชิกใช้เป็นแนวทางในการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์ และเมื่อปี ค.ศ. 2014 ได้เริ่มจัดทำรายงานลำดับประเทศสมาชิก ITU ที่มีการดำเนินนโยบายอย่างจริงจังในเรื่องความมั่นคงปลอดภัยไซเบอร์ โดย ITU ได้กำหนดดัชนีตัวชี้วัดออกเป็น 5 ด้าน ดังนี้

1) ด้านกฎหมาย (legal measures) โดยวิเคราะห์จากกรอบกฎหมายที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

2) ด้านเทคนิค (technical measures) โดยวิเคราะห์จากกรอบงานทางเทคนิคที่มีอยู่จริงในการเผชิญปัญหาภัยคุกคามไซเบอร์

3) ด้านองค์กร (organizational measures) โดยวิเคราะห์จากสถาบัน องค์กรที่ประสานงานเชิงนโยบาย และวิเคราะห์จากยุทธศาสตร์ชาติในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

4) ด้านการเสริมสร้างศักยภาพ (capacity building) โดยวิเคราะห์จากการศึกษาวิจัยและการพัฒนา (R&D) การฝึกอบรม การรับรองหน่วยงานภาครัฐและหน่วยงานระดับมืออาชีพที่ส่งเสริมการพัฒนาศักยภาพ

5) ด้านความร่วมมือ (cooperation) โดยวิเคราะห์จากหุ้นส่วนพันธมิตร กรอบความร่วมมือและเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง

ITU ได้ทำรายงานผลการจัดอันดับครั้งแรกในปี ค.ศ. 2014 และครั้งที่ 2 ในปี 2017 และล่าสุดในปี 2018 ซึ่ง ITU ได้มีการปรับตัวชี้วัดย่อยซึ่งมีทั้งสิ้น 25 ตัว และปรับค่าน้ำหนักในแต่ละตัวชี้วัดหลักจากเดิมตัวละ 1.000 เป็นตัวชี้วัดละ 0.2 อย่างไรก็ดี ผลคะแนนรวมจะอยู่ที่ 1.000 เช่นกัน โดยผลปรากฏว่าประเทศสิงคโปร์มีผลการดำเนินการในเรื่องความมั่นคงปลอดภัยไซเบอร์ติดอันดับ 4 ของภูมิภาคเอเชียและแปซิฟิก และอันดับ 6 ของโลก ในปี ค.ศ. 2014 และในปี 2017 สิงคโปร์มีพัฒนาการก้าวกระโดด ขึ้นมาเป็นอันดับ 1 ของภูมิภาคฯ และของโลก และในปี ค.ศ. 2018 อันดับโลกของสิงคโปร์ตกลงมาเป็นอันดับที่ 6 แต่ยังคงเป็นอันดับ 1 ของภูมิภาค รายละเอียดปรากฏตามตารางที่ 3

ตารางที่ 3 คะแนนและอันดับของประเทศสิงคโปร์ในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

ปี	ด้านกฎหมาย	ด้านเทคนิค	ด้านองค์กร	ด้านเสริมสร้างศักยภาพ	ด้านความร่วมมือ	คะแนนรวม	อันดับในภูมิภาค	อันดับโลก
2014	0.7500	0.6667	0.7500	0.7500	0.5000	0.6765	4	6
2017	0.95	0.96	0.88	0.97	0.87	0.92	1	1
2018	0.200 (1.000)	0.186 (0.93)	0.192 (0.96)	0.195 (0.975)	0.125 (0.625)	0.898	1	6

ที่มา: ITU Global Cybersecurity Index (GCI) 2014, 2017 and 2018

ผลการศึกษาโดยวิเคราะห์ตามตัวชี้วัดหลักทั้ง 5 ตัว มีดังนี้

3.2.1 ด้านกฎหมาย (Legal Measures)

จากการศึกษาพบว่ารัฐบาลสิงคโปร์ให้ความสำคัญกับการออกกฎหมายกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เนื่องจากเป็นเครื่องมือสำคัญในการดำเนินการและเป็นกรอบกฎหมายที่กำหนดนโยบาย ขั้นตอนดำเนินการ และแนวทางปฏิบัติ เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการ โดยมีแผนแม่บทและกฎหมายอื่นที่เกี่ยวข้องไม่ว่าจะเป็นกฎหมายเกี่ยวกับการแทรกแซงระบบคอมพิวเตอร์ กฎหมายเกี่ยวกับข้อมูล รวมทั้งการกำหนดกฎระเบียบหรือแนวทางปฏิบัติเกี่ยวกับการป้องกันข้อมูล การแจ้งเมื่อมีการละเมิดข้อมูล การให้ประกาศนียบัตรหรือใบรับรองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการตรวจสอบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล การโอนเงินและการทำธุรกรรมอิเล็กทรอนิกส์ โดยรัฐบาลได้มีการแก้ไขและออกกฎหมายและกฎระเบียบอย่างต่อเนื่องและโดยที่เทคโนโลยีดิจิทัลมีพัฒนารวดเร็ว ดังนั้น รัฐบาลสิงคโปร์จึงให้ความสำคัญกับขั้นตอนก่อนการตรากฎหมายหรือกฎระเบียบต่างๆ โดยมีการหารือและทำการศึกษากับทุกภาคส่วนที่เกี่ยวข้อง รวมทั้งนักวิชาการ นักเทคนิค สถาบันการศึกษา และสถาบันวิจัย

แผนแม่บทและกฎหมายที่สำคัญของสิงคโปร์ ได้แก่ แผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์ ฉบับแรก คือ Infocomm Security Masterplan 2005–2007 สาระสำคัญของแผนแม่บทเพื่อประสานงานระหว่างหน่วยงานของรัฐในเรื่องความมั่นคงปลอดภัยไซเบอร์ โดยให้ความสำคัญอันดับแรกคือการเสริมสร้างความสามารถในหน่วยงานภาครัฐในการบรรเทา และรับมือกับภัยคุกคามไซเบอร์ ต่อมา ปี ค.ศ. 2008 ได้ประกาศแผนแม่บทฯ ฉบับที่ 2 สำหรับปี 2008–2012 ซึ่งเป็นแผนแม่บทที่มุ่งเน้นเรื่องการรักษาความมั่นคงปลอดภัยต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Infrastructure Information หรือ CII) ของสิงคโปร์ ในปี ค.ศ. 2013 ได้ประกาศใช้แผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฉบับที่ 3 ครอบคลุมระบบนิเวศน์สารสนเทศและการสื่อสารกว้างขึ้น ทั้งภาคเอกชน และปัจเจกบุคคล ไม่เฉพาะเพียง CII เพื่อให้สิงคโปร์เป็นศูนย์กลางสารสนเทศและการสื่อสารที่มั่นใจและเข็มแข็งได้ นอกจากนี้ สิงคโปร์ยังได้ประกาศใช้แผนปฏิบัติการต่อต้านอาชญากรรมไซเบอร์แห่งชาติ (National Cybercrimes Action Plan) เมื่อเดือนกรกฎาคม ปี ค.ศ. 2016 โดยกระทรวงกิจการภายใน และในปี ค.ศ. 2017 มีการแก้ไขกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์และการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse and Cybersecurity Act) การดำเนินการอย่างจริงจัง ครอบคลุม และต่อเนื่องดังกล่าวสอดคล้องกับผลคะแนนตัวชี้วัดด้านกฎหมายของสิงคโปร์ โดยมีคะแนนขึ้นจาก 0.75 ในปี ค.ศ. 2014 เป็น 0.95 ในปี ค.ศ. 2017 และเมื่อกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) มีผลบังคับใช้เมื่อวันที่ 2 มีนาคม ค.ศ. 2018 ซึ่งเป็นกรอบกฎหมายสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงทำให้คะแนนของสิงคโปร์ในส่วนของตัวชี้วัดด้านกฎหมาย ในปี ค.ศ. 2018 ได้คะแนนเต็ม 0.2000 โดยภายใต้กฎหมายฉบับนี้ได้มีการกำหนดนโยบาย หน้าที่หน่วยงานที่เกี่ยวข้อง ขั้นตอนปฏิบัติในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุมคามไซเบอร์ และการฟื้นตัวหลังเกิดเหตุการณ์ บทลงโทษ อย่างชัดเจน แต่ปัจจัยที่สำคัญที่สุดคือ 1 ใน 4 ยุทธศาสตร์หลัก คือการกำหนดกรอบในการออกใบอนุญาตสำหรับผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดย CAS

ใช้วิธีแบบ light–touch (การอนุญาตให้หน่วยงานผู้ขอรับอนุญาตใช้สิทธิ) ซึ่งสิงคโปร์เป็นประเทศแรกที่มีการออกกฎหมายสำหรับใบอนุญาตในรูปแบบนี้

หน่วยงานปฏิบัติสำคัญคือ Cyber Security Agency ก็ได้มีการออกกรอบดำเนินการและคู่มือต่างๆ เพื่อให้หน่วยงานที่เกี่ยวกข้องได้นำไปปฏิบัติ เช่น Security–by–Design Framework เพื่อเป็นแนวทางให้หน่วยงาน CII พัฒนาระบบรักษาความปลอดภัย และ Security–by–Design Framework Checklist ซึ่งเป็นกรอบในการทำ worksheet ในแต่ละขั้นตอนสำหรับผู้ปฏิบัติงานรักษาความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ ตามกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ยังได้กำหนดให้มีการทำงานไปในทิศทางเดียวกับกฎหมายอื่นๆ ที่มีอยู่รวมทั้งทำงานร่วมกับหน่วยงานกำกับดูแลอิสระอื่นที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการใช้คอมพิวเตอร์ในทางที่ผิด (Computer Misuse Act) กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act 2012) แนวทางการจัดการการล่วงละเมิดข้อมูล (Guide to Managing Data Breaches) แนวทางการรักษาความปลอดภัยข้อมูลส่วนบุคคล แนวทางการสร้างเว็บไซต์สำหรับวิสาหกิจขนาดกลางและขนาดย่อม (Guide to Building Websites for small and medium–sized enterprises (SMEs)) เป็นต้น

3.2.2 ด้านเทคนิค (Technical Measures)

เนื่องจากภัยคุกคามไซเบอร์มีการพัฒนาไปตามเทคโนโลยีที่ก้าวหน้าไปอย่างรวดเร็ว รวมทั้งมีรูปแบบและความซับซ้อนมากขึ้น และจะทวีความรุนแรงมากขึ้นเมื่อมีการใช้เทคโนโลยี 5G และ Internet of Things (IoT) อย่างเต็มรูปแบบ สิงคโปร์ตระหนักและให้ความสำคัญกับการพัฒนาเทคโนโลยีการสื่อสารโทรคมนาคมและเทคโนโลยีใหม่ๆ เพื่อให้เท่าทันและสามารถป้องกันและรับมือกับภัยคุมคามไซเบอร์ โดยการจัดสรรงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ มีรายงานจาก www.fticonsultanting.com ว่า สิงคโปร์ได้ลงทุนในเรื่องความมั่นคงปลอดภัยไซเบอร์จำนวน 2.82 พันล้านเหรียญสิงคโปร์ จากการศึกษารายงาน Singapor Cyber Landscape 2017 ซึ่งจัดทำโดย Cyber Security Agency, Singapore พบว่า ในปี ค.ศ. 2017 หน่วยงานรัฐบาลเผชิญกับภัยคุกคามไซเบอร์รวมถึงการบุกรุกเข้าระบบและเว็บไซต์หลอกลวง ดังนั้น เพื่อลดโอกาสในการเกิดจู่โจมไซเบอร์ทางอินเทอร์เน็ตและเพื่อป้องกันระบบและข้อมูลของประชาชน ในปี ค.ศ. 2017 สิงคโปร์ได้กำหนดให้หน่วยงานรัฐบาลแยกการใช้อินเทอร์เน็ตหรือการท่องอินเทร์เน็ต (internet surfing) จากโครงข่ายของรัฐบาล ซึ่งมีรายงานว่ามีจำนวนคอมพิวเตอร์ของภาครัฐถึง 100,000 เครื่อง ที่ต้องทำการล้างเครื่องใหม่ทั้งหมด และห้ามใช้ internet surfing

เพื่อป้องกันระบบข้อมูลของหน่วยงานภาครัฐ สิงคโปร์กำหนดจะจัดตั้ง Government Security Operations Centre ที่มีอุปกรณ์ปัญญาประดิษฐ์ (Artificial intelligence หรือ AI) และระบบการวิเคราะห์แบบก้าวหน้า ภายในปี ค.ศ. 2020 แทนศูนย์เฝ้าระวังไซเบอร์ (Cyber Watch Centre) ในปัจจุบัน นอกจากนี้ สิงคโปร์ยังกระตุ้นให้หน่วยงานภาครัฐและเอกชนจัดสรรเงินจำนวนร้อยละ 8 ของงบประมาณในส่วนเทคโนโลยีสารสนเทศ (IT) เพื่อใช้สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งถือว่าเป็นการลงทุนในการจัดการความเสี่ยง

ปัจจัยสำคัญอีกประการหนึ่งที่สิงคโปร์ประสบความสำเร็จในตัวชี้วัดเทคนิคคือ การมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT) ซึ่งมีหน้าที่ประกาศเตือน และแนะนำการปฏิบัติงานเชิงเทคนิคเมื่อเกิดเหตุ ส่งเสริมการสร้างความตระหนักรู้ผ่านการสัมมนา ประชุมปฏิบัติการ และการซ้อมรับมือกับสถานการณ์จริง (cyber drills) และร่วมมือกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์อื่นๆ เพื่อรับมือกับเหตุเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดย่อยหนึ่งของตัวชี้วัดเทคนิคคือ การมีกรอบมาตรฐานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานต่างๆ และการมีองค์ที่จัดทำด้านมาตรฐาน ในปี ค.ศ. 2013 IMDA ของสิงคโปร์ได้ร่วมมือกับวิสาหกิจและภาคอุตสาหกรรมของสิงคโปร์ในการพัฒนามาตรฐานระบบคลาวด์หลายชั้น (multi–tiered cloud computing) ครั้งแรกของโลก ที่จัดการการให้บริการ cloud ด้านความมั่นคงปลอดภัย ที่จัดหาโดยหน่วยงานภาครัฐและเอกชน มาตรฐานใหม่นี้จัดหาให้ในระดับความมั่นคงปลอดภัยที่แตกต่างกันขึ้นอยู่กับระดับความสามารถของผู้ให้บริการที่จะสามารถให้ผู้ใช้บริการ นอกจากนี้ สภามาตรฐานอุตสาหกรรมสิงคโปร์ (Singapore Standards Council) ยังได้เริ่มพัฒนามาตรฐานใหม่ๆ ที่ปัจจุบันยังไม่มีในระดับระหว่างประเทศ ซึ่งรวมถึงมาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับยานพาหนะไร้คนขับ และข้อกำหนดทั่วไปสำหรับความมั่นคงปลอดภัยใน IoT ในโครงการ Smart Nation ของสิงคโปร์ ในปี ค.ศ. 2018 สิงคโปร์ได้ออก Industrial Control Systems Cybersecurity Guidelines สำหรับผู้ประกอบการในระบบควบคุมอุตสาหกรรม (CIS) ซึ่งเป็นข้อแนะนำและแนวทางปฏิบัติในการปรับปรุงกระบวนการและการควบคุมระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ในระบบแต่ละอุตสาหกรรม เช่น น้ำ พลังงาน การขนส่งทางถนน และการขนส่งทางทะเล เป็นต้น

สิงคโปร์ยังพัฒนามาตรฐานด้าน Cybersecurity สู่ระดับสากล จากเว็บไซต์ https://www.zdnet.com/article/singapore-now-able-to-certify-global-cybersecurity-standard/ พบว่า สิงคโปร์กลายเป็น 1 ใน 18 ประเทศที่สามารถออกใบรับรองผลิตภัณฑ์ที่ผ่านมาตรฐานสากลของการตรวจสอบด้าน Cybersecurity ทำให้ผู้พัฒนาผลิตภัณฑ์ในประเทศสามารถรับใบรับรองได้รวดเร็วมากขึ้นและลดค่าใช้จ่าย รัฐบาลสิงคโปร์กล่าวว่า การที่สิงคโปร์สามารถออกใบรับรองได้เองนั้น จะส่งเสริมการแข่งขันในตลาดโลกได้ Common Criteria หรือ CC เป็นเป็นมาตรฐานด้านเทคนิคที่ใช้รับรองและตรวจสอบผลิตภัณฑ์ด้าน Cybersecurity โดยสิงคโปร์เป็น 1 ใน 18 ประเทศที่สามารถออกใบรับรอง CC ได้ ซึ่งรวมถึง อินเดีย มาเลเซีย ออสเตรเลีย เยอรมนี ฝรั่งเศส และสหราชอาณาจักร โดยอีก 12 ประเทศ สามารถรับใบรับรองดังกล่าวแสดงมาตรฐานของผลิตภัณฑ์ แต่ไม่สามารถออกใบรับรองเองได้ อาทิ อินโดนีเซีย กรีซ และอิสราเอล ทั้งนี้ CSA สิงคโปร์เป็นหน่วยงานที่ตรวจสอบและออกใบรับรองดังกล่าว และเป็นผู้ประเมินผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐาน นักพัฒนาผลิตภัณฑ์ต้องขอรับการทดสอบผลิตภัณฑ์จากห้องทดลองโดยนักพัฒนาผลิตภัณฑ์ในสิงคโปร์ไม่ต้องส่งผลิตภัณฑ์ไปตรวจสอบนอกประเทศ หรือให้ผู้ตรวจสอบเดินทางมายังสิงคโปร์อีกต่อไป ทำให้ประหยัดเวลาและค่าใช้จ่ายสำหรับนักพัฒนาในสิงคโปร์ ซึ่งจะทำให้สิงคโปร์กลายเป็นจุดศูนย์กลางของภูมิภาคในการประเมินและออกใบรับรองผลิตภัณฑ์ด้วย

จากการศึกษายังพบว่า ภาครัฐและภาคเอกชนของสิงคโปร์ได้ร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งมีพันธมิตรเพิ่มขึ้นเรื่อยๆ ในการพัฒนาและนำมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์มาลดช่องว่างมาตรฐานความมั่นคงปลอดภัยไซเบอร์ จนทำให้สิงคโปร์ได้คะแนนตัวชี้วัดเทคนิคเพิ่มจาก 0.6667 ในปี 2014 เป็น 0.96 ในปี ค.ศ. 2017 และลดลงเล็กน้อยในปี ค.ศ. 2018 ซึ่งได้คะแนน 0.93 สอดคล้องกับรายงานที่พบว่า ร้อยละ 80 ของการซื้อขายในสิงคโปร์จะใช้ผ่านคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ การใช้ซอฟต์แวร์สำหรับรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นการป้องกันในระดับแรกในการถูกโจรกรรมหรือถูกบุกรุกข้อมูลหรือระบบ สิงคโปร์ได้มีการนำซอฟต์แวร์มาใช้ทั้งในหน่วยงานราชการ หน่วยงานเอกชน และครัวเรือน โดยบริษัทต่างๆ ในสิงคโปร์ก็ได้ผลิตซอฟต์แวร์ที่ได้มาตรฐาน เช่น บริษัท Cisco สิงคโปร์ ได้จัดทำซอฟต์แวร์สำคัญและให้บริการบน Cloud Security Platform ได้แก่ Network security, Data security, Antivirus software และ Mobile device security

3.2.3 ด้านองค์กร (Organizational Measures)

จากการศึกษาพบว่าคะแนนด้านองค์กรของสิงคโปร์ เพิ่มสูงขึ้นเป็นลำดับทุกปี โดยเริ่มจากปี 2014 ได้คะแนน 0.7500 ปี ค.ศ. 2017 ได้ 0.88 คะแนน ปี ค.ศ. 2018 ได้ 0.96 คะแนน สอดคล้องกับหลักฐานการศึกษาที่แสดงให้เห็นถึงพัฒนาการในการจัดตั้งองค์กรหรือหน่วยงานที่กำหนดนโยบาย มีการกำหนดยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ รวมทั้งมีหน่วยงานที่รับผิดชอบการรับมือกับภัยคุกคามไซเบอร์ได้อย่างครอบคลุม และมีการประสานงานข้ามองค์กรระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทำให้การดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ประสบความสำเร็จบรรลุตามเป้าหมายและแผนยุทธศาสตร์ระดับชาติ

โครงสร้างองค์กรหลักที่รับผิดชอบในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์อยู่ภายใต้การควบคุมของคณะรัฐมนตรี โดยแบ่งออกเป็น

3.2.3.1 Ministry of Communication and Information ซึ่งมีหน่วยปฏิบัติงานดังนี้

1) Info–Communications Media Development Authority (IMDA) เป็นหน่วยงานตามกฎหมาย (statutory body) และเป็นหน่วยงานกำกับดูแลอุตสาหกรรมสารสนเทศและการสื่อสาร โดยมีหน้าที่ส่งเสริมให้เกิดอุตสาหกรรมสารสนเทศและการสื่อสารที่มีการแข่งขันและยั่งยืน นอกจากนี้ ยังรับผิดชอบในการส่งเสริมและกำกับดูแลการปกป้องข้อมูล ซึ่งดำเนินการโดยหน่วยงาน Personal Data Protection Commission

2) Personal Data Protection Commission (PDPC) เป็นหน่วยงานหลักที่รับผิดชอบเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล ให้ความช่วยเหลือภาคธุรกิจในการดำเนินการตามนโยบายการคุ้มครองข้อมูลที่ภาคธุรกิจต้องในไปปฏิบัติ รวมทั้ง สร้างความตระหนักรู้ในเรื่องการปกป้องข้อมูลส่วนบุคคลให้แก่ องค์กรและหน่วยงานต่างๆ ในสิงคโปร์

3) Cyber Security Agency (CSA) เป็นหน่วยงานรัฐภายใต้สำนักนายกรัฐมนตรี แต่ดำเนินงานภายใต้กำกับดูแลของ Ministry of Communication and Information โดย CSA มีหน้าที่พัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ การป้องกัน CII และการให้บริการ

ที่จำเป็น และประสานความร่วมมือในระดับชาติในการรับมือกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ นอกจากนี้ CSA ยังมีหน้าที่พัฒนาและบังคับใช้กฎระเบียบ นโยบาย การปฏิบัติงาน ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ พัฒนาระบบนิเวศน์ความมั่นคงปลอดภัยไซเบอร์ให้มีความมั่นคงเข้มแข็ง และสร้างความมั่นใจในการตอบสนองรับมือต่ออาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ ทั้งนี้ การปฏิบัติงานของ CSA จะประสานงานกับทั้งภาครัฐ ภาคอุตสาหกรรม สถาบันการศึกษา ภาคธุรกิจ และภาคประชาสังคม รวมถึงระดับระหว่างประเทศ โดยมีหน่วยงานใต้สังกัดที่สำคัญคือศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT)

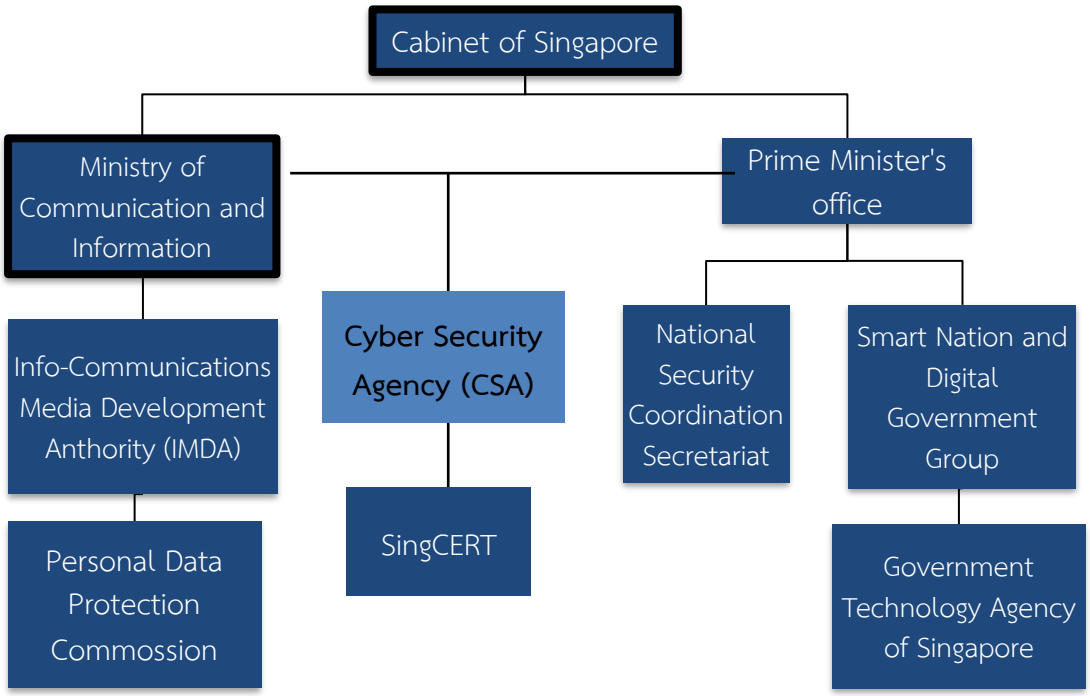
4) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT) ซึ่งจัดตั้งเมื่อปี ค.ศ. 1997 โดย IDA (ซึ่งต่อมาคือ IMDA) ร่วมกับศูนย์วิจัยอินเทอร์เน็ต และมหาวิทยาลัยแห่งชาติสิงคโปร์ ซึ่งต่อมาได้ถูกรวมเข้ากับ Cyber Security Agency เมื่อปี ค.ศ. 2015 วัตถุประสงค์ในการจัดตั้ง SingCERT เพื่ออำนวยความสะดวกในการติดตาม แก้ไข และป้องกันรักษาความมั่นคงปลอดภัย ในเรื่องที่เกี่ยวกับเหตุจากอินเทอร์เน็ต

3.2.3.2 สำนักนายกรัฐมนตรี (Prime Minister's Office หรือ PMO) จะพิจารณามอบหมายให้หนึ่งในรัฐมนตรีในคณะรัฐบาลทำงานภายใต้การกำกับดูแลของนายกรัฐบมนตรี โดยองค์กรภายใต้กำกับสำนักนายกที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ได้แก่

1) The National Security Coordination Secretariat (NSCS) เป็นศูนย์รวมในการวางแผนความมั่นคงระดับชาติและประสานงานข้ามหน่วยงานภาครัฐ เพื่อสนับสนุนความมั่นคงของชาติ การเตรียมการและรับมือกับภัยคุกคามไซเบอร์ในเชิงกลยุทธ์ รวมทั้งความสามารถในการฟื้นตัวหลังเกิดภัยคุกคาม

2) The Smart Nation and Digital Government Group (SNDGG) เป็นหน่วยงานรับผิดชอบในการประยุกต์ใช้เทคโนโลยีดิจิทัลเพื่อพัฒนาคุณภาพชีวิตประชาชน พัฒนาแพลต์ฟอร์มดิจิทัลและสภาพแวดล้อมที่เกื้อหนุนเพื่อให้บรรลุนโยบาย Smart Nation และขับเคลื่อนการเปลี่ยนผ่านเข้าสู่ยุคดิจิทัลในการให้บริการสาธารณะ

3) The Government Technology Agency of Singapore (GovTech) เป็นหน่วยงานตามกฎหมาย จัดตั้งเมื่อเดือนตุลาคม ปี ค.ศ. 2016 หลังการปรับโครงสร้างจาก Infocomm Development Authority เป็น IMDA หลังจากก่อตั้ง GovTech ได้มีการจัดตั้ง SNDGG ในเดือนพฤษภาคม ปี ค.ศ. 2017 GovTech เป็นหน่วยปฏิบัติภายใต้ SNDGG โดยทำงานร่วมกับหน่วยงานภาครัฐเพื่อพัฒนาและให้บริการดิจิทัลที่มั่นคงปลอดภัยและเทคโนโลยีประยุกต์สำหรับภาคธุรกิจและปัจเจกบุคคลในสิงคโปร์ GovTech ยังเป็นศูนย์กลางชั้นนำในเทคโนโลยีสารสนเทศและการสื่อสาร และวิศวกรรมที่เกี่ยวกับ IoT, Data Science และการพัฒนาแอพพริเคชั่น นอกจากนี้ ยังมีหน้าที่เสริมสร้างศักยภาพรัฐบาลสิงค์โปร์ในเรื่องดังกล่าวด้วย โครงสร้างองค์กรหลักที่รับผิดชอบงานด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ปรากฏตามภาพที่ 4



ภาพที่ 4 โครงสร้างองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์
ที่มา: Cybersecurity for Critical Information Infrastructure in Thailand, ThaiCERT ETDA

นอกจากหน่วยงานรัฐหลักๆ ที่ได้กล่าวมาแล้ว สิงคโปร์ยังมีหน่วยงานอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทั้งภาครัฐและเอกชน โดยเฉพาะอย่างยิ่ง หน่วยงานที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ซึ่งตามกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ได้กำหนดได้แก่ พลังงาน น้ำ การเงินและการธนาคาร ระบบดูแลสุขภาพ การขนส่ง (บก น้ำ อากาศ) สารสนเทศและการสื่อสาร สื่อ ความมั่นคงปลอดภัยและการให้บริการฉุกเฉิน และรัฐบาล โดยหน่วยงานที่เกี่ยวข้องต่างๆ ของสิงคโปร์ได้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด ทำให้ระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์เป็นไปอย่างมีประสิทธิภาพ แม้จะมีช่องโหว่อยู่บ้าง แต่ก็สามารถรับมือได้อย่างทันท่วงที ทำให้ลดความเสียหายที่จะเกิดขึ้น

3.2.4 ด้านการเสริมสร้างศักยภาพ (capacity building)

ตัวชี้วัดด้านการเสริมสร้างศักยภาพจะพิจารณาจากการรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่สาธารณะชน การส่งเสริมเรื่องมาตรฐาน cybersecurity และการให้ใบรับรองแก่ผู้เชี่ยวชาญ/ผู้ชำนาญการในเรื่องดังกล่าว การฝึกอบรมให้แก่ผู้เชี่ยวชาญ/ผู้ชำนาญการด้าน cybersecurity การมีหลักสูตรในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ การมีโครงการศึกษาวิจัยและการพัฒนา (R&D) การมีมาตรการส่งเสริมแรงจูงใจ และการส่งเสริมอุตสาหกรรมเกี่ยวกับความมั่นคงปลอดภัยให้เติบโตในประเทศ

จากการศึกษาพบว่า ในปี ค.ศ. 2017 สิงคโปร์ให้ความสำคัญในการดำเนินการและพัฒนาในด้านการส่งเสริมศักยภาพด้านดิจิทัลอย่างยิ่ง โดยได้กำหนดวิสัยทัศน์ว่าจะเป็น “Pioneers of the next generation” สิงคโปร์เล็งเห็นว่าในโลกยุคดิจิทัล เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว มีผลทำให้วงจรของนวัตกรรมจะสั้นลง เศรษฐกิจในอนาคตจะต้องอาศัยคนที่มีทักษะอย่างเชี่ยวชาญและต้องได้รับแรงจูงใจที่จะเรียนรู้ได้ตลอดชีวิต ภาคธุรกิจจะต้องอาศัยนวัตกรรม โดยหนึ่งในยุทธศาสต์ที่สิงคโปร์กำหนดไว้เพื่อบรรลุวิสัยทัศน์ดังกล่าวคือ การเสริมสร้างศักยภาพด้านดิจิทัลให้แข็งแรง โดยจะต้องส่งเสริมการใช้เทคโนโลยีดิจิทัลในทุกภาคส่วนของเศรษฐกิจและจะต้องสร้างความสามารถในด้านเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการวิเคราะห์ข้อมูลและความมั่นคงปลอดภัยไซเบอร์ รัฐบาลสามารถใช้ข้าราชการให้พัฒนาทักษะด้าน cybersecurity เชิงลึก ในกลุ่มข้าราชการที่ทำงานเต็มเวลา (Report of Committee on the Future Economy Pioneer of the Next Generation, 2017) จนได้คะแนนเพิ่มขึ้นอย่างต่อเนื่องในทุกปี โดยในปี ค.ศ. 2018 ได้คะแนนถึง 0.195 (จากคะแนนเต็ม 0.2)

รัฐบาลสิงคโปร์ทำงานอย่างใกล้ชิดกับภาคอุตสาหกรรมและสถาบันการศึกษาในการริเริ่มโครงการต่างๆ ที่ส่งเสริมการเติบโตและพัฒนาสายงานอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ จากรายงาน Singapore Cyber Landscape 2017 พบว่า สิงคโปร์ได้มีการดำเนินการดังนี้

1) การพัฒนาหลักสูตรการศึกษาทักษะที่จำเป็นสำหรับการทำงานในอนาคต (Skills Future Work–Study Degree) และการจัดกิจกรรมแลกเปลี่ยนประสบการณ์ในการทำงาน หรือ โปรแกรมการทำงานนอกเวลา (Earn and Learn Programmes) เพื่อสนับสนุนให้นักเรียนมีความสามารถด้านการรักษาความปลอดภัยไซเบอร์ในระดับอุดมศึกษา รวมถึงการส่งเสริมการเรียนรู้จากการปฏิบัติงานจริง

2) การจัดกิจกรรมเกี่ยวกับการจัดการความท้าทายในการป้องกันและรักษาความปลอดภัยไซเบอร์ อาทิ การจัดการประกวดแข่งขัน การจัดการแข่งขันรอบชิงชนะเลิศในสหราชอาณาจักร เป็นต้น เพื่อสร้างแรงบันดาล และการตระหนักถึงความสำคัญของการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนมีความกระตือรือร้น และความมุ่งมั่นในการประกอบอาชีพสาขาดังกล่าว

3) การจัดโปรแกรมฝึกหัดให้กับนักศึกษาจบใหม่ และบุคลากรที่อยู่ในช่วงกลางของอาชีพและต้องการ เปลี่ยนแปลงสายงาน อาทิ โปรแกรม Cyber Security Associates and Technologists (CSAT) และ โปรแกรม Professional Conversion เป็นต้น

4) การจัดทำกรอบการดำเนินงานการพัฒนาทักษะด้านไอซีทีเพื่อเป็นแนวทางให้กับภาคอุตสาหกรรมและหน่วยงานทางวิชาการในการพัฒนาทักษะด้านการรักษาความปลอดภัยไซเบอร์ภายในหน่วยงาน

5) การจัดทำแผนพัฒนาอาชีพสาขาการรักษาความปลอดภัยไซเบอร์ในภาคการบริการสาธารณะให้เป็นอาชีพที่ดึงดูดความสนใจ โดยมีค่าตอบแทนเป็นแรงจูงใจ

6) การสร้างอาชีพด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานทางทหาร โดยในปี 2018 กระทรวงกลาโหมของสิงคโปร์ได้จัดอบรม Full–time National Servicemen (NSF) เพื่อเป็นผู้ปกป้องไซเบอร์อย่างเต็มเวลา อันเป็นส่วนหนึ่งของยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์

ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์จะเข้ารับการอบรมที่ Singapore Institute of Technology Cybersecurity Degree

ในส่วนของการวิจัยและพัฒนา สิงคโปร์ได้ดำเนินการดังนี้

1) พัฒนาความสามารถในเรื่องความปลอดภัย Cyber–Physical Systems และเทคโนโลยี blockchain สำหรับอุตสาหกรรมโลจิสติกส์

2) จัดทำกฎเกณฑ์การประเมินผลที่ทำให้ง่ายขึ้นในการรับรองมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ IoT และผลิตภัณฑ์อื่นๆ ที่เกี่ยวข้อง

3) สนับสนุนการเติบโตและการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในกลุ่มผู้ประกอบการตั้งต้น (startup) ซึ่งเป็นตัวขับเคลื่อนสำคัญในเศรษฐกิจดิจิทัล

สิงคโปร์ได้ริเริ่มดำเนินโครงการต่างๆ ที่เป็นแรงจูงใจให้มีการพัฒนาทักษะความเชี่ยวชาญด้าน cybersecurity เช่น CSA ได้จัดทำ Co–innovation and Development Proof–of–Concept Funding Scheme เพื่อสนับสนุนผู้ให้บริการการแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ (cybersecurity solution providers) และผู้ใช้ (cybersecurity end–users) โดย CSA ได้ให้ทุนในการดำเนินการสูงสุดถึง 500,000 เหรียญสิงคโปร์ สำหรับระยะเวลาสูงสุดไม่เกิน 12 เดือน

นอกจากนี้ สิงคโปร์ยังให้ความสำคัญกับการส่งเสริมให้เยาวชนมีทักษะและสนใจในด้าน cybersecurity หนึ่งในโครงการที่ประสบความสำเร็จคือ Youth Cyber Exploration Programme (YCEP) ซึ่งเริ่มครั้งแรกในปี ค.ศ. 2018 จัดโดย CSA ร่วมกับ Singapore Polytechnic เป็นโครงการที่ดำเนินกิจกรรม 4 วัน ออกแบบเพื่อให้เยาวชนมีความสนใจและตื่นเต้นในการงานอาชีพที่เกี่ยวกับ cybersecurity มีเด็กนักเรียนเข้าร่วมโครงการ 97 คน จากโรงเรียนมัธยมศึกษา 18 แห่ง โปรแกรมดังกล่าวจะสอนเด็กให้เข้าใจหลักการพื้นฐานของความมั่นคงปลอดภัยไซเบอร์และเปิดโอกาสให้มีส่วนร่วมในการฝึกปฏิบัติจริงและร่วมแข่งขัน โดยเด็กที่มีความโดดเด่นจะได้รับรางวัลเป็นโอกาสในการฝึกอบรมเพิ่มเติมและเด็กที่ผ่านการทดสอบจะได้รับใบรับรองโดย Singapore Polytechnic ในทะเบียนประวัติผลงาน (portfolio) เพื่อใช้ในการสอบ Early Admission

ปัจจัยสำคัญในการเสริมสร้างศักยภาพคือ การสร้างความตระหนักรู้แก่ประชาชนและคนทั่วไปเกี่ยวกับภัยคุกคามทางไซเบอร์ และการจัดการกับภัยคุกคามดังกล่าว สิงคโปร์ให้ความสำคัญอันดับแรกคือ การให้ความรู้เกี่ยวกับการปฏิบัติที่จะป้องกันข้อมูลและทำให้เครื่องมืออุปกรณ์ดิจิทัลสะอาดปลอดภัยจากไวรัสที่มาจากไซเบอร์

อย่างไรก็ดี CSA ได้ทำการสำรวจความตระหนักรู้ของสาธารณชน (Public Awareness Survey) เมื่อปี ค.ศ. 2017 มีผู้ตอบแบบสอบถามจำนวน 2,035 คน พบว่า คนสิงคโปร์ส่วนใหญ่ทราบว่า ทุกคนมีบทบาทในเรื่องความมั่นคงปลอดภัยไซเบอร์และมีส่วนเกี่ยวข้องกับความเสี่ยงจากภัยคุกคามไซเบอร์ แต่พบว่ายังมีช่องโหว่ในเรื่องอุปนิสัยในเรื่องการจัดการกับรหัสผ่าน (password) และการอัพเดทซอฟต์แวร์ (https://www.csa.gov.sg/news/press-releases/cyber-threats-in-singapore-grew-in-2017-mirooing-global-trends) รัฐบาลสิงคโปร์จึงต้องเร่งสร้างความตระหนักรู้และหาวิธีการหรือมาตรการจูงใจให้ประชาชนปฏิบัติการเพื่อสร้างความมั่นคงปลอดภัยของระบบนิเวศน์ไซเบอร์สิงคโปร์ได้ทั้งระบบ

3.2.5 ด้านความร่วมมือ (cooperation)

ITU วิเคราะห์และให้คะแนนตัวชี้วัดนี้จากหุ้นส่วนพันธมิตร กรอบความร่วมมือและเครือข่ายในการแบ่งปันข้อมูลที่มีอยู่จริง โดยแบ่งตัวชี้วัดย่อยเป็น 5 ตัว ประกอบด้วย การจัดทำความตกลงทวิภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำข้อตกลงและ/หรือการเข้าร่วมความตกลงพหุภาคี การเข้าร่วมในเวทีระหว่างประเทศ ความร่วมมือระหว่างภาครัฐและเอกชน ความร่วมมือกับหน่วยงานระหว่างประเทศ และการมีแบบปฏิบัติที่ดีด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity best practices)

จากผลการศึกษาพบว่า ในช่วงปี ค.ศ. 2014 สิงคโปร์ได้คะแนนด้านความร่วมมือเพียง 0.5000 แต่หลังจากมีการจัดตั้ง Cyber Security Agency (CSA) ในปี ค.ศ. 2015 พบว่า สิงคโปร์ได้มีการจัดทำความตกลงด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานต่างๆ ทั้งหน่วยงานภายในประเทศ และหน่วยงานในระดับระหว่างประเทศ ทั้งในส่วนของการแลกเปลี่ยนข้อมูลเกี่ยวกับเหตุการณ์ภัยคุกคาม การแบ่งปันแบบปฏิบัติที่ดีในเรื่องการปกป้อง CII การพัฒนาระบบนิเวศน์ไซเบอร์ รวมทั้งการร่วมมือในการฝึกอบรม โดยสิงคโปร์ได้ขยายความร่วมมือกับประเทศต่างๆ เพิ่มขึ้นทุกปี จนทำให้คะแนนด้านความร่วมมือของสิงคโปร์เพิ่มขึ้นอย่างมีนัยสำคัญใน ปี ค.ศ. 2017 ที่คะแนน 0.87 ซึ่งในเฉพาะปี ค.ศ. 2017 สิงคโปร์ได้ลงนามบันทึกความเข้าใจว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับออสเตรเลีย เยอรมันนี ญี่ปุ่น และสหราชอาณาจักร และในปี ค.ศ. 2018 สิงคโปร์ได้ลงนามใน MoU กับแคนาดา

ด้านความร่วมมือระหว่างภาครัฐและเอกชน ข้อมูลจากเว็บไซต์ CSA พบว่า CSA ได้จัดทำ Memorandum of Collaboration ว่าด้วยความร่วมมือในการจัดทำกรอบดำเนินงานสำหรับความมั่นคงปลอดภัยไซเบอร์กับ Cisco System นอกจากนี้ CSA ร่วมกับ GovTech ได้ร่วมมือกับ HackerOne ซึ่งเป็นชุมชนใหญ่ที่สุดในโลกที่รวมนักวิจัย Cybersecurity และแฮกเกอร์ (“white hat” hackers) ทั้งในและนอกประเทศ ในการจัดทำโปรแกรม Government Bug Bounty Programme (GBBP) ระหว่างเดือนธันวาคม ปี ค.ศ. 2018–เดือนมกราคม 2019 เพื่อให้แฮกเกอร์ค้นหาจุดอ่อนไหวในระบบสารสนเทศและการสื่อสารของหน่วยงานภาครัฐที่คัดเลือกมา 5 หน่วยงาน ที่มีการใช้อินเทอร์เน็ตและเว็บไซต์สูง โดยแฮกเกอร์จะได้รับเงินรางวัลตอบแทน ซึ่งมีจำนวนตั่งแต่ 250–10,000 เหรียญสหรัฐอเมริกา ทั้งนี้ขึ้นอยู่กับความรุนแรงของตัวปัญหาหรือ “bug” ที่ค้นพบ

ในส่วนของการเข้าร่วมในเวทีระหว่างประเทศ สิงคโปร์จัดงาน Singapore International Cyber Week (SICW) เป็นประจำทุกปี เริ่มตั้งแต่ ปี ค.ศ. 2016 จากรายงาน Singapore Cyber Landscape 2017 พบว่างาน Singapore International Cyber Week ครั้งที่ 2 เมื่อปี ค.ศ. 2017 มีผู้นำด้าน Cybersecurity จากทั้งระดับภูมิภาคและระหว่างประเทศเข้าร่วมงานเพื่อพูดคุยแลกเปลี่ยนประสบการณ์และเสริมสร้างความร่วมมือระหว่างกัน มีผู้มีส่วนได้ส่วนเสียเข้าร่วมงานมากกว่า 7,000 คน จาก 50 ประเทศ ทั้งจากผู้กำหนดนโยบาย ผู้เชี่ยวชาญจากภาคอุตสาหกรรม และหน่วยงานอื่นๆ ที่มิใช่ภาครัฐ งาน SICW จะประกอบด้วยการประชุมหารือและการสัมมนาเชิงปฏิบัติการด้านไซเบอร์ เช่น การสัมมนาเชิงปฏิบัติการด้านไซเบอร์ของผู้นำ การประชุม ASEAN Cyber Prosecutors Roundtable การประชุม IoT Cyber Roundtable การหารือความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค เป็นต้น

ในการประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยทางสารสนเทศ ครั้งที่ 3 (The 3rd ASEAN Ministerial Conference on Cybersecurity–AMCC) และงาน The 3rd Singapore International Cyber Week ระหว่างวันที่ 17–20 กันยายน 2561 ณ สาธารณรัฐสิงคโปร์ สิงคโปร์ได้แสดงบทบาทผู้นำด้านความมั่นคงปลอดภัยทางสารสนเทศในเวที ASEAN โดยได้นำเสนอแนวทางสำหรับกลไกเพื่อส่งเสริมการประสานงานด้านความมั่นคงปลอดภัยทางสารสนเทศของอาเซียน (Cybersecurity Coordination Efforts in ASEAN) ประกอบด้วย แนวทางที่ 1 การขยายขอบเขตและความรับผิดชอบของการประชุมรายสาขาของอาเซียนที่มีอยู่แล้ว (Expand the Mandate of an Existing ASEAN Sectoral Body) ให้ครอบคลุมประเด็นด้านความมั่นคงปลอดภัยทางสารสนเทศ และแนวทางที่ 2 การจัดตั้งสาขาความร่วมมือใหม่เฉพาะด้านความมั่นคงปลอดภัยทางสารสนเทศ (Establishing a New Cybersecurity Sectoral in ASEAN) โดยที่ประชุมเห็นควรให้มีการนำข้อเสนอและแนวทางดังกล่าวของสิงคโปร์ไปพิจารณาต่อไป รวมทั้งเห็นควรสนับสนุนให้การประชุม AMCC ที่ริเริ่มโดยสิงคโปร์ เป็นเวทีการประชุมชั่วคราวอย่างไม่เป็นทางการ เพื่อหารือประเด็นด้านความมั่นคงปลอดภัยทางสารสนเทศไปก่อน

นอกจากนี้ สิงคโปร์ยังได้นำเสนอเรื่องบรรทัดฐานพฤติกรรมของรัฐในด้านไซเบอร์ (Norms of State Behavior in Cyberspace) โดยได้เสนอให้พิจารณารับรองหลักการของบรรทัดฐานความมั่นคงปลอดภัยทางสารสนเทศ ซึ่งเป็นข้อเสนอแนะบรรทัดฐานโดยสมัครใจและไม่ผูกพัน เพื่อให้รัฐมีพฤติกรรมที่มีความรับผิดชอบในโลกไซเบอร์ โดยอ้างอิงจากรายงานสหประชาชาติของกลุ่มผู้เชี่ยวชาญของรัฐเกี่ยวกับการพัฒนาสาขาสารสนเทศและโทรคมนาคมในบริบทของความมั่นคงระหว่างประเทศ ปี ค.ศ. 2015 (The 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security หรือ UNGGE) ซึ่งที่ประชุมได้เห็นชอบในหลักการเกี่ยวกับบรรทัดฐานความมั่นคงปลอดภัยทางสารสนเทศ 11 รายการ ที่ตั้งอยู่บนพื้นฐานของความสมัครใจและไม่ผูกพัน โดยอ้างอิงจากรายงาน UNGGE ตลอดจนส่งเสริมการเสริมสร้างขีดความสามารถของภูมิภาคเพื่อนำไปสู่การปฏิบัติ โดยสนับสนุนให้อาเซียนมีการพิจารณาและหารือต่อไป และเห็นพ้องในการสนับสนุนความจำเป็นของการจัดทำบัญชีรายชื่อผู้ประสานงานด้านไซเบอร์อาเซียน

ในส่วนของความร่วมมือระหว่างประเทศในการเสริมสร้างความสามารถของทรัพยากรมนุษย์ สิงคโปร์ได้เป็นผู้นำและทำงานร่วมมือกับประเทศสมาชิกอาเซียน ตัวอย่างที่เด่นชัดคือ ASEAN Cyber Capacity Programme (ACCP) ซึ่งมีมูลค่าโครงการถึง 10 ล้านเหรียญสิงคโปร์ เพื่อสร้างความสามารถด้านเทคนิค นโยบาย และยุทธศาสตร์ ในกลุ่มประเทศสมาชิกอาเซียน สิงคโปร์ได้ริเริ่มโครงการนี้เมื่อปี ค.ศ. 2017 มีเจ้าหน้าที่ด้าน Cybersecurity และเจ้าหน้าที่ที่รับผิดชอบในการรับมือกับเหตุภัยคุกคาม (incident responders) จากประเทศสมาชิกอาเซียน เข้าร่วมการฝึกอบรมมากกว่า 120 คน (ข้อมูลเมื่อปี ค.ศ. 2017) ผ่านหลักสูตรต่างๆ เช่น ASEAN Cyber Norms Workshop และ US–Singapore Workshop on Cybersecurity เป็นต้น

อย่างไรก็ตาม จากรายงาน ITU Global Cybersecurity Index ปี ค.ศ. 2018 คะแนนของสิงคโปร์ในส่วนของด้านความร่วมมือตกลงจาก 0.87 ในปี ค.ศ. 2017 เป็น 0.625 (หรือ 0.125 ตามค่าน้ำหนักใหม่ในปี ค.ศ. 2018) ทำให้คะแนนรวมของสิงคโปร์ตกลงจากปี ค.ศ. 2017

และมีผลทำให้อันดับโลกของสิงคโปร์ลดลงจากอันดับ 1 ในปี ค.ศ. 2017 ไปเป็นอันดับ 6 ในปี ค.ศ. 2018 โดยคะแนนด้านความร่วมมือของประเทศที่ได้คะแนนมากสุด 5 อันดับแรก มีคะแนนสูงกว่าสิงคโปร์ทั้งสิ้น รายละเอียดปรากฏตามตารางที่ 4

ตารางที่ 4 อันดับ GCI ของโลก 6 อันดับแรก ในปี ค.ศ. 2018

Rank	States	GCI Score	Legal	Technical	Organiza–tional	Capacity building	Coopera–tion
1	U.K	0.931	0.200	0.191	0.200	0.189	0.151
2	U.S.A	0.926	0.200	0.184	0.200	0.191	0.151
3	France	0.918	0.200	0.193	0.200	0.186	0.139
4	Lithuania	0.908	0.200	0.168	0.200	0.185	0.155
5	Estonia	0.905	0.200	0.195	0.186	0.170	0.153
6	Singapore	0.898	0.200	0.186	0.192	0.195	0.125

ที่มา: ITU Global Cybersecurity Index (GCI) 2018

จากการศึกษาข้อมูลอาจสมมติฐานได้ว่า สิงคโปร์มีอัตราการขยายความร่วมมือกับหน่วยงานในประเทศและกับองค์กรระหว่างประเทศลดลงจากปี ค.ศ. 2017 ในขณะที่ประเทศสหราชอาณาจักร และสหรัฐอเมริกามีการขยายความร่วมมือในด้านความมั่นคงปลอดภัยที่สูงกว่า

3.3 สภาพการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของไทย

รัฐบาลไทยได้กำหนดนโยบายไทยแลนด์ 4.0 ซึ่งขับเคลื่อนเศรษฐกิจและสังคมด้วยนวัตกรรมและการใช้เทคโนโลยีสารสนเทศและการสื่อสาร เทคโนโลยีดิจิทัลในทุกภาคส่วน และตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของประเทศไทย ก็ได้กำหนดกรอบยุทธศาสตร์การพัฒนาไว้ 6 ด้าน โดยยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล ซึ่งมุ่งเน้นการมีกฎหมาย กฎระเบียบ กติกาและมาตรฐานที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมและทำธุรกรรมออนไลน์ต่างๆ รวมถึงสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัลในทุกภาคส่วน เพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลและการใช้งานที่เพิ่มขึ้นในอนาคต โดยยุทธศาสตร์นี้ประกอบด้วยแผนงานเพื่อขับเคลื่อนยุทธศาสตร์ 3 ด้าน ดังนี้

1) กำหนดมาตรฐาน กฎ ระเบียบ และกติกา ด้านดิจิทัลให้มีความทันสมัยและมีประสิทธิภาพโดยเฉพาะอย่างยิ่งเพื่ออำนวยความสะดวกด้านการค้าและการใช้ประโยชน์ในภาคเศรษฐกิจและสังคม

2) ปรับปรุงกฎหมายที่เกี่ยวข้องกับเศรษฐกิจและสังคมดิจิทัลให้มีความทันสมัย สอดคล้องต่อพลวัตของเทคโนโลยีดิจิทัลและบริบทของสังคม

3) สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์ ด้วยการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล การคุ้มครองผู้บริโภค

จากข้อมูล ITU Global Cybersecurity Index (GCI) ปี ค.ศ. 2014, 2017 และ 2018 พบว่า ประเทศไทยอยู่อันดับ 7 ในภูมิภาคเอเชียและแปซิฟิก และอยู่ในอันดับที่ 15 ของโลกในปี ค.ศ. 2014 และตกมาเป็นอันดับที่ 20 และ 35 ในปี ค.ศ. 2017 และ 2018 ตามลำดับ แต่หากพิจารณาจากคะแนนรวม ประเทศไทยได้คะแนนรวมเพิ่มขึ้นเป็นลำดับ จาก 0..4118 ในปี ค.ศ. 2014 เป็น 0.796 ในปี ค.ศ. 2018 แสดงให้เห็นว่า ประเทศไทยมีพัฒนาการในการดำเนินนโนบายด้านความมั่นคงปลอดภัยไซเบอร์อย่างเห็นได้ชัด อย่างไรก็ตาม ข้อมูลจากรายงานในปี ค.ศ. 2014 แต่ละอันดับจะมีหลายประเทศที่ได้คะแนนเท่ากัน และในรายงานของ ITU ปี ค.ศ. 2017 และ 2018 จะแสดงให้เห็นคะแนนแต่ละตัวชี้วัดเฉพาะ 10 อันดับแรก ทำให้ขาดข้อมูลประกอบการพิจารณาในส่วนของประเทศไทยในแต่ละตัวชี้วัด รายละเอียดคะแนนและอันดับของประเทศไทยในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ปรากฏตาม ตารางที่ 5

ตารางที่ 5 คะแนนและอันดับของประเทศไทยในการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์

ปี	ด้านกฎหมาย	ด้านเทคนิค	ด้านองค์กร	ด้านเสริมสร้างศักยภาพ	ด้านความร่วมมือ	คะแนนรวม	อันดับในภูมิภาค	อันดับโลก
2014	0.500	0.3333	0.5000	0.2500	0.5000	0.4118	7	15
2017	NA	NA	NA	NA	NA	0.684	7	20
2018	NA	NA	NA	NA	NA	0.796	7	35

ที่มา: ITU Global Cybersecurity Index (GCI) 2014, 2017 and 2018

ผลจากการศึกษาการดำเนินการของไทย แบ่งตามตัวชี้วัดทั้ง 5 ตัว มีดังนี้

3.3.1 ด้านกฎหมาย

ปัจจุบัน ประเทศไทยได้มีพระราชบัญญัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ดังนี้

1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
3) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562
4) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560

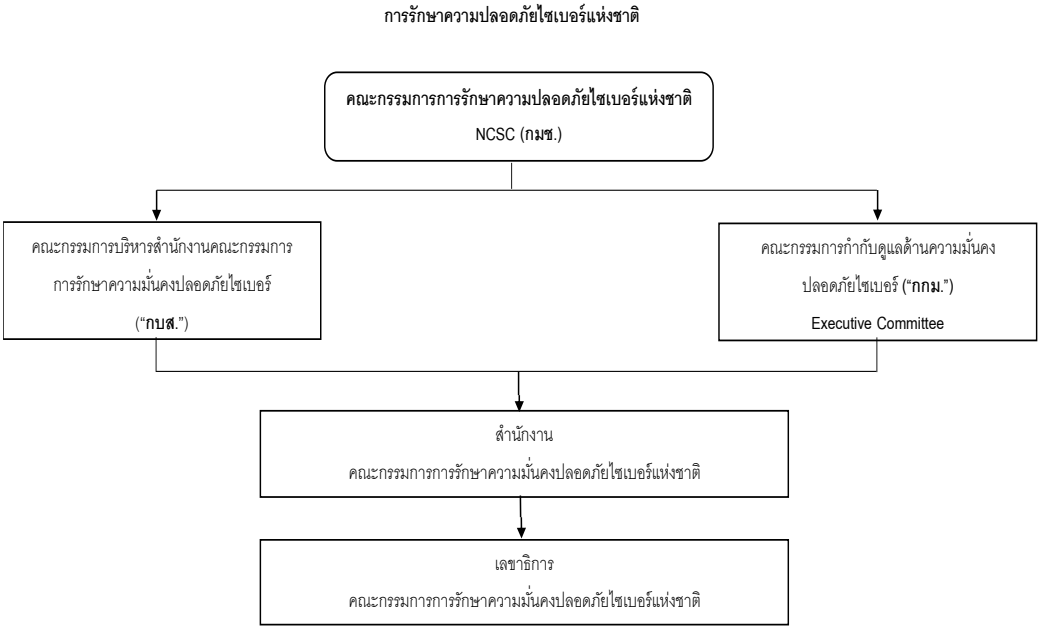
พระราชบัญญัติที่สำคัญเพิ่งมีผลบังคับใช้เมื่อเดือนพฤษภาคม พ.ศ. 2562 จึงอาจคาดได้ว่าหลังจากนี้ ประเทศไทยจะมีความคืบหน้าในการดำเนินการนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง และปรับอันดับ GCI ที่ ITU จัดทำสำหรับปี 2019

3.3.2 ด้านเทคนิค

ประเทศไทยยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย ที่ทำหน้าที่เพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

3.3.3 ด้านองค์กร

หลังจากพระราชพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 โดยในบทเฉพาะการได้กำหนดให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และในระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ ดังนั้น ในระหว่างนี้ สำนักงานปลัดกระทรวงจะต้องมีการเตรียมการและดำเนินการเพื่อให้เป็นไปตามข้อกำหนดตามพระราชบัญญัตินี้ โดยเฉพาะอย่างยิ่งการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่มีหน้าที่ลักษณะเดียวกันกับ Cyber Security Agency ของสิงคโปร์ ภาพที่ 5 แสดงให้เห็นถึงโครงสร้างของหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่กำหนดไว้ในพระราชพระราชบัญญัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562



ภาพที่ 5 โครงสร้างของหน่วยงานที่รับผิดชอบด้าน Cybersecurity ของไทย
ที่มา: กองกฎหมาย สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

3.3.4 ด้านการเสริมสร้างศักยภาพ

ประเทศไทยโดยหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ และสภาความมั่นคงแห่งชาติได้ตระหนักถึงความสำคัญในการเตรียมบุคลากรที่มีทักษะและความเชี่ยวชาญดังกล่าวโดยมีการจัดหลักสูตรฝึกอบรมด้านนี้ แต่ยังขาดการประสานงานระหว่างหน่วยงานต่างๆ โดยเฉพาะอย่างยิ่งการประสานงานกับสถาบันการศึกษา และภาคธุรกิจและภาคอุตสาหกรรมในการจัดเตรียมบุคลากร และสายงานอาชีพในด้านความมั่นคงปลอดภัย ภาคธุรกิจและประชาชนยังขาดความตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์

3.3.5 ด้านความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานระหว่างประเทศ

ประเทศไทยโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้มีความคืบหน้าในเรื่องนี้อย่างต่อเนื่อง กระทรวงฯ ได้ลงนามบันทึกความเข้าใจกับกระทรวงที่รับผิดชอบเทคโนโลยีสารสนเทศและการสื่อสารของประเทศต่างๆ รวมทั้งสิงคโปร์ โดยขอบเขตความร่วมมือจะครอบคลุมไปถึงด้านความมั่นคงปลอดภัยไซเบอร์ แต่ยังไม่มีการดำเนินความร่วมมือในด้านนี้อย่างเป็นรูปธรรม ในส่วนของ ThaiCERT ในฐานะที่เป็นสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/ Forum of Incident Response and Security Teams) จึงมีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้ กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง

นอกจากนี้ ในเวทีของ ASEAN ไทยยังได้รับเลือกให้เป็นที่ตั้งศูนย์ความร่วมมืออาเซียน–ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN–Japan Cybersecurity Capacity Building Centre) โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์เป็นจัดหาพื้นที่จัดตั้งศูนย์ และประเทศญี่ปุ่นจะให้เงินสนับสนุนการดำเนินงาน จำนวน 5 ล้านเหรียญสหรัฐอเมริกา เป็นระยะเวลา 4 ปี คาดว่าจะเปิดตัวศูนย์ฯ อย่างเป็นทางการในปลายปี พ.ศ. 2562 โดยมีเป้าหมายอบรมด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้าราชการและเจ้าหน้าที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกว่า 700 คน โดยจะมีการอบรม ปีละ 6 ครั้ง ครั้งละ 24 คน ตลอดระยะเวลา 4 ปี และจัดการแข่งขัน Cyber SEA Game ซึ่งเป็นการแข่งขันทางเทคนิคด้านความมั่นคงปลอดภัยไซเบอร์ระดับอาเซียน เรียกว่า Capture the Flag (CTF) เป็นการแบ่งกลุ่มทำโจทย์ทางเทคนิค เช่น การเจาะเซิร์ฟเวอร์ที่มีช่องโหว่ การวิเคราะห์มัลแวร์ เป็นต้น โดยจะมีผู้เข้าร่วมปีละ 40 คนจาก 10 ประเทศอาเซียน ติดต่อกัน 4 ปี สำหรับหลักสูตรฝึกอบรม มี 3 หลักสูตร ดังนี้

1) CYDER (Cyber Defense Exercise for Recurrence) ความสามารถการรับมือภัยคุกคามไซเบอร์ (incident Response) โดยจะเป็นการจำลองสถานการณ์และซ้อมการรับมือสถานการณ์ภัยคุกคามไซเบอร์

2) Forensics ความสามารถในการหาร่องรอยการโจมตีและตรวจพิสูจน์พยานหลักฐานดิจิทัล

3) Malware Analysis ความสามารถวิเคราะห์มัลแวร์ประเภทต่าง ๆ ตามภัยคุกคามทางไซเบอร์

3.4 ผลการศึกษาเชิงเปรียบเทียบ

จากการเปรียบตัวชี้วัด 5 ด้าน ที่ ITU ได้กำหนดไว้ ระหว่างสิงคโปร์และไทย ในปี ค.ศ. 2014, 2017 และ 2018 ซึ่งสามารถสรุปได้ตามตารางที่ 3.4 อย่างไรก็ดี ยังขาดข้อมูลในส่วนของคะแนนตัวชี้วัดแต่ละด้านของไทย จึงพิจารณาจากข้อมูลทุติยภูมิอื่นๆ ประกอบการศึกษา

ตารางที่ 6 เปรียบเทียบคะแนนตัวชี้วัด 5 ด้าน ระหว่างสิงคโปร์และไทย

ปี	ตัวชี้วัด	สิงคโปร์	ไทย
2014	ด้านกฎหมาย	0.7500	0.5000
	ด้านเทคนิค	0.6667	0.3333
	ด้านองค์กร	0.7500	0.5000
	ด้านเสริมสร้างศักยภาพ	0.7500	0.2500
	ด้านความร่วมมือ	0.5000	0.5000
	คะแนนรวม	**0.6765**	**0.4118**
2017	**คะแนนรวม**	**0.92**	**0.684**
2018	**คะแนนรวม**	**0.898**	**0.796**

ที่มา: ITU Global Cybersecurity Index (GCI) 2014, 2017 and 2018

ผลจากการศึกษาเชิงเปรียบเทียบระหว่างสิงคโปร์และไทย พบว่า

3.4.1 ด้านกฎหมาย

ในภาพรวมทั้งสิงคโปร์และไทยมีพัฒนาการที่ดีอย่างต่อเนื่องในเรื่องการออกกฎหมายกฎระเบียบที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีการออกกฎหมายและกฎระเบียบต่างๆ ที่เกี่ยวข้องเพื่อรองรับในเรื่องดังกล่าว และตอบสนองยุทธศาสตร์ประเทศในการใช้เทคโนโลยีและนวัตกรรมเพื่อขับเคลื่อนเศรษฐกิจและสังคมให้มีความยั่งยืน และบรรลุเป้าหมายประเทศ สิงคโปร์กำหนดที่จะบรรลุเป้าหมายการเป็น Smart Nation ในขณะที่ประเทศไทยกำหนดเป้าหมายสู่ Thailand 4.0 โดยหนึ่งในยุทธศาสตร์ที่สำคัญคือ การสร้างความมั่นคงและความเชื่อมั่นในการใช้เทคโนโลยีและนวัตกรรมสารสนเทศ

ทั้งไทยและสิงคโปร์ได้มีการดำเนินการออกกฎหมายที่เกี่ยวข้อง เช่น กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎหมายเกี่ยวกับคอมพิวเตอร์ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมอิเล็กทรอนิกส์ กฎหมายเกี่ยวกับ Child online protection รวมทั้งคู่มือแนวทางในการดำเนินการต่างๆ ที่เกี่ยวข้อง

อย่างไรก็ดี สิงคโปร์ได้เริ่มดำเนินการเกี่ยวกับกฎหมายต่างๆ มาเป็นระยะเวลานาน โดยเริ่มดำเนินการอย่างจริงจังตั้งแต่ปี ค.ศ. 2005 ด้วยการจัดทำแผนแม่บทด้านความมั่นคงปลอดภัย

ไซเบอร์ ฉบับแรก ขึ้น และดำเนินการอย่างต่อเนื่อง จริงจัง และเป็นระบบ ในส่วนของประเทศไทย มีการดำเนินการหลังสิงคโปร์ และปัญหาที่ผ่านมาคือ ไทยยังไม่มีกฎหมายรองรับและไม่มีหน่วยงานที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์โดยตรง ทั้งนี้ คาดว่าคะแนนตัวชี้วัดด้านกฎหมายของไทยจะเพิ่มขึ้นในปี ค.ศ. 2019 น่าจะเพิ่มขึ้น เนื่องจากกฎหมายที่เกี่ยวข้อง 3 ฉบับ มีผลบังคับใช้ ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562 อย่างไรก็ตาม ประเทศไทยก็จะต้องมีการดำเนินการตามกฎหมายอย่างจริงจัง รวมทั้งการจัดทำกฎหมายลูกหรือกฎระเบียบอื่นที่เกี่ยวข้องต่อไป

3.4.2 ด้านเทคนิค

ถึงแม้ว่าไทยจะมีหน่วยงาน ThaiCERT ที่ทำหน้าที่เพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ แต่ก็เป็นเพียงส่วนหนึ่งและเป็นการจัดการที่ปลายเหตุ ซึ่งหากเปรียบเทียบตัวชี้วัดด้านเทคนิคแล้ว สิงคโปร์มีการดำเนินการได้ดีกว่าประเทศไทยอย่างมาก สิงคโปร์ให้ความสำคัญกับการพัฒนาเทคโนโลยีการสื่อสารโทรคมนาคมและเทคโนโลยีใหม่ๆ เพื่อให้เท่าทันและสามารถป้องกันและรับมือกับภัยคุมคามไซเบอร์ โดยการจัดสรรงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย ตลอดจนการนำเทคโนโลยีที่ทันสมัยมาใช้ รวมทั้ง การส่งเสริมเรื่องการจัดทำมาตรฐาน ในขณะที่ประเทศไทยยังไม่มีการดำเนินการในเรื่องนี้อย่างเป็นรูปธรรมและเพียงพอ จากข้อมูลผลสำรวจของ ITU ในปี ค.ศ. 2014 ไทยได้คะแนนด้านเทคนิคต่ำเป็นอันดับ 4 ใน 5 ด้าน คือ 0.333 ซึ่งสะท้อนให้เห็นว่า ประเทศไทยยังต้องพัฒนาในด้านนี้อย่างจริงจัง

3.4.3 ด้านองค์กร

สิงคโปร์ได้มีการจัดตั้ง Cyber Security Agency (CSA) เมื่อปี ค.ศ. 2015 ซึ่งเป็นหน่วยงานภายใต้สำนักนายกรัฐมนตรี แต่ดำเนินงานภายใต้กระทรวงสื่อสารและสารสนเทศ โดยมีการรวมหน่วยงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์เข้าด้วยกัน รวมทั้ง SingCERT และยังมีการทำงานร่วมกับฝ่ายความมั่นคงอย่างใกล้ชิด หากเปรียบเทียบกับของประเทศไทย ซึ่งอยู่ในระหว่างการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามที่กำหนดไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ไทยอาจพิจารณาการรวมหน่วยงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์เช่นเดียวกับสิงคโปร์ เพื่อให้มีการรบูรณาการทั้งบุคลากร ทรัพยากร และการทำงาน

3.4.4 ด้านการเสริมสร้างศักยภาพ

หากเปรียบเทียบด้านการเสริมสร้างศักยภาพ สิงคโปร์ได้คะแนนทิ้งห่างกับประเทศไทยอย่างมาก ผลการรายงานของ ITU ในปี ค.ศ. 2014 ไทยได้คะแนนด้านการเสริมสร้างศักยภาพต่ำสุดใน 5 ด้าน อยู่ที่คะแนน 0.2500 ในขณะที่สิงคโปร์ได้คะแนน 0.7500 และเพิ่มขึ้นเป็นลำดับทุกปี ซึ่งล่าสุด ปี ค.ศ. 2018 ได้คะแนนถึง 0.975 แสดงให้เห็นว่า ประเทศไทยต้องให้ความสำคัญและหามาตรการ และกำหนดกลยุทธ์และแผนงานในการเสริมสร้างศักยภาพ เช่นเดียวกับที่สิงคโปร์ได้มีการดำเนินการอย่างต่อเนื่อง ไม่ว่าจะเป็นเรื่องการส่งเสริมการใช้เทคโนโลยีดิจิทัลในทุกภาคส่วนของเศรษฐกิจและจะต้องสร้างความสามารถในด้านเทคโนโลยีดิจิทัล การรณรงค์สร้างความตระหนักรู้ด้าน

ความมั่นคงปลอดภัยไซเบอร์ให้แก่สาธารณะชนอย่างต่อเนื่อง การให้ใบรับรองแก่ผู้เชี่ยวชาญ/ผู้ชำนาญการในเรื่องดังกล่าว การฝึกอบรมให้แก่ผู้เชี่ยวชาญ/ผู้ชำนาญการด้าน cybersecurity การมีหลักสูตรในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ การมีโครงการศึกษาวิจัยและการพัฒนา การมีมาตรการส่งเสริมแรงจูงใจ และการส่งเสริมอุตสาหกรรมเกี่ยวกับความมั่นคงปลอดภัยให้เติบโตในประเทศ

3.4.5 ด้านความร่วมมือ

คะแนนด้านความร่วมมือของสิงคโปร์และไทยเท่ากันในปี ค.ศ. 2014 ที่คะแนน 0.500 โดยสิงคโปร์ได้คะแนนเพิ่มขึ้นอย่างมีนัยสำคัญใน ปี ค.ศ. 2017 เป็น 0.92 และลดลงเล็กน้อยในปี ค.ศ. 2018 เป็น 0.898 อันเป็นผลมาจาการดำเนินงานของสิงคโปร์ในการร่วมมือกับทุกภาคส่วนทั้งในประเทศและระหว่างประเทศ แต่เนื่องจากไม่มีข้อมูลในส่วนของประเทศไทยในปี ค.ศ. 2017 และ ค.ศ. 2018 ทำให้ไม่สามารถระบุพัฒนาการในด้านนี้ของประเทศไทย อย่างไรก็ดี จากรายงานผลความร่วมมือที่ประเทศไทยได้เข้าไปมีบทบาทในเวทีระหว่างประเทศโดยเฉพาะกรอบอาเซียน และเอเปค อาจกล่าวว่าประเทศไทยมีพัฒนาการด้านนี้และมีส่วนทำให้คะแนนรวมของไทยสูงขึ้นจาก 0.4118 ในปี ค.ศ. 2014 เป็น 0.796 ในปี ค.ศ. 2017 และเมื่อศูนย์ความร่วมมืออาเซียน–ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ เปิดอย่างเป็นทางการในปลายปีนี้ ก็คาดว่าคะแนนของไทยน่าจะเพิ่มขึ้น ทั้งนี้ ไทยควรให้ความสำคัญกับการส่งเสริมความร่วมมือกับทุกภาคส่วนในประเทศไปพร้อมๆ กัน

จากผลการศึกษาเชิงเปรียบเทียบ ผู้เขียนเห็นว่า ประเทศไทยควรให้ความสำคัญอันดับแรกกับการพัฒนาด้านการเสริมสร้างศักยภาพ โดยเฉพาะอย่างยิ่ง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ประชาชน และการพัฒนาบุคลากร ผู้เชี่ยวชาญ นักเทคนิคตลอดจนการมีหลักสูตร Cybersecurity ในสถาบันการศึกษา ซึ่งเป็นปัจจัยพื้นฐานสำคัญในการขับเคลื่อนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ และอันดับที่ 2 คือ ด้านเทคนิค โดยการจัดสรรงบประมาณในการส่งเสริมการศึกษาและวิจัย การจัดทำมาตรฐาน การนำเทคโนโลยีทันสมัยมาใช้และการร่วมมือกับภาคอุตสาหกรรม

ทั้งนี้ ด้วยข้อจำกัดด้านระยะเวลาในการศึกษา ข้อมูลส่วนใหญ่เป็นข้อมูลทุติยภูมิจากหน่วยงานภาครัฐ จึงทำให้ขาดข้อมูลจากผู้มีส่วนได้ส่วนเสียโดยตรง โดยเฉพาะอย่างยิ่ง จากภาคอุตสาหกรรมและประชาชน ผู้เขียนเห็นว่า หากมีการศึกษาเชิงลึกทั้ง 5 ด้าน จากทั้งสิงคโปร์และไทยก็จะเป็นประโยชน์ต่อการใช้ประกอบการพัฒนาแนวทางการดำเนินการตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยมากยิ่งขึ้น

บทที่ 4
บทสรุปและข้อเสนอแนะ

4.1 สรุปผลการศึกษา

จากคำถามการศึกษาว่า อะไรคือปัจจัย และมีการดำเนินการอย่างไร ที่ทำให้สิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และจะสามารถนำปัจจัยความสำเร็จและวิธีดำเนินนโยบายของสิงคโปร์มาปรับใช้เพื่อการพัฒนาแนวทางการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยได้หรือไม่ อย่างไร สามารถสรุปผลการศึกษาได้ว่า ปัจจัยที่ทำให้สิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ คือ รัฐบาลสิงคโปร์มีวิสัยทัศน์กว้างไกล เล็งเห็นถึงปัญหาและภัยคุกคามไซเบอร์ที่จะมาบั่นทอนโอกาสในการพัฒนาเศรษฐกิจและสังคมที่ต้องขับเคลื่อนด้วยการใช้เทคโนโลยีดิจิทัลและนวัตกรรม จึงได้ให้ความสำคัญกับเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีการดำเนินการอย่างจริงจัง ต่อเนื่องและเป็นระบบ เริ่มตั้งแต่ ปี ค.ศ. 2005 โดยมีการดำเนินการในด้านต่างๆ ที่เป็นปัจจัยสำคัญของความสำเร็จ 5 ด้าน ดังนี้

4.1.1 ด้านกฎหมาย

รัฐบาลสิงคโปร์ให้ความสำคัญกับการออกกฎหมายกฎระเบียบที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เนื่องจากเป็นเครื่องสำคัญในการดำเนินการและเป็นกรอบกฎหมายที่กำหนดนโยบาย ขั้นตอนดำเนินการ และแนวทางปฏิบัติ เพื่อให้หน่วยงานที่เกี่ยวข้องดำเนินการ โดยมีแผนแม่บทและกฎหมายอื่นที่เกี่ยวข้องไม่ว่าจะเป็นกฎหมายเกี่ยวกับการแทรกแซงระบบคอมพิวเตอร์ กฎหมายเกี่ยวกับข้อมูล รวมทั้งการกำหนดกฎระเบียบหรือแนวทางปฏิบัติเกี่ยวกับการป้องกันข้อมูล การแจ้งเมื่อมีการละเมิดข้อมูล การให้ประกาศนียบัตรหรือใบรับรองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการตรวจสอบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ การคุ้มครองข้อมูลส่วนบุคคล การโอนเงินและการทำธุรกรรมอิเล็กทรอนิกส์ โดยรัฐบาลได้มีการแก้ไขและออกกฎหมายและกฎระเบียบอย่างต่อเนื่อง และโดยที่เทคโนโลยีดิจิทัลมีพัฒนารวดเร็ว ดังนั้น รัฐบาลสิงคโปร์จึงให้ความสำคัญกับขั้นตอนก่อนการตรากฎหมายหรือกฎระเบียบต่างๆ โดยมีการหารือและทำการศึกษากับทุกภาคส่วนที่เกี่ยวข้องรวมทั้งนักวิชาการ นักเทคนิค สถาบันการศึกษา และสถาบันวิจัย

4.1.2 ด้านเทคนิค

สิงคโปร์ตระหนักและให้ความสำคัญกับการพัฒนาเทคโนโลยีการสื่อสารโทรคมนาคมและเทคโนโลยีใหม่ๆ เพื่อให้เท่าทันและสามารถป้องกันและรับมือกับภัยคุมคามไซเบอร์ โดยการจัดสรรงบประมาณในการส่งเสริมโครงการต่างๆ ที่จะพัฒนาด้านเทคนิค ส่งเสริมการศึกษาและวิจัย รวมทั้งการนำเทคโนโลยีที่ทันสมัยมาใช้ สิงคโปร์ยังกระตุ้นให้หน่วยงานภาครัฐและเอกชนจัดสรรเงินจำนวนร้อยละ 8 ของงบประมาณในส่วนเทคโนโลยีสารสนเทศ (IT) เพื่อใช้สำหรับ

การรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งถือว่าเป็นการลงทุนในการจัดการความเสี่ยง นอกจากนี้ สิงคโปร์ยังมีกรอบมาตรฐานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานต่างๆ และการมีองค์กรที่จัดทำด้านมาตรฐาน มีการออกใบรับรองผลิตภัณฑ์ที่ผ่านมาตรฐานสากลของการตรวจสอบด้าน Cybersecurity และปัจจัยสำคัญอีกประการหนึ่งคือ ภาครัฐและภาคเอกชนของสิงคโปร์ได้ร่วมมือและทำงานร่วมกันอย่างใกล้ชิดและต่อเนื่อง รวมทั้งมีพันธมิตรเพิ่มขึ้นเรื่อยๆ ในการพัฒนาและนำมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์มาใช้

4.1.3 ด้านองค์กร

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นนโยบายสำคัญลำดับต้นๆ ของสิงคโปร์ ดังนั้นรัฐบาลและคณะรัฐมนตรีจึงเป็นหน่วยควบคุมดูแลสูงสุด มีการจัดตั้งองค์กร หน่วยงานที่กำหนดนโยบาย มีการกำหนดยุทธศาสตร์ในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ รวมทั้งมีหน่วยงานที่รับผิดชอบการรับมือกับภัยคุกคามไซเบอร์ได้อย่างครอบคลุม และมีการประสานงานข้ามองค์กรระหว่างหน่วยงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ทำให้การดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ประสบความสำเร็จบรรลุตามเป้าหมายและแผนยุทธศาสตร์ระดับชาติ โดยมีการจัดตั้งหน่วยงานสำคัญคือ Cyber Security Agency (CSA) ที่มีหน้าที่พัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ การป้องกัน CII และการให้บริการที่จำเป็นและประสานความร่วมมือในระดับชาติในการรับมือกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ รวมทั้งยังมีหน้าที่พัฒนาและบังคับใช้กฎระเบียบ นโยบาย การปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ พัฒนาระบบนิเวศน์ความมั่นคงปลอดภัยไซเบอร์ให้มีความมั่นคงเข้มแข็ง และสร้างความมั่นใจในการตอบสนองรับมือต่ออาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ โดยทำงานประสานงานกับทั้งภาครัฐ ภาคอุตสาหกรรม สถาบันการศึกษา ภาคธุรกิจ และภาคประชาสังคม รวมถึงระดับระหว่างประเทศ โดยมีหน่วยงานใต้สังกัดที่สำคัญคือศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศสิงคโปร์ (SingCERT) ทั้งนี้ ผลการศึกษายังพบว่า หน่วยงานที่เกี่ยวข้องต่างๆ ของสิงคโปร์ได้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องอย่างเคร่งครัด ทำให้ระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์เป็นไปอย่างมีประสิทธิภาพ แม้จะมีช่องโหว่อยู่บ้าง แต่ก็สามารถรับมือได้อย่างทันท่วงที ทำให้ลดความเสียหายที่จะเกิดขึ้น

4.1.4 ด้านการเสริมสร้างศักยภาพ

รัฐบาลสิงคโปร์เล็งเห็นว่าในโลกยุคดิจิทัล เทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็ว มีผลทำให้วงจรของนวัตกรรมจะสั้นลง เศรษฐกิจในอนาคตจะต้องอาศัยคนที่มีทักษะอย่างเชี่ยวชาญ และต้องได้รับแรงจูงใจที่จะเรียนรู้ได้ตลอดชีวิต ภาคธุรกิจจะต้องอาศัยนวัตกรรม โดยหนึ่งในยุทธศาสตร์ที่สิงคโปร์กำหนดไว้เพื่อบรรลุวิสัยทัศน์ดังกล่าวคือ การเสริมสร้างศักยภาพด้านดิจิทัลให้แข็งแรง โดยจะต้องส่งเสริมการใช้เทคโนโลยีดิจิทัลในทุกภาคส่วนของเศรษฐกิจและจะต้องสร้างความสามารถในด้านเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการวิเคราะห์ข้อมูลและความมั่นคงปลอดภัยไซเบอร์ รัฐบาลสิงคโปร์มีการรณรงค์สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่สาธารณะชนอย่างต่อเนื่อง มีนโยบายส่งเสริมเรื่องมาตรฐาน cybersecurity และการให้ใบรับรองแก่ผู้เชี่ยวชาญ/ผู้ชำนาญการในเรื่องดังกล่าว มีการฝึกอบรมให้แก่ผู้เชี่ยวชาญ/ผู้ชำนาญการด้าน

cybersecurity มีหลักสูตรในสถาบันการศึกษาและในโปรแกรมการศึกษาของประเทศ ส่งเสริมให้เยาวชนมีทักษะและสนใจในด้าน cybersecurity ผ่านโครงการต่างๆ การมีโครงการศึกษาวิจัยและการพัฒนา (R&D) มีมาตรการส่งเสริมแรงจูงใจ และการส่งเสริมอุตสาหกรรมเกี่ยวกับความมั่นคงปลอดภัยให้เติบโตในประเทศ โดยรัฐบาลสิงคโปร์ทำงานอย่างใกล้ชิดกับภาคอุตสาหกรรมและสถาบันการศึกษาในการริเริ่มโครงการต่างๆ ที่ส่งเสริมการเติบโตและพัฒนาสายงานอาชีพด้านความมั่นคงปลอดภัยไซเบอร์

4.1.5 ด้านความร่วมมือ

สิงคโปร์ได้มีการจัดทำความตกลงทวิภาคีและพหุภาคีว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับหน่วยงานทั้งภายในประเทศและระหว่างประเทศ และหน่วยงานในระดับระหว่างประเทศ ทั้งในส่วนของการแลกเปลี่ยนข้อมูลเกี่ยวกับเหตุการณ์ภัยคุกคาม การแบ่งปันแบบปฏิบัติที่ดีในเรื่องการปกป้อง CII การพัฒนาระบบนิเวศน์ไซเบอร์ รวมทั้งความร่วมมือในการฝึกอบรมและแลกเปลี่ยนผู้เชี่ยวชาญ โดยสิงคโปร์ได้ขยายความร่วมมือกับประเทศต่างๆ และภาคอุตสาหกรรมด้าน Cybersecurity เพิ่มขึ้นทุกปี นอกจากนี้ ในส่วนของการเข้าร่วมในเวทีระหว่างประเทศ สิงคโปร์จัดงาน Singapore International Cyber Week เป็นประจำทุกปี เริ่มตั้งแต่ปี ค.ศ. 2016 ซึ่งมีผู้นำด้าน Cybersecurity จากทั้งระดับภูมิภาคและระหว่างประเทศเข้าร่วมงานเพื่อพูดคุยแลกเปลี่ยนประสบการณ์และเสริมสร้างความร่วมมือระหว่างกัน ทั้งจากผู้กำหนดนโยบาย ผู้เชี่ยวชาญจากภาคอุตสาหกรรม และหน่วยงานอื่นๆ ที่มิใช่ภาครัฐ ความสำเร็จที่เด่นชัดของสิงคโปร์ในด้านนี้คือ การเป็นผู้นำและทำงานร่วมมือกับประเทศสมาชิกอาเซียนในเรื่องข้อเสนอการจัดทำแนวทางสำหรับกลไกเพื่อส่งเสริมการประสานงานด้านความมั่นคงปลอดภัยทางสารสนเทศของอาเซียน และการจัดทำบรรทัดฐานพฤติกรรมของรัฐในด้านไซเบอร์

4.2 ข้อเสนอแนะ

4.2.1 ข้อเสนอแนะเชิงนโยบาย

ยุทธศาสตร์ชาติ พ.ศ. 2561–2580 เป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืน และเป็นกรอบในการจัดทำแผนต่างๆ ของประเทศไทยให้สอดคล้องและบูรณาการกันเพื่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว โดยภายใต้ประเด็นยุทธศาสตร์ชาติด้านความมั่นคงข้อ 4.2 การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง กำหนดให้มีการแก้ไขปัญหาเดิมที่มีอยู่อย่างตรงประเด็นจนหมดไปอย่างรวดเร็ว และป้องกันไม่ให้ปัญหาใหม่เกิดขึ้น ซึ่งรวมถึงปัญหาอาชญากรรมทางไซเบอร์ และการติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่ ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ นอกจากนี้ ประเด็นยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขันภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ ได้ระบุถึงการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยไซเบอร์เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ ต่อเศรษฐกิจและสังคม และปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล

จากการศึกษาปัจจัยที่ทำให้ประเทศสิงคโปร์ประสบความสำเร็จในการดำเนินนโยบายด้านความมั่นคงปลอดภัยไซเบอร์พบว่าสอดคล้องกับประเด็นยุทธศาสตร์ชาติด้านความมั่นคงและด้านการสร้างความสามารถในการแข่งขัน จึงเห็นว่าสามารถนำปัจจัยความสำเร็จและวิธีดำเนิน

นโยบายของสิงคโปร์ โดยเฉพาะประเด็น 5 ด้านหลัก ได้แก่ ด้านกฎหมาย ด้านเทคนิค ด้านองค์กร ด้านการเสริมสร้างศักยภาพ และด้านความร่วมมือ มาปรับใช้เพื่อการพัฒนาแนวทางการดำเนินนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยได้ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมสามารถนำผลการศึกษานี้ใช้ประกอบการพิจารณาดำเนินการเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และเพื่อให้เกิดความร่วมมือในมิติด้านการต่างประเทศอย่างเป็นรูปธรรม เห็นควรเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมขยายความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับกระทรวงสื่อสารและสารสนเทศของสิงคโปร์ ภายใต้บันทึกความเข้าใจระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแห่งราชอาณาจักรไทยและกระทรวงการสื่อสารและสารสนเทศแห่งสาธารณรัฐสิงคโปร์ว่าด้วยความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ฉบับลงนามเมื่อวันที่ 31 พฤษภาคม 2559 อย่างไรก็ดี โดยที่บันทึกความเข้าใจฉบับดังกล่าวมีผลใช้บังคับในวันที่ลงนามโดยคู่ภาคี และมีผลใช้บังคับเป็นระยะเวลา 36 เดือน หลังจากนั้น ประกอบกับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เปลี่ยนเป็นกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงเห็นควรเสนอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการเจรจากับกระทรวงการสื่อสารและสารสนเทศของสิงคโปร์เพื่อขอขยายระยะเวลาของบันทึกความเข้าใจดังกล่าว และจัดทำรายละเอียดความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์แนบท้ายบันทึกความเข้าใจที่จะได้จัดทำระหว่างกันต่อไป

4.2.2 ข้อเสนอแนะในการดำเนินการ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดในบทเฉพาะการให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ และในระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จให้สำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ ในการนี้ เห็นควรเสนอแนะแนวทางการดำเนินการดังนี้

1) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยหน่วยงานที่เกี่ยวข้องกับการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะต้องรวบรวม ศึกษาวิเคราะห์ ข้อมูลที่เกี่ยวข้อง เพื่อจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยในเบื้องต้น อาจศึกษาวิเคราะห์ข้อมูลบนพื้นฐานตัวชี้วัด 5 เสาหลักที่สหภาพโทรคมนาคมระหว่างประเทศได้กำหนดไว้

2) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ควรกำหนดแนวทางและขอบเขตความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์กับสิงคโปร์ว่า ต้องการได้ประโยชน์อะไรและอย่างไรจากสิงคโปร์ เช่น การไปศึกษาดูงานของสิงคโปร์ ควรกำหนดว่าต้องการไปดูงานเรื่องอะไร พบหารือกับใคร ระดับไหน หน่วยงานไหน

3) ในด้านความร่วมมือระหว่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมควรพิจารณาว่าสามารถใช้ประโยชน์จากบันทึกความเข้าใจด้านเทคโนโลยีสารสนเทศและการสื่อสารและเทคโนโลยีดิจิทัล ที่มีกับประเทศต่างๆ เพื่อขยายความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างไรบ้าง รวมทั้ง พิจารณาความเป็นไปได้ในการขยายความร่วมมือทั้งในลักษณะทวิภาคีและพหุ

ภาคีกับประเทศ กลุ่มประเทศ หรือองค์การระหว่างประเทศอื่นๆ ที่เห็นว่าจะเป็นประโยชน์ต่อประเทศไทย โดยอาจทำในลักษณะการดำเนินงานภายใต้ MoU การจัดการประชุมหรือกิจกรรมประจำปีร่วมกับพันธมิตรทั้งในประเทศและต่างประเทศ โดยเฉพาะอย่างยิ่งในกรอบของอาเซียนและเอเปค

4) เนื่องจากการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นเรื่องที่ต้องมีการดำเนินงานข้ามองค์กร (cross–sectorial) ทั้งระหว่างหน่วยงานของรัฐ ระหว่างภาคอุตสาหกรรม และทั้งในลักษณะความร่วมมือระหว่างภาครัฐและเอกชน ประเทศไทยควรพิจารณารูปแบบการทำงานเพื่อทำให้การดำเนินงานบรรลุตามเป้าหมาย

5) รัฐบาลไทยอาจพิจารณาจัดสรรงบประมาณเพิ่มเติมและเป็นประจำทุกปี เพื่อใช้ในการส่งเสริมพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ การวิจัยและพัฒนาการจัดหาเทคโนโลยีที่รองรับและเพิ่มประสิทธิภาพการทำงาน

6) ประเทศไทยควรดำเนินการเรื่องการสร้างความตระหนักรู้ทั้งในระดับภาครัฐ ภาคอุตสาหกรรมและผู้ประกอบการ และประชาชนทุกระดับ โดยกระทำอย่างต่อเนื่องร่วมกับทุกภาคส่วน โดยอาจใช้สื่อสังคมออนไลน์เป็นช่องทางในการเผยแพร่ช่องทางหนึ่ง

บรรณานุกรม

หนังสือ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ยุทธศาสตร์ชาติ พ.ศ. 2561–2580

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, 2559.

เคอร์บาลิจา โจวาน. เปิดประตูสู่การอภิบาลอินเทอร์เน็ต. แปลโดย พิภพ อุดมอิทธิพงศ์. กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง, 2558.

Tapscott Don. เศรษฐกิจดิจิทัล. แปลและเรียบเรียงโดย พรศักดิ์ อุรัจฉัทชัยรัตน์. กรุงเทพมหานคร: แมคกรอ–ฮิล อินเตอร์เนชั่นแนล เอ็นเตอร์ไพรส์ แอลแอลซี, 2558.

ASEAN Secretariat. The ASEAN ICT Masterplan 2020. Jakarta: ASEAN, 2015.

Cyber Security Agency of Singapore. Singapore Cyber Landscape 2016. Singapore: Cyber Security Agency of Singapore, 2017.

_____. Singapore Cyber Landscape 2017. Singapore: Cyber Security Agency of Singapore, 2018.

_____. Singapore's Cybersecurity Strategy. Singapore: Cyber Security Agency of Singapore, 2016.

International Telecommunication Union. Global Cybersecurity Index & Cyberwellness Profiles. Geneva: International Telecommunication Union, 2015.

_____. Global Cybersecurity Index (GCI) 2017. Geneva: International Telecommunication Union, 2017.

_____. Global Cybersecurity Index (GCI) 2018. Geneva: International Telecommunication Union, 2018.

ThaiCERT, Electronic Transactions Development Agency (Public Organization). Cybersecurity for Critical Information Infrastructure in Thailand. 1st Edition. Bangkok: Thailand Computer Emergency Response Team (ThaiCERT), 2018.

สื่ออิเล็กทรอนิกส์

ไทยเซิร์ต. ThaiCERT Annual Report 2016. [ออนไลน์]. 2561. แหล่งที่มา: www.thaicert.or.th.

วิกิพีเดีย สารานุกรมเสรี. นวัตกรรม. [ออนไลน์]. 2562. แหล่งที่มา: https://th.wikipedia.org/.

สำนักงานสถิติแห่งชาติ. สรุปผลที่สำคัญ การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2561 (ไตรมาส 1). [ออนไลน์]. 2561. แหล่งที่มา: www.nso.go.th

อิสระสรรค์ กันทะอุโมงค์. Digital Economy โอกาสที่มาพร้อมกับความท้าทาย. [ออนไลน์]. 2018. แหล่งที่มา: https://www.scbeic.com/th/detail/product/3010

Hackman Mark. 7 ภัยคุกคามไซเบอร์ที่น่ากลัวที่สุดในโลก จัดอันดับโดย SANS Institute. แปลและเรียบเรียงโดย Techtalkthai. [ออนไลน์]. 2017. แหล่งที่มา: https://www.techtalkthai.com/7-deadly-attacks-by-sans/

ThaiCERT ETDA. สถิติภัยคุกคาม. [ออนไลน์]. 2018. แหล่งที่มา: https://www.thaicert.or.th/statistics2018.html.

Committee on the Future Economy. Report of the Committee on the Future Economy: Pioneers of the Next Generation. [Online]. 1997. Available from: https://www.gov.sg/~/media/cfe/downloads/cfe%20report.pdf?la=en.

Cyber Security Agency of Singapore. CSA and Cisco Systems Sign Memorandum of Collaboration to Establish a Framework for Cybersecurity Cooperation. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press-releases/csa-and-cisco-systems-sign-memorandum-of-collaboration-to-establish-a-framework-for-cybersecurity-cooperation.

_____. Cybersecurity Act. [Online]. 2019. Available from: https://www.csa.gov.sg/legislation/cybersecurity-act

_____. Cyber Threats in Singapore Grew in 2017, Mirroring Global Trends. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press-releases/cyber-threats-in-singaporegrew-in-2017-mirooing-global-trends.

_____. GovTech and CSA Partner Cybersecurity Community on Government Bug Bounty Programme. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press–releases/govtech-and-csa-partner-cybersecurity-community-on-government-bug-bounty-programme.

_____. Singapore and New Zealand Sign Formal Arrangement to Further Cybersecurity Cooperation. [Online]. 2018. Available from: https://www.csa.gov.sg/news/press–releases/singapore-and-new-zealand-sign-formal-arrangement-to-further-cybersecurity-cooperation.

Drew & Napier LLC. Cybersecurity in Singapore. [Online]. 2019. Available from: https://www.todayonline.com/. [29 April 2019].

FTI Consulting. Singapore's Approach to Cyber Security. [Online]. 2016. Available from: www.fticonsulting.com.

Todayonline. A growing threat. [Online]. 2019. Available from: https://www.todayonline.com/big-read/big-read-mpre-cyber-aattacks-loom-singapore-weal-first-line-defence. [6 June 2019].

World Economic Forum. The Global Risks Report 2019. 14th Edition. [Online]. 2019. Available from: www.weforum.org.

Yu Eileen. Singapore now able to certify products under global cybersecurity Standard. [Online]. 2019. Available from: https://www.zdnet.com/article/singapore-now-able-to-certify-global-cybersecurity-standard/.

ประวัติผู้เขียน

ชื่อ–สกุล นางสาวกัลยา ชินาธิวร

ประวัติการศึกษา
– Master of Business (Public Sector Management), Victoria University, Australia
– ศิลปศาตร์บัณฑิต (เอกภาษาอังกฤษ) มหาวิทยาลัยเชียงใหม่

ประวัติการรับราชการ

ประวัติการทำงานและการรับราชการ			
ชื่อตำแหน่ง	**สังกัด**	**ช่วงเวลาที่ดำรงตำแหน่ง**	**รวมเวลาดำรงตำแหน่ง**
1. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 3–6)	สำนักงานปลัดกระทรวงคมนาคม (กองกิจการระหว่างประเทศ)	17 มิ.ย. 34–30 พ.ย. 47	13 ปี 5 เดือน
2. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 6)	สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ)	30 พ.ย. 47–8 พ.ค. 48	5 เดือน
3. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 7)	สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ)	9 พ.ค 48–19 ก.ย. 50	2 ปี 3 เดือน
4. เจ้าหน้าที่วิเทศสัมพันธ์ (ระดับ 8 และระดับชำนาญการพิเศษ)	สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (สำนักกิจการระหว่างประเทศ) ปัจจุบันคือกองการต่างประเทศ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	20 ก.ย. 50–27 ม.ค. 62	11 ปี 4 เดือน

ตำแหน่งปัจจุบัน ผู้อำนวยการกองการต่างประเทศ (อำนวยการสูง)
สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ผลงานด้านการต่างประเทศที่สำคัญ

1. เป็นผู้รับผิดชอบหลักในการสมัครรับเลือกตั้งตำแหน่งสมาชิกสภาบริหารของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ของไทย ปี ค.ศ 2006 ค.ศ. 2010 ค.ศ. 2014 และ ค.ศ. 2018 โดยไทยได้รับเลือกตั้งและดำรงตำแหน่งติดต่อกันทั้ง 4 สมัย
2. การทำหน้าที่เป็นผู้ประสานงานหลักในการจัดงาน ITU Telecom Asia 2008 ระหว่างวันที่ 2–5 กันยายน 2551 ณ ศูนย์แสดงสินค้าและการประชุมอิมแพ็ค เมืองทองธานี เป็นการจัดงานร่วมกับ ITU ที่เป็นทบวงการชำนัญพิเศษภายใต้สหประชาชาติ และถือเป็นงานแรกของกระทรวงเทคโนโลยีสารสนเทศ (ปัจจุบันคือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) ในการจัดงานระดับ World Class ด้านการแสดงนวัตกรรมด้านโทรคมนาคมและ ICT ซึ่งรวมทั้งการจัดการประชุมเชิงวิชาการ
3. การทำหน้าที่เป็นหน่วยงานกลางของประเทศไทยในการเตรียมการเข้าร่วมการประชุมสำคัญด้านโทรคมนาคมทั้งในระดับภูมิภาคและระดับโลก โดยการจัดตั้งคณะกรรมการและคณะทำงานที่เกี่ยวข้อง ทั้งด้านสารัตถะและพิธีการ และการแต่งตั้งคณะผู้แทนไทยตลอดจนการประสานงานกับองค์การระหว่างประเทศที่เกี่ยวข้อง เข้าร่วมการประชุมในฐานะผู้แทนไทยทั้งการประชุมระดับภูมิภาคและระดับโลก จัดทำท่าทีสำหรับคณะผู้แทนไทย จัดทำร่างคำกล่าวสำหรับผู้บริหาร เตรียมการเกี่ยวกับการหารือทวิภาคี และจัดทำรายงานการประชุมต่างๆ ที่สำคัญ เช่น
   - การประชุมสุดยอดผู้นำว่าด้วยสังคมสารสนเทศ ปี 2548 ณ ประเทศตูนีเซีย
   - การประชุมใหญ่ผู้แทนผู้มีอำนาจเต็ม ปี 2549 ณ ประเทศตุรกี /ปี 2553 ณ ประเทศเม็กซิโก / ปี 2557 ณ สาธารณรัฐเกาหลี/ และปี 2561 ณ สหรัฐอาหรับเอมิเรตส์
   - การประชุมระดับโลกว่าด้วยการพัฒนาโทรคมนาคม ปี 2549 ณ ประเทศการ์ตา/ ปี 2553 ณ ประเทศอินเดีย/ ปี 2557 ณ สหรัฐอาหรับเอมิเรตส์/ และปี 2560 ณ ประเทศอาเจนตินา
   - การประชุมระดับโลกว่าด้วยมาตรฐานโทรคมนาคม ปี 2551 ณ ประเทศแอฟริกาใต้/ ปี 2555 ณ สหรัฐอาหรับอิมิเรตส์
   - การประชุมระดับโลกว่าด้วยนโยบายโทรคมนาคม ปี 2551 ณ ประเทศโปรตุเกส
   - การประชุมระดับโลกว่าด้วยกฎระเบียบโทรคมนาคมระหว่างประเทศ ปี 2553 ณ สหรัฐอาหรับเอมิเรตส์
   - การประชุมรัฐมนตรีด้านเทคโนโลยีสารสนเทศและการสื่อสารของภูมิภาคเอเชียและแปซิฟิกขององค์การโทรคมนาคมแห่งเอเชียและแปซิฟิก ณ บรูไนดารุสซาลาม ระหว่างวันที่ 10–11 กันยายน 2557
   - การประชุมสภาบริหารของ ITU ณ นครเจนีวา สมาพันธรัฐสวิส ระหว่างปี 2558–2561

– การประชุมสมัชชาและการประชุมคณะกรรมการจัดการและการประชุมอื่นๆ ขององค์การโทรคมนาคมแห่งเอเชียและแปซิฟิก ระหว่างปี 2548–ปัจจุบัน

4. การทำหน้าที่ผู้ประสานงานหลักในการจัดการประชุม Connect Asia–Pacific Summit 2013

เป็นการจัดประชุมระดับผู้นำครั้งแรกสำหรับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (เดิม) มีผู้นำประเทศเข้าร่วมการประชุมจำนวน 7 ประเทศ ผู้แทนระดับรัฐมนตรีจากประเทศสมาชิกในภูมิภาคฯ จำนวน 30 ประเทศ รวมผู้เข้าประชุมกว่า 600 คน วัตถุประสงค์หลักเพื่อรับรองเอกสารวิสัยทัศน์ผู้นำที่ระบุถึงการตระหนักรู้ถึงความสำคัญของการใช้ประโยชน์จากโอกาสอันมากมายสำหรับการพัฒนาโครงสร้างพื้นฐานและการประยุกต์ใช้ที่สร้างสรรค์ เพื่อเปลี่ยนชีวิตของประชาชนไปในทางที่ดีขึ้น ซึ่งจะเกิดควบคู่ไปกับการมุ่งหน้าสู่ความสำเร็จตามวิสัยทัศน์ “Smartly DIGITAL” ภายในปี ค.ศ. 2020

5. การสมัครรับเลือกตั้งตำแหน่งเลขาธิการและรองเลขาธิการขององค์การโทรคมนาคมแห่งเอเชียและแปซิฟิก (Asia–Pacific Telecommunity: APT)

รับผิดชอบ การกำหนดยุทธศาสตร์ แผนงาน/กลยุทธ์ แผนงบประมาณ และดำเนินการในการเสนอชื่อผู้สมัครของไทยในตำแหน่งเลขาธิการและรองเลขาธิการของ APT ตามนโยบายของรัฐบาลในการส่งเสริมบทบาทของคนไทยในเวทีองค์การระหว่างประเทศ โดยได้ดำเนินการ 4 สมัยดังนี้

– ตำแหน่งรองเลขาธิการ (นายไกรสร พรสุธี) วาระปี ค.ศ. 2008–2011 และวาระปี ค.ศ. 2012–2014
– ตำแหน่งเลขาธิการ (นางสาวอารีวรรณ ฮาวรังษี) วาระปี ค.ศ. 2015–2018 และวาระปี ค.ศ. 2018–2021

6. ทำหน้าที่ในนามผู้แทนไทยในคณะทำงาน/กลุ่มศึกษาต่างๆ ขององค์การระหว่างประเทศอาทิ

– ทำหน้าที่รองประธานในคณะทำงานเตรียมการภูมิภาคเอเชียและแปซิฟิกสำหรับการประชุมใหญ่ผู้แทนผู้มีอำนาจเต็ม ปี ค.ศ. 2010 ระยะเวลาดำรงตำแหน่ง 4 ปี
– ทำหน้าที่รองประธานในคณะทำงานเตรียมการภูมิภาคเอเชียและแปซิฟิกสำหรับการประชุมระดับโลกว่าด้วยการพัฒนาโทรคมนาคม ปี ค.ศ. 2016 ระยะเวลาดำรงตำแหน่ง 4 ปี
– ทำหน้าที่ในคณะทำงาน Working Group of Management Committee on APT Legal Instruments ขององค์การโทรคมนาคมแห่งเอเชียและแปซิฟิก (ปี 2558–ปัจจุบัน)
– เป็นกรรมการในคณะกรรมการจัดการโครงการ ITU Asia–Pacific Centres of Excellence (ASP CoEs) ระหว่างปี 2557–2561 และทำหน้าที่เป็นประธานกรรมการ 3 ครั้ง
– จัดทำร่างข้อเสนอในนามประเทศไทยในการประชุมระหว่างประเทศและนำเสนอในนามของประเทศไทยและภูมิภาคเอเชียและแปซิฟิก

7. เป็นวิทยากรในนามของประเทศไทย ดังนี้
   - เป็นวิทยากรในนามตัวแทนของภูมิภาคเอเชียแปซิฟิก บรรยายในหัวข้อ “The ITU Asia–Pacific Centre of Excellence: Experiences and implementation of the new Strategy” ในการประชุม ITU Asia–Pacific Regional Development Forum 2015: SMARTLY DIGITAL ณ กรุงเทพ ระหว่างวันที่ 21–22 สิงหาคม 2558
   - เป็นวิทยากรร่วมบรรยายและอภิปรายในหัวข้อ “ITU Centres of Excellence model” โดยได้ใช้กรณีศึกษาของประเทศไทยประกอบการบรรยาย ในการประชุม Global ICT Capacity Building Symposium (CBS–2016) ณ กรุงไนโรบี ประเทศเคนยา ระหว่างวันที่ 6–8 กันยายน 2559
   - เป็นวิทยากรบรรยายหัวข้อ “Facilitating Asia–Pacific Regional Initiatives through research, study, initiatives, partnerships and capacity building” ในการประชุม The Asia–Pacific Regional Development Forum 2018 (ASP–RDF–18) ณ กรุงเทพฯ ระหว่างวันที่ 21–22 พฤษภาคม 2561