คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

อริย์ธัช แก้วเกาะสะบ้า
วิทยากรชำนาญการพิเศษ
กลุ่มงานบริการวิชาการ 1 สำนักวิชาการ

ประเทศไทยให้ความสำคัญกับความมั่นคงปลอดภัยไซเบอร์ โดยคณะรัฐมนตรีได้อนุมัติหลักการร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... เมื่อวันที่ 6 มกราคม 2558 ซึ่งได้กำหนดกรอบแนวความคิดของร่างพระราชบัญญัติให้ครอบคลุมในเรื่องความมั่นคงปลอดภัยของระบบข้อมูล สิทธิเสรีภาพของประชาชน การรักษาความมั่นคงของประเทศ และการร่วมมือกันของบุคคลที่เกี่ยวข้องกับโลกไซเบอร์ ในระหว่างการจัดทำกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อเสนอต่อสภานิติบัญญัติแห่งชาติ จำเป็นต้องให้มีคณะกรรมการเตรียมการด้านรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเตรียมการด้านการพัฒนาและรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ได้อย่างทันท่วงทีอันจะช่วยคุ้มครองและสร้างความเชื่อมั่นให้กับบุคคลที่เกี่ยวข้องทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคม รัฐบาลได้ประกาศใช้ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 ซึ่งเป็นการเตรียมการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อรับมือกับการถูกโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) เป็นกระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรไม่มีความเสี่ยงและความเสียหายที่ส่งผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่ออาชญากรรมทางคอมพิวเตอร์ การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล 3 ประการ ได้แก่ 1) การรักษาความลับของข้อมูล (Confidentiality) 2) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และ3) ความพร้อมใช้งานของข้อมูล (Availability) ซึ่งความมั่นคงปลอดภัยไซเบอร์มีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้น การที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้น ได้ถูกกำหนดเอาไว้เป็นมาตรฐานเป็นที่ยอมรับโดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตน และอาจเพิ่มเติมหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ

ความหมายของความมั่นคงปลอดภัยไซเบอร์

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้ความหมายของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” คือ ภาพรวมของเครื่องมือ นโยบาย แนวคิดการรักษาความปลอดภัย การรักษาความปลอดภัย แนวทาง วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีปฏิบัติที่เป็นเลิศ การรับประกัน และเทคโนโลยีที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ ประเทศไทยยังไม่มีนิยามของคำว่าความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศได้ให้นิยามคำว่า “ความมั่นคงปลอดภัยไซเบอร์” คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ (ส่วนนโยบายอิเล็กทรอนิกส์, 2559) ดังนั้น ความหมายของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” อาจจะมีความหมายแตกต่างกันของแต่ละองค์กร อย่างไรก็ตาม ประเทศไทยมีความหมายของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 ดังนี้

“ไซเบอร์” หมายความว่า กิจกรรมที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ การสื่อสารข้อมูลคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์

“ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการและการดำเนินการเพื่อปกป้อง ป้องกัน การส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

ทั้งนี้ เพื่อเป็นการเตรียมการด้านการรักษาความปลอดภัยไซเบอร์ จึงได้มีการตั้งคณะกรรมการขึ้นมาคณะหนึ่ง เรียกว่า “คณะกรรมการเตรียมการด้านการรักษาความปลอดภัยไซเบอร์แห่งชาติ” โดยมีนายกรัฐมนตรีเป็นประธานกรรมการและมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเลขานุการ โดยคณะกรรมการฯ มีหน้าที่และอำนาจ ดังต่อไปนี้

1. จัดทำนโยบายและแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอให้คณะรัฐมนตรีเพื่อพิจารณาอนุมัติ

2. เสนอแนะต่อคณะรัฐมนตรีเกี่ยวกับการดำเนินการตามนโยบายและแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งเสนอมาตรการการแก้ไขปัญหาอุปสรรค การปฏิบัติการตามนโยบายและแผนระดับชาติ เพื่อให้การดำเนินการปกป้อง รับมือ ป้องกัน และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศมีความมั่นคงและยั่งยืน

3. ติดตาม ตรวจสอบ และประเมินผลการดำเนินการ รวมทั้งประสานความร่วมมือกับคณะกรรมการระดับชาติหรือคณะกรรมการที่ตั้งขึ้นตามกฎหมายอื่น เพื่อให้รับเอาหรือให้มีการดำเนินนโยบายสานต่อหรือ

สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้การดำเนินการและการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสอดคล้องและเป็นไปในทิศทางเดียว

4. เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมาย กฎ ระเบียบ และข้อบังคับต่าง ๆ ที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์อันกระทบต่อความมั่นคงของชาติ

5. เสนอแนะต่อคณะรัฐมนตรีเกี่ยวกับการประสานความร่วมมือกับหน่วยงานของรัฐและหน่วยงานเอกชน เพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

6. เสนอแนะต่อคณะรัฐมนตรีเกี่ยวกับการประสานความร่วมมือแนวทางการพิจารณาอนุมัติโครงการที่เป็นการพัฒนาเพื่อยับยั้งปัญหาภัยคุกคามไซเบอร์ระหว่างหน่วยงานของรัฐและหน่วยงานเอกชนในกิจการของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

7. กำกับดูแลและติดตามการดำเนินการตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

8. เชิญเจ้าหน้าที่ของรัฐ บุคคล หรือหน่วยงานที่เกี่ยวข้องมาชี้แจง ให้ข้อเท็จจริง ความเห็น หรือคำแนะนำ หรือขอให้จัดส่งเอกสารหรือหลักฐานที่เกี่ยวข้องเพื่อประกอบการพิจารณาได้ตามความจำเป็น

9. แต่งตั้งคณะอนุกรรมการหรือคณะทำงาน เพื่อพิจารณาหรือทำการใด ๆ ตามที่คณะกรรมการมอบหมาย

10. เตรียมการจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

11. ปฏิบัติการอื่นใดเพื่อให้เป็นไปตามระเบียบนี้ หรือตามที่คณะรัฐมนตรีหรือนายกรัฐมนตรีมอบหมาย

นอกจากนี้ เพื่อเป็นการรักษาความมั่นคงปลอดภัยไซเบอร์ยังได้มีนโยบายและแผนระดับชาติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีแนวทางการดำเนินการในเรื่อง ดังต่อไปนี้

1. การบูรณาการและการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึงความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ รวมถึงที่อาจจะส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวมให้มีความเป็นเอกภาพ

2. การพัฒนาและการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งการจัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น โดยให้ครอบคลุมถึงมิติการรักษาความมั่นคงปลอดภัยทางการทหาร การรักษาความสงบเรียบร้อยภายในประเทศ โครงสร้างพื้นฐานสำคัญของประเทศ และรักษาความมั่นคงทางเศรษฐกิจ

3. การปกป้องด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ในเรื่องของระบบความปลอดภัยด้านสาธารณสุข พลังงาน เศรษฐกิจ ระบบการเตือนภัยต่าง ๆ และการละเมิดสิทธิส่วนบุคคลที่มีกรอบเนื้อหาที่ชัดเจน และมีระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย สามารถรับมือกับภัยที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิผล

4. การประสานความร่วมมือระหว่างหน่วยงานของรัฐและหน่วยงานเอกชนในการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ และการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

5. การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยการสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน ตลอดจนการพัฒนาทางด้านไอทีที่มีประสิทธิภาพ

6. การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ควรจะมีกฎหมายที่บังคับใช้ในด้านการจารกรรมไซเบอร์ที่ชัดเจน เหมาะสม และสามารถบังคับใช้ได้จริง

7. การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

8. การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ ตลอดจนการสร้างประชาคมข่าวสารเพื่อแลกเปลี่ยนความรู้ ความร่วมมือ และควรจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศให้มีความชัดเจนยิ่งขึ้น

ดังนั้น คณะกรรมการพิจารณากำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศและวางกรอบการประสานความร่วมมือระหว่างหน่วยงานของรัฐและหน่วยงานเอกชนโดยอย่างน้อยต้องประกอบด้วย

1. หน่วยงานประสานงานกลางว่าด้วยความมั่นคงปลอดภัยไซเบอร์

2. หน่วยงานเผชิญเหตุฉุกเฉินทางไซเบอร์

3. กรอบมาตรฐานการรักษาความปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐและหน่วยงานภาคเอกชนตามหลักการบริหารความเสี่ยงต้องประกอบด้วย 1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นกับระบบ ทรัพย์สิน ข้อมูล และอื่น ๆ 2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น 3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามไซเบอร์ 4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามไซเบอร์ 5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามไซเบอร์

การเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การถูกโจมตีทางไซเบอร์เกิดจากหลายปัจจัย ซึ่งเป็นผลจากการพัฒนาเทคโนโลยีอย่างรวดเร็ว ใช้ง่ายและมีราคาถูก ทำให้คนทั่วโลกสามารถเข้าถึงข้อมูลข่าวสารได้อย่างไร้ขีดจำกัด จึงนำมาซึ่งภัยคุกคามไซเบอร์ที่ก่อให้เกิดผลกระทบที่ร้ายแรง เช่น การรั่วไหลของข้อมูลที่สำคัญหรือข้อมูลที่มีชั้นความลับอันอาจจะส่งผลกระทบต่อเสถียรภาพทางเศรษฐกิจและความมั่นคงของชาติ โดยสภาวะภัยคุกคามไซเบอร์ของไทยนั้นไม่ใช่เพราะเหตุจูงใจเรื่องผลประโยชน์ทางการเงินเพียงอย่างเดียว แต่ยังเกิดจากความหละหลวมในการไม่ใส่ใจต่อความมั่นคงปลอดภัยไซเบอร์ของคนในองค์กร การเตรียมการเพื่อรับมือกับการโจมตีไซเบอร์ รัฐบาลได้มีการประกาศใช้ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 เพื่อนำมาใช้ป้องกันภัยจากการถูกโจมตีไซเบอร์ในภาครัฐ ภาคเอกชน และภาคประชาสังคม รวมทั้งองค์กรที่แสวงหากำไรและไม่แสวงหากำไร ซึ่งรัฐบาลได้ดำเนินมาตรการป้องกันมาโดยตลอด ทั้งนี้ พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี และนายพิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวง

ดิจิทัลเพื่อเศรษฐกิจและสังคม ได้เตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และการเพิ่มศักยภาพในการป้องกันการโจมตีทางไซเบอร์ของประเทศไทย ดังนี้

1. รัฐบาลได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อวันที่ 24 เมษายน 2561 ซึ่งคณะรัฐมนตรีมีมติอนุมัติตามที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เสนอจำนวน 7 คน คือ 1) นายภูมิ ภูมิรัตน กรรมการผู้ทรงคุณวุฒิ ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ 2) นายกิตติ โฆษะวิสุทธิ์ กรรมการผู้ทรงคุณวุฒิ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร 3) นายไพบูลย์ อมรภิญโญเกียรติ กรรมการผู้ทรงคุณวุฒิ ด้านนิติศาสตร์ 4) พันตำรวจเอก ญาณพล ยั่งยืน กรรมการผู้ทรงคุณวุฒิ ด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร 5) พลเอก บรรเจิด เทียนทองดี กรรมการผู้ทรงคุณวุฒิ ด้านโทรคมนาคมหรือดาวเทียม 6) นางมรกต กุลธรรมโยธิน กรรมการผู้ทรงคุณวุฒิ ด้านการบริหารจัดการเทคโนโลยีสารสนเทศ 7) รองศาสตราจารย์ปณิธาน วัฒนายากร กรรมการผู้ทรงคุณวุฒิ ด้านความสัมพันธ์ระหว่างประเทศ

2. รัฐบาลได้ยกร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งคณะรัฐมนตรีมีมติอนุมัติหลักการร่างพระราชบัญญัติฉบับนี้เมื่อวันที่ 6 มกราคม 2558 ซึ่งร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ได้มีการรับฟังความคิดเห็นระหว่างวันที่ 8 มีนาคม 2561-25 มีนาคม 2561 เพื่อให้เป็นไปตามมติคณะรัฐมนตรีเมื่อวันที่ 4 เมษายน 2560 ในเรื่องเกี่ยวกับการจัดทำและการเสนอร่างกฎหมายตามบทบัญญัติมาตรา 77 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดประชุมคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2561 โดยมีพลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานในการประชุมครั้งนี้ได้พิจารณาและมีมติเห็นชอบ 4 เรื่อง คือ 1) กรอบแนวคิดนโยบายและแผนระดับชาติเพื่อปกป้อง รับมือ ป้องกัน และลดความเสี่ยง และให้มีความสอดคล้องไปในทิศทางเดียวกัน 2) แนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศและแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ 3) แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน 4) แนวทางการจัดตั้งหน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความมั่นคงปลอดภัยไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

ทั้งนี้ นายพิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้กล่าวถึงผลของการประชุมที่ผ่านมากับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในปัจจุบัน ดังนี้

1. การประชุมคณะเตรียมการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่ประชุมได้มีมติเห็นชอบให้จัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) 6 กลุ่ม คือ 1) กลุ่มความมั่นคงและบริการภาครัฐ 2) กลุ่มการเงิน 3) กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม 4) กลุ่มการขนส่งและโลจิสติกส์ 5) กลุ่มพลังงานและสาธารณูปโภค 6) กลุ่มสาธารณสุข

2. จัดทำแผนเร่งด่วนและการยกระดับการพัฒนาบุคลากรทางด้านไซเบอร์ มีการเตรียมความพร้อมยกระดับแผนการทำงานร่วมกัน เช่น ซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมถึงจัดทำแผนปฏิบัติการรับมือไซเบอร์ คือ แผนเร่งด่วนขับเคลื่อนความเข้มแข็งไซเบอร์ ส่วนเรื่องของยุทธศาสตร์ด้านการรักษาความมั่นคง

ปลอดภัยไซเบอร์ของประเทศ ถือว่าเป็นสิ่งสำคัญมากในการขับเคลื่อนประเทศ โดยคณะกรรมการชุดนี้ได้กำหนดแผนงานระยะเร่งด่วน 6 เดือน 1 ปี และ 2 ปี ที่หน่วยงานจะร่วมกันทำต่อไปใน 8 ด้าน ที่สอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 คือ 1) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ 3) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ 4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ 5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนากฎหมาย ระเบียบ และมาตรฐานเพื่อความมั่นคงปลอดภัยไซเบอร์ 7) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ 8) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

3. การจัดอันดับด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย สำหรับดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เมื่อเปรียบเทียบกับต่างประเทศนั้น ในปี 2560 สหภาพโทรคมนาคมระหว่างประเทศได้ทำการสำรวจระดับความเอาจริงเอาจัง ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ 5 ด้าน ได้แก่ 1) ด้านกฎหมาย 2) ด้านเทคนิค 3) ด้านหน่วยงานและนโยบาย 4) ด้านการพัฒนาศักยภาพ 5) ด้านความร่วมมือ ซึ่งผลจากการสำรวจพบว่า ประเทศไทยอยู่ในอันดับที่ 22 จาก 194 ประเทศ ขณะเดียวกันเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียน ประเทศไทยอยู่อันดับที่ 3 รองจากประเทศสิงคโปร์ และประเทศมาเลเซีย ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงานที่เกี่ยวข้องจะช่วยกันขับเคลื่อนให้ประเทศไทยอยู่ใน 20 อันดับแรกของประเทศที่มีความพร้อมด้านไซเบอร์ต่อไป

4. ด้านการพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ ประเทศไทยได้จัดตั้ง “ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre) ตามมติที่ประชุม TELMIN-Japan ซึ่งมีการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่นที่ประเทศกัมพูชา โดยประเทศไทยได้รับเลือกให้เป็นเจ้าภาพจัดตั้งศูนย์ฯ และได้มีการเปิดศูนย์ฯ อย่างเป็นทางการเมื่อเดือนมิถุนายน 2561 ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้มอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) เป็นเจ้าภาพหลักในการดำเนินงาน เนื่องจากเป็นหน่วยงานที่มีประสบการณ์ในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศมาอย่างต่อเนื่อง โดยศูนย์ฯ นี้ ได้รับการสนับสนุนจากประเทศญี่ปุ่นทั้งด้านงบประมาณและองค์ความรู้ต่าง ๆ ทำให้สามารถดำเนินการฝึกอบรมให้แก่ประเทศสมาชิกอาเซียนได้อย่างมีประสิทธิภาพ ซึ่งนับเป็นโอกาสสำคัญที่จะได้รับการถ่ายทอดความรู้และประสบการณ์จากประเทศชั้นนำด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นก้าวสำคัญในการยกระดับขีดความสามารถของบุคลากร ซึ่งจะส่งผลดีต่อการประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ในเวทีสากล รวมถึงการพัฒนาให้ประเทศไทยอยู่ในอันดับที่ 20 ของโลกให้ได้ และได้ดำเนินโครงการพัฒนาเพื่อผลิตบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้นอีก 1,000 คน โดยความร่วมมือของภาครัฐ ภาคเอกชน และสถาบันการศึกษา

5. การเตรียมความพร้อมของหน่วยงานประสานงานกลาง โดยมอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ทำหน้าที่เป็นหน่วยประสานงานกลางเป็นการชั่วคราวระหว่างจัดตั้ง (Cyber Security Agency) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ และทำงานร่วมกับหน่วยงานที่เกี่ยวข้อง ลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ (“นายกรัฐมนตรี เป็นประธานประชุม คกก.เตรียมการไซเบอร์แห่งชาติครั้งแรก DE พร้อมตั้งเป้าให้ไทยติดอันดับ 1 ใน 20 ของโลกที่มีความพร้อม,” 2561)

ผลกระทบจากการถูกโจมตีทางไซเบอร์ของประเทศไทย

การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack: DOS) การโจมตีทุกครั้งจะสร้างความเสียหายอย่างมหาศาล กระทบต่อความมั่นคง ความปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ รวมทั้งระบบเศรษฐกิจและความมั่นคงของประเทศ ในปี 2560 ประเทศไทยได้รับการแจ้งเหตุในการโจมตีทางไซเบอร์จำนวน 67 ครั้ง (สราวุธ ปิติยาศักดิ์, น. 1-3) ทั้งนี้ บริษัท ฟรอสต์ แอนด์ ซัลลิแวน (ประเทศไทย) จำกัด ได้ร่วมมือกับบริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด ทำการวิจัยและวิเคราะห์ผลกระทบจากการถูกโจมตีทางไซเบอร์ของประเทศไทย ได้เปิดเผยรายงานการวิจัยพบว่า ความเสียหายทางเศรษฐกิจในประเทศไทยที่เป็นผลกระทบมาจากการถูกโจมตีทางไซเบอร์มีสูงถึง 2.86 แสนล้านบาทหรือเท่ากับร้อยละ 2.2 ของผลิตภัณฑ์มวลรวมของประเทศ ทั้งนี้ พบว่า 3 ใน 5 ขององค์กรในประเทศไทยเคยได้รับผลกระทบจากการถูกโจมตีทางไซเบอร์ และบางองค์กรไม่แน่ใจว่าเคยถูกโจมตีทางไซเบอร์ร้อยละ 47 เพราะองค์กรเหล่านั้นยังขาดกระบวนการตรวจสอบหรือวิเคราะห์ภัยคุกคามทางไซเบอร์ ทั้งนี้ ได้มีผู้ให้ความคิดเห็นเกี่ยวกับความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ดังนี้

โอม ศิวะดิตถ์ ผู้บริหารด้านนโยบายภาครัฐ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด ได้กล่าวว่า ยุคที่คลาวด์และโมบายคอมพิวติ้งมีบทบาทในการทำหน้าที่เชื่อมต่อธุรกิจกับลูกค้า และช่วยเพิ่มศักยภาพในการทำงาน ทุกองค์กรจึงต้องเผชิญกับความเสี่ยงใหม่ ๆ ไปพร้อมกัน เมื่อระบบไอทีแบบดั้งเดิมหายไปผู้ประสงค์ร้ายก็มีช่องทางและเป้าหมายใหม่ ๆ สำหรับการโจมตีมากขึ้น ส่วนองค์กรที่ตกเป็นเป้าหมายก็อาจประสบความเสียหาย มีการรั่วไหลข้อมูลขององค์กร จึงเกิดความเสียหายทางการเงินเป็นมูลค่ามหาศาล และยังสูญเสียความพึงพอใจของลูกค้าและความน่าเชื่อถือทางธุรกิจอีกด้วย

ณัฐชัย จารุศิลาวงศ์ ที่ปรึกษาธุรกิจของกลุ่มโมบิลิตี้ บริษัท ฟรอสต์ แอนด์ ซัลลิแวน (ประเทศไทย) จำกัด ได้กล่าวว่า ความเสียหายที่แท้จริงจากภัยอันตรายบนโลกไซเบอร์ ครอบคลุมทั้งเชิงเศรษฐกิจ โอกาสทางธุรกิจ และการตกงาน ซึ่งรายงานวิจัยพบว่าองค์กรขนาดใหญ่ในประเทศไทยอาจประสบความเสียหายทางเศรษฐกิจเป็นมูลค่าสูงถึง 408 ล้านบาท ซึ่งสูงกว่าความเสียหายขององค์กรธุรกิจขนาดกลางที่จะเสียหายประมาณ 9 แสนบาท ในระยะ 12 เดือนที่ผ่านมาประมาณ 3 ใน 5 ขององค์กรทั้งหมดหรือประมาณร้อยละ 60 ต้องมีการปลดพนักงานออกในหลายตำแหน่งเนื่องจากผลกระทบของภัยคุกคามทางไซเบอร์ และมีการสร้างแบบจำลองเพื่อประเมินมูลค่าความเสียหายที่อาจเกิดขึ้น โดยนำปัจจัยเชิงเศรษฐกิจองค์รวม และข้อมูลเชิงลึก

มาพิจารณาแบ่งผลกระทบที่สามารถเกิดขึ้นเป็น 3 แบบ ได้แก่ 1) ผลกระทบทางตรง ความเสียหายทางด้านการเงิน ประสิทธิภาพในการทำงานที่ลดลง ระยะเวลาในการฟื้นฟู และค่าเสียหายที่ต้องชดใช้ 2) ผลกระทบทางอ้อม การสูญเสียโอกาสทางธุรกิจ เช่น การสูญเสียลูกค้าเพราะขาดความเชื่อมั่น 3) ผลกระทบวงกว้างและผลกระทบมวลรวมเชิงเศรษฐกิจ เช่น สภาพคล่องทางการใช้จ่ายขององค์กรและผู้บริโภคลดลง การโจมตีทางไซเบอร์สามารถก่อความเสียหายอย่างมาก ซึ่งไม่สามารถตรวจพบในทันที จึงทำให้มูลค่าความเสียหายที่แท้จริงของภัยจากการถูกโจมตีทางไซเบอร์มักถูกประเมินไว้ต่ำกว่าความเป็นจริงอยู่เสมอ เมื่อมีความสูญเสียด้านการเงินแล้ว ยังทำลายความสามารถขององค์กรไทยในการคว้าโอกาสทางธุรกิจในยุคเศรษฐกิจดิจิทัล โดยผลสำรวจเปิดเผยว่าร้อยละ 73 ของผู้เข้าร่วมการสำรวจพบว่า องค์กรของตนได้หยุดแผนการนำเทคโนโลยีดิจิทัลเข้ามาปฏิรูปธุรกิจ เนื่องจากความกังวลด้านภัยคุกคามทางไซเบอร์และขาดวิสัยทัศน์เชิงกลยุทธ์การโจมตีจากอาชญากรไซเบอร์ด้วยมัลแวร์เรียกค่าไถ่ ซึ่งส่งผลกระทบไปทั่วโลกและส่งผลกระทบขนาดใหญ่ต่อองค์กรธุรกิจ แต่ผลการวิจัยระบุว่า สำหรับองค์กรไทยแล้วภัยจากการถูกโจมตีทางไซเบอร์ที่มีผลกระทบสูงสุดและใช้เวลาแก้ไขฟื้นฟูนานที่สุด คือ การเลียนแบบตัวตนของแบรนด์ในโลกออนไลน์ การขโมยข้อมูลและการทำลายข้อมูล จึงมีข้อเสนอแนะว่าอย่าให้เรื่องความปลอดภัยเป็นแค่เรื่องภายหลัง แม้ว่าองค์กรจำนวนมากจะผ่านการถูกโจมตีทางไซเบอร์มาแล้ว แต่กลับมีองค์กรเพียงร้อยละ 26 เท่านั้นที่นำประเด็นด้านความปลอดภัยในโลกไซเบอร์มาพิจารณาก่อนที่จะเริ่มดำเนินงานในโครงการดิจิทัลทรานส์ฟอร์เมชัน

สำหรับองค์กรที่ยังไม่เคยถูกโจมตีนั้น มีการนำปัจจัยด้านความปลอดภัยมาพิจารณาก่อนเริ่มดำเนินงานคิดเป็นร้อยละ 37 ส่วนองค์กรที่เหลือนั้นจะเริ่มพิจารณาเรื่องความปลอดภัยหลังจากที่เริ่มดำเนินงานไปแล้วหรืออาจไม่พิจารณาถึงเลยก็เป็นได้ ซึ่งองค์กรในกลุ่มหลังนี้จะไม่สามารถพัฒนาผลิตภัณฑ์หรือโซลูชัน (แนวทางแก้ปัญหา) ที่มีรากฐานอยู่บนความปลอดภัยอย่างแท้จริงขึ้นมาได้ จึงอาจทำให้ผลิตภัณฑ์หรือบริการที่ขาดความปลอดภัยหลุดออกไปสู่ตลาดได้ ขณะที่การมีระบบซับซ้อนไม่ได้แปลว่ามีความปลอดภัย ซึ่งมีความเชื่อกันว่าการนำโซลูชันด้านความปลอดภัยจำนวนมากมาใช้งานร่วมกันจะช่วยให้ระบบในภาพรวมมีความปลอดภัยสูงขึ้น แต่ผลวิจัยในครั้งนี้กลับเปิดเผยให้เห็นว่า กลุ่มองค์กรที่ใช้โซลูชันด้านความปลอดภัยรวม 26-50 โซลูชัน มีเพียงร้อยละ 15 เท่านั้นที่สามารถแก้ไขปัญหาและฟื้นฟูจากผลกระทบของการโจมตีทางไซเบอร์ได้ภายในเวลาหนึ่งชั่วโมง ขณะที่องค์กรที่ใช้โซลูชันด้านดังกล่าวน้อยกว่า 10 โซลูชัน มีอัตราส่วนการแก้ไขปัญหาภายในหนึ่งชั่วโมงสูงอยู่ที่ร้อยละ 22 ขณะนี้องค์กรจำนวนมากเริ่มหันมาปฏิรูปธุรกิจด้วยนวัตกรรมดิจิทัลกัน เพื่อช่วงชิงความได้เปรียบในการแข่งขัน แต่งานวิจัยครั้งนี้ก็ยังชี้ให้เห็นว่าองค์กรร้อยละ 33 ยังเห็นความปลอดภัยเป็นเพียงแค่ปัจจัยในการปกป้ององค์กรจากผู้ประสงค์ร้าย โดยมีเพียงร้อยละ 28 ที่เล็งเห็นว่ากลยุทธ์ด้านความปลอดภัยขององค์กรเป็นหัวใจสำคัญของกระบวนการดิจิทัลทรานส์ฟอร์เมชัน และมีองค์กรร้อยละ 73 หยุดแผนนำเทคโนโลยีดิจิทัลมาปฏิรูปธุรกิจเนื่องจากกังวลด้านภัยคุกคามทางไซเบอร์ (“โจรไซเบอร์พุ่งโจมตีองค์กรไทยเสี่ยงสูญ 2.86 แสนล้าน,” 2561)

การดำเนินงานของภาครัฐ ภาคเอกชน และภาคประชาสังคม ซึ่งนำระบบเครือข่ายคอมพิวเตอร์มาใช้ในการปฏิบัติงาน เพื่อเปลี่ยนผ่านไปสู่ระบบเศรษฐกิจดิจิทัลเพิ่มมากขึ้น และการติดต่อสื่อสารระหว่างหน่วยงานต่าง ๆ ในการปฏิบัติงานและการทำธุรกรรมของลูกค้า ภาคเอกชนต้องการที่จะแข่งขันในการทำธุรกิจ

จะต้องดำเนินการให้บริษัทเหล่านั้นเปลี่ยนผ่านไปสู่การทำธุรกิจในระบบดิจิทัล เพื่อตอบสนองต่อความต้องการของลูกค้าเพื่อความรวดเร็วและทันสมัย มีความน่าเชื่อถือ บริษัทเหล่านั้นต้องเตรียมความพร้อมในการรักษาความปลอดภัยทางไซเบอร์ เพื่อสร้างความมั่นใจว่าข้อมูลของลูกค้าไม่รั่วไหลจนเกิดความเสียหาย หรือถูกโจรกรรมข้อมูล บริษัทเอกชนจะต้องลงทุนในระบบเครือข่ายคอมพิวเตอร์ และระบบป้องกันการถูกโจมตีทางไซเบอร์ และต้องมีบุคลากรที่เชี่ยวชาญเมื่อถูกโจมตีทางไซเบอร์จะต้องฟื้นสภาพให้ได้อย่างรวดเร็ว และบริษัทเอกชนเมื่อตรวจพบการโจมตีทางไซเบอร์ต้องแจ้งแก่หน่วยงานภาครัฐที่รับผิดชอบทันที เพื่อป้องกันความเสียหายที่ส่งผลกระทบในวงกว้าง

บทสรุปและข้อเสนอแนะของผู้ศึกษา

การโจมตีทางไซเบอร์ถือเป็นภัยคุกคามที่ก่อความเสียหายให้แก่ภาครัฐ ภาคเอกชน และภาคประชาสังคมหรือประชาชน หน่วยงานภาครัฐต้องทำหน้าที่หลักในการปกป้อง ป้องกัน และรับมือกับสถานการณ์ที่ถูกโจมตีทางไซเบอร์และต้องร่วมมือกับภาคเอกชน และภาคประชาสังคมหรือประชาชน ซึ่งเป็นผู้ที่ได้รับผลกระทบจากการถูกโจมตีทางไซเบอร์เช่นเดียวกัน ภาครัฐต้องมีมาตรการทางเทคนิคและกฎหมายให้ภาคเอกชนปฏิบัติ โดยเฉพาะองค์กรที่เกี่ยวข้องกับความมั่นคงของชาติ อาทิ กิจการธนาคาร สายการบิน ระบบสาธารณูปโภค ต้องมีมาตรการบริหารความเสี่ยง และมีเทคนิคที่ดีมีความต่อเนื่อง ต้องจัดให้มีระบบตั้งค่าความปลอดภัย มีระบบควบคุมการเข้าถึง มีระบบควบคุมชุดคำสั่งที่ไม่พึงประสงค์ จัดการปิดช่องโหว่ของระบบเครือข่ายคอมพิวเตอร์ เพื่อป้องกันผู้บุกรุกเข้าโจมตีระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานภาครัฐ ภาคเอกชน และภาคประชาสังคม จึงต้องมีการสำรองข้อมูลสำคัญ ภาคเอกชนต้องมีหน้าที่บริหารความเสี่ยงในการจัดการทางเทคนิคในการรักษาความปลอดภัยทางไซเบอร์ เช่น ไฟร์วอลล์ขอบเขต เกตเวย์อินเทอร์เน็ต ระบบตั้งค่าความปลอดภัย ระบบควบคุมการเข้าถึงหน่วยงานภาคเอกชนที่มีกิจการสำคัญ อาทิ กิจการธนาคารและการเงิน สายการบิน พลังงาน สาธารณสุข และสาธารณูปโภค เป็นต้น เมื่อถูกโจมตีทางไซเบอร์ต้องรายงานให้หน่วยงานของรัฐทราบในทันที เพื่อป้องกันความเสียหายที่ส่งผลกระทบในวงกว้าง ส่วนภาคประชาสังคม คือ ประชาชนต้องได้รับความคุ้มครองสิทธิเสรีภาพในโลกไซเบอร์ แต่ทั้งนี้ การที่หน่วยงานรัฐออกมาตรการทางกฎหมายที่เข้มงวดต้องคำนึงถึงสิทธิเสรีภาพของประชาชนด้วย

บรรณานุกรม

การรับฟังความคิดเห็นกฎหมายไทย. (8 มีนาคม 2561). สืบค้น 18 กรกฎาคม 2561 จาก http://www.lawamendment.go.th/index.php/component/k2/item/1211-2018-03-08-01-17-38

โจรไซเบอร์พุ่งโจมตีองค์กรไทยเสี่ยงสูญ 2.86 แสนล้าน. (20 มิถุนายน 2561). **กรุงเทพธุรกิจ.** สืบค้น 22 มิถุนายน 2561 จาก http://www.bangkokbiznews.com/news/detail/805293

นายกรัฐมนตรี เป็นประธานประชุม คกก.เตรียมการไซเบอร์แห่งชาติครั้งแรก DE พร้อมตั้งเป้าให้ไทยติดอันดับ 1 ใน 20 ของโลกที่มีความพร้อม. (9 พฤษภาคม 2561)**.** สืบค้น 19 กรกฎาคม 2561 จาก http://www.thaigov.go.th/news/contents/details/12111

“รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560” (6 เมษายน 2560). **ราชกิจจานุเบกษา**, เล่ม 134 ตอนที่ 40 ก, น. 20.

“ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560” (20 ตุลาคม 2560). **ราชกิจจานุเบกษา,** เล่ม 134 ตอนพิเศษ 259 ง, น. 1-7.

สรุปข่าวการประชุมคณะรัฐมนตรี. (4 เมษายน 2560). สืบค้น 19 กรกฎาคม 2561 จาก http://www.thaigov.go.th/news/contents/details/2880

สราวุธ ปิติยาศักดิ์. (2 ธันวาคม 2560). **ภัยคุกคามทางไซเบอร์กับกฎหมายไทย.** สืบค้น 20 กรกฎาคม 2561 จาก https://www.prachachat.net/columns/news-81915

ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ สำนักงานรัฐบาล อิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.). (10 กันยายน 2559). **ความมั่นคงปลอดภัยทางไซเบอร์.** สืบค้น 19 กรกฎาคม 2561 จาก https://www.dga.or.th/upload/temp/file_505c8b497a84db48703ce777ba565d9d.pdf