กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน : ศึกษากรณีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

โดย

อมรรัตน์ อินนุมาตร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต
สาขากฎหมายระหว่างประเทศ
คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2566

THE LAW ON CYBERSECURITY AND HUMAN RIGHTS PROTECTION: A CASE STUDY OF THE CYBERSECURITY ACT B.E. 2562

BY

AMORNRAT INNUMAT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF MASTER OF LAWS

INTERNATIONAL LAW

FACULTY OF LAW

THAMMASAT UNIVERSITY

ACADEMIC YEAR 2023

มหาวิทยาลัยธรรมศาสตร์
คณะนิติศาสตร์

วิทยานิพนธ์

ของ

อมรรัตน์ อินนุมาตร

เรื่อง

กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน :
ศึกษากรณีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
นิติศาสตรมหาบัณฑิต

เมื่อ วันที่ 9 สิงหาคม พ.ศ. 2567

ประธานกรรมการสอบวิทยานิพนธ์ _____
(ดร. ธเนศ สุจารีกุล)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(ศาสตราจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช)

กรรมการสอบวิทยานิพนธ์ _____
(ศาสตราจารย์ ดร. จุมพต สายสุนทร)

คณบดี _____
(รองศาสตราจารย์ ดร. ปกป้อง ศรีสนิท)

หัวข้อวิทยานิพนธ์	กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน : ศึกษากรณีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ชื่อผู้เขียน	อมรรัตน์ อินนุมาตร
ชื่อปริญญา	นิติศาสตรมหาบัณฑิต
สาขาวิชา/คณะ/มหาวิทยาลัย	ระหว่างประเทศ นิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ศาสตราจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช
ปีการศึกษา	2566

บทคัดย่อ

วิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อศึกษาความสัมพันธ์ระหว่างกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน โดยมุ่งเน้นการวิเคราะห์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (Cybersecurity Act B.E. 2562) ของประเทศไทย และผลกระทบที่กฎหมายฉบับนี้มีต่อสิทธิมนุษยชนในบริบทของยุคดิจิทัล การศึกษานี้เริ่มต้นด้วยการทบทวนแนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) และสิทธิมนุษยชนในยุคดิจิทัล รวมถึงแนวทางฐานสิทธิมนุษยชนที่เกี่ยวข้อง จากนั้นได้ทำการวิเคราะห์ตราสารระหว่างประเทศและกฎหมายต่างประเทศที่เกี่ยวข้อง เพื่อเปรียบเทียบกับกฎหมายไทย

ผลการศึกษาพบว่า พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีมาตรการหลายประการที่อาจกระทบต่อสิทธิมนุษยชน เช่น การเข้าถึงข้อมูลส่วนบุคคล และการจำกัดเสรีภาพในการแสดงออก โดยเฉพาะในส่วนที่เกี่ยวข้องกับการควบคุมและการเข้าถึงข้อมูลและระบบสารสนเทศของภาคเอกชนและประชาชนทั่วไป การวิจัยชี้ให้เห็นถึงความจำเป็นในการปรับปรุงกฎหมายดังกล่าว เพื่อให้สอดคล้องกับมาตรฐานสิทธิมนุษยชนระหว่างประเทศ โดยเน้นให้มีความสมดุลระหว่างการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองสิทธิมนุษยชน

ข้อเสนอแนะจากการศึกษาคือการสร้างกลไกการกำกับดูแลที่โปร่งใสและเป็นธรรม การให้ความรู้แก่ประชาชนเกี่ยวกับสิทธิและความปลอดภัยทางไซเบอร์ และการสร้างความร่วมมือระหว่างประเทศในการพัฒนากรอบกฎหมายความมั่นคงปลอดภัยไซเบอร์ เพื่อรับมือกับความท้าทายที่เกิดขึ้นอย่างมีประสิทธิภาพ

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, สิทธิมนุษยชน, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์, กฎหมายระหว่างประเทศ, สิทธิมนุษยชนในยุคดิจิทัล

Thesis Title	THE LAW ON CYBERSECURITY AND HUMAN RIGHTS PROTECTION: A CASE STUDY OF THE CYBERSECURITY ACT B.E. 2562
Author	Amornrat Innumat
Degree	Master of Laws
Major Field/Faculty/University	International Law Law Thammasat University
Thesis Advisor	Professor Prasit Pivavatnapanich, Ph.D.
Academic Year	2023

ABSTRACT

This thesis aims to explore the interplay between cybersecurity law and human rights protection, focusing on the analysis of Thailand's Cybersecurity Act B.E. 2562 and its impact on human rights in the digital age. The study begins with a review of cybersecurity and digital human rights concepts, including the human rights-based approach relevant to this context. It then analyzes international instruments and foreign laws to compare with Thai legislation.

The findings reveal that the Cybersecurity Act B.E. 2562 includes several measures that may affect human rights, such as access to personal data and limitations on freedom of expression, particularly regarding control and access to information and information systems of the private sector and the general public. The research highlights the need to amend the law to align with international human rights standards, emphasizing a balance between cybersecurity and human rights protection.

Recommendations from the study include establishing transparent and fair oversight mechanisms, educating the public about their rights and cybersecurity, and fostering international cooperation in developing a cybersecurity legal framework to effectively address emerging challenges.

Keywords: Cybersecurity, Human Rights, Cybersecurity Act, International Law, Digital Human Rights

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จได้ด้วยความกรุณาจากศาสตราจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช ที่ได้กรุณาเสียสละเวลารับเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งช่วยให้ผู้เขียนได้แนวทางในการค้นคว้าข้อมูล และการเรียบเรียงวิทยานิพนธ์ ผู้เขียนขอขอบพระคุณศาสตราจารย์ ดร. ประสิทธิ์ ปิวาวัฒนพานิช เป็นอย่างสูงที่ให้ความเมตตา ให้ความรู้ คำปรึกษา และคำแนะนำต่าง ๆ อันเป็นประโยชน์ต่อผู้เขียนเสมอมา นอกจากนี้ ผู้เขียนขอขอบพระคุณ ดร.ธเนศ สุจารีกุล และศาสตราจารย์ ดร. จุมพต สายสุนทร ที่กรุณารับเป็นกรรมการสอบวิทยานิพนธ์ พร้อมทั้งได้ให้คำแนะนำและข้อสังเกตต่าง ๆ อันเป็นประโยชน์ ซึ่งเป็นแนวทางให้ผู้เขียนนำไปปรับปรุงวิทยานิพนธ์ให้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบคุณสำนักงานเลขาธิการวุฒิสภา ที่ได้สนับสนุนทุนการศึกษาตลอดหลักสูตร ในฐานะข้าราชการรัฐสภาสามัญ ผู้เขียนขอสัญญาว่าจะนำความรู้ที่ได้รับจากการศึกษาไปพัฒนาการปฏิบัติราชการให้เกิดประโยชน์ต่อองค์กร ประชาชน และประเทศชาติต่อไป

ขอขอบคุณผู้บังคับบัญชาทุกลำดับชั้น เพื่อนร่วมงาน เพื่อนนักศึกษาปริญญาโทสาขากฎหมายระหว่างประเทศ และเพื่อน ๆ จากทุกช่วงชีวิต ที่คอยสนับสนุน เป็นกำลังใจให้ผู้เขียนผ่านอุปสรรคต่าง ๆ ในชีวิต และไม่ย่อท้อจนเดินทางมาถึงวันนี้

ขอขอบคุณคณาจารย์สาขากฎหมายระหว่างประเทศ ที่เปิดโลกด้านกฎหมายระหว่างประเทศของผู้เขียนให้กว้างขวางมากขึ้น และพร้อมจะต่อยอดความรู้ต่อไปได้ในอนาคต ตลอดจนเจ้าหน้าที่บัณฑิตศึกษา คณะนิติศาสตร์ทุกท่าน ที่ให้ความช่วยเหลือ อำนวยความสะดวก และให้คำแนะนำในขั้นตอนต่าง ๆ ตลอดการศึกษา

สุดท้ายนี้ ผู้เขียนขอกราบขอบพระคุณคุณพ่อฉัตรชัย อินนุมาตร ที่สอนให้ลูกคนนี้เป็นคนรักในการเรียนรู้ เป็นกำลังใจที่สำคัญเสมอมา ไม่ละทิ้งการศึกษา แม้ว่าวันนี้ท่านจะไม่ได้อยู่บนโลกใบนี้แล้ว เชื่อว่าท่านจะมองเห็นความสำเร็จของลูกและยินดีไปด้วยอย่างแน่นอน รวมถึงขอขอบคุณพันตำรวจโท สิทธิชัย โสภา และพี่น้องครอบครัวอินนุมาตรทุกคน ที่คอยเป็นกองหนุนให้รู้ว่าผู้เขียนไม่ได้อยู่ในโลกนี้เพียงลำพัง และขอบใจเจ้าแมวน้อยตัวแสบทั้งสี่ที่คอยฮีลใจในเวลาเหนื่อยล้า

หากวิทยานิพนธ์ฉบับนี้จักมีประโยชน์และคุณค่าในทางวิชาการต่อผู้ใด ไม่มากก็น้อย ผู้เขียนขอยกความดีทั้งหลายนั้นมอบแด่ บิดา มารดา ครอบครัว ครูบาอาจารย์และผู้มีพระคุณต่อชีวิตผู้เขียนทุกท่าน ทั้งนี้ หากมีความบกพร่องผิดพลาดประการใดเกิดขึ้นในวิทยานิพนธ์ฉบับนี้ ผู้เขียนขอน้อมรับไว้แต่เพียงผู้เดียว

อมรรัตน์ อินนุมาตร

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและสภาพปัญหา

เป็นที่ทราบกันดีว่าในปัจจุบันอินเทอร์เน็ตมีความสำคัญต่อกิจกรรมต่าง ๆ ของมนุษย์เป็นอย่างมาก ไม่ว่าจะในระดับปัจเจก ระดับองค์กร ระดับรัฐ หรือระดับระหว่างประเทศ กิจกรรมที่เคยต้องมีการเคลื่อนไหวทางกายภาพก็กลายเป็นกิจกรรมที่เกิดขึ้นผ่านระบบออนไลน์แทน เช่น การซื้อขายสินค้าต่าง ๆ การใช้บริการทางการเงินกับสถาบันการเงิน การศึกษา รวมไปถึงการติดต่อสื่อสารระหว่างกันก็เป็นไปอย่างง่ายดายและไร้พรมแดนต่างกับในอดีตเป็นอย่างมาก พื้นที่ในโลกไซเบอร์ (Cyberspace) เป็นโลกเสมือนจริงที่กิจกรรมมากมายเกิดขึ้นโดยไม่มีสิ่งที่จับต้องได้ แต่สามารถทำให้กิจกรรมเหล่านั้นสำเร็จตามวัตถุประสงค์ของบุคคลต่าง ๆ ได้เช่นเดียวกับรูปแบบดั้งเดิมของกิจกรรมนั้นในอดีต นอกจากนี้อินเทอร์เน็ตยังมีส่วนสำคัญในการทำให้เกิดการพัฒนาทางเศรษฐกิจ การสื่อสารโทรคมนาคม การควบคุมโครงสร้างพื้นฐานหรือสาธารณูปโภคที่สำคัญ รวมไปถึงการรักษาความมั่นคงของรัฐอีกด้วย ลักษณะของโลกไซเบอร์มีความเป็นระหว่างประเทศอยู่ในตัวเอง โดยคอมพิวเตอร์ สมาร์ทโฟน หรืออุปกรณ์อื่น ๆ ที่เชื่อมต่ออินเทอร์เน็ตได้ สามารถทำกิจกรรมทางออนไลน์ระหว่างกันแม้จะอยู่คนละซีกโลกในเวลาอันรวดเร็วโดยไม่ต้องข้ามพรมแดนทางกายภาพไป

แต่ในขณะที่มนุษย์ได้รับประโยชน์มากมายจากการใช้อินเทอร์เน็ตและการนำกิจกรรมต่าง ๆ เข้าไปอยู่ในโลกไซเบอร์ ใช้อินเทอร์เน็ตเชื่อมโยงทุกสิ่งเข้าด้วยกัน (Internet of Thing: IoT) โดยสามารถเข้าถึงสิ่งเหล่านั้น ๆ ได้อย่างง่ายดาย ก็อาจเสี่ยงต่อภัยคุกคามทางไซเบอร์ (Cyber Threat) ซึ่งภัยคุกคามมีทั้งระดับที่ไม่ร้ายแรง เกิดกับบุคคลทั่วไป จนถึงภัยคุกคามที่ร้ายแรงส่งผลกระทบต่อการดำรงชีวิตของประชาชนจำนวนมากและความมั่นคงของรัฐ เช่น การทำลายระบบควบคุมโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) การจารกรรม (Espionage) ความลับที่เกี่ยวกับความมั่นคง หรือความลับทางการค้าที่สำคัญ (Trade Secret) การใช้มัลแวร์ (Malware) หรือชุดคำสั่งทำลายระบบการทำงานของคอมพิวเตอร์หรือระบบเครือข่ายที่สำคัญให้ไม่สามารถทำงานได้อย่างปกติ โดยผู้ก่อให้เกิดภัยคุกคามเหล่านั้นอาจกระทำการจากสถานที่ใดในโลกก็ได้ ไม่จำเป็นต้องอยู่ภายในรัฐที่ได้รับความเสียหาย ซึ่งในปัจจุบันประเทศต่าง ๆ ทั่วโลกรวมถึงองค์การระหว่างประเทศมีความตื่นตัวในเรื่องภัยคุกคามทางไซเบอร์เป็นอย่างมาก เนื่องจากสถิติของภัยคุกคามทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็ว มีรูปแบบใหม่ ๆ ที่แตกต่างจากเดิม และมีการพัฒนารูปแบบอยู่ตลอดเวลา

อีกทั้งการโจมตีทางไซเบอร์ (Cyber Attack) นั้นสามารถสร้างความเสียหายได้สูงมากเกินกว่าจะคาดการณ์ได้ ทำให้ประเทศต่าง ๆ มีการพัฒนามาตรการและบัญญัติกฎหมาย เพื่อรับมือกับภัยคุกคามทางไซเบอร์ รวมไปถึงมีการสร้างความร่วมมือในระดับระหว่างประเทศเพื่อร่วมกันวางแนวปฏิบัติที่เป็นมาตรฐาน ให้คำแนะนำในการเฝ้าระวังและต่อสู้กับภัยคุกคามดังกล่าว

ตัวอย่างเช่น United Nations Group of Governmental Experts on Developments in The Field of Information and Telecommunications in the Context of International Security หรือ UNGGE ซึ่งเป็นองค์ประชุมในด้านข้อมูลสารสนเทศที่จัดตั้งโดยสหประชาชาติ ได้ให้ความสำคัญกับประเด็นด้านความมั่นคงไซเบอร์ โดยในปี 2015 ได้มีการลงมติและออกรายงานที่ A/70/174 ระบุว่ากฎหมายระหว่างประเทศมีความสำคัญในการสร้างความมั่นคงปลอดภัยให้แก่รัฐในการใช้เทคโนโลยีสารสนเทศ ดังนั้นควรมีการนำกฎหมายระหว่างประเทศมาบังคับใช้กับโลกไซเบอร์ด้วย[1] ปัจจุบันหลายประเทศได้นำมติและแนวทางของ UNGGE มาใช้ในการสร้างความร่วมมือระหว่างกันทั้งในระดับทวิภาคี และความร่วมมือในระดับภูมิภาค ทว่าการนำเอาคำแนะนำของ UNGGE มาดำเนินการบังคับใช้อย่างเท่าเทียมกันในแต่ละประเทศยังคงไม่มีความชัดเจน จึงมีความพยายามของรัฐต่าง ๆ รวมถึงเอกชน อาทิ บริษัทไมโครซอฟท์ ที่พยายามสนับสนุนให้มีการจัดทำอนุสัญญา Digital Geneva Convention เพื่อระบุให้ประเทศต่าง ๆ นำเอามาตรฐานด้านความมั่นคงไซเบอร์ที่จะถูกพัฒนาขึ้นมาไปใช้ดำเนินการเพื่อให้โลกไซเบอร์มีความปลอดภัย เพื่อเป็นการคุ้มครองและเยียวยาพลเรือนที่ต้องได้รับผลกระทบจากการกระทำอันไม่พึงประสงค์ทางไซเบอร์ซึ่งได้รับการสนับสนุนโดยรัฐ โดยมุ่งจะคุ้มครองพลเรือนตามหลักการสิทธิมนุษยชนระหว่างประเทศและกฎหมายมนุษยธรรมระหว่างประเทศ ดังเช่นที่เคยมีอนุสัญญาเจนีวา 1949 (Geneva Convention 1949)

สำหรับในระดับประเทศนั้น ประเทศต่าง ๆ มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ และความมั่นคงทางไซเบอร์กันออกมาเป็นจำนวนมาก รวมไปถึงนโยบายและแผนระดับชาติอีกด้วย แต่กฎหมาย มาตรการ และนโยบายด้านความมั่นคงไซเบอร์เหล่านั้นส่งผลกระทบโดยตรงกับสิทธิมนุษยชน เช่น สิทธิในความเป็นส่วนตัว (Right to Privacy) เสรีภาพในการแสดงออก (Freedom of Expression) สิทธิในการเข้าถึงข้อมูลข่าวสาร (Right to Access to Information) เป็นต้น โดยผู้มีอำนาจกำหนดนโยบายหรือผู้มีอำนาจตรากฎหมายมีวัตถุประสงค์เพื่อจะปกป้องโลกไซเบอร์ตลอดจนระบบเทคโนโลยีสารสนเทศจากการกระทำในทางไม่พึงประสงค์ ซึ่งในปัจจุบันไม่เพียงแต่บุคคลหรือกลุ่มบุคคลที่เป็นมิจฉาชีพ หรือกระทำในลักษณะการก่อการร้าย แต่ยังอาจรวมไปถึงการ

---

[1] United Nations, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ <https://undocs.org/A/70/174> สืบค้นเมื่อ 25 มีนาคม 2564.

กระทำภายใต้การสนับสนุนโดยรัฐใดรัฐหนึ่ง โดยมีเจตนามุ่งร้ายต่อรัฐอื่น ๆ ทำให้กฎหมายและมาตรการต่าง ๆ ที่ออกมาให้น้ำหนักไปในเรื่องความมั่นคงเป็นหลัก แทนที่จะมุ่งไปในเรื่องการรักษาความปลอดภัยของระบบ จนทำให้กฎเกณฑ์ในเรื่องความมั่นคงทางไซเบอร์ในประเทศต่าง ๆ มีมากมายและกว้างเกินไป ขาดความชัดเจนและปราศจากการตรวจสอบถ่วงดุล หรือกลไกความรับผิดต่อระบอบ (regime) อื่น ๆ การเยียวยาผู้ได้รับผลกระทบจากการบังคับใช้มาตรการต่าง ๆ เหล่านั้น ซึ่งสามารถนำไปสู่การละเมิดสิทธิมนุษยชนได้

ในกรณีของประเทศไทยได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และมีผลใช้บังคับตั้งแต่วันที่ 28 พฤษภาคม 2562[2] ซึ่งพระราชบัญญัติฉบับนี้ถูกวิพากษ์วิจารณ์โดยภาคส่วนต่าง ๆ ในสังคมอย่างกว้างขวาง ด้วยความวิตกกังวลว่าจะก่อให้เกิดการละเมิดสิทธิมนุษยชน เพราะความไม่ชัดเจนในการให้นิยามของคำสำคัญในบทบัญญัติต่าง ๆ รวมไปถึงการใช้ดุลพินิจของเจ้าหน้าที่ผู้มีอำนาจหน้าที่ในการบังคับใช้กฎหมายดังกล่าว

วิทยานิพนธ์นี้จึงมุ่งศึกษากฎหมายระหว่างประเทศ มาตรฐานและแนวปฏิบัติที่ได้รับการยอมรับในปัจจุบัน ตลอดจนศึกษากฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของประเทศต่าง ๆ และของประเทศไทย โดยอาศัยแนวทางฐานสิทธิมนุษยชน (Human Rights-Based Approach) ในการวิเคราะห์ว่ากฎหมายที่ตราขึ้นใช้เพื่อรักษาความมั่นคงทางไซเบอร์นั้น มีการสร้างความสมดุลกับมิติด้านสิทธิมนุษยชนหรือไม่ เพื่อเป็นแนวทางในการปรับปรุงกฎหมายว่าด้วยความมั่นคงไซเบอร์ของประเทศไทยให้มีความเหมาะสม มีมาตรฐานในระดับสากล บรรลุเจตนารมณ์ในการรักษาความมั่นคงทางไซเบอร์ ในขณะเดียวกันก็ส่งเสริมและปกป้องสิทธิมนุษยชนด้วย

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาลักษณะของความมั่นคงทางไซเบอร์ ประเภทของภัยคุกคาม เพื่อทำความเข้าใจเหตุผลในการออกมาตรการทางกฎหมายเพื่อรับมือกับภัยคุกคามทางไซเบอร์

1.2.2 เพื่อศึกษาว่าสิทธิมนุษยชนด้านใดบ้างที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงทางไซเบอร์

---

[2] ราชกิจจานุเบกษา, ‘พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562’ <http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF> สืบค้นเมื่อ 27 พฤษภาคม 2562.

1.2.3 เพื่อศึกษาแนวทางฐานสิทธิมนุษยชนที่จะใช้สร้างสมดุลในการพัฒนานโยบายและมาตรการทางกฎหมายด้านความมั่นคงทางไซเบอร์

1.2.4 เพื่อศึกษากฎหมาย มาตรฐาน และแนวปฏิบัติในทางระหว่างประเทศที่ได้รับการยอมรับอย่างกว้างขวางในปัจจุบัน ตลอดจนกฎหมายภายในประเทศต่าง ๆ ที่น่าสนใจเพื่อเปรียบเทียบมาตรการการรักษาความมั่นคงทางไซเบอร์ และมาตรการในการคุ้มครองสิทธิมนุษยชนในกฎหมายเหล่านั้น

1.2.5 เพื่อศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในเรื่องความสมดุลของมิติด้านความมั่นคงและมิติด้านสิทธิมนุษยชน เพื่อให้สามารถเสนอแนะแนวทางในการปรับปรุงกฎหมายดังกล่าวให้เกิดความสมดุลต่อไป

1.3 สมมติฐานของการศึกษา

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของประเทศไทยยังขาดความชัดเจน ขาดการคำนึงถึงมิติด้านสิทธิมนุษยชน และความสอดคล้องกับมาตรฐานระหว่างประเทศ ทำให้กฎหมายที่ออกมาบังคับใช้กระทบต่อสิทธิมนุษยชน ต้องมีการนำแนวทางด้านสิทธิมนุษยชนและมาตรฐานระหว่างประเทศมาพิจารณาร่วมด้วยเพื่อปรับปรุงกฎหมายดังกล่าว

1.4 ขอบเขตของการศึกษา

วิทยานิพนธ์นี้มุ่งศึกษาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายต่างประเทศว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ กฎหมายของสหรัฐอเมริกา จีน และสิงคโปร์ ตลอดจนศึกษาตราสารระหว่างประเทศที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น ตราสารของสหประชาชาติ สหภาพยุโรป และสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ เพื่อเปรียบเทียบกับกฎหมายของไทย และศึกษาถึงสิทธิมนุษยชนโดยเฉพาะด้านที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงแนวทางที่จะนำมาใช้ปรับสมดุลของกฎหมายดังกล่าว

1.5 วิธีดำเนินการศึกษา

วิทยานิพนธ์นี้เป็นการศึกษาวิจัยทางเอกสารโดยศึกษาและวิเคราะห์จากหนังสือ วารสาร บทความ งานวิจัย ตราสารระหว่างประเทศ ตัวบทกฎหมายและข้อมูลอิเล็กทรอนิกส์ทั้งของประเทศไทยและต่างประเทศ และวิเคราะห์เพื่อเสนอแนวทางในการปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์โดยไม่ละเลยมิติด้านสิทธิมนุษยชน

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการศึกษา

1.6.1 ได้ทราบถึงลักษณะของความมั่นคงทางไซเบอร์ ประเภทของภัยคุกคาม และมีความเข้าใจเหตุผลความจำเป็นในการออกมาตรการทางกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของประเทศต่าง ๆ

1.6.2 ได้ทราบว่าสิทธิมนุษยชนด้านใดบ้างที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงทางไซเบอร์

1.6.3 มีความรู้ความเข้าใจในแนวทางสิทธิมนุษยชนที่จะใช้สร้างสมดุลในการพัฒนานโยบายและมาตรการทางกฎหมายด้านความมั่นคงทางไซเบอร์

1.6.4 สามารถวิเคราะห์หาแนวทางที่เป็นประโยชน์จากกฎหมาย มาตรฐาน และแนวปฏิบัติในทางระหว่างประเทศ และวิเคราะห์ข้อดี ข้อด้อยของกฎหมายภายในประเทศต่าง ๆ สามารถเปรียบเทียบมาตรการการรักษาความมั่นคงทางไซเบอร์ และมาตรการในการคุ้มครองสิทธิมนุษยชนในกฎหมายเหล่านั้นได้

1.6.5 สามารถวิเคราะห์พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในเรื่องความสมดุลของมิติด้านความมั่นคงและมิติด้านสิทธิมนุษยชน และสามารถเสนอแนะแนวทางในการพัฒนาปรับปรุงกฎหมายดังกล่าวได้

บทที่ 2
ความทั่วไปว่าด้วยความมั่นคงปลอดภัยไซเบอร์ สิทธิมนุษยชนในยุคดิจิทัล และแนวทางฐานสิทธิมนุษยชน

ในยุคเทคโนโลยีสารสนเทศเช่นปัจจุบัน ความมั่นคงไซเบอร์ (Cybersecurity) เป็นเรื่องที่ทุกประเทศต้องให้ความสำคัญ ก่อนที่จะไปสำรวจตรวจสอบกฎหมายที่ออกมาเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ จำเป็นต้องทำความเข้าใจเสียก่อนว่าความมั่นคงปลอดภัยทางไซเบอร์คืออะไร ภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่จะสร้างความเสียหายให้เกิดขึ้นมีลักษณะเช่นไรบ้าง และผู้ที่ทำให้เกิดภัยคุกคามเหล่านั้นเป็นใคร รวมถึงการทำความเข้าใจว่าอะไรคือโครงสร้างพื้นฐานหรือสาธารณูปโภคที่สำคัญ (Critical Infrastructure) ซึ่งต้องได้รับการป้องกันการจากการถูกโจมตี และตัวอย่างของเหตุการณ์โจมตีทางไซเบอร์ (Cyber Attack) หรือเหตุการณ์ทางไซเบอร์ (Cyber Incident) ที่เกิดขึ้นอันเป็นหลักฐานที่แสดงให้เห็นว่าการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้นมีความจำเป็นอย่างยิ่ง จากนั้นจึงจะศึกษามิติของสิทธิมนุษยชนในยุคดิจิทัลว่าหมายถึงสิทธิใดบ้าง ซึ่งอาจถูกกระทบจากการเกิดขึ้นของมาตรการเพื่อรักษาความมั่นคงไซเบอร์ และส่วนสุดท้ายของบทนี้จึงจะนำเสนอแนวทางฐานสิทธิมนุษยชน (Human Rights-Based Approach) เพื่อนำมาเป็นเครื่องมือในการวิเคราะห์มาตรการและกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ในบทต่อ ๆ ไป

2.1 ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

นิยามของความมั่นคงปลอดภัยทางไซเบอร์นั้น ได้มีการให้นิยามไว้โดยองค์การระหว่างประเทศ และในกฎหมายภายในเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศต่าง ๆ

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU)[1] ได้ให้นิยามไว้ว่า[2] *"ความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) คือ ภาพรวม*

---

[1] International Telecommunication Union, 'SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security: Overview of cybersecurity Recommendation ITU-T X.1205' 2 <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[2] Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices,

ของเครื่องมือ นโยบาย แนวคิดด้านการรักษาความปลอดภัย การรักษาความปลอดภัย แนวทาง วิธีการบริหารความเสี่ยง การปฏิบัติ การอบรม วิธีปฏิบัติที่เป็นเลิศ การรับประกัน และเทคโนโลยีที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ และสินทรัพย์ขององค์กรและของผู้ใช้งาน ซึ่งรวมไปถึงอุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ เอกลักษณ์บุคคล โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบโทรคมนาคม และภาพรวมของข้อมูลที่ส่งผ่านหรือเก็บไว้ในสภาพแวดล้อมไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์มุ่งมั่นที่จะทำให้มั่นใจว่าได้บรรลุถึงและธำรงรักษาไว้ซึ่งความปลอดภัยของทรัพย์สินขององค์กรและของผู้ใช้ ป้องกันความเสี่ยงที่เกี่ยวข้องในสภาพแวดล้อมไซเบอร์ วัตถุประสงค์ความมั่นคงปลอดภัยโดยทั่วไปประกอบด้วย :

- *ความพร้อมใช้งาน*
- *ความครบถ้วนถูกต้อง ซึ่งอาจรวมถึง การระบุตัวบุคคล และการห้ามปฏิเสธความรับผิด*
- *การรักษาความลับ"*

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ได้ให้นิยามไว้ว่า[3] *"ความมั่นคงปลอดภัยทางไซเบอร์ คือ กระบวนการในการปกป้องข้อมูล โดยการป้องกัน ตรวจจับ และตอบโต้ ต่อการโจมตี [4]"*

---

assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

[3] National Institute of Standards and Technology, 'Cybersecurity Framework Manufacturing Profile' 46 <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[4] The process of protecting information by preventing, detecting, and responding to attacks.

นอกจากนี้ยังมีนิยามที่ปรากฏในกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ที่น่าสนใจ เช่น ในมาตรา 2(1) ของ **ข้อบังคับว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของสหภาพยุโรป** (REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)) ที่ให้ความหมายว่า[5] *"ความมั่นคงปลอดภัยไซเบอร์ หมายถึง กิจกรรมที่จำเป็นในการปกป้องระบบเครือข่ายและระบบสารสนเทศ ผู้ใช้ระบบดังกล่าว และบุคคลอื่น ๆ ที่ได้รับผลกระทบจากภัยคุกคามไซเบอร์"*[6] ซึ่งข้อบังคับดังกล่าวได้ผ่านกระบวนการนิติบัญญัติของสหภาพยุโรปแล้ว เมื่อวันที่ 17 เมษายน 2562 (ค.ศ. 2019) และได้ประกาศลงใน EU Official Journal เมื่อวันที่ 7 มิถุนายน ค.ศ. 2019 โดยมีผลบังคับใช้กับประเทศสมาชิกของสหภาพยุโรปแล้วเมื่อวันที่ 27 มิถุนายน ค.ศ. 2019[7]

กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของสาธารณรัฐประชาชนจีน มาตรา 76(2)[8] ให้นิยามไว้ว่า *"ความมั่นคงปลอดภัยไซเบอร์ หรือ ความมั่นคงปลอดภัยของเครือข่าย หมายถึงการใช้มาตรการที่จำเป็นเพื่อป้องกันการโจมตีทางไซเบอร์ การบุกรุก การแทรกแซง การทำลายและการใช้งานที่ผิดกฎหมาย รวมถึงอุบัติเหตุที่ไม่คาดคิด เพื่อวางเครือข่าย*

---

[5] Council of the European Union, 'Regulation of the European Parliament and of the Council on ENISA (The European Union Agency for Cybersecurity) and on Information and Communication Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (EU Cybersecurity Act)' 63 <https://data.consilium.europa.eu/doc/document/PE-86-2018-REV-1/en/pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[6] (1) 'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

[7] European Parliament, 'LEGISLATIVE TRAIN SCHEDULE: EU CYBERSECURITY AGENCY AND THE CYBERSECURITY ACT' <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-eu-cybersecurity-agency-and-cybersecurity-act> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[8] National People's Congress of the People's Republic of China, '中华人民共和国网络安全法"' (The People's Republic of China Cyber Security Law) <http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm> สืบค้นเมื่อ 19 พฤษภาคม 2562.

ในสถานะการดำเนินงานที่เสถียรและเชื่อถือได้ รวมถึงการรับรองความสามารถข้อมูล เครือข่ายที่สมบูรณ์ เป็นความลับและใช้งานได้"[9]

และ**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562** ของประเทศไทย ซึ่งประกาศในราชกิจจานุเบกษาเมื่อวันที่ 27 พฤษภาคม 2562 และมีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 โดยในมาตรา 3 ได้ให้นิยามไว้ว่า[10] *"การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ"*

จากนิยามต่าง ๆ ที่ได้นำเสนอไปข้างต้นนั้น บางส่วนก็มีความใกล้เคียงกัน แต่ยังมีนิยามบางส่วนที่ยังไม่มีความชัดเจน แต่โดยสรุปแล้ว ความมั่นคงปลอดภัยไซเบอร์ คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรและผู้ใช้ปราศจากความเสี่ยง และความเสียหายที่มีต่อความปลอดภัยของข้อมูลและระบบในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการโจมตี การบ่อนทำลาย การบุกรุก การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล 3 ประการ ได้แก่ การรักษาความลับ (Confidentiality) ความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งาน (Availability)

2.2 ภัยคุกคามทางไซเบอร์ (Cyber Threat)

ภัยคุกคามทางไซเบอร์นั้น มีพัฒนาการด้านรูปแบบไปอย่างมาก รวมถึงสถิติของการเกิดภัยคุกคามก็เพิ่มสูงขึ้นทั่วโลก อันเป็นผลมาจากการที่พลเมืองทั่วโลกสามารถเข้าถึงอินเทอร์เน็ตได้มากขึ้น ทำให้เกิดช่องโหว่มากมายในโลกไซเบอร์ที่ผู้ไม่ประสงค์ดีจะเข้าโจมตีได้ จึงทำให้รัฐบาลของประเทศต่าง ๆ ทั่วโลกเกิดความตื่นตระหนกต่อภัยคุกคามทางไซเบอร์นี้ และได้พัฒนานโยบาย รวมถึงมาตรการทางกฎหมายต่าง ๆ เพื่อรับมือกับภัยคุกคามนี้

---

[9] (2) "Cybersecurity" [网络安全, also "network security"] refers to taking the necessary measures to prevent cyber attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as ensuring the capacity for network data to be complete, confidential, and usable.

[10] ราชกิจจานุเบกษา (เชิงอรรถ 2) 2.

2.2.1 ประเภทของภัยคุกคามทางไซเบอร์

การจำแนกภัยคุกคามทางไซเบอร์นั้น หน่วยงาน The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือในสหภาพยุโรป ได้จำแนกไว้ 9 หมวดหมู่ ซึ่งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (Thailand Computer Emergency Response Team: ThaiCERT) ก็ได้นำวิธีการจำแนกของ eCSIRT มาใช้เป็นหลักเกณฑ์ในการเฝ้าระวังและรับแจ้งเหตุภัยคุกคามเช่นเดียวกัน ซึ่งมีรายละเอียดดังนี้[11]

2.2.1.1 เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) หมายถึง ภัยคุกคามที่เกิดจากการใช้หรือเผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (Spam)

2.2.1.2 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) หมายถึง ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคารสถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

2.2.1.3 การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) หมายถึง ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

2.2.1.4 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) หมายถึง ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบ เป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing)

---

[11] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), 'ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)' <https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf> สืบค้นเมื่อ 18 มีนาคม 2562.

และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)

2.2.1.5 การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) หมายถึง ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized Modification) ได้

2.2.1.6 ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) หมายถึง ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVECommon Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุกหรือเจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่มหรือเดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)

2.2.1.7 การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) หมายถึง ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุกหรือเจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

2.2.1.8 โปรแกรมไม่พึงประสงค์ (Malicious Code) หมายถึง ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่าง ๆ

2.2.1.9 ภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) หมายถึง ภัยคุกคามประเภทอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่น ๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

2.2.2 แหล่งที่มาของภัยคุกคามทางไซเบอร์

การเกิดขึ้นของภัยคุกคามทางไซเบอร์นั้นอาจเกิดขึ้นจากกลุ่มบุคคลหรือองค์กรที่มีความชำนาญในการปฏิบัติการเพื่อเข้าถึงเครือข่ายและข้อมูล ซึ่งการเข้าถึงอาจเกิดขึ้นได้จากบุคคลที่ได้รับความเชื่อถือภายในหน่วยงานนั้นเอง หรือการเข้าถึงระยะไกลจากบุคคลนิรนามผ่านทางอินเทอร์เน็ต โดยศูนย์บูรณาการความมั่นคงปลอดภัยไซเบอร์และการสื่อสารแห่งชาติ (The National Cybersecurity and Communications Integration Center: NCCIC) ซึ่งเป็นหน่วยงานภายใต้

กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security) ของสหรัฐอเมริกา ได้จำแนกกลุ่มบุคคลและองค์กรที่ทำให้เกิดภัยคุกคามไซเบอร์ออกเป็น 5 กลุ่มหลัก[12] ได้แก่

2.2.2.1 รัฐบาลแห่งชาติ (National Governments) การโจมตีของกลุ่มงานความมั่นคงหรือกองทัพ ด้วยจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้นกับประเทศเป้าหมายทั้งการก่อกวนเว็บไซต์ การโฆษณาชวนเชื่อและการสร้างความรำคาญให้แก่เว็บเพจโดยมีความเสียหายระดับต่ำไปจนถึงการจารกรรมข้อมูล การโจมตีที่ร้ายแรงถึงชีวิต และแม้แต่สร้างความเสียหายให้กับโครงสร้างพื้นฐานที่สำคัญของประเทศ ซึ่งสหรัฐอเมริกาเชื่อว่าภัยคุกคามทางไซเบอร์ที่ทรงอานุภาพเช่นนั้นเป็นการกระทำที่ได้รับการสนับสนุนจากรัฐ แน่นอนว่าประเทศที่ถูกจับตามองเป็นพิเศษ ได้แก่ จีน ซึ่งถูกระบุว่า ผู้ที่เข้ามาโจมตีเว็บไซต์พาณิชย์ของสหรัฐอเมริกา รวมถึงจารกรรมข้อมูลสมาชิกของผู้ให้บริการบนระบบเครือข่ายอินเตอร์เน็ต

2.2.2.2 ผู้ก่อการร้าย (Terrorists) โดยทั่วไปมีจุดมุ่งหมายเพื่อที่จะทำลายผลประโยชน์ของชาติอยู่แล้ว กลุ่มนี้จะใช้โลกไซเบอร์สร้างแบบแผนหาเงินทุน เผยแพร่แนวความคิด และเป็นช่องทางการสื่อสาร โดยมีเป้าหมายเพื่อกระจายความหวาดกลัวไปยังพลเรือน

2.2.2.3 สายลับของเอกชนและองค์กรอาชญากรรม (Industrial Spies and Organized Crime Groups) มีการใช้โลกไซเบอร์ในการบุกรุกและโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลและทรัพย์สินทั้งจากภาครัฐและเอกชน อาจมีการโจมตีโครงสร้างพื้นฐานเพื่อให้เกิดผลประโยชน์กับคู่แข่งของเอกชนที่ถูกโจมตี หรือเกิดประโยชน์กับกลุ่มอื่น ๆ โดยมีการขโมยความลับทางการค้าแล้วนำข้อมูลไปขาย หรือแบล็คเมล์บริษัทที่ถูกขโมยข้อมูลโดยใช้ความเสี่ยงภัยของสาธารณะเป็นเครื่องมือในการข่มขู่

2.2.2.4 แฮกทิวิส (Hacktivists) คือกลุ่มแฮกเกอร์ที่ใช้แรงจูงใจทางการเมืองเพื่อรวมกลุ่มและผลักดันให้เกิดความเปลี่ยนแปลงทางความคิด หรือการต่อต้านรัฐ โดยการสนับสนุนวาระทางการเมือง การสร้างมูลเหตุที่ส่งผลต่อทางการเมืองและสังคมมากกว่าการสร้างความเสียหายให้กับโครงสร้างพื้นฐาน

2.2.2.5 แฮกเกอร์ (Hackers) คือผู้ที่พยายามหาวิธีการหรือหาช่องโหว่ของระบบเพื่อแอบลักลอบเข้าสู่ระบบ ล้วงความลับหรือแอบดูข้อมูลข่าวสาร จนถึงทำลายข้อมูลข่าวสารและทำความเสียหายให้กับองค์กร ในปัจจุบันปัญหาในเรื่องอาชญากรรมทางด้านเทคโนโลยี โดยเฉพาะในเรื่องแฮกเกอร์ก็มีให้เห็นมากขึ้น ผู้ที่แอบลักลอบเข้าสู่ระบบจึงมาได้จากทั่วโลก ทำให้ดำเนินการ

---

[12] NCCIC, Department of Homeland Security, 'Cyber Threat Source Descriptions' <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions> สืบค้นเมื่อ 15 พฤษภาคม 2562.

ป้องกันหรือสืบหาตัวผู้กระทำผิดเป็นไปได้ยาก ในอดีตเหล่าแฮกเกอร์สามารถสร้างความเสียหายเพียงระดับต่ำถึงปานกลาง แต่เมื่อมีแฮกเกอร์จำนวนมากขึ้นประกอบกับการพัฒนาทักษะที่เป็นอันตรายอาจทำให้มีความเสี่ยงที่แฮกเกอร์เหล่านี้จะทำการโจมตีที่ทำให้เกิดความเสียหายในระดับร้ายแรงได้

2.3 โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure)

ภัยคุกคามทางไซเบอร์ที่ได้กล่าวถึงไปข้างต้นนั้น สามารถทำให้เกิดความเสียหายได้หลายระดับ แต่ภัยคุกคามที่จะทำให้เกิดความเสียหายในระดับร้ายแรงมักเป็นภัยคุกคามที่มุ่งโจมตีโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งจะกระทบต่อการดำรงชีวิตของประชาชนจำนวนมาก และอาจร้ายแรงถึงขั้นบาดเจ็บและเสียชีวิตได้ เช่น โรงไฟฟ้านิวเคลียร์ ระบบผลิตและจ่ายกระแสไฟฟ้า กิจการขนส่งมวลชน การจราจรทางอากาศ บริการสาธารณสุข บริการทางการเงิน เป็นต้น ซึ่งจะส่งผลกระทบไปยังความมั่นคงของรัฐในด้านเศรษฐกิจ สังคม และด้านอื่น ๆ อย่างไม่อาจหลีกเลี่ยงได้ การเฝ้าระวังการโจมตีต่อโครงสร้างพื้นฐานที่สำคัญนี้เอง ทำให้รัฐต่าง ๆ ออกแบบนโยบาย และมาตรการเพื่อรับมืออย่างเข้มงวด

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้นิยามไว้[13] สรุปได้ว่า โครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure: CI) เป็นระบบที่เป็นหัวใจของการให้บริการหรือการทำงาน ซึ่งหากถูกทำให้หยุดชะงักหรือถูกทำลายจะส่งผลกระทบให้เกิดความอ่อนแอลงของการสาธารณสุข ความปลอดภัย การพาณิชย์ และความมั่นคงของชาติ หรือหลายประการข้างต้นรวมกัน

การกำหนดว่าสิ่งใดเป็นโครงสร้างพื้นฐานที่สำคัญก็มีความแตกต่างกันไปในแต่ละประเทศ ซึ่งมีทั้งส่วนที่อยู่ในภาครัฐและภาคเอกชน เช่น ประเทศไทยได้มีประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559[14] ซึ่งระบุชื่อหน่วยงานจำนวน 121 หน่วยงาน โดยธุรกรรมทางอิเล็กทรอนิกส์

---

[13] Frederick Wamala, *The ITU National Cybersecurity Strategy Guide*, (Geneva : International Telecommunication Union 2012) 25.

[14] ราชกิจจานุเบกษา, ‘ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559’

ของหน่วยงานนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน

นอกจากนี้ยังมีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งหมายถึง ระบบสารสนเทศที่หน่วยงานซึ่งเป็นโครงสร้างพื้นฐานสำคัญของประเทศใช้ในการดำเนินงานและให้บริการ หากระบบถูกรบกวนจะทำให้ไม่สามารถดำเนินงานหรือให้บริการได้ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้แบ่ง CII ออกเป็นกลุ่มใหญ่ๆ 6 กลุ่ม[15] ได้แก่ 1) กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ 2) กลุ่มการเงิน 3) กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม 4) กลุ่มการขนส่งและโลจิสติกส์ 5) กลุ่มพลังงานและสาธารณูปโภค และ 6) กลุ่มสาธารณสุข

2.4 เหตุการณ์ไม่พึงประสงค์ทางไซเบอร์ (Cyber Incident)

มีเหตุการณ์การโจมตีจำนวนมากที่ส่งผลกระทบในระดับที่รัฐต่าง ๆ จำเป็นต้องให้ความสนใจกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเหตุการณ์ไม่พึงประสงค์ทางไซเบอร์เหล่านั้นเป็นหลักฐานอันชัดเจนที่แสดงให้เห็นว่ามาตรการและกฎหมายต่าง ๆ มีความจำเป็นเพียงใด ในการปกป้องโครงสร้างพื้นฐานที่สำคัญ และต่อสู้ป้องกันกับภัยคุกคามที่กระทบต่อประชาชนของรัฐ รวมถึงต่อความมั่นคงของรัฐเอง ซึ่งในรายงานนี้จะยกตัวอย่างเหตุการณ์ที่เกิดขึ้นและได้สร้างความเสียหายอย่างมีนัยสำคัญทั้งในระดับโลก หรือในระดับเฉพาะเจาะจงรัฐ

2.4.1 เหตุการณ์ WannaCry Ransomware Attack

เมื่อวันที่ 12 พฤษภาคม 2560 (ค.ศ. 2017) บริษัท Avast ได้รายงานการแพร่ระบาดของมัลแวร์ (Malware) เรียกค่าไถ่ชื่อ WannaCry โดย มัลแวร์ WannaCry เป็นมัลแวร์ประเภท Ransomware ซึ่งไม่ได้เข้าไปลบไฟล์หรือขโมยข้อมูลในคอมพิวเตอร์ แต่ทำการเข้ารหัสลับข้อมูลในคอมพิวเตอร์ไม่ให้ผู้ใช้งานเข้าถึงไฟล์ ถ้าจะเข้าถึงต้องเสียค่าไถ่เป็นสกุลเงินบิทคอยน์ (Bitcoin)

<https://ictlawcenter.etda.or.th/files/law/file/78/e37c4fe15bbaeee06907537bdd4a7795.pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[15] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ‘Critical Infrastructures (CI) และ Critical Information Infrastructures (CII) ความจำเป็นที่ต้องให้ความสำคัญและต้องทบทวน การประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานที่สำคัญของประเทศ’ (2561) 8 - 9.

ซึ่งเป็นเงินสกุลดิจิทัลที่ไม่สามารถติดตามตัวผู้รับโอนเงินได้เหมือนการโอนเงินผ่านธนาคารในโลกความเป็นจริง

โดยมัลแวร์นี้สามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ระบบ SMB (Server Message Block) ของวินโดวส์ (Windows) ผู้ใช้งานที่ไม่อัปเดตระบบปฏิบัติการวินโดวส์มีความเสี่ยงที่จะติดมัลแวร์นี้ โดยมีคอมพิวเตอร์ที่ถูกโจมตีจากมัลแวร์นี้มากกว่า 200,000 เครื่อง ใน 150 ประเทศ ตัวอย่างประเทศที่ได้รับผลกระทบเป็นอย่างมาก เช่น ประเทศอังกฤษซึ่งได้รับผลกระทบต่อหน่วยงานสาธารณสุข ทำให้ผู้ป่วยกว่า 6,900 ราย ไม่สามารถใช้บริการได้ ซึ่งช่องโหว่ที่ทำให้มัลแวร์นี้เข้ามาโจมตีได้ ส่วนหนึ่งเกิดจากภาคเอกชนที่เป็นผู้ผลิตซอฟท์แวร์ไม่ได้มีการจัดการที่ดีพอในการอัปเดตเพื่อปิดช่องโหว่ต่าง ๆ และสำหรับผู้ให้บริการ เช่น บริการสาธารณสุข รัฐก็ไม่ได้มีมาตรการพื้นฐานที่บังคับให้ต้องรับประกันความเสถียรและความปลอดภัยของระบบ[16] สำหรับในประเทศไทยพบผู้ติดมัลแวร์นี้อยู่บ้าง แต่ยังไม่พบการแพร่กระจายในวงกว้าง ซึ่งเมื่อเกิดเหตุการณ์ของ WannaCry ขึ้น ทำให้ผู้กำหนดนโยบายของประเทศต่าง ๆ ตื่นตระหนกกันเป็นอย่างมาก และให้ความสำคัญกับมาตรการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้น[17]

2.4.2 เหตุการณ์ Petya Attack

มัลแวร์นี้เป็นชนิด Ransomware เช่นเดียวกับ WannaCry ซึ่งเริ่มต้นระบาดจากประเทศยูเครนเมื่อปี 2560 (ค.ศ. 2017) ภายหลังเหตุการณ์ของ WannaCry สงบลงเพียงไม่นาน โดยมัลแวร์ตัวนี้แพร่ระบาดไปทั่วโลกส่งผลกระทบต่อหน่วยงานรัฐ ธนาคาร บริษัทสื่อสาร เครือข่ายรถไฟฟ้าใต้ดิน สนามบิน Boryspil[18] ในเมือง Kiev หรือแม้กระทั่งคอมพิวเตอร์ของโรงไฟฟ้านิวเคลียร์เชอร์โนบิลก็ติดมัลแวร์ตัวนี้จนกระทั่งต้องเปลี่ยนการตรวจจับรังสีมาเป็นระบบแมนนวลแทน

---

[16] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'WannaCry Campaign: Potential State Involvement Could Have Serious Consequences' <https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/> สืบค้นเมื่อ 16 พฤษภาคม 2562.

[17] Matthias C. Kettemann, 'Ensuring Cybersecurity through International Law' in Revista Española de Derecho Internacional, (2017) 289.

[18] Russell Brandom, 'A new ransomware attack is infecting airlines, banks, and utilities across Europe' <https://www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry> สืบค้นเมื่อ 19 พฤษภาคม 2562.

นอกจากนี้ประเทศเดนมาร์กยังได้ยืนยันว่าระบบสารสนเทศของบริษัทขนส่งทางเรือ Maersk[19] ถูกโจมตีและต้องปิดระบบลงเช่นกัน รวมไปถึงบริษัทน้ำมัน Rosneft ของรัสเซีย ซึ่งเมื่อคอมพิวเตอร์ติดมัลแวร์นี้ จะแสดงข้อความว่าไฟล์ในเครื่องถูกเข้ารหัส และให้จ่ายเงินค่าไถ่เป็นเงินสกุลบิทคอยน์เพื่อรับรหัสปลดล็อกไฟล์

2.4.3 เหตุการณ์ Estonia Cyber Attack

ปี 2550 (ค.ศ. 2007) ประเทศเอสโตเนีย ถูกโจมตีทางไซเบอร์ครั้งร้ายแรงด้วยวิธี DDoS[20] ทำให้ระบบและเว็บไซต์ต่าง ๆ ล่มไป โดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่าง ๆ รวมถึงการสแปม โพสต์ข้อความเสื่อมเสียจำนวนมากและคอมเมนต์ในหน้าข่าวต่าง ๆ ของเอสโตเนียรวมถึงพรรคปฏิรูปที่เป็นรัฐบาล จากเหตุการณ์นี้ทำให้รัฐบาลเอสโตเนียจัดตั้งระบบศูนย์ป้องกันภัยไซเบอร์ร่วมกันของ NATO โดยมีชื่อเล่นว่า “พยัคฆ์พิทักษ์” Tiigrikaitse[21] การป้องกันภัยคุกคามดังกล่าวของเอสโตเนีย ก้าวถึงขั้นที่ฝากระบบของรัฐทั้งหมดไว้ในคลาวด์ (Cloud) หากดินแดนเอสโตเนียถูกกองทัพยึดครองก็ยังสามารถอพยพย้ายไปอยู่ประเทศอื่น แล้วเรียกคืน (restore) ระบบของรัฐที่สำรอง (back up) ไว้ขึ้นมาใช้เพื่อบริหารกิจการของรัฐต่อไปได้ ปัจจุบัน

---

[19] Thomas Brewster, ‘Another Massive Ransomware Outbreak Is Going Global Fast’ <https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#1fe143c37abd> สืบค้นเมื่อ 19 พฤษภาคม 2562.

[20] DDoS ดีดอส หรือ Distributed Denial-of-Service คือ ลักษณะหรือวิธีการหนึ่งของการโจมตีเครื่องคอมพิวเตอร์เป้าหมายหรือระบบเป้าหมายบนอินเทอร์เน็ตของแฮกเกอร์ เพื่อทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการให้บริการ (Denial-of-Service) การโจมตีจะเกิดขึ้นพร้อม ๆ กันและมีเป้าหมายเดียวกัน โดยเครื่องที่ตกเป็นเหยื่อทั้งหมด จะสร้างข้อมูลขยะขึ้นมา แล้วส่งไปที่ระบบเป้าหมาย กระแสข้อมูลที่ไหลเข้ามาในปริมาณมหาศาลทำให้ระบบเป้าหมายต้องทำงานหนักขึ้นและช้าลงเรื่อย ๆ เมื่อเกินกว่าระดับที่รับได้ ก็จะหยุดการทำงานลงในที่สุด อันเป็นเหตุให้ผู้ใช้ไม่สามารถใช้บริการระบบเป้าหมายได้ตามปกติ เป้าหมายหลัก ของ DDoS คือ 1) การโจมตีให้เป้าหมายไม่สามารถให้บริการผู้ใช้งานตามปกติได้ 2) ตรวจจับและป้องกันยาก เพราะผู้ทำการโจมตีมีจำนวนหลากหลายและการจำแนกผู้โจมตีออกจากผู้ใช้งานจริงก็ทำได้ยากด้วยเช่นกัน

[21] ธีรภัทร เจริญสุข, ‘พยัคฆ์ทะยาน โครงการก้าวกระโดดแบบเอสโตเนีย จิตวิญญาณสตาร์ทอัพระดับประเทศ’ <https://www.the101.world/estonia-startup-country> สืบค้นเมื่อวันที่ 24 พฤษภาคม 2562.

เอสโตเนียเป็นประเทศที่มีการรักษาความมั่นคงปลอดภัยทางไซเบอร์อยู่ในระดับต้น ๆ ของโลก และมีศักยภาพในด้านไซเบอร์สูงมากประเทศหนึ่งของโลก

2.4.4 เหตุการณ์โจมตีโรงปฏิกรณ์นิวเคลียร์อิหร่าน

ช่วงปี 2552 – 2553 เกิดเหตุการณ์โรงปฏิกรณ์นิวเคลียร์ของอิหร่านถูกโจมตีโดยไวรัส Stuxnet ซึ่งคาดว่าเป็นความร่วมมือระหว่างสหรัฐอเมริกากับอิสราเอล โดย Stuxnet เป็นการโจมตีโรงปฏิกรณ์นิวเคลียร์ของอิหร่านด้วยวิธีการแทรกซึมเข้าไป ส่งไวรัส Stuxnet เข้าสู่เครื่องคอมพิวเตอร์ระบบควบคุมและประมวลผลแบบศูนย์รวม (Supervisory Control And Data Acquisition: SCADA) ที่ใช้ในการควบคุมและดูแลโครงสร้างพื้นฐานต่าง ๆ เช่น โรงงานไฟฟ้า โรงงานประปา ระบบควบคุมการจราจร ระบบควบคุมเขื่อน ระบบควบคุมแท่นขุดเจาะน้ำมันของอิหร่านผ่านทาง USB Flash Drive แม้ว่าคอมพิวเตอร์นั้นจะไม่ได้เชื่อมต่ออินเทอร์เน็ต ซึ่งการปฏิบัติการครั้งนี้พุ่งเป้าไปที่โรงปฏิกรณ์นิวเคลียร์โดยการปิดหรือเปลี่ยนแปลงแรงดันของเตาปฏิกรณ์นิวเคลียร์ ทำลายเครื่องจักร “Centrifuges” ที่ใช้เพิ่มประสิทธิภาพของแร่ยูเรเนียม มากกว่า 1,000 เครื่องและแพร่กระจายไปยังคอมพิวเตอร์มากกว่า 200,000 เครื่อง จนส่งผลกระทบต่อขีดความสามารถทางนิวเคลียร์ของอิหร่านทำให้ต้องหยุดชะงักไป

2.4.5 เหตุการณ์แทรกแซงการเลือกตั้งสหรัฐอเมริกา ปี 2559 (ค.ศ. 2016)

เหตุการณ์นี้แตกต่างจากการโจมตีอื่น ๆ ที่ได้กล่าวถึงข้างต้น เนื่องจากไม่เกิดความเสียหายขึ้นต่อระบบ การให้บริการ หรือการทำงานของอุปกรณ์ต่าง ๆ แต่เป็นการแฮกเข้าระบบเพื่อขโมยข้อมูล โดยในเหตุการณ์นี้รัสเซียตกเป็นประเทศที่ถูกกล่าวหาว่าสนับสนุนการปฏิบัติการแทรกแซงการเลือกตั้งของสหรัฐอเมริกา โดยได้ใช้ทรัพยากรของรัฐเพื่อให้ได้มาซึ่งข้อมูลที่อ่อนไหวจากทั้งจากคณะกรรมการระดับชาติของพรรคเดโมแครต (Democratic National Committee) และคณะกรรมการระดับชาติของพรรครีพับลิกัน (Republican National Committee) และเผยแพร่ข้อมูลจากอีเมลของนางฮิลลารี คลินตัน กว่า 20,000 ฉบับ ที่ส่งหรือได้รับโดยสมาชิกระดับสูงในคณะกรรมการระดับชาติของพรรคเดโมแครต ผ่านทางเว็บไซต์ Wikileaks และยังได้เผยแพร่อีเมลของนาย John Podesta ผู้จัดการทีมงานรณรงค์หาเสียงเลือกตั้งของคลินตันอีกด้วย[22] ทำให้ความสัมพันธ์ระหว่างประเทศของรัสเซียและสหรัฐอเมริกาเกิดความตึงเครียดขึ้น และมีมาตรการตอบโต้กันไปมาตลอดเวลา โดยสหรัฐฯ มองว่าการแทรกแซงการเลือกตั้งทางไซเบอร์เป็นภัยคุกคามที่สำคัญเป็นการละเมิดอธิปไตยของสหรัฐฯ โดยการบุกรุกทางข้อมูลและการโฆษณาชวนเชื่อ ซึ่งเป็น

---

[22] Jacqueline Van De Velde, ‘The Law of Cyber Interference in Elections’ 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828> สืบค้นเมื่อ 11 กุมภาพันธ์ 2562.

วิธีการชี้นำทางความคิด กำหนดการกระทำของคนในรัฐให้ผิดแผกไปจากที่ควรจะเป็น และทำลายระบอบประชาธิปไตย

2.4.6 เหตุการณ์ข้อมูลส่วนบุคคลของคนไทยถูกแฮกจากระบบ

เหตุการณ์ข้อมูลคนไทยที่ถูกแฮกเกิดขึ้นอย่างต่อเนื่องตั้งแต่ปี 2563-2566 ซึ่งส่วนใหญ่ล้วนเกิดขึ้นกับระบบโรงพยาบาล ระบบสาธารณสุข ดังนี้[23]

2.4.6.1 ปี 2563 โรงพยาบาลสระบุรี ถูกโจมตีด้วยไวรัสเรียกค่าไถ่ จนระบบไม่สามารถใช้งานได้ มีการอ้างอิงตัวเลขเงินที่ถูกเรียกคือ 200,000 บิทคอยน์ คิดเป็นเงินไทยเป็นมูลค่าประมาณ 63,000 ล้านบาท ก่อนที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จะเข้าทำการกู้ข้อมูลคนไข้จากระบบมัลแวร์ และพบว่าแฮกเกอร์โจมตีมาจากประเทศสหรัฐอเมริกา

2.4.6.2 ปี 2564 โรงพยาบาลรัฐถูกโจมตี 2 ครั้งติดต่อกัน โดยในช่วงเดือนกันยายน 2564 โรงพยาบาลสถาบันโรคไตภูมิราชนครินทร์ ถูกลักลอบเจาะข้อมูลคนไข้ไปกว่า 40,000 ราย เมื่อตรวจสอบพบว่า แฮกเกอร์ได้เจาะระบบนำข้อมูลคนไข้ไป เช่น ข้อมูลส่วนตัวคนไข้ ประวัติการฟอกไต และประวัติการรักษาและผลเอ็กซเรย์ของคนไข้ ส่วนใหญ่เป็นผู้สูงอายุที่เข้ามารับการรักษา จากนั้นแฮกเกอร์ซึ่งเป็นชายพูดภาษาอังกฤษโทรศัพท์มาที่โรงพยาบาลขอเจรจาต่อรองกับผู้มีอำนาจ พร้อมบอกว่า ขณะนี้ยังไม่มีบุคคลภายนอกรู้เรื่องนี้ และนัดโทรมาอีกครั้ง แต่สุดท้ายก็ไม่มีการติดต่อเข้ามา ทางโรงพยาบาลจึงเข้าแจ้งความ

หลังจากนั้นเกิดเหตุการณ์ที่ข้อมูลคนไข้ของกระทรวงสาธารณสุข ถูกแฮกจากระบบไปกว่า 16 ล้านคน โดยการแฮกในครั้งนี้มีการเรียกค่าไถ่ข้อมูล ซึ่งถูกวางขายอยู่บนเว็บไซต์ Raidforum รายละเอียดบนเว็บไซต์ระบุว่า ข้อมูลทั้งหมด 16 ล้านคน ประกอบไปด้วยข้อมูลของคนไข้ ได้แก่ ที่อยู่ เบอร์โทรศัพท์ เลขบัตรประจำตัวประชาชน เบอร์โทรศัพท์มือถือ วันเดือนปีเกิด ชื่อบิดา ชื่อโรงพยาบาลที่เข้ารักษาตัว ข้อมูลทั้งหมดเกี่ยวกับแพทย์ และรหัสผ่านทั่วไปของระบบในโรงพยาบาล รวมถึงข้อมูลทั่วไปอื่น ๆ ขนาดฐานข้อมูลมีประมาณ 3.7 GB กระทรวงดีอีเอสพบว่าถูกโจมตีมาจากประเทศสหรัฐอเมริกา จึงประสานกับหน่วยงานในสหรัฐ และหน่วยงานสากลช่วยสืบสวนติดตามกลุ่มแฮกเกอร์ดังกล่าวให้กับทางการไทย

2.4.6.3 ปี 2566 ข้อมูลคนไทยโดนแฮกไป 55 ล้านราย เยอะที่สุดในประวัติศาสตร์ ช่วงวันที่ 15 มีนาคม 2566 "แฮกเกอร์ ออนไลน์" ในนาม กลุ่ม 9Near ประกาศขายข้อมูลของคนไทยกว่า 55 ล้านราย ที่แฮกมาได้จากหน่วยงานไทยแห่งหนึ่ง ข้อมูลที่ขายระบุถึง ชื่อ วันเกิด

---

[23] ขวัญเรียม แก้วสุวรรณ, ‘โดนล้วงอื้อ! ย้อนรอย 3 เหตุการณ์คนไทยโดน 'แฮกเกอร์ออนไลน์’ <https://www.komchadluek.net/quality-life/well-structured/546508> สืบค้นเมื่อวันที่ 9 กรกฎาคม 2567.

เบอร์โทรศัพท์ ที่อยู่ และหมายเลขบัตรประชาชน บนเว็บไซต์ BreachForums รวมทั้งมีการโพสต์ลักษณะข่มขู่หน่วยงานและประชาชนในวงกว้าง โดยระบุว่า ถ้าไม่ติดต่อกลับ จะปล่อยข้อมูล ส่วนข้อมูลที่นำมาเปิดเผยทางการสงสัยอาจหลุดมาจากแอปพลิเคชันหมอพร้อม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอศาลออกคำสั่งปิดกั้นการเข้าถึงเว็บไซต์ 9near.org ซึ่งกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยียืนยันรู้ตัวผู้ก่อเหตุ เป็นทหารบกยศจ่าสิบโท สังกัดกรมการขนส่งทหารบก จึงขออำนาจศาลอาญาออกหมายจับ

2.5 สิทธิมนุษยชนในยุคดิจิทัล

รัฐมีหน้าที่ในการปกป้องส่งเสริมสิทธิเสรีภาพขั้นพื้นฐานของประชาชน ซึ่งสิทธิต่าง ๆ ได้มีการรับรองไว้ทั้งในกฎหมายของประเทศ เช่น รัฐธรรมนูญ พระราชบัญญัติ ตลอดจนกฎหมายลำดับรองต่าง ๆ และรับรองไว้โดยกฎหมายระหว่างประเทศ ทั้งที่เป็น Soft Law เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) และที่เป็นความตกลงระหว่างประเทศที่มีค่าบังคับ เช่น กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights: ICESCR) เป็นต้น โดยที่สิทธิต่าง ๆ อยู่บนพื้นฐานเรื่องความเท่าเทียม ความเสมอภาค การไม่เลือกปฏิบัติ เช่น เสรีภาพในการแสดงความคิดเห็น สิทธิในความเป็นส่วนตัว เสรีภาพในการรวมกลุ่มและการสมาคม เสรีภาพสื่อ ทั้งนี้การใช้สิทธิทั้งหลายต้องไม่เป็นการละเมิดสิทธิของผู้อื่น เช่น การเคารพสิทธิ ความเชื่อ และความคิดเห็นของผู้อื่น ตลอดจนต้องคำนึงถึงประโยชน์ของส่วนรวมด้วย

สิทธิมนุษยชนในยุคดิจิทัลนั้นเป็นการพัฒนาต่อยอดมาจากหลักการสากลด้านสิทธิมนุษยชน โดยในวิทยานิพนธ์นี้ขอใช้แนวทางด้านสิทธิมนุษยชนในยุคดิจิทัลจากกฎบัตรว่าด้วยสิทธิมนุษยชนและหลักการพื้นฐานสำหรับอินเทอร์เน็ต (Charter of Human Rights and Principles for the Internet) ของที่ประชุมว่าด้วยธรรมาภิบาลด้านอินเทอร์เน็ต (Internet Governance Forum: IGF) ซึ่งเป็นการประชุมที่จัดตั้งขึ้นโดยสหประชาชาติ เป็นการประชุมเกี่ยวกับนโยบายสาธารณะที่เกี่ยวข้องกับอินเทอร์เน็ต โดยถือเป็นหนึ่งในกลไกขององค์การสหประชาชาติด้านอินเทอร์เน็ตนอกเหนือไปจากเวทีหรือการประชุมปกติ เช่น กลไก ITU เป็นต้น

IGF ถูกก่อตั้งขึ้นในปี 2006 จากมติของที่ประชุม World Summit on the Information Society ปี 2005 ซึ่งเป็นการประชุมด้านเทคโนโลยีและการสื่อสารขององค์การสหประชาชาติ โดย IGF มีวัตถุประสงค์ในการเป็นพื้นที่ให้กับผู้มีส่วนได้เสีย (stakeholder) เข้ามา

พูดคุยถึงแนวนโยบายสาธารณะของอินเทอร์เน็ตเป็นหลัก การบริหารงานอยู่ภายใต้การกำกับขององค์การสหประชาชาติ โดยมีสำนักงานเลขาธิการตั้งอยู่ภายในอาคารที่ทำการขององค์การสหประชาชาติ ณ นครเจนีวา สมาพันธรัฐสวิส และมีคณะกรรมการที่ปรึกษา ซึ่งแต่งตั้งโดยเลขาธิการองค์การสหประชาชาติ ทำหน้าที่ช่วยดูแลและจัดการประชุม[24]

IGF ได้พัฒนากฎบัตรโดยการตีความมาตรฐานด้านสิทธิมนุษยชนมาปรับใช้กับสภาพแวดล้อมอินเทอร์เน็ต และหลักการนโยบายด้านอินเทอร์เน็ตจะต้องรักษาไว้ซึ่งสภาพแวดล้อมที่สนับสนุนสิทธิมนุษยชนอย่างสูงสุดเท่าที่จะเป็นไปได้[25] กฎบัตรนี้มีความมุ่งหมายที่จะสร้างสังคมสารสนเทศที่มีประชาชนเป็นศูนย์กลาง ซึ่งเคารพและรักษาไว้ซึ่งสิทธิมนุษยชนขั้นพื้นฐานที่สะท้อนอยู่ใน UDHR นอกจากนี้ภายใต้กฎหมายระหว่างประเทศ รัฐมีพันธะหน้าที่ตามกฎหมายที่จะต้องเคารพ ปกป้อง และส่งเสริมสิทธิมนุษยชนของพลเมือง ซึ่งหน้าที่ดังกล่าวเรียกร้องให้รัฐต้องปกป้องสิทธิมนุษยชนจากการละเมิดไม่ว่าจากผู้ใดก็ตาม นอกจากนี้รัฐยังมีหน้าที่ในการสืบสวน และลงโทษผู้กระทำการละเมิดดังกล่าวนั้นภายในดินแดนหรือภายใต้เขตอำนาจของตน ยิ่งไปกว่านั้นบุคคลอื่น ๆ นอกเหนือจากรัฐรวมไปถึงปัจเจกชนแต่ละรายล้วนมีความรับผิดชอบภายใต้ระบอบสิทธิมนุษยชนสากลนี้ โดยต้องสนับสนุนและเคารพสิทธิมนุษยชนของผู้อื่นด้วย กฎบัตรของ IGF มีทั้งสิ้น 21 ข้อ[26] ในแต่ละข้อจะประกอบไปด้วยสิทธิและหน้าที่ย่อยลงไปอีก ซึ่งสามารถสรุปได้พอสังเขปดังต่อไปนี้

1) สิทธิในการเข้าถึงอินเทอร์เน็ต (Right to Access to the Internet) ซึ่งเป็นสิทธิขั้นพื้นฐานและเป็นรากฐานของสิทธิอื่น ๆ ในกฎบัตรฉบับนี้ โดยสิทธิในการเข้าถึงนี้รวมทั้งการเข้าถึงบริการที่มีคุณภาพ เสรีภาพในการเลือกระบบและการใช้ซอฟท์แวร์ มีความเสมอภาคทางอินเทอร์เน็ต (net neutrality)

2) สิทธิที่จะไม่ถูกเลือกปฏิบัติในการเข้าถึงอินเทอร์เน็ต การใช้ และธรรมาภิบาล (Right to Non-Discrimination in Internet Access, Use and Governance) สิทธิข้อนี้สะท้อนอยู่ใน

---

[24] Blognone, '[IGF 2014] รู้จักกับ Internet Governance Forum เวทีประชุมด้านนโยบายของอินเทอร์เน็ตระดับนานาชาติ' <https://www.blognone.com/node/59436> สืบค้นเมื่อ 24 พฤษภาคม 2562.

[25] Adrian Cristian Moise, 'Cybersecurity and Human Rights' (2016) 2016 Revista Universal Juridic 160, 162.

[26] 'UN Internet Governance Forum Charter of Human Rights and Principles for the Internet' 9 – 27 <https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf> สืบค้นเมื่อ 17 พฤษภาคม 2562.

ข้อ 2 ของ UDHR “ทุกคนย่อมมีสิทธิและอิสรภาพบรรดาที่กำหนดไว้ในปฏิญญานี้ โดยปราศจากความแตกต่างไม่ว่าชนิดใด ๆ ดังเช่น เชื้อชาติ ผิว เพศ ภาษา ศาสนา ความคิดเห็นทางการเมืองหรือทางอื่น เผ่าพันธุ์แห่งชาติ หรือสังคม ทรัพย์สิน กำเนิด หรือสถานะอื่น ๆ”

3) สิทธิในการมีเสรีภาพและความมั่นคงปลอดภัยบนอินเทอร์เน็ต (Right to Liberty and Security on the Internet) ซึ่งสอดคล้องกับ ข้อ 3 ของ UDHR “คนทุกคนมีสิทธิในการดำรงชีวิต เสรีภาพ และความมั่นคงแห่งตัวตน” กล่าวคือต้องได้รับการปกป้องจากอาชญากรรมทุกรูปแบบ และมีความมั่นคงปลอดภัยบนอินเทอร์เน็ต

4) สิทธิในการพัฒนาผ่านอินเทอร์เน็ต (Right to Development through the Internet) เช่น การขจัดความอดอยาก การพัฒนามนุษย์ และการใช้สิ่งแวดล้อมอย่างยั่งยืน

5) เสรีภาพในการแสดงออกและเสรีภาพในการรับส่งข้อมูลบนอินเทอร์เน็ต (Freedom of Expression and Information on the Internet) เสรีภาพในข้อนี้ ปรากฏชัดในข้อ 19 ของ UDHR ซึ่งในสภาพแวดล้อมอินเทอร์เน็ต เสรีภาพนี้ยังรวมไปถึง เสรีภาพในการประท้วงออนไลน์ เสรีภาพจากการถูกปิดกั้น สิทธิในการรับส่งข้อมูลข่าวสาร เสรีภาพสื่อ รวมถึงเสรีภาพที่จะไม่ถูกรบกวนจากคำพูดที่แสดงความเกลียดชัง (Freedom from hate speech)

6) เสรีภาพในการนับถือศาสนาและความเชื่อบนอินเทอร์เน็ต (Freedom of Religion and Belief on the Internet) เช่นเดียวกับที่บัญญัติไว้ในข้อ 18 ของ UDHR รวมไปถึงการเผยแผ่ การปฏิบัติ การบูชา แต่ไม่อาจใช้สิทธินี้เพื่อจำกัดสิทธิมนุษยชนด้านอื่น ๆ อย่างผิดกฎหมาย

7) เสรีภาพในการชุมนุมและการสมาคมออนไลน์ (Freedom of Online Assembly and Association) โดยไม่ถูกขัดขวาง

8) สิทธิในความเป็นส่วนตัวบนอินเทอร์เน็ต (Right to Privacy on the Internet) เช่นเดียวกับข้อ 12 ของ UDHR โดยสิทธิในข้อนี้ได้กำหนดให้รัฐต้องมีกฎหมายที่จะคุ้มครองความเป็นส่วนตัว การให้บริการต่าง ๆ บนอินเทอร์เน็ตต้องมีการกำหนดนโยบายความเป็นส่วนตัว มีมาตรฐานของการรักษาความลับและความถูกต้องสมบูรณ์ของข้อมูลในระบบเทคโนโลยีสารสนเทศ สิทธิที่จะไม่เปิดเผยตัวตนและการเข้ารหัส เสรีภาพจากการถูกสอดแนม และเสรีภาพจากการถูกหมิ่นประมาท

9) สิทธิในการได้รับความคุ้มครองข้อมูลดิจิทัล (Right to Digital Data Protection) อันเป็นข้อมูลส่วนบุคคล โดยสร้างพันธกรณีให้กับผู้รวบรวมหรือผู้เก็บข้อมูล และมีมาตรฐานขั้นต่ำในการใช้ข้อมูลส่วนบุคคล นอกจากนี้การคุ้มครองข้อมูลจะต้องได้รับการตรวจสอบจากหน่วยงานที่เป็นอิสระปราศจากการครอบงำของธุรกิจหรือการเมือง

10) สิทธิที่จะได้รับการศึกษาจากอินเทอร์เน็ตหรือเกี่ยวกับอินเทอร์เน็ต (Right to Education on and about the Internet) ตรงกับสิทธิข้อ 26 ของ UDHR กล่าวคือการได้รับ

การศึกษาผ่านทางอินเทอร์เน็ต เช่น การสืบค้นข้อมูล สิ่งพิมพ์ ตำรา หลักสูตรการเรียนออนไลน์ เป็นต้น รวมทั้งการศึกษาเกี่ยวกับความรู้ด้านการใช้อินเทอร์เน็ตและสิทธิมนุษยชนด้วย

11) สิทธิในการมีส่วนร่วมทางวัฒนธรรมและเข้าถึงความรู้บนอินเทอร์เน็ต (Right to Culture and Access to Knowledge on the Internet) ดังที่ปรากฏในข้อ 27 ของ UDHR อันได้แก่ สิทธิในการมีส่วนร่วมทางด้านวัฒนธรรมกับชุมชน ยอมรับในความหลากหลายของภาษาและวัฒนธรรม และสิทธิในการเข้าถึงความรู้ที่เป็นสมบัติสาธารณะ รวมทั้งซอฟท์แวร์ที่เป็น Open Source

12) สิทธิเด็กและอินเทอร์เน็ต (Rights of Children and the Internet) สิทธิข้อนี้ปรากฏอยู่ในข้อ 25 ของ UDHR และข้อ 5 ของอนุสัญญาว่าด้วยสิทธิเด็ก (Convention on the Rights of the Child: CRC) ซึ่งกฎบัตรได้กำหนดให้สิทธิในข้อนี้หมายรวมถึง สิทธิที่จะได้รับประโยชน์จากการใช้อินเทอร์เน็ต มีเสรีภาพจากการถูกแสวงประโยชน์และการล่วงละเมิด สิทธิในการที่จะแสดงความคิดเห็นและได้รับการรับฟัง และมีผลประโยชน์สูงสุดของเด็กเป็นที่ตั้ง ดังที่ระบุไว้ใน CRC ข้อ 3

13) สิทธิคนพิการและอินเทอร์เน็ต (Rights of People with Disabilities and the Internet) สิทธินี้สะท้อนอยู่ในข้อ 4 ของอนุสัญญาว่าด้วยสิทธิของคนพิการ (Convention on the Rights of the Persons with Disabilities: CRPD) ซึ่งรัฐมีหน้าที่ต้องรับประกันและส่งเสริมการทำให้สิทธิมนุษยชนและเสรีภาพขั้นพื้นฐานของคนพิการเป็นความจริงโดยปราศจากการเลือกปฏิบัติทุกรูปแบบอันเนื่องมาจากเหตุแห่งความพิการ ซึ่งในกฎบัตรนี้ได้ระบุให้คนพิการต้องมีสิทธิเข้าถึงอินเทอร์เน็ต และอินเทอร์เน็ตต้องพร้อมใช้งานสำหรับคนพิการด้วย

14) สิทธิในการทำงานและอินเทอร์เน็ต (Right to Work and the Internet) ดังที่สะท้อนอยู่ในข้อ 23 ของ UDHR ซึ่งบนอินเทอร์เน็ตสิทธิของผู้ทำงานต้องได้รับการเคารพเช่นกัน และสามารถใช้อินเทอร์เน็ตเป็นสถานที่ทำงานได้ หรือทำงานผ่านอินเทอร์เน็ตได้

15) สิทธิที่จะมีส่วนร่วมในกิจการสาธารณะ (Right to Online Participation in Public Affairs) สิทธิข้อนี้มาจากหลักการในข้อ 21 ของ UDHR บุคคลมีสิทธิที่จะเข้าถึงบริการทางอิเล็กทรอนิกส์ในประเทศของตนได้ และสิทธิที่จะมีส่วนร่วมรัฐบาลอิเล็กทรอนิกส์

16) สิทธิการคุ้มครองผู้บริโภคบนอินเทอร์เน็ต (Rights to Consumer Protection on the Internet) บุคคลทุกคนต้องได้รับการเคารพ และปกป้องสิทธิในฐานะผู้บริโภค ซึ่งการพาณิชย์อิเล็กทรอนิกส์ต้องมีกฎเกณฑ์ที่รับประกันว่าผู้บริโภคจะได้รับการปกป้องในระดับเดียวกันกับผู้บริโภคที่ไม่ได้ทำธุรกรรมผ่านทางอิเล็กทรอนิกส์

17) สิทธิในการเข้าถึงบริการสาธารณสุขและบริการทางสังคมบนอินเทอร์เน็ต (Right to Health and Social Services on the Internet) ซึ่งสะท้อนมาจากหลักการในข้อ 25 ของ UDHR คือทุกคนมีสิทธิเข้าถึงบริการที่เกี่ยวกับสุขภาพและบริการทางสังคมออนไลน์

18) สิทธิที่จะได้รับการเยียวยาตามกฎหมายและการพิจารณาคดีที่เป็นธรรมสำหรับการกระทำที่เกี่ยวกับอินเทอร์เน็ต (Right to Legal Remedy and Fair Trial for actions involving the Internet) ซึ่งสิทธิที่จะได้รับการเยียวยาตามกฎหมาย มาจากหลักการในข้อ 8 ของ UDHR และสิทธิในการได้รับการพิจารณาคดีที่เป็นธรรม มาจากหลักการในข้อ 10 ของ UDHR นอกจากนี้การพิจารณาคดีทางอาญาต้องเป็นการพิจารณาที่ยุติธรรมซึ่งระบุไว้ใน UDHR ข้อ 9-11 และ ICCPR ข้อ 9 และ 14-16 นอกจากนี้ทุกคนมีสิทธิที่จะดำเนินการตามกระบวนการที่เกี่ยวข้องกับการเรียกร้องทางกฎหมายหรือการฝ่าฝืนกฎหมายที่เกี่ยวข้องกับอินเทอร์เน็ต

19) สิทธิในระเบียบทางสังคมและระหว่างประเทศสำหรับอินเทอร์เน็ต (Right to Appropriate Social and International Order for the Internet) สิทธิในข้อนี้มีหลักการเดียวกับข้อ 28 ของ UDHR ซึ่งกฎบัตรกำหนดให้รัฐต้องมีธรรมาภิบาลอินเทอร์เน็ตเพื่อส่งเสริมสิทธิมนุษยชนและอินเทอร์เน็ตในฐานะระเบียบทางสังคมและระเบียบระหว่างประเทศจะยืนยันหลักการความหลากหลายทางภาษา พหุนิยมและรูปแบบชีวิตทางวัฒนธรรมที่แตกต่างกันทั้งในรูปแบบและสาระสำคัญ รวมถึงให้ทุกคนมีสิทธิที่จะมีส่วนร่วมในธรรมาภิบาลอินเทอร์เน็ต

20) หน้าที่และความรับผิดชอบบนอินเทอร์เน็ต (Duties and Responsibilities on the Internet) นอกจากสิทธิที่บุคคลพึงมีตามกฎบัตรนี้แล้ว ทุกคนยังมีหน้าที่และความรับผิดชอบด้วย ซึ่งมาจากหลักการในข้อ 29 ของ UDHR ซึ่งบนอินเทอร์เน็ตนั้นทุกคนมีหน้าที่ต่อสังคมในอันที่จะเคารพสิทธิของผู้อื่นที่อยู่บนสภาพแวดล้อมออนไลน์ ผู้มีอำนาจจะต้องใช้อำนาจอย่างมีความรับผิดชอบ ละเว้นจากการละเมิดสิทธิมนุษยชน และเคารพ ปกป้อง ตลอดจนส่งเสริมสิทธิมนุษยชนอย่างสูงสุดเท่าที่จะเป็นไปได้

21) ความทั่วไป (General Clauses) สิทธิทั้งหมดในกฎบัตรฉบับนี้ใช้ร่วมกันและส่งเสริมกัน หากมีมาตรการใด ๆ ที่จะจำกัดสิทธิในกฎบัตรนี้จะเป็นความผิดตามกฎหมายนอกจากเป็นสถานการณ์ยกเว้น ซึ่งข้อจำกัดสิทธิเหล่านั้นอย่างน้อยต้องได้รับการยอมรับว่าถูกต้องตามกฎหมายภายใต้กฎหมายระหว่างประเทศ และได้สัดส่วนที่จำเป็น และหากกฎบัตรนี้มีความไม่สมบูรณ์ หากมีสิทธิและหลักการบางอย่างที่ไม่ได้กล่าวถึงในกฎบัตรก็ไม่ได้ขัดขวางการมีอยู่ของสิทธิดังกล่าว และไม่อาจใช้กฎบัตรนี้เพื่อตีความให้แก่รัฐใด กลุ่มบุคคล หรือบุคคลใด ๆ ในการดำเนินการใด ๆ ที่มุ่งทำลายสิทธิเสรีภาพที่ระบุไว้ในที่นี้

จะเห็นได้ว่าสิทธิต่าง ๆ ที่ระบุไว้ในกฎบัตรนี้เป็นการรวมเอาหลักการและมาตรฐานสิทธิมนุษยชนที่ได้รับการยอมรับในระดับระหว่างประเทศมาปรับเข้ากับสภาพแวดล้อมอินเทอร์เน็ต หรือสภาพแวดล้อมดิจิทัล เพื่อให้เห็นภาพชัดเจนขึ้นว่าสิทธิที่ได้รับการรับรองในโลกออฟไลน์ (Offline) จะสามารถนำมาใช้กับโลกออนไลน์ (Online) ได้อย่างไรบ้าง

เมื่อพูดถึงประเด็นทางด้านความมั่นคงปลอดภัยทางไซเบอร์อาจกล่าวถึงสิทธิมนุษยชนได้ในสองมุมมอง มุมมองแรกคือสิทธิมนุษยชนที่ถูกกระทบโดยภัยคุกคามทางไซเบอร์ เช่น การละเมิดสิทธิความเป็นส่วนตัว การขโมยข้อมูลส่วนบุคคล เป็นต้น ซึ่งในมุมนี้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์จะเป็นเครื่องมือหนึ่งในการปกป้องสิทธิมนุษยชนเหล่านั้น แต่ในอีกมุมมองหนึ่งกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์นี้เองที่ทำให้เกิดการละเมิดสิทธิมนุษยชน ด้วยเหตุที่ว่าผู้มีอำนาจในการกำหนดนโยบาย หรือผู้มีอำนาจในการตรากฎหมาย ไม่ได้ให้ความสำคัญกับสิทธิมนุษยชนในกระบวนการพิจารณากฎหมาย หรือขาดการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสีย โดยให้น้ำหนักกับการรักษาความมั่นคงแห่งรัฐมากเสียยิ่งกว่าการมองว่าภัยคุกคามทั้งหลายที่เกิดขึ้นนั้นสุดท้ายแล้วผู้ที่จะได้รับผลกระทบคือมนุษย์ มิใช่เพียงระบบ ทำให้มีการออกมาตรการหรือกฎหมายที่ละเลยสิทธิมนุษยชน เกิดปัญหาในการบังคับใช้ และไม่ได้รับการยอมรับจากสังคมที่อยู่ภายใต้บังคับของกฎหมายเหล่านั้น เช่น การปิดกั้นการเข้าถึงอินเทอร์เน็ต การถูกสอดแนมโดยรัฐโดยอ้างเหตุผลในการเฝ้าระวังด้านความมั่นคง การยึดอุปกรณ์คอมพิวเตอร์ การเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้ผ่านการตรวจสอบโดยศาล (Judicial Review) เป็นต้น

2.5.1 กรณีตัวอย่าง – โรมาเนีย

เมื่อเดือนมกราคม ค.ศ. 2015 ศาลรัฐธรรมนูญของโรมาเนียได้วินิจฉัยและประกาศว่ากฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ซึ่งผ่านความเห็นชอบของสภาแล้วนั้นขัดต่อรัฐธรรมนูญของโรมาเนีย

กฎหมายดังกล่าวรัฐบาลโรมาเนียเสนอต่อสภาและสภาได้ให้ความเห็นชอบแล้วเมื่อวันที่ 19 ธันวาคม ค.ศ. 2014 โดยกฎหมายดังกล่าวถูกวิพากษ์วิจารณ์อย่างกว้างขวางในการให้อำนาจกับเจ้าหน้าที่อย่างอิสระในการแทรกแซงชีวิตความเป็นส่วนตัวของประชาชน เนื่องจากกฎหมายนี้ให้อำนาจหน่วยงานข่าวกรองของโรมาเนีย (Romanian Intelligence Agency: SRI) และหน่วยงานรัฐอีก 9 หน่วยงาน เข้าถึงข้อมูลคอมพิวเตอร์ใด ๆ ซึ่งเป็นของบริษัทเอกชน โดยไม่ต้องมีคำสั่งจากศาล และยังสามารถเข้าถึงข้อมูลจากระบบเทคโนโลยีสารสนเทศใด ๆ ซึ่งเป็นเจ้าของครอบครอง จัดการ ปฏิบัติการ หรือใช้ โดยนิติบุคคล และให้สิทธิโดยปราศจากการตรวจสอบใด ๆ จากศาลเช่นกัน โดยกฎหมายไม่ได้กำหนดรายละเอียดว่าข้อมูลประเภทใดบ้างที่อนุญาตให้เจ้าหน้าที่เข้าถึงได้ อีกทั้งยังไม่มีรายละเอียดเกี่ยวกับมาตรการปกป้องสิทธิในกรณีที่เกิดการละเมิดจากการใช้กฎหมายดังกล่าว ทำให้เกิดความล้มเหลวในการคุ้มครองข้อมูลส่วนบุคคล ภายหลังกฎหมายดังกล่าวผ่านสภา สมาชิกพรรคฝ่ายค้านยื่นคำร้องต่อศาลรัฐธรรมนูญให้วินิจฉัยว่ากฎหมายฉบับนี้ขัดต่อรัฐธรรมนูญ

ศาลมีคำวินิจฉัยเมื่อวันที่ 21 มกราคม ค.ศ. 2015 ประกาศว่ากฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ขัดต่อรัฐธรรมนูญ โดยละเมิดรัฐธรรมนูญ มาตรา 1(3) และ (5)

มาตรา 21 มาตรา 23(1) มาตรา 26 มาตรา 28 มาตรา 53 มาตรา 119 และมาตรา 148 ซึ่งหมายถึง กฎหมายฉบับนี้ขัดต่อหลักนิติธรรม และการมอบหมายให้หน่วยงานทางทหารอย่างหน่วยงานข่าวกรองของโรมาเนีย ทำหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ ขัดแย้งกับหน้าที่ของรัฐในการสงวนรักษาสิทธิขั้นพื้นฐานและเสรีภาพ นอกจากนี้กฎหมายยังละเมิดเรื่องการเข้าถึงกระบวนการยุติธรรม เสรีภาพและความปลอดภัยส่วนบุคคล ชีวิตความเป็นส่วนตัว ความลับทางการสื่อสาร สร้างข้อกำจัดในการใช้สิทธิและเสรีภาพ นอกจากละเมิดรัฐธรรมนูญของโรมาเนียแล้ว ยังละเมิดอนุสัญญาว่าด้วยสิทธิมนุษยชนของยุโรป (European Convention on Human Rights: ECHR) อีกด้วย[27]

ซึ่งในขณะนั้นสหภาพยุโรปยังไม่มีกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ มีเพียงร่าง The Directive on security of network and information systems (NIS Directive) ซึ่งยังไม่มีผลบังคับใช้ ทั้งนี้ในร่างดังกล่าว ข้อ 15 วรรค 6 กำหนดว่า “รัฐสมาชิกจะต้องรับประกันว่าพันธกรณีใด ๆ ที่กำหนดไว้เป็นโทษแก่ผู้ประกอบการ ... จะต้องได้รับการทบทวนจากศาล”[28]

ต่อมาในวันที่ 27 มกราคม ค.ศ. 2016 กระทรวงเพื่อการสื่อสารและสังคมสารสนเทศ (Ministry for Communication and for Information Society: MCIS) ของโรมาเนีย ได้เสนอร่างกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ฉบับใหม่ โดยเผยแพร่ไว้บนเว็บไซต์ของกระทรวง ซึ่งมีหน่วยงานภาคเอกชนจำนวนมากส่งจดหมายเปิดผนึกถึงกระทรวง เพื่อให้ดำเนินการโดยยึดหลักความโปร่งใส โดยการขยายระยะเวลาการปรึกษาหารือร่างกฎหมายให้มีระยะเวลาอย่างน้อย 30 วัน รวมถึงร้องขอให้ใช้ระยะเวลาดังกล่าวต่อการรับฟังความคิดเห็นสาธารณะด้วย ทั้งนี้ ร่างกฎหมายดังกล่าวก็ยังคงถูกวิพากษ์วิจารณ์ว่า ขาดความชัดเจน ตีความได้ยาก และไม่ได้สัดส่วน โดยแทบไม่ได้นำเอาคำวินิจฉัยของศาลรัฐธรรมนูญที่เกิดขึ้นกับร่างกฎหมายฉบับก่อนมาแก้ไขจุดบกพร่อง นอกจากนี้ยังไม่ได้นำบทบัญญัติของ EU NIS Directive ซึ่งกำลังจะมีผลบังคับใช้ทั่วสหภาพยุโรปมาพิจารณาร่วมด้วย[29]

---

[27] Valentina Pavel Burloiu, ‘The Aftermath of Digital Rights Ireland: Romanian Constitutional Court Declares Overarching Cybersecurity Law Unconstitutional’ (2015) 2 European Data Protection Law Review 144, 146.

[28] Daniel Marius Morar, Mihaela Senia Costinescu, ‘Constitutional Court of Romania: National Cybersecurity versus Fundamental Rights and Freedoms’ (2015) 9 Vienna Journal on International Constitutional Law 605, 606.

[29] Valentina Pavel Burloiu, ‘Romania: Another Episode in Trying to Adopt Cybersecurity Regulation, Another (Possible) Failure for Human Rights’ (2016) 2 European Data Protection Law Review 117, 117-120.

จากกรณีตัวอย่างจะเห็นได้ว่ารัฐมีพันธะหน้าที่อันชัดเจนในการปกป้อง ส่งเสริมสิทธิมนุษยชน กฎหมายใด ๆ ก็ตามที่รัฐตราขึ้นล้วนเป็นเครื่องมือที่รัฐจะใช้เพื่อสนับสนุนหน้าที่ดังกล่าว มิใช่เป็นสิ่งที่ทำให้เกิดการลิดรอนสิทธิเสรีภาพเสียเอง ความมั่นคงทางไซเบอร์เป็นเรื่องสำคัญที่ไม่อาจมองข้ามหรือขาดซึ่งมาตรการกฎหมายในการจัดการป้องกันภัยคุกคามได้ แต่ขณะเดียวกันต้องมีความสมดุลและมีมาตรการที่ปกป้องสิทธิขั้นพื้นฐานทั้งหลายซึ่งประชาชนทุกคนมีอยู่อย่างเท่าเทียมกัน

2.6 แนวทางฐานสิทธิมนุษยชน (Human Rights-Based Approach)

การใช้แนวทางฐานสิทธิมนุษยชนเป็นแนวทางที่ริเริ่มโดยสหประชาชาติ และมีการนำสิทธิมนุษยชนมาเป็นหลักในการทำงานของสหประชาชาติ โดยแนวทางฐานสิทธิมนุษยชนเป็นกรอบแนวคิดสำหรับกระบวนการพัฒนามนุษย์ซึ่งอยู่บนพื้นฐานของสิทธิมนุษยชนระหว่างประเทศและดำเนินการโดยตรงเพื่อส่งเสริมและคุ้มครองสิทธิมนุษยชน ซึ่งจะวิเคราะห์ความไม่เท่าเทียมซึ่งเป็นหัวใจของปัญหาการพัฒนาในด้านต่าง ๆ และแก้ไขการเลือกปฏิบัติ และการกระจายอำนาจที่ไม่เป็นธรรมซึ่งเป็นอุปสรรคต่อการพัฒนา การกำหนดแผน นโยบาย และกระบวนการต่าง ๆ ต้องยึดหลักแนวทางสิทธิมนุษยชนและพันธกรณีภายใต้กฎหมายระหว่างประเทศ ซึ่งจะเปิดโอกาสให้คนทุกคนมีส่วนร่วมในการกำหนดนโยบายและรับผิดชอบต่อหน้าที่ของตนเอง

แนวทางฐานสิทธิมนุษยชนไม่มีสูตรตายตัว ขึ้นอยู่กับเป้าหมายของสิ่งที่จะพัฒนาขึ้นว่าเป็นเรื่องใด เช่น การใช้แนวทางฐานสิทธิมนุษยชนในการขจัดความยากจน (Human Rights-Based Approach to Poverty Reduction) การใช้แนวทางฐานสิทธิมนุษยชนเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (Human Rights-Based Approach to Cybersecurity) ซึ่งการใช้แนวทางนี้เป็นเครื่องมือในขณะที่มีการกำหนดนโยบาย มาตรการ กฎหมาย หรือโครงการพัฒนาต่าง ๆ วัตถุประสงค์หลักก็เพื่อบรรลุถึงสิทธิมนุษยชน โดยเสริมสร้างความเข้มแข็งให้กับผู้ถือสิทธิให้ตระหนักของสิทธิของตนเองในฐานะพลเมืองและในความเป็นมนุษย์ และเรียกร้องให้ผู้มีหน้าที่ต้องเคารพ ปกป้อง และเติมเต็ม (Respect, Protect, and Fulfill) สิทธิต่าง ๆ เหล่านั้น โดยดำเนินงานเพื่อเสริมสร้างขีดความสามารถของผู้ถือสิทธิในการเรียกร้องสิทธิของพวกเขา หลักการและมาตรฐานระหว่างประเทศด้านสิทธิมนุษยชนควรเป็นแนวทางในการร่วมมือ การพัฒนา การกำหนดนโยบาย มาตรการ แผนงาน ฯลฯ ในทุกภาคส่วนและในทุกขั้นตอน

2.6.1 หลักการของสิทธิมนุษยชน (Human Rights Principles)

สงครามโลกครั้งที่ 2 คร่าชีวิตพลเมืองของประเทศต่าง ๆ ไปหลายสิบล้านคน และยังส่งผลกระทบในด้านอื่น ๆ ต่อความเป็นอยู่และศักดิ์ศรีของมนุษย์ ในหลากหลายรูปแบบ ไม่ว่าจะเป็นความอดอยาก การทรมานนักโทษ การใช้แรงงานเยี่ยงทาส รวมไปถึงการฆ่าล้างเผ่าพันธุ์ ดังนั้น

เมื่อสงครามโลกครั้งที่สองสิ้นสุดลง และได้มีการก่อตั้งองค์การสหประชาชาติขึ้น ประเทศสมาชิกสหประชาชาติจึงได้ให้คำมั่นในอันที่จะร่วมกันป้องกันมิให้เกิดเหตุการณ์เลวร้ายดังกล่าวขึ้นอีก จึงเป็นบ่อเกิดของปฏิญญาสากลว่าด้วยสิทธิมนุษยชน เพื่อเป็นหลักการสำคัญในการคุ้มครองสิทธิมนุษยชนของประชาคมโลก โดยคณะกรรมการภายใต้คณะกรรมาธิการสิทธิมนุษยชนแห่งสหประชาชาติ ซึ่งประกอบไปด้วยสมาชิก จำนวน 8 คน ซึ่งมีนางเอเลนอร์ รูสเวลต์ ภรรยาอดีตประธานาธิบดีสหรัฐฯ เป็นประธาน และถือเป็นหนึ่งในบุคคลสำคัญที่ผลักดันให้ประเทศต่าง ๆ ให้การสนับสนุนและรับรองปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ได้ยกร่างปฏิญญาฯ ขึ้นในปี ค.ศ. 1947 และที่ประชุมสมัชชาใหญ่แห่งสหประชาชาติได้ลงมติรับรองและประกาศใช้ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน เมื่อวันที่ 10 ธันวาคม ค.ศ. 1948 ณ กรุงปารีส ประเทศฝรั่งเศส โดยมีประเทศที่ลงคะแนนเสียงสนับสนุน จำนวน 48 ประเทศ รวมถึงประเทศไทย งดออกเสียง จำนวน 8 ประเทศ ทั้งนี้ ไม่มีประเทศใดลงคะแนนเสียงคัดค้าน ปฏิญญาฉบับนี้จึงถือเป็นเอกสารทางประวัติศาสตร์ในการวางรากฐานด้านสิทธิมนุษยชนระหว่างประเทศฉบับแรกของโลก นอกจากนี้ยังเป็นพื้นฐานสำคัญของสนธิสัญญาหรือกฎหมายระหว่างประเทศด้านสิทธิมนุษยชนอื่น ๆ อีกหลายฉบับ รวมถึงการพัฒนากฎหมายภายในของประเทศต่าง ๆ ด้านสิทธิมนุษยชนด้วย เพื่อส่งเสริมและคุ้มครองสิทธิมนุษยชนของประชาชนในประเทศของตน ทั้งนี้ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชนมีสถานะเป็นกฎหมายจารีตประเพณีระหว่างประเทศที่ทุกประเทศทั่วโลกให้ความสำคัญในฐานะแม่บทของสิทธิมนุษยชน[30]

ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) ได้นำเสนอหลักการของสิทธิมนุษยชน นอกเหนือจากการระบุขอบเขตว่าสิทธิมนุษยชนครอบคลุมสิทธิอะไรบ้าง ซึ่งถือเป็นหลักการที่ใช้อ้างอิงความเป็นสากลของสิทธิมนุษยชน และเป็นเครื่องบ่งชี้ได้ว่าสังคมใดให้การเคารพและยึดถือปฏิบัติตามหลักการสิทธิมนุษยชนหรือไม่ ซึ่งประกอบด้วยหลักการดังนี้[31]

2.6.1.1 ทุกคนมีศักดิ์ศรีความเป็นมนุษย์ (Human Dignity) เป็นสิทธิติดตัวทุกคนตามธรรมชาติตั้งแต่เกิด (National Rights)

---

[30] กระทรวงการต่างประเทศ, ‘ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน - Universal Declaration of Human Rights’ <https://humanrights.mfa.go.th/th/humanrights/obligation/index.php> สืบค้นเมื่อ 16 พฤษภาคม 2565.

[31] UNDP, ‘Indicators for Human Rights Based Approaches to Development in UNDP Programming: A Users’ Guide 2006’ <http://www.undp-aciac.org/publications/other/undp/hr/humanrights-indicators-06e.pdf> สืบค้นเมื่อ 29 พฤษภาคม 2562.

2.6.1.2 สิทธิมนุษยชนเป็นสากลและไม่สามารถถ่ายโอนกันได้ (Universality and Inalienability) หมายความว่า สิทธิมนุษยชนเป็นของคนทุกคนโดยไม่เลือกเชื้อชาติ สัญชาติ ไม่ว่าจะอยู่ที่ใดบนโลก ย่อมมีสิทธิมนุษยชนประจำตัวทุกคน และไม่สามารถโอนให้แก่กันได้ เพราะสิทธิมนุษยชนเป็นสิทธิประจำตัวของมนุษย์ ต่างกับการครอบครองทรัพย์สินอื่น ๆ

2.6.1.3 สิทธิมนุษยชนเป็นองค์รวมแยกเป็นส่วน ๆ ไม่ได้และพึ่งพิงกัน (Indivisibility and Interdependently) กล่าวคือ ไม่สามารถแบ่งแยกว่าสิทธิใดสำคัญยิ่งไปกว่ากัน ทุกสิทธิมีความสำคัญเท่าเทียมกัน และเกื้อหนุนพึ่งพิงกัน

2.6.1.4 ความเสมอภาคและห้ามการเลือกปฏิบัติ (Equality and Non-Discrimination) คนทุกคนต้องได้รับการปฏิบัติอย่างเท่าเทียมกัน ไม่ว่าจะเป็นคนจน คนรวย คนพิการ เด็ก หรือผู้สูงอายุ คนป่วยหรือมีสุขภาพดี

2.6.1.5 การมีส่วนร่วมและการเป็นส่วนหนึ่งของสิทธินั้น (Participation and Inclusion) หมายความว่า ประชาชนแต่ละคน หรือกลุ่มประชาชน หรือประชาสังคมย่อมมีส่วนร่วมอย่างแข็งขันในการเข้าถึงและได้รับประโยชน์จากสิทธิพลเมือง สิทธิทางการเมือง และสิทธิทางเศรษฐกิจ สังคมและวัฒนธรรม

2.6.1.6 ตรวจสอบได้และใช้หลักนิติธรรม (Accountability and the Rule of Law) หมายถึง รัฐและองค์กรที่มีหน้าที่ในการก่อให้เกิดสิทธิมนุษยชน ต้องมีหน้าที่ตอบคำถามให้ได้ว่าสิทธิมนุษยชนได้รับการปฏิบัติให้เกิดผลจริงในประเทศของตน ส่วนสิทธิใดยังไม่ได้ดำเนินการให้เป็นไปตามหลักการสากลก็ต้องอธิบายต่อสังคมได้ว่าจะมีขั้นตอนดำเนินการอย่างไร โดยเฉพาะรัฐต้องมีมาตรการปกครองประเทศโดยใช้หลักนิติธรรมหรือปกครองโดยอาศัยหลักการที่ใช้กฎหมายอย่างเที่ยงธรรม ประชาชนเข้าถึงกระบวนการยุติธรรมได้โดยง่าย มีกระบวนการไม่ซับซ้อนเป็นไปตามหลักกฎหมายและมีความเท่าเทียมกันเมื่ออยู่ต่อหน้ากฎหมาย ไม่มีใครอยู่เหนือกฎหมายได้

2.6.2 สิทธิมนุษยชนที่อาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้กลายเป็นความกังวลสูงสุดสำหรับรัฐบาลทั่วโลก ในขณะที่ภัยคุกคามทางไซเบอร์ยังคงพัฒนาและเพิ่มจำนวนขึ้นเรื่อย ๆ รัฐบาลได้ใช้กฎหมายและมาตรการบังคับใช้ความปลอดภัยทางไซเบอร์ต่าง ๆ เพื่อปกป้องพลเมืองและโครงสร้างพื้นฐานที่สำคัญ อย่างไรก็ตาม ในการแสวงหาการรักษาความมั่นคงปลอดภัยและป้องกันอาชญากรรมทางไซเบอร์ มีความเสี่ยงที่อาจเกิดขึ้นจากการรุกล้ำสิทธิมนุษยชนขั้นพื้นฐาน ในหัวข้อนี้จึงจะได้ตรวจสอบประเด็นสำคัญที่สิทธิมนุษยชนอาจถูกกระทบจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ และความท้าทายที่ต้องเผชิญในการสร้างสมดุลที่ละเอียดอ่อนระหว่างความปลอดภัยและเสรีภาพส่วนบุคคล

เมื่อพิจารณาจากกฎหมายระหว่างประเทศด้านสิทธิมนุษยชนที่สำคัญ 3 ฉบับ ได้แก่ ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) ซึ่งมีสถานะเป็นกฎหมายจารีตประเพณีระหว่างประเทศ และความตกลงระหว่างประเทศที่มีผลผูกพันทางกฎหมายอีกสองฉบับ ได้แก่ กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR)[32] และกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights: ICESCR)[33] พบว่ามีสิทธิมนุษยชนที่สำคัญซึ่งอาจถูกกระทบจากการบังคับใช้กฎหมายและมาตรการความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

2.6.2.1 สิทธิในความเป็นส่วนตัว (Right to Privacy) คือหนึ่งในสิทธิมนุษยชนที่สำคัญที่สุดที่ได้รับผลกระทบจากการบังคับใช้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ แม้ว่ารัฐบาลจะมีหน้าที่รับผิดชอบในการปกป้องพลเมืองของตนจากภัยคุกคามทางไซเบอร์ แต่มาตรการเฝ้าระวังที่มากเกินไปอาจละเมิดสิทธิความเป็นส่วนตัวได้ ในการตรวจสอบภัยคุกคามทางไซเบอร์และติดตามผู้ต้องสงสัย หน่วยงานบังคับใช้กฎหมายมักต้องเข้าถึงข้อมูลส่วนบุคคล การสื่อสาร และกิจกรรมออนไลน์ ทั้งนี้ มาตรการต่าง ๆ เช่น การเฝ้าระวังข้อมูล การดักฟังโทรศัพท์ และนโยบายการเก็บรักษาข้อมูลอาจละเมิดสิทธิความเป็นส่วนตัวของแต่ละบุคคล ซึ่งอาจนำไปสู่การบุกรุกข้อมูลส่วนบุคคลและการสอดแนมสื่อสารที่ไม่สมควร การสร้างสมดุลระหว่างความปลอดภัยและความเป็นส่วนตัว โดยการดำเนินการรวบรวมและวิเคราะห์ข้อมูลโดยกำหนดเป้าหมายที่เฉพาะเจาะจง โดยมีมาตรการเยียวยาและการกำกับดูแลโดยศาล

2.6.2.2 เสรีภาพในการแสดงออก (Freedom of Expression) การมาถึงของมาตรการบังคับใช้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์มีผลกระทบต่อเสรีภาพในการแสดงออก รัฐอาจใช้การกรองเนื้อหา การเซ็นเซอร์ และการเฝ้าระวังเพื่อต่อสู้กับภัยคุกคามทางไซเบอร์ เช่น คำพูดแสดงความเกลียดชัง การก่อการร้าย และการบิดเบือนข้อมูล แต่ในบางกรณี ด้วยคำจำกัดความที่คลุมเครือของบทบัญญัติแห่งกฎหมายและอำนาจบังคับใช้ที่กว้างขวาง รัฐอาจใช้การตีความกฎหมายความมั่นคงปลอดภัยทางไซเบอร์เพื่อยับยั้งผู้เห็นต่างหรือปิดปากฝ่ายตรงข้ามทางการเมือง

---

[32] กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) ประเทศไทยเข้าเป็นภาคีโดยการภาคยานุวัติ เมื่อวันที่ 29 ตุลาคม 2539 และมีผลใช้บังคับกับไทยเมื่อวันที่ 29 มกราคม 2540

[33] กติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights: ICESCR) ประเทศไทยเข้าเป็นภาคีโดยการภาคยานุวัติ เมื่อวันที่ 5 กันยายน 2542 และมีผลใช้บังคับกับไทยเมื่อวันที่ 5 ธันวาคม 2542

การสอดแนม การจำกัดเสรีภาพทางอินเทอร์เน็ต และจำกัดการไหลเวียนของข้อมูลอย่างเสรี ซึ่งสามารถบ่อนทำลายสิทธิในการแสดงความคิดเห็นและการแบ่งปันข้อมูล ซึ่งขัดขวางการมีส่วนร่วมในระบอบประชาธิปไตยและบ่อนทำลายคุณค่าทางประชาธิปไตย สิ่งสำคัญคือต้องกำหนดแนวทางที่ชัดเจนและกลไกการกำกับดูแลเพื่อป้องกันการใช้อำนาจในทางที่ผิด และทำให้แน่ใจว่าข้อจำกัดเสรีภาพในการแสดงออกได้สัดส่วนและสอดคล้องกับมาตรฐานสิทธิมนุษยชนระหว่างประเทศ

2.6.2.3 กระบวนการอันชอบธรรมและหลักนิติธรรม (Due Process and Rule of Law) การบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ มักเกี่ยวข้องกับการระบุตัวตน การสอบสวน และการดำเนินคดีกับอาชญากรไซเบอร์ ซึ่งควรเป็นไปตามหลักการของกระบวนการอันชอบธรรมและหลักนิติธรรม กฎหมายความมั่นคงทางไซเบอร์อาจให้อำนาจแก่หน่วยงานบังคับใช้กฎหมายอย่างกว้างขวางโดยไม่มีการตรวจสอบและถ่วงดุลที่เพียงพอ เช่น ดำเนินการตรวจค้น ยึด และจับกุม โดยปราศจากการกำกับดูแลของศาลอย่างเหมาะสม ซึ่งอาจส่งผลให้เกิดการกระทำตามอำเภอใจและการเลือกปฏิบัติที่บ่อนทำลายหลักการพื้นฐานของความยุติธรรม การพิจารณาคดีที่เป็นธรรม และการสันนิษฐานว่าเป็นผู้บริสุทธิ์ รัฐบาลต้องสร้างกรอบกฎหมายที่ชัดเจนซึ่งกำหนดขอบเขตและข้อจำกัดของการดำเนินการบังคับใช้ความปลอดภัยทางไซเบอร์ การรับประกันว่าบุคคลจะได้รับสิทธิในการพิจารณาคดีอย่างยุติธรรม การมีตัวแทนทางกฎหมาย และการเข้าถึงพยานหลักฐาน

2.6.2.4 สิทธิในการเข้าถึงข้อมูลและความเหลื่อมล้ำทางดิจิทัล (Right of Access to Information and Digital Divide) มาตรการรักษาความปลอดภัยทางไซเบอร์ที่มุ่งปกป้องโครงสร้างพื้นฐานที่สำคัญหรือข้อมูลที่ละเอียดอ่อนสามารถจำกัดสิทธิในการเข้าถึงข้อมูลโดยไม่ได้ตั้งใจและทำให้ความเหลื่อมล้ำทางดิจิทัลรุนแรงขึ้น การปิดระบบอินเทอร์เน็ตตามคำสั่งของรัฐ การเซ็นเซอร์ การบล็อกเว็บไซต์ หรือการลบเนื้อหาเพื่อจำกัดการเข้าถึงของประชาชน เป็นการจำกัดความสามารถของบุคคลในการเข้าถึงความรู้และการใช้สิทธิในการแสวงหาและรับข้อมูล การสร้างสมดุลระหว่างความปลอดภัยในโลกไซเบอร์และสิทธิของประชาชนในการเข้าถึงข้อมูลเป็นสิ่งสำคัญ โดยต้องส่งเสริมความรู้ด้านดิจิทัล ปิดช่องว่างของความเหลื่อมล้ำทางดิจิทัล และนำมาตรการรักษาความปลอดภัยทางไซเบอร์มาใช้โดยไม่ส่งผลกระทบต่อชุมชนชายขอบอย่างไม่เหมาะสมหรือขัดขวางการเข้าถึงข้อมูลและโอกาส นอกจากนี้ มาตรการความปลอดภัยทางไซเบอร์ยังอาจส่งผลที่ไม่ได้ตั้งใจในช่วงวิกฤตด้านมนุษยธรรม การจำกัดการเข้าถึงอินเทอร์เน็ตหรือการจำกัดช่องทางการสื่อสารในกรณีฉุกเฉินสามารถขัดขวางการเข้าถึงข้อมูลที่สำคัญ ขัดขวางความพยายามในการบรรเทาทุกข์ และขัดขวางความสามารถของแต่ละบุคคลในการขอความช่วยเหลือและปกป้องสิทธิมนุษยชน

2.6.2.5 สิทธิในการศึกษา (Right to Education) ผลกระทบที่อาจเกิดขึ้นกับสิทธิในการศึกษาเกิดขึ้นจากการเฝ้าระวัง การเซ็นเซอร์ หรือการจำกัดในการเข้าถึงเทคโนโลยี

สารสนเทศและการสื่อสารที่มากเกินไป มาตรการเหล่านี้อาจส่งผลให้เกิดการจำกัดการไหลเวียนของข้อมูลอย่างเสรี จำกัดเสรีภาพทางวิชาการ ขัดขวางการทำงานร่วมกันและการวิจัยทางออนไลน์ และลดการเข้าถึงทรัพยากรทางการศึกษา รวมถึงความพร้อมใช้งานและความหลากหลายของสื่อและทรัพยากรทางการศึกษา ซึ่งเป็นอุปสรรคต่อสิทธิในการศึกษาที่มีคุณภาพ การเซ็นเซอร์หรือการตรวจสอบแพลตฟอร์มออนไลน์และสื่อสังคมออนไลน์สามารถขัดขวางเสรีภาพในการแสดงออกและจำกัดความสามารถของนักเรียนในการมีส่วนร่วมในการอภิปรายอย่างเปิดเผยและแสดงความคิดเห็นได้อย่างอิสระ ดังนั้น นโยบายเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และมาตรการต่าง ๆ ที่นำมาบังคับใช้ต้องมีลักษณะที่ส่งเสริมสิทธิมนุษยชน รวมถึงสิทธิในการศึกษา โดยการรับรองว่าข้อจำกัดที่มีต่อกิจกรรมออนไลน์นั้นจำเป็น ได้สัดส่วน และสอดคล้องกับมาตรฐานสิทธิมนุษยชนระหว่างประเทศ รัฐบาลควรส่งเสริมความโปร่งใส ความรับผิดชอบ และการมีส่วนร่วมของประชาชนในการกำหนดและบังคับใช้กฎหมายความปลอดภัยทางไซเบอร์ เพื่อป้องกันการละเมิดและปกป้องสิทธิส่วนบุคคล

2.6.2.6 การเลือกปฏิบัติทางไซเบอร์ (Cyber Discrimination) มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์อาจนำไปสู่การเลือกปฏิบัติทางไซเบอร์ โดยการกำหนดเป้าหมายไปที่กลุ่มคนบางกลุ่มอย่างไม่ได้สัดส่วน การเฝ้าระวังในวงกว้างอาจกำหนดเป้าหมายไปยังบางกลุ่มโดยพิจารณาจากปัจจัยต่าง ๆ เช่น สัญชาติ เชื้อชาติ หรือศาสนา สิ่งนี้ไม่เพียงละเมิดสิทธิมนุษยชนเท่านั้น แต่ยังสร้างอคติในสังคมด้วย ทำให้ความไม่เท่าเทียมกันทางสังคมรุนแรงขึ้น รัฐต้องตรวจสอบให้แน่ใจว่ามาตรการรักษาความปลอดภัยทางไซเบอร์นั้นไม่เลือกปฏิบัติ ภายใต้การกำกับดูแลที่เป็นอิสระ และมีพื้นฐานมาจากการประเมินความเสี่ยงตามหลักฐานที่เชื่อถือได้

2.6.3 แนวทางฐานสิทธิมนุษยชนเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (Human Rights-Based Approach to Cybersecurity)

การใช้แนวทางฐานสิทธิมนุษยชนเพื่อการสร้างความมั่นคงปลอดภัยทางไซเบอร์นั้นเป็นกระแสหนึ่งซึ่งองค์การระหว่างประเทศ กลุ่มความร่วมมือ และที่ประชุมซึ่งเกี่ยวข้องกับไซเบอร์และอินเทอร์เน็ตต่างให้ความสำคัญกันมากขึ้น โดยแนวทางที่น่าสนใจในเรื่องนี้ เป็นคำแนะนำ (Recommendation) ของกลุ่ม Freedom Online Coalition ซึ่งเป็นกลุ่มความร่วมมือของรัฐบาล 30 ประเทศ เช่น สหรัฐอเมริกา แคนาดา ญี่ปุ่น ออสเตรเลีย นิวซีแลนด์ ฝรั่งเศส เอสโตเนีย เป็นต้น เพื่อที่จะทำงานร่วมกันในการพัฒนาเสรีภาพทางอินเทอร์เน็ต โดยให้ผู้มีส่วนได้ส่วนเสียทั้งหลายได้มีส่วนร่วม โดยสร้างแนวบรรทัดฐานผ่านแถลงการณ์ร่วม (Joint Statement) ภายหลังการประชุมร่วมกัน โดยประเทศที่เข้าร่วมให้พันธะสัญญาว่า “จะสนับสนุนเสรีภาพในการแสดงออก การสมาคม และการชุมนุมอย่างสงบผ่านทางอินเทอร์เน็ตและเทคโนโลยีการเชื่อมต่ออื่น ๆ” นอกจากนี้ยังรับรองหลักการที่ว่าสิทธิมนุษยชนของผู้ที่อยู่ในโลกออนไลน์ควรได้รับการคุ้มครองเช่นเดียวกับโลกออฟไลน์ การดำเนินงานต่าง ๆ ของกลุ่มอยู่บนหลักการของข้อมติสหประชาชาติ The Promotion, Protection

and Enjoyment of Human Rights on the Internet (A/HRC/RES/26/13) ที่รับรองโดยสหประชาชาติในเดือนกรกฎาคม 2555 (ค.ศ. 2014)

โดยคำแนะนำ (Recommendation) ของกลุ่ม Freedom Online Coalition ออกมาเมื่อ 17 ตุลาคม 2559 (ค.ศ. 2016) ในการประชุมที่เมืองซานโฮเซ คอสตาริกา มี 13 ข้อ[34] ดังนี้

(1) นโยบายความปลอดภัยทางไซเบอร์และกระบวนการตัดสินใจควรปกป้องและเคารพสิทธิมนุษยชน

(2) การพัฒนากฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์ควรเคารพสิทธิมนุษยชนตั้งแต่เริ่มออกแบบ

(3) กฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ควรส่งเสริมความปลอดภัยของบุคคลทั้งแบบออนไลน์และออฟไลน์โดยคำนึงถึงภัยคุกคามที่ไม่เหมาะสมที่บุคคลและกลุ่มต่าง ๆ มีความเสี่ยงที่จะต้องเผชิญอยู่

(4) การพัฒนาและการดำเนินการตามกฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์ควรสอดคล้องกับกฎหมายระหว่างประเทศ รวมถึงกฎหมายสิทธิมนุษยชนระหว่างประเทศ และกฎหมายด้านมนุษยธรรมระหว่างประเทศ

(5) ไม่ควรใช้กฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์เพื่อเป็นข้ออ้างในการละเมิดสิทธิมนุษยชน โดยเฉพาะอย่างยิ่งการแสดงออกอย่างอิสระ การสมาคม การชุมนุม และความเป็นส่วนตัว

(6) การตอบสนองต่อเหตุการณ์ในโลกไซเบอร์ไม่ควรละเมิดสิทธิมนุษยชน

(7) กฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ควรสนับสนุนและปกป้องความมั่นคงและความปลอดภัยของอินเทอร์เน็ต และไม่ควรทำลายความสมบูรณ์ของโครงสร้างพื้นฐาน ฮาร์ดแวร์ ซอฟต์แวร์ และบริการ

(8) กฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ควรสะท้อนให้เห็นถึงบทบาทสำคัญของการเข้ารหัสและการไม่เปิดเผยตัวตน ซึ่งเป็นการปฏิบัติตามสิทธิมนุษยชนโดยเฉพาะการแสดงออกอย่างอิสระ การสมาคม การชุมนุมและความเป็นส่วนตัว

---

[34] Freedom Online Coalition, 'Recommendations for human rights based approaches to cybersecurity' <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FOC-WG1-Recommendations-discussion-draft-IGF-20151.pdf> สืบค้นเมื่อ 22 พฤษภาคม 2562.

(9) กฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์ไม่ควรเป็นอุปสรรคต่อการพัฒนาทางเทคโนโลยีที่นำไปสู่การคุ้มครองสิทธิมนุษยชน

(10) กฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์ในระดับประเทศ ระดับภูมิภาคและระดับระหว่างประเทศควรได้รับการพัฒนาผ่านแนวทางที่เปิดกว้าง ครอบคลุม และโปร่งใสซึ่งรวมผู้มีส่วนได้ส่วนเสียทั้งหมดไว้ด้วย

(11) ผู้มีส่วนได้ส่วนเสียควรส่งเสริมการศึกษา ความเท่าทันดิจิทัล และการฝึกอบรมด้านเทคนิคและกฎหมาย เพื่อเป็นแนวทางในการปรับปรุงความปลอดภัยทางไซเบอร์และการตระหนักถึงสิทธิมนุษยชน

(12) สิทธิมนุษยชนให้ความเคารพแนวปฏิบัติที่เป็นเลิศเกี่ยวกับความปลอดภัยทางไซเบอร์ ควรมีการแบ่งปันและส่งเสริมในกลุ่มผู้มีส่วนได้เสีย

(13) การสร้างขีดความสามารถในการรักษาความปลอดภัยไซเบอร์มีบทบาทสำคัญในการเสริมสร้างความปลอดภัยของบุคคลทั้งออนไลน์และออฟไลน์ ความพยายามดังกล่าวควรส่งเสริมสิทธิมนุษยชนที่เคารพแนวทางในการรักษาความปลอดภัยทางไซเบอร์

จากคำแนะนำข้างต้นจะเห็นได้ว่าสิทธิมนุษยชนเป็นสิ่งสำคัญอย่างยิ่งประการหนึ่งในการพัฒนากฎหมาย นโยบาย และแนวปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในทางกลับกันหลักการสิทธิมนุษยชนเองก็ต้องให้ความสำคัญกับเทคนิค แนวปฏิบัติในการรักษาความปลอดภัยทางไซเบอร์ด้วย ผู้กำหนดนโยบายถกเถียงกันมานานแล้วว่าจะรักษาสมดุลระหว่างความปลอดภัยและเสรีภาพในอินเทอร์เน็ตได้อย่างไร เนื่องจากภัยคุกคามด้านความปลอดภัยนั้นมีการเปลี่ยนแปลงอยู่เสมอ ดุลยพินิจของรัฐบาลและผู้ให้บริการอินเทอร์เน็ตจึงเป็นสิ่งจำเป็น แต่ควรตรวจสอบดุลยพินิจนั้นด้วยมาตรการที่เชื่อถือได้[35] ดังนั้นกฎหมายจึงต้องมีความสมดุลระหว่าง การรักษาความมั่นคงปลอดภัยซึ่งอาจเน้นไปทางด้านเทคนิคและความมั่นคงของผู้ใช้ องค์กร รัฐ รวมถึงประชาคมระหว่างประเทศ ในขณะเดียวกันก็ต้องไม่ละเมิดสิทธิมนุษยชน ปกป้อง ส่งเสริม และให้ผู้มีส่วนได้ส่วนเสียได้มีส่วนร่วมในการดำเนินการตั้งแต่การเริ่มออกแบบนโยบาย กฎหมาย ไปจนถึงขั้นตอนการบังคับใช้ การเผยแพร่ความรู้ และแลกเปลี่ยน เพื่อส่งเสริมซึ่งกันและกัน อันจะทำให้กฎหมายเกิดประสิทธิภาพ ได้รับความร่วมมือจากทุกฝ่าย เกิดความเข้มแข็งในการต่อสู้กับภัยคุกคามทางไซเบอร์อย่างแท้จริง ซึ่งในบทต่อไปจะได้ศึกษาเกี่ยวกับแนวทางระหว่างประเทศและแนวทางกฎหมายของประเทศต่าง ๆ ในเรื่องนี้

---

[35] Marvin Ammori & Keira Poellet, ‘“Security versus Freedom” in the internet: Cybersecurity and Net Neutrality’ (2010) 30 SAIS Review of International Affairs 51, 63.

บทที่ 3
ตราสารระหว่างประเทศที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ และกฎหมายต่างประเทศว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์

ดังที่ได้กล่าวไว้ในตอนต้นว่าในปัจจุบันประเทศต่าง ๆ ตลอดจนองค์การระหว่างประเทศและกลุ่มความร่วมมือระหว่างประเทศ ให้ความสำคัญและตื่นตัวกับเรื่องภัยคุกคามทางไซเบอร์เป็นอย่างมาก ทำให้เกิดการพัฒนามาตรการ แนวปฏิบัติ บรรทัดฐาน และกฎหมาย เพื่อรับมือกับปัญหาภัยคุกคามทางไซเบอร์ เนื่องจากองค์การระหว่างประเทศต่างตระหนักดีว่าปัญหาความมั่นคงทางไซเบอร์นั้น ไม่เพียงกระทบต่อความมั่นคงและการป้องกันของรัฐสมาชิกเท่านั้น แต่ยังกระทบถึงตัวองค์การเองด้วยเช่นกัน ในบทนี้จึงจะนำเสนอตราสารระหว่างประเทศที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ขององค์การระหว่างประเทศที่สำคัญ ได้แก่ สหประชาชาติ (United Nations: UN) สหภาพยุโรป (European Union: EU) องค์การสนธิสัญญาแอตแลนติกเหนือ (North Atlantic Treaty Organisation: NATO) และสมาคมประชาชาติเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations: ASEAN) เพื่อตรวจสอบมาตรฐานในระดับระหว่างประเทศต่อการรับมือปัญหาภัยคุกคามทางไซเบอร์ รวมถึงกฎหมายต่างประเทศว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ สหรัฐอเมริกา จีน และสิงคโปร์ ทั้งนี้ นอกจากการพิจารณาด้านการรักษาความมั่นคงปลอดภัยแล้ว ผู้เขียนจะได้วิเคราะห์ตราสารและกฎหมายเหล่านี้ในมิติทางด้านสิทธิมนุษยชนร่วมด้วย เพื่อให้เห็นว่าในระดับนานาชาติ มีความตระหนักถึงความสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับสิทธิมนุษยชนหรือไม่

3.1 ตราสารระหว่างประเทศ

3.1.1 สหประชาชาติ (United Nations)

ที่ประชุมสมัชชาใหญ่แห่งองค์การสหประชาชาติเริ่มให้ความสำคัญกับประเด็นความมั่นคงปลอดภัยทางไซเบอร์ในปี ค.ศ. 1999 โดยประเทศรัสเซียได้ยื่นข้อเสนอในการแก้ไขปัญหาความมั่นคงปลอดภัยทางไซเบอร์ต่อสหประชาชาติ เมื่อวันที่ 30 กันยายน ค.ศ. 1998 และที่ประชุมสมัชชาใหญ่ให้การรับรองข้อมติ 53/70 เมื่อวันที่ 4 มกราคม ค.ศ. 1999 ซึ่งเป็นการริเริ่มพัฒนาความร่วมมือในทุกระดับ และริเริ่มพัฒนาหลักปฏิบัติร่วมกันในระดับนานาชาติเพื่อรักษาความมั่นคงทางด้านสารสนเทศและระบบโทรคมนาคม เพื่อต่อต้านการก่อการร้ายและอาชญากรรม ถัดมาในปี ค.ศ. 2004 สหประชาชาติได้ตั้ง United Nations Group of Governmental Experts on Developments

in The Field of Information and Telecommunications in the Context of International Security หรือ UNGGE ซึ่งเป็นที่ประชุมผู้เชี่ยวชาญในด้านสารสนเทศและโทรคมนาคม เพื่อเสาะหาแนวทางในการสร้างความเข้มแข็งให้แก่สันติภาพและความมั่นคงของโลก ตลอดจนมีมาตรการที่สร้างความมั่นใจให้เกิดขึ้นในโลกไซเบอร์ โดยการพัฒนาบรรทัดฐานหรือมาตรฐาน สำหรับพฤติกรรมที่มีความรับผิดชอบของรัฐในโลกไซเบอร์

3.1.1.1 บรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ (The United Nations (UN) Norms of Responsible State Behaviour in Cyberspace) ในปี ค.ศ. 2013 รายงานของ UNGGE ได้รับการรับรองโดยที่ประชุมสมัชชาใหญ่ของสหประชาชาติ ตามข้อมติ 68/243 เมื่อวันที่ 24 มิถุนายน ค.ศ. 2013 มีเนื้อหาแสดงความตระหนักถึงการนำกฎหมายระหว่างประเทศ โดยเฉพาะกฎบัตรสหประชาชาติ มาปรับใช้กับโลกไซเบอร์[1] ต่อมาในปี ค.ศ. 2015 UNGGE ได้ออกรายงานอีกฉบับหนึ่ง ซึ่งที่ประชุมสมัชชาใหญ่ให้การรับรองข้อมติ 70/237 วันที่ 30 ธันวาคม ค.ศ. 2015 โดยร้องขอให้รัฐภาคีนำแนวบรรทัดฐานจากรายงานของ UNGGE 2015 ไปเป็นแนวทางในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร[2] ซึ่ง The United Nations (UN) Norms of Responsible State Behaviour in Cyberspace หรือบรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ มีจำนวน 11 ข้อ[3] ดังนี้

(1) เพื่อให้สอดคล้องกับวัตถุประสงค์ของสหประชาชาติ ซึ่งรวมถึงการรักษาสันติภาพและความมั่นคงระหว่างประเทศ รัฐควรร่วมมือในการพัฒนาและใช้มาตรการเพื่อเพิ่มเสถียรภาพและความปลอดภัยในการใช้ ICT และเพื่อป้องกันการปฏิบัติด้าน ICT ที่ได้รับการยอมรับว่าเป็นอันตรายหรืออาจก่อให้เกิดภัยคุกคามต่อสันติภาพและความมั่นคงระหว่างประเทศ

---

[1] UNGA Resolution A/Res/68/243 “19. International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”

[2] UNGA Resolution A/RES/70/237 “2(a) To be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts;”

[3] United Nations, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ <https://dig.watch/wp-content/uploads/2022/08/UN-GGE-2015-report.pdf> สืบค้นเมื่อ 22 พฤษภาคม 2562.

(2) ในกรณีเกิดเหตุการณ์ทาง ICT รัฐควรพิจารณาข้อมูลที่เกี่ยวข้องทั้งหมด รวมถึงบริบทที่กว้างขวางของเหตุการณ์ ความท้าทายของการวิเคราะห์สภาพแวดล้อม ICT และลักษณะและขอบเขตของผลที่ตามมา

(3) รัฐไม่ควรยอมให้ใช้ดินแดนของตนในการใช้ ICT เพื่อการกระทำที่มิชอบระหว่างโดยเจตนา

(4) รัฐควรพิจารณาวิธีที่ดีที่สุดในการร่วมมือกันเพื่อแลกเปลี่ยนข้อมูล ช่วยเหลือซึ่งกันและกัน การดำเนินการทางกฎหมายกับผู้ก่อการร้ายและอาชญากรซึ่งใช้ ICT กระทำความผิด และใช้มาตรการความร่วมมืออื่น ๆ เพื่อจัดการกับภัยคุกคามดังกล่าว รัฐอาจต้องพิจารณาว่าจำเป็นต้องมีการพัฒนามาตรการใหม่ในส่วนนี้หรือไม่

(5) ในการสร้างความมั่นใจในการใช้ ICT อย่างปลอดภัย รัฐควรเคารพข้อมติคณะมนตรีสิทธิมนุษยชนที่ 20/8 และ 26/13 ว่าด้วยการส่งเสริม การคุ้มครอง และการใช้สิทธิมนุษยชนบนอินเทอร์เน็ต เช่นเดียวกับมติสมัชชาใหญ่ที่ 68/167 และ 69/166 ว่าด้วยสิทธิในความเป็นส่วนตัวในยุคดิจิทัล เพื่อรับประกันการเคารพสิทธิมนุษยชนอย่างเต็มที่ รวมถึงสิทธิที่จะมีเสรีภาพในการแสดงออก

(6) รัฐไม่ควรดำเนินการหรือสนับสนุนกิจกรรม ICT อันขัดต่อพันธกรณีภายใต้กฎหมายระหว่างประเทศ ที่เจตนาทำลายโครงสร้างพื้นฐานที่สำคัญ หรือทำให้การใช้งานและการดำเนินงานของโครงสร้างพื้นฐานสำคัญในการให้บริการแก่สาธารณะบกพร่อง

(7) รัฐควรใช้มาตรการที่เหมาะสมในการปกป้องโครงสร้างพื้นฐานที่สำคัญของตนจากภัยคุกคามด้าน ICT โดยคำนึงถึงข้อมติสมัชชาใหญ่ที่ 58/199 ว่าด้วยการสร้างวัฒนธรรมความปลอดภัยในโลกไซเบอร์และการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และข้อมติอื่น ๆ ที่เกี่ยวข้อง

(8) รัฐควรมีการตอบสนองต่อคำร้องขอที่เหมาะสม สำหรับการขอความช่วยเหลือจากอีกรัฐหนึ่ง ซึ่งมีโครงสร้างพื้นฐานที่สำคัญตกอยู่ภายใต้การกระทำที่มุ่งร้ายด้าน ICT รัฐควรตอบสนองต่อคำขอที่เหมาะสม ในการจำกัดกิจกรรม ICT ที่เป็นอันตรายซึ่งมุ่งเป้าไปที่โครงสร้างพื้นฐานที่สำคัญของรัฐอื่นที่เกิดจากดินแดนของตน โดยคำนึงถึงอำนาจอธิปไตย

(9) รัฐควรดำเนินการตามสมควรเพื่อรับรองความสมบูรณ์ของห่วงโซ่อุปทาน เพื่อให้ผู้ใช้ปลายทางสามารถมั่นใจในความปลอดภัยของผลิตภัณฑ์ ICT รัฐควรหาทาง

ป้องกันการแพร่หลายของเครื่องมือและเทคนิคด้าน ICT ที่เป็นอันตราย และการใช้ฟังก์ชันซ่อนเร้นที่เป็นอันตราย

(10) รัฐควรสนับสนุนให้มีการรายงานอย่างมีความรับผิดชอบเกี่ยวกับช่องโหว่ของ ICT และแบ่งปันข้อมูลที่เกี่ยวข้องกับการแก้ไขที่มีอยู่สำหรับช่องโหว่ดังกล่าว เพื่อจำกัดและอาจกำจัดภัยคุกคามที่อาจเกิดขึ้นกับ ICT และโครงสร้างพื้นฐานที่ต้องอาศัย ICT

(11) รัฐไม่ควรดำเนินการหรือสนับสนุนกิจกรรมโดยรู้ว่าจะเป็นอันตรายต่อระบบข้อมูลของทีมตอบโต้เหตุฉุกเฉิน (หรือเรียกว่า ทีมตอบโต้เหตุฉุกเฉินทางคอมพิวเตอร์หรือทีมตอบโต้เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์) ของรัฐอื่น รัฐไม่ควรใช้ทีมตอบโต้เหตุฉุกเฉินไปมีส่วนร่วมในกิจกรรมระหว่างประเทศที่เป็นอันตราย

ภาพ 3.1 UN Norms of Responsible State Behaviour in Cyberspace

ที่มา : Australian Strategic Policy Institute

เมื่อพิจารณาแนวบรรทัดฐานของสหประชาชาติซึ่งมุ่งเน้นไปที่การสร้างพฤติกรรมที่มีความรับผิดชอบของรัฐบนโลกไซเบอร์ เพื่อมิให้เกิดอันตรายต่อรัฐตนและรัฐอื่น ตลอดจนการให้ความร่วมมือและช่วยเหลือซึ่งกันและกันในภาวะที่ประสบภัยคุกคาม สหประชาชาติยังให้ความสำคัญกับสิทธิมนุษยชน โดยกำหนดไว้ในบรรทัดฐานข้อที่ 5 ในการดำเนินการต่าง ๆ เพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ ต้องคำนึงถึงการส่งเสริม การคุ้มครอง และการใช้สิทธิมนุษยชนบนอินเทอร์เน็ต สิทธิในความเป็นส่วนตัว เสรีภาพในการแสดงออก และการเคารพสิทธิมนุษยชนอย่างเต็มที่ อย่างไรก็ดี บรรทัดฐานของสหประชาชาติยังมีสถานะเป็นเพียง Soft Law ซึ่งไม่มีค่าบังคับทางกฎหมาย แต่เป็นแนวทางที่ขอให้รัฐภาคีใช้ร่วมกันในการปฏิบัติตามโดยสมัครใจมากกว่า เพื่อให้สามารถรักษาไว้ซึ่งสันติภาพและความมั่นคงของสังคมระหว่างประเทศ ซึ่งปัญหาประการหนึ่งในการเปลี่ยนคำแนะนำหรือบรรทัดฐานเหล่านี้ให้เป็นกฎที่มีผลผูกพันตามกฎหมาย คือธรรมชาติที่ซับซ้อนของพื้นที่ไซเบอร์และผู้มีส่วนได้ส่วนเสียในวงกว้าง ซึ่งไม่เพียงแค่รัฐเท่านั้นแต่รวมถึงภาคเอกชนด้วย[4] ทั้งนี้ ในปัจจุบันมีประเทศ กลุ่มความร่วมมือ และกลุ่มประเทศในภูมิภาคต่าง ๆ ของโลก กำลังพิจารณานำแนวบรรทัดฐานนี้ไปปรับใช้ในกลุ่มหรือประเทศของตนมากขึ้น รวมถึงภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ หรือ อาเซียน ซึ่งประเทศไทยเป็นสมาชิกอยู่ด้วย เป็นองค์การระหว่างประเทศระดับภูมิภาคองค์การแรก ที่นำแนวบรรทัดฐาน 11 ข้อไปปรับใช้ในภูมิภาค อันจะได้กล่าวถึงรายละเอียดต่อไป

3.1.2 สหภาพยุโรป (European Union: EU)

สหภาพยุโรปเป็นการรวมกลุ่มของประเทศในภูมิภาคยุโรปทั้งด้านการเมือง เศรษฐกิจ และสังคมในลักษณะสถาบันแบบเหนือรัฐ (Supranational Institution) ที่ใหญ่ที่สุดและก้าวหน้าที่สุดในโลก โดยมีวัตถุประสงค์เพื่อเสริมสร้างสันติภาพเป็นการถาวรระหว่างประเทศในภูมิภาคยุโรปภายหลังสงครามโลกครั้งที่ 2 รวมไปถึงการเสริมสร้างความเข้มแข็งทางเศรษฐกิจแก่ประเทศสมาชิกและการมีบทบาทนำของสหภาพยุโรปในประชาคมโลก สำหรับด้านความมั่นคงปลอดภัยทางไซเบอร์ สหภาพยุโรปได้เริ่มกำหนดยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์มาตั้งแต่ปี ค.ศ. 2013 และตั้งแต่ปี ค.ศ. 2017 เป็นต้นมา สหภาพยุโรปก็เริ่มมีบทบาทชัดเจนมากขึ้นในการปกป้องประชาชนยุโรปจากภัยคุกคามด้านไซเบอร์ โดยเฉพาะเรื่องความปลอดภัยของระบบเครือข่ายและข้อมูล (network and information security) และการปกป้องสิทธิของประชาชนออนไลน์

---

[4] Ilona Stadnik, 'What Is an International Cybersecurity Regime and How We Can Achieve It?' (2017) 11 Masaryk University Journal of Law and Technology 129, 145.

3.1.2.1 ยุทธศาสตร์ด้านความมั่นคงและปลอดภัยไซเบอร์ของยุโรป เน้นเป้าหมายหลัก 5 ประการ[5] ได้แก่

(1) บรรลุความยืดหยุ่นทางไซเบอร์ (Achieving cyber resilience) ซึ่งหมายถึง ความยืดหยุ่นคล่องตัวในการเตรียมตัว และการตอบสนองต่อการเปลี่ยนแปลง การบุกรุกหรือการโจมตี

(2) ลดการเกิดอาชญากรรมไซเบอร์หรือภัยคุกคาม (Drastically reducing cybercrime)

(3) การพัฒนานโยบายการป้องกันทางไซเบอร์และความสามารถที่เกี่ยวข้องกับกรอบของนโยบาย Common Security and Defence Policy (CSDP) ของสหภาพยุโรป (Developing cyber defence policy and capabilities related to the framework of the Common Security and Defence Policy (CSDP))

(4) พัฒนาทรัพยากรด้านอุตสาหกรรมและเทคโนโลยีที่สนับสนุนความมั่นคงและปลอดภัยไซเบอร์ (Develop industrial and technological resources for cybersecurity)

(5) กำหนดนโยบาย Cyberspace ระหว่างประเทศที่สอดคล้องกันสำหรับสหภาพยุโรป และส่งเสริมค่านิยมหลักของสหภาพยุโรป (Establish a coherent international cyberspace policy for the European Union and promote core EU values)

ในขณะที่กฎหมายและกฎระเบียบในยุโรปเริ่มเข้มข้นและเป็นระบบขึ้น ยุโรปเดินหน้านโยบายการทูตด้านไซเบอร์ไปพร้อม ๆ กัน คือเน้นการสร้างเครือข่ายและการหารืออย่างกว้างขวางกับประเทศและภูมิภาคพันธมิตร ทั้งภาครัฐและองค์กรที่ไม่ใช่ภาครัฐทั่วโลก อาทิ บราซิล จีน อินเดีย ญี่ปุ่น เกาหลีใต้ สหรัฐอเมริกา รวมทั้งในอเมริกาใต้ และเอเชีย เพื่อสร้างและสนับสนุนความร่วมมือและปรับใช้กรอบกฎหมายระหว่างประเทศด้าน Cyberspace และส่งเสริมการสร้างบรรทัดฐานระหว่างประเทศ ในการจัดการกับการโจมตีและภัยคุกคามในโลกอินเตอร์เน็ตโดยเน้นการให้ความร่วมมือด้านการเสริมสร้างขีดความสามารถ (capacity building) กับประเทศต่าง ๆ ทั่วโลก

---

[5] European Union, ‘EU Cyber Security Strategy’ <https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie> สืบค้นเมื่อ 15 พฤษภาคม 2565.

3.1.2.2 Directive on Security of Network and Information Systems 2016 หรือ NIS Directive[6] เป็นกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับแรกของสหภาพยุโรป ถูกสร้างขึ้นเพื่อความปลอดภัยบนเครือข่ายและระบบข้อมูล โดยใช้มาตรฐานระดับสูงอย่างเท่าเทียมกันและเป็นไปในทิศทางเดียวกันทั่วทั้งสหภาพยุโรป ส่งเสริมการรักษาความปลอดภัยทางไซเบอร์ที่แข็งแกร่งและเชื่อถือได้ระหว่างกัน สนับสนุนการสื่อสารข้ามพรมแดนและส่งเสริมการทำงานร่วมกันอย่างปลอดภัยและราบรื่นระหว่างองค์กรต่าง ๆ ทั่วสหภาพยุโรป ด้วยหลักปฏิบัติ 3 ประการ คือ

(1) การเพิ่มขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ภายในประเทศ โดยสมาชิกสหภาพยุโรปทุกชาติมีหน้าที่กำหนดยุทธศาสตร์ด้านความปลอดภัยบนเครือข่ายและระบบข้อมูลของประเทศ แต่งตั้งหน่วยงานที่รับผิดชอบด้านความมั่นคงปลอดภัยบนเครือข่ายและระบบข้อมูล (National NIS Authority) ซึ่งอาจมีได้มากกว่าหนึ่งหน่วยงานตามความเหมาะสม และแต่งตั้งศูนย์กลางการติดต่อ หรือ Single Point Of Contact (SPOC) สำหรับประสานความร่วมมือระหว่างประเทศ รวมถึงแต่งตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (Computer Security Incident Response Team หรือ CSIRT) เพื่อให้สามารถตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วในระดับประเทศ โดยมีมาตรฐานไม่ต่ำกว่าที่กำหนดใน NIS Directive

(2) การเพิ่มความร่วมมือระหว่างประเทศสมาชิกทั้งในด้านนโยบายด้วยการแต่งตั้งกลุ่มความร่วมมือ (Cooperation Group) และเครือข่ายความร่วมมือระหว่างองค์กร CSIRT ระดับประเทศ (CSIRTs Network) โดยกลุ่มความร่วมมือ มีประธานสภาแห่งสหภาพยุโรปเป็นผู้นำ และมีผู้แทนจากประเทศสมาชิก ผู้แทนจากคณะกรรมาธิการยุโรปเป็นเลขาธิการ และองค์กรความปลอดภัยบนเครือข่ายและระบบข้อมูลของสหภาพยุโรป (European Union Agency for Network and Information Security หรือ ENISA) จัดตั้งขึ้นเพื่อสนับสนุนและประสานงานด้านความร่วมมือในระดับยุทธศาสตร์ และแลกเปลี่ยนข้อมูลกันระหว่างประเทศสมาชิก สร้างความเชื่อใจและความมั่นใจในการทำงานร่วมกัน ขับเคลื่อนการดำเนินงานต่าง ๆ ภายใต้ NIS Directive และมีหน้าที่รายงานผลการดำเนินงานต่อคณะกรรมาธิการยุโรปทุกหนึ่งปีครึ่งเพื่อประเมินผลของ NIS Directive ส่วนเครือข่ายความร่วมมือระหว่างองค์กร CSIRT ระดับประเทศ ประกอบด้วยผู้แทนจาก CSIRT ของประเทศสมาชิก และ CERT-c EU (Computer Emergency Response Team for the

---

[6] European Union, 'Directive on Security of Network and Information Systems 2016' <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148&from=EN> สืบค้นเมื่อ 25 มีนาคม 2565.

EU Institutions, Agencies and Bodies) ของสหภาพยุโรป สนับสนุนให้การปฏิบัติงานเป็นไปได้อย่างรวดเร็วและมีประสิทธิภาพเมื่อต้องทำงานร่วมกัน มีการรายงานผลการดำเนินงานในส่วนที่เกี่ยวข้องกับประสบการณ์ที่ได้รับจากการทำงานร่วมกัน บทสรุป และคำแนะนำต่อคณะกรรมาธิการยุโรปทุก 18 เดือน เป็นส่วนหนึ่งในการประเมินผลของ NIS Directive อีกด้วย

(3) การกำหนดข้อบังคับด้านการบริหารจัดการความเสี่ยงและการรายงานผลกรณีที่เกิดเหตุขึ้น สำหรับผู้ให้บริการในกิจการที่มีความสำคัญ (Operators of Essential Services หรือ OESs) สำหรับการดำรงอยู่ของกิจกรรมทางเศรษฐกิจและสังคมของประเทศ และผู้ให้บริการในกิจการดิจิทัล (Digital Service Providers หรือ DSPs) แต่ไม่รวมวิสาหกิจขนาดกลางและขนาดย่อมตามกฎหมาย Commission Recommendation 2003/362/EC โดยผู้ให้บริการในกิจการที่มีความสำคัญมีหน้าที่ใช้มาตรการด้านความปลอดภัยที่เหมาะสมและรายงานผลต่อองค์กรที่เกี่ยวข้องในกรณีที่มีเหตุภัยคุกคามขั้นรุนแรง ซึ่งพิจารณาระดับความรุนแรงจาก จำนวนผู้ใช้บริการที่ได้รับผลกระทบ ระยะเวลาที่เกิดเหตุ และพื้นที่ที่ได้รับผลกระทบ ส่วนผู้ให้บริการในกิจการดิจิทัลมีหน้าที่ใช้มาตรการด้านความปลอดภัยที่เหมาะสม มีลักษณะเดียวกันกับผู้ให้บริการในกิจการที่มีความสำคัญ และรายงานเหตุภัยคุกคามที่ส่งผลกระทบขั้นรุนแรงต่อองค์กรที่เกี่ยวข้อง หรือ CSIRT โดยพิจารณาความรุนแรงจากจำนวนผู้ใช้บริการที่ได้รับผลกระทบ ระยะเวลาที่เกิดเหตุ พื้นที่ที่ได้รับผลกระทบ ลักษณะการหยุดชะงักของบริการ และผลกระทบที่มีต่อภาคเศรษฐกิจและสังคมซึ่งจะมีการกำหนดให้รายงานผลต่อองค์กรที่เกี่ยวข้อง หรือ CSIRT เมื่อมีเหตุให้ไม่สามารถให้บริการได้มากกว่า 5 ล้านคนต่อชั่วโมง มีผู้ได้รับผลกระทบจากบริการที่หยุดชะงักมากกว่า 100,000 คน สร้างความเสียหายต่อความมั่นคงปลอดภัยของชีวิตและทรัพย์สินสาธารณะ หรือสร้างความเสียหายมากกว่า 1 ล้านยูโร

3.1.2.3 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ (EU Cyber Security Act 2018)

ช่วงปลายปี ค.ศ. 2018 ทีมเจรจาจากคณะมนตรีแห่งยุโรปและสภายุโรปสามารถบรรลุข้อตกลงทางการเมืองร่วมกันได้ และประกาศกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ (EU Cyber Security Act 2018)[7] ซึ่งมีผลบังคับใช้ในประเทศสมาชิก ตั้งแต่วันที่ 27 มิถุนายน 2562 เป็นก้าวแรกในการจัดให้มีระบบตรวจสอบและรับรองมาตรฐานความปลอดภัยทางไซเบอร์ (Cybersecurity Certification) สำหรับ EU (Europe-wide) ของสินค้าและบริการ ตลอดจนการประมวลผลทาง IT ต่าง ๆ ตามเกณฑ์ที่กำหนดก่อนจะสามารถจัดจำหน่ายหรือให้บริการใน EU ได้

[7] European Union, ‘EU Cyber Security Act 2018’ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881> สืบค้นเมื่อ 25 มีนาคม 2565.

อีกทั้งยังเป็นกฎหมายโดยตรงที่จะรับรองบทบาทและหน้าที่ของศูนย์ Cybersecurity Agency ของ EU หรือที่เรียกย่อ ๆ ว่า ENISA: European Agency for Network and Information Security ในการต่อต้านภัยคุกคาม ด้านความมั่นคงทางไซเบอร์และจัดสรรงบประมาณในการดำเนินการใด ๆ ของหน่วยงานดังกล่าวอีกด้วย

เห็นได้ว่า EU มีความมุ่งมั่นที่จะยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศสมาชิกให้เข้มแข็งเพื่อปฏิรูปและรับมือกับภัยไซเบอร์ที่มีแนวโน้มจะเกิดเพิ่มมากขึ้น รวมถึงส่งเสริมการรับรองมาตรฐานของความปลอดภัยสำหรับผลิตภัณฑ์โดยให้ความสำคัญกับมิติงานด้านการวางรากฐานการค้นคว้า วิจัย และ พัฒนางานด้านความปลอดภัยทางไซเบอร์ในระยะยาว นอกจากนี้ กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ฉบับนี้สอดคล้องกับความต้องการของ EU ที่ต้องเร่งเตรียมแผนการรับมือกับความท้าทายที่เกิดขึ้นใหม่อย่างฉับไวเพื่อที่จะดูแลความปลอดภัยให้กับพลเมือง EU ตลอดจนสามารถแข่งขันในเวทีโลกได้ รวมถึง การจัดตั้งกรอบ Certification Framework และการแบ่งปันข้อมูลและข่าวสารผ่านเครือข่าย Cybersecurity Competence Centre สำหรับประเทศสมาชิก ตลอดจน NIS Directive ยังเป็นกลไกที่ช่วยดำเนินการยกระดับภาคอุตสาหกรรม EU เข้าสู่ยุค Digital และปกป้องผลประโยชน์ของประเทศสมาชิกตามวิถีประชาธิปไตยของ EU

3.1.2.4 บทบาทและหน้าที่ของศูนย์ ENISA

EU ได้จัดตั้งศูนย์ ENISA ขึ้นเมื่อปี 2557 (ค.ศ. 2014) เพื่อเป็นหน่วยงานกลางในการประสานงานด้านการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์ โดยมีสำนักงานตั้งอยู่ที่ประเทศกรีซ อันมีหน้าที่สำคัญ ดังนี้

(1) พัฒนานโยบายหรือแนวทางการดำเนินงานด้านความมั่นคงทางไซเบอร์ของหน่วยงานของ EU

(2) พัฒนาหลักสูตรการฝึกอบรมแก่บุคลากรด้านการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์ทั้งจากหน่วยงานของ EU และประเทศสมาชิก และเมื่อภัยคุกคามทางไซเบอร์มีขอบเขตกว้างมากขึ้นเรื่อย ๆ ทำให้ศูนย์ ENISA เข้ามามีบทบาทมากยิ่งขึ้นในการวางหลักเกณฑ์และขั้นตอนการขอรับรองมาตรฐานความปลอดภัยทางไซเบอร์ ตลอดจนการออกใบรับรองและเผยแพร่ข้อมูลต่าง ๆ ให้ประชาชนรับรู้ผ่านทางหน้าเว็บไซต์

นอกจากนั้นศูนย์ ENISA ยังมีหน้าที่ประสานงานและติดต่อสื่อสารระหว่างหน่วยงาน EU และประเทศสมาชิกเพื่อตรวจสอบและตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยเมื่อเกิดภัยพิบัติและปฏิบัติงานในฐานะเลขานุการของ National Computer Security Incidents Response Team (CSIRT) Network ซึ่งถูกตั้งขึ้นภายใต้ NIS Directive

3.1.2.5 การรับรองมาตรฐานความปลอดภัยทางไซเบอร์ (Certification Framework)

การรับรองมาตรฐานความปลอดภัยทางไซเบอร์ (Certification Framework) นี้ มีวัตถุประสงค์เพื่อให้ผู้บริโภคมีความมั่นใจในความปลอดภัยของระบบบริการออนไลน์และอุปกรณ์ไอทีต่าง ๆ ว่ามีความน่าเชื่อถือจากการตรวจสอบความปลอดภัยที่สามารถประเมินความเสี่ยงได้อย่างเฉพาะเจาะจงเป็นรายกรณี (Tailor-made) ก่อนที่ EU จะออกใบรับรองให้

ในด้านผู้ประกอบการเองก็จะได้รับความสะดวกจากการขอรับการรับรองและตรวจประเมินเพียงครั้งเดียวว่าสินค้าและบริการ ตลอดจนการประมวลผลทางไอทีต่าง ๆ เป็นไปตามมาตรฐานแบบ/รุ่น/วัตถุประสงค์ของการใช้งานที่ผ่านการตรวจทดสอบแล้ว เอกสารนี้เป็นการประกันให้สินค้าสามารถหมุนเวียนระหว่างประเทศใน EU ได้อย่างเสรีโดยจะระบุถึงอายุของใบรับรองผลิตภัณฑ์ตามมาตรฐานไว้ด้วย ทั้งนี้ ศูนย์ ENISA จะดำเนินการออกหลักเกณฑ์ วิธีการ และเงื่อนไขการออกใบรับรองมาตรฐาน เมื่อได้รับการร้องขอจากคณะกรรมาธิการยุโรปหรือหน่วยงานของประเทศสมาชิก (European Cybersecurity Certification Group) โดยแนวทางดังกล่าวจะต้องได้รับความเห็นชอบจากคณะกรรมาธิการยุโรปเพื่อให้มีผลบังคับใช้เป็นกฎหมายต่อไป

โดยในชั้นแรก ENISA จะได้มีการนำมาตรฐานแบบสมัครใจ (Voluntary Standards) มาใช้ปฏิบัติในกรณีที่สินค้ามีความเสี่ยงต่ำ โดยจะอนุญาตให้หน่วยงานประเภทบุคคลที่สาม (Third Party) หรือผู้ผลิตรับรองตนเอง (Self-attestation) ว่าได้ดำเนินการทดสอบ การตรวจการประเมิน และให้การรับรองผลิตภัณฑ์ กระบวนการและบริการต่าง ๆ ตามมาตรฐานที่กำหนดได้ และจะพิจารณาเพื่อเตรียมออกมาตรฐานบังคับเพิ่มเติมต่อไปสำหรับสินค้าและบริการบางประเภท

เมื่อวันที่ 16 ธันวาคม 2563 สหภาพยุโรปได้เสนอแผนกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ โดยมุ่งมั่นที่จะส่งเสริมและปกป้องโลกไซเบอร์ที่เปิดกว้าง มั่นคง และปลอดภัย รวมถึงการปกป้องค่านิยมของสหภาพยุโรปและสิทธิพื้นฐาน เพื่อให้ประชาชนในสหภาพยุโรปสามารถใช้ชีวิตดิจิทัลอย่างอิสระและปลอดภัย

สหภาพยุโรปจึงเสนอให้เพิ่มมิติของความปลอดภัยทางไซเบอร์ในทุกภาคส่วนของห่วงโซ่อุปทาน รวมถึงอุปกรณ์เชื่อมต่ออินเตอร์เน็ตต่าง ๆ โดยเสนอให้มีการปรับปรุงและ/หรือออกกฎหมายใหม่ส่งเสริมการลงทุน และริเริ่มร่างนโยบายใหม่ควบคู่ไปกับการบูรณาการเครื่องมือของสหภาพยุโรปอาทิ ตลาดภายใน กฎหมาย ช่องทางการทูต และช่องทางการกลาโหม เพื่อเตรียมพร้อมในการรับมือ

กับการโจมตีออนไลน์และสร้างกลไกด้านการรักษาความปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากขึ้น โดยสรุปสาระสำคัญได้[8] ดังนี้

1) ปรับปรุงและออกกฎหมายด้านความปลอดภัยไซเบอร์ สหภาพยุโรปได้เสนอร่างกฎหมาย NIS2 ทดแทนกฎหมายฉบับปัจจุบัน (Directive (EU) 2016/1148 on security of network and information systems (NIS)) และเสนอร่างกฎหมายด้านความยืดหยุ่นทางไซเบอร์ของหน่วยงานที่จำเป็น (Directive on Cyber Resilience of Critical Entities (CER)) เพื่อยกระดับความปลอดภัยให้ครอบคลุมอุตสาหกรรมและภาคส่วนอื่น ๆ ที่ต้องการความยืดหยุ่น (นอกเหนือจากการคุ้มครองของ NIS) อาทิ ศูนย์จัดเก็บข้อมูล ห้องปฏิบัติการเพื่อการวิจัย อุตสาหกรรมการผลิตยาและอุปกรณ์การแพทย์ และการไปรษณีย์/บริการจัดส่งพัสดุ เป็นต้น โดยกฎหมายทั้งสองจะทำงานสอดคล้องกันและส่งเสริมกัน

2) เพิ่มมาตรฐานความปลอดภัยทางไซเบอร์ในอุปกรณ์เชื่อมต่อกับอินเตอร์เน็ต สหภาพยุโรปเสนอให้มีการกำหนดหลักเกณฑ์สำหรับอุปกรณ์เชื่อมต่อที่จะวางขายในตลาดยุโรป เพื่อสร้าง “Internet of Secure Things”

3) ใช้ AI ในการสร้าง “เกราะความปลอดภัยทางไซเบอร์” สหภาพยุโรปเสนอให้มีการจัดตั้งหน่วยงานด้านความปลอดภัย (Security Operations Centres) ในสหภาพยุโรปเพื่อพัฒนา European Cyber Shield หรือ เกราะความปลอดภัยทางไซเบอร์ โดยใช้เทคโนโลยี AI ในการตรวจจับสัญญาณของการโจมตีออนไลน์ตั้งแต่เนิ่น ๆ เพื่อให้สหภาพยุโรปสามารถตอบโต้ได้ทันก่อนจะเกิดความเสียหาย

4) ตั้งเป้าหมายในการจัดหาเครือข่ายโทรคมนาคมในอนาคตที่ทันสมัยกว่าเทคโนโลยี 5G สหภาพยุโรปร่วมกับ ENISA หน่วยงานด้านความปลอดภัยทางไซเบอร์ของสหภาพยุโรป ได้ออกคำแนะนำเพื่อสนับสนุนให้ประเทศสมาชิกดำเนินการตาม “EU 5G Toolbox” ซึ่งได้กำหนดแนวทางการนำเทคโนโลยี 5G และเครือข่ายโทรคมนาคมในอนาคตมาใช้อย่างปลอดภัย อาทิ แนะนำให้ประเทศสมาชิกหลีกเลี่ยงผู้ให้บริการที่มีความเสี่ยงสูงและ/หรือการพึ่งพาซัพพลายเออร์ดังกล่าว เป็นต้น และแสวงหาแนวทางการพัฒนาเทคโนโลยี 6G

5) จัดตั้งหน่วยงานไซเบอร์กลางของสหภาพยุโรปและการเสริมสร้างความรวมมือด้านไซเบอร์ สหภาพยุโรปเสนอให้มีการจัดตั้ง Joint Cyber Unit เพื่อเสริมสร้างความร่วมมือระหว่าง

---

[8] European Commission, ‘New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient’ <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> สืบค้นเมื่อ 31 มีนาคม 2565.

หน่วยงานของสหภาพยุโรปและประเทศสมาชิกในการรับมือการโจมตีออนไลน์ รวมถึงการจัดตั้งเครือข่ายองค์การประสานงานวิกฤตไซเบอร์ของสหภาพยุโรป (Cyber Crisis Liaison Organisation Network (CyCLONe)) ภายใต้ร่างกฎหมาย NIS2 เพื่อป้องกันและตอบโต้การโจมตีออนไลน์ขนาดใหญ่และวิกฤตไซเบอร์ในระดับสหภาพยุโรป อาทิ การโจมตีทางไซเบอร์ข้ามประเทศ โดยใช้สหภาพยุโรป Cyber Diplomacy Toolbox เป็นเครื่องมือในการยกระดับความร่วมมือด้านการป้องกันทางไซเบอร์ระหว่างประเทศ และจัดตั้งหน่วยงาน European Cybersecurity Competence Centre ที่จะจัดตั้งขึ้นที่โรมาเนีย และเสริมสร้างความร่วมมือกับนานาชาติ รวมถึง NATO และองค์กรระหว่างประเทศอื่น ๆ

อย่างไรก็ดี ENISA รายงานว่า[9] ตั้งแต่ช่วงปี 2019 สหภาพยุโรปตกเป็นเหยื่อของการโจมตีออนไลน์ (cyber-attack) ถี่ขึ้น โดยแต่ละการโจมตีนั้นมีความซับซ้อนและตรวจสอบได้ยากขึ้น อาทิ มัลแวร์ (malware) จากอีเมลที่สามารถผ่านการกรองของโปรแกรมรักษาความปลอดภัย และการขโมยข้อมูลทางการเงิน โดยเฉพาะในช่วงการแพร่ระบาดของเชื้อไวรัสโควิด-19 ที่หน่วยงานต่าง ๆ จำเป็นต้องพึ่งพาการทำงานออนไลน์มากขึ้น อาทิ กรณีที่โรงพยาบาลในสาธารณรัฐเช็กถูกเจาะระบบขโมยข้อมูลเมื่อเดือนมีนาคม 2564 และล่าสุดเว็บไซต์ของศาลสิทธิมนุษยชนยุโรป (European Court of Human Rights) ถูกโจมตีเมื่อวันที่ 23 ธันวาคม 2563 จึงเป็นการตอกย้ำถึงจุดอ่อนด้านความปลอดภัยทางไซเบอร์ของสหภาพยุโรป ซึ่งเป็นเรื่องเร่งด่วนที่สหภาพยุโรปต้องเพิ่มการรักษาความปลอดภัยบนโลกดิจิทัล

สหภาพยุโรปยังได้จัดสรรงบประมาณกว่า 2 พันล้านยูโรสำหรับการดำเนินงานตามแผนยุทธศาสตร์ด้านความปลอดภัยทางไซเบอร์ในช่วงปี 2021-2027 ภายใต้โครงการ Digital Europe และโครงการ Horizon Europe โดยเน้นการสนับสนุนธุรกิจ SMEs ซึ่งยังไม่รวมเงินลงทุนเพิ่มเติมจากประเทศสมาชิกและภาคเอกชน และเงินสนับสนุนจาก European Defence Fund ในส่วนของการเสริมสร้างเทคโนโลยีตอบโต้ทางไซเบอร์ ทั้งนี้ สหภาพยุโรปได้มีการจัดสรรเงินช่วยเหลือเพิ่มเติมประมาณร้อยละ 20 จากแผนฟื้นฟูเศรษฐกิจของสหภาพยุโรปให้กับห่วงโซ่อุปทานสำหรับอุตสาหกรรมเทคโนโลยีดิจิทัลอีกด้วย[10]

---

[9] European Union Agency for Cybersecurity, ‘Main incidents in the EU and worldwide’ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport> สืบค้นเมื่อ 19 สิงหาคม 2565.

[10] EURONEWS, ‘EU reveals new cybersecurity strategy with plans for a joint unit and an AI-enabled Cyber Shield’ <https://www.euronews.com/my-

3.1.2.6 Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union 2022 หรือที่เรียกกันว่า NIS2 มีผลใช้บังคับเมื่อวันที่ 16 มกราคม 2566 โดยเข้ามาแทนที่ NIS Directive (Directive (EU) 2016/1148) ฉบับเดิม[11] โดย NIS2 ได้แก้ไขปรับปรุงสถานะความปลอดภัยทางไซเบอร์ที่มีอยู่ทั่วสหภาพยุโรป ดังนี้

(1) การสร้างโครงสร้างการจัดการวิกฤตทางไซเบอร์ที่จำเป็น (CyCLONe)

(2) เพิ่มระดับของการประสานกันเกี่ยวกับข้อกำหนดด้านความปลอดภัยและภาระหน้าที่ในการรายงาน

(3) สนับสนุนให้รัฐสมาชิกแนะนำประเด็นใหม่ ๆ ที่น่าสนใจ เช่น ห่วงโซ่อุปทาน การจัดการช่องโหว่ อินเทอร์เน็ตหลัก และสุขอนามัยในโลกไซเบอร์ ยุทธศาสตร์ความปลอดภัยทางไซเบอร์ระดับชาติ

(4) นำเสนอแนวคิดใหม่ ๆ เช่น การทบทวนร่วมกันเพื่อเพิ่มความร่วมมือและการแบ่งปันความรู้ระหว่างประเทศสมาชิก

(5) ครอบคลุมสัดส่วนที่ใหญ่ขึ้นของเศรษฐกิจและสังคมโดยรวมภาคส่วนต่าง ๆ มากขึ้น ซึ่งหมายความว่า หน่วยงานที่จำเป็นต้องดำเนินมาตรการเพื่อเพิ่มระดับความปลอดภัยทางไซเบอร์ของตนจะมีจำนวนเพิ่มมากขึ้น

ENISA มีบทบาทสำคัญในการดำเนินการให้เป็นไปตาม NIS2 โดยให้ความช่วยเหลือประเทศสมาชิกในการดำเนินการปรับใช้ Directive ฉบับใหม่ นอกจากนี้ ENISA ยังมีหน้าที่อื่น ๆ เช่น ระบุแนวปฏิบัติที่ดีในประเทศสมาชิกเกี่ยวกับการปฏิบัติตามคำสั่งของ NIS สนับสนุนกระบวนการรายงานสำหรับเหตุการณ์ด้านความปลอดภัยในโลกไซเบอร์ทั่วสหภาพยุโรป พัฒนาเกณฑ์ แม่แบบ และเครื่องมือ การตกลงในแนวทางและขั้นตอนร่วมกัน ช่วยเหลือประเทศสมาชิกในการแก้ไขปัญหาความปลอดภัยทางไซเบอร์ทั่วไป ทั้งนี้ ประเทศสมาชิกมีเวลา 21 เดือนในการปรับปรุงกรอบกฎหมายของประเทศให้สอดคล้องกับ NIS2

---

europe/2020/12/16/eu-reveals-new-cybersecurity-strategy-with-plans-for-a-joint-unit-and-an-ai-enabled-cyber-> สืบค้นเมื่อ 19 สิงหาคม 2565.

[11] European Union Agency for Cybersecurity, ‘Supporting the implementation of Union policy and law regarding cybersecurity’ <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new> สืบค้นเมื่อ 19 สิงหาคม 2565.

3.1.2.7 ความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองสิทธิเสรีภาพของสหภาพยุโรป

สิทธิมนุษยชนเป็นประเด็นพื้นฐานของสหภาพยุโรป ซึ่งให้ความสำคัญอย่างยิ่งต่อการปกป้องและส่งเสริมสิทธิมนุษยชนภายในประเทศสมาชิกและประเทศอื่น ๆ สิทธิมนุษยชนในสหภาพยุโรปได้รับการคุ้มครองผ่านเครื่องมือทางกฎหมาย สถาบัน และกลไกต่าง ๆ ได้แก่

1) กฎบัตรสิทธิขั้นพื้นฐาน (Charter of Fundamental Rights) เป็นเอกสารสำคัญที่สรุปมาตรฐานสิทธิมนุษยชนภายในสหภาพยุโรป ครอบคลุมสิทธิต่าง ๆ มากมาย รวมถึงศักดิ์ศรี เสรีภาพ ความเสมอภาค ความเป็นน้ำหนึ่งใจเดียวกัน สิทธิของพลเมือง และความยุติธรรม กฎบัตรมีผลผูกพันตามกฎหมายและใช้กับประเทศสมาชิกสหภาพยุโรปทั้งหมด

2) อนุสัญญายุโรปว่าด้วยสิทธิมนุษยชน (European Convention on Human Rights: ECHR) แม้ว่า ECHR จะไม่ใช่เอกสารของสหภาพยุโรป แต่ก็มีผลกระทบอย่างมากต่อการคุ้มครองสิทธิมนุษยชนภายในสหภาพยุโรป สหภาพยุโรปมุ่งมั่นที่จะสนับสนุน ECHR และประเทศสมาชิกสหภาพยุโรปทั้งหมดเป็นภาคีในอนุสัญญา บุคคลสามารถฟ้องร้องคดีสิทธิมนุษยชนต่อศาลสิทธิมนุษยชนแห่งยุโรป European Court of Human Rights: ECtHR) ได้ หากการเยียวยาภายในประเทศหมดลงแล้ว

3) ศาลยุติธรรมแห่งยุโรป (European Court of Justice: ECJ) เป็นศาลสูงสุดของสหภาพยุโรป และมีบทบาทสำคัญในการตีความและรับรองการปฏิบัติตามกฎหมายของสหภาพยุโรป รวมถึงบทบัญญัติด้านสิทธิมนุษยชน ทำให้มั่นใจได้ว่าประเทศสมาชิกสหภาพยุโรปเคารพและปฏิบัติตามมาตรฐานสิทธิมนุษยชนที่กำหนดโดยกฎหมายของสหภาพยุโรป

4) หน่วยงานสิทธิขั้นพื้นฐาน (Fundamental Rights Agency: FRA) เป็นหน่วยงานอิสระของสหภาพยุโรปที่รับผิดชอบในการส่งเสริมและปกป้องสิทธิขั้นพื้นฐานภายในสหภาพยุโรป ให้ความเชี่ยวชาญ ข้อมูล และคำแนะนำเกี่ยวกับประเด็นด้านสิทธิมนุษยชนแก่สถาบันของสหภาพยุโรปและประเทศสมาชิก

5) รัฐสภายุโรป (European Parliament) ในฐานะองค์กรนิติบัญญัติที่ได้รับการเลือกตั้งโดยตรงของสหภาพยุโรป รัฐสภายุโรปมีบทบาทในการส่งเสริมและปกป้องสิทธิมนุษยชน ตรวจสอบสถานการณ์ด้านสิทธิมนุษยชนภายในสหภาพยุโรปและทั่วโลก และสามารถมีอิทธิพลต่อนโยบายและกฎหมายของสหภาพยุโรปในเรื่องนี้

6) นโยบายและคำสั่งของสหภาพยุโรป (EU Policies and Directives) สหภาพยุโรปพัฒนานโยบายและคำสั่งที่มีเป้าหมายเพื่อปกป้องและส่งเสริมสิทธิมนุษยชน สิ่งเหล่านี้

รวมถึงการต่อสู้กับการเลือกปฏิบัติ การส่งเสริมความเท่าเทียมทางเพศ การปกป้องความเป็นส่วนตัวและสิทธิ์ในข้อมูล และการจัดการปัญหาต่างๆ เช่น การขอลี้ภัยและการย้ายถิ่นฐาน

7) การมีส่วนร่วมของภาคประชาสังคม (Civil Society Engagement) สหภาพยุโรปสนับสนุนการมีส่วนร่วมอย่างแข็งขันขององค์กรภาคประชาสังคมและนักปกป้องสิทธิมนุษยชนในการส่งเสริมและปกป้องสิทธิมนุษยชน ภาคประชาสังคมมีบทบาทสำคัญในการติดตามสถานการณ์ด้านสิทธิมนุษยชน เรียกร้องการเปลี่ยนแปลง และสร้างความตระหนักรู้

โดยใน NIS Directive ทั้งสองฉบับ ได้ระบุถึงสิทธิมนุษยชนไว้เช่นเดียวกัน โดยใน Directive on Security of Network and Information Systems 2016 หรือ NIS Directive ฉบับแรก บัญญัติไว้ในอารัมภบท ข้อ 75 ว่า

"(75) กฎนี้เคารพในสิทธิขั้นพื้นฐานและปฏิบัติตามหลักการซึ่งเป็นที่ยอมรับโดยกฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป โดยเฉพาะอย่างยิ่งสิทธิในการเคารพชีวิตส่วนตัวและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการดำเนินธุรกิจ สิทธิในทรัพย์สิน สิทธิในการได้รับการเยียวยาที่มีประสิทธิภาพต่อหน้าศาล และสิทธิที่จะได้รับการพิจารณาคดี ซึ่งการบังคับใช้กฎนี้ควรดำเนินการสอดคล้องตามสิทธิและหลักการเหล่านั้น"[12]

และใน Directive on measures for a high common level of cybersecurity across the Union 2022 หรือ NIS2 บัญญัติไว้ในอารัมภบท ข้อ 70 ว่า

"(70) เหตุการณ์และวิกฤตการณ์ด้านความปลอดภัยทางไซเบอร์ขนาดใหญ่ในระดับสหภาพ จำเป็นต้องดำเนินการร่วมกันเพื่อให้แน่ใจว่ามีการตอบสนองที่รวดเร็วและมีประสิทธิภาพ เนื่องจากการพึ่งพาซึ่งกันและกันในระดับสูงระหว่างภาคส่วนและรัฐสมาชิก ความพร้อมใช้งานของเครือข่ายและระบบข้อมูลที่ยืดหยุ่นทางไซเบอร์ และความพร้อมใช้งาน การรักษาความลับ และความสมบูรณ์ของข้อมูล มีความสำคัญต่อการรักษาความปลอดภัยของสหภาพและสำหรับการปกป้องพลเมือง ธุรกิจ และสถาบันจากเหตุการณ์และภัยคุกคามทางไซเบอร์ ความไว้วางใจของบุคคลและองค์กรในความสามารถของสหภาพในการส่งเสริมและปกป้อง

---

[12] (75) This Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union, in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard. This Directive should be implemented in accordance with those rights and principles,

โลกไซเบอร์ที่เปิดกว้าง เสรี มั่นคง และปลอดภัย ซึ่งมีพื้นฐานมาจากสิทธิมนุษยชน เสรีภาพขั้นพื้นฐาน ประชาธิปไตย และหลักนิติธรรม”[13]

เป็นที่น่าสังเกตว่าการนำไปใช้และการตีความข้อกำหนด NIS นั้นอาจแตกต่างกันไปในแต่ละประเทศสมาชิกสหภาพยุโรป องค์กรนิติบัญญัติของรัฐและหน่วยงานกำกับดูแลมีบทบาทสำคัญในการทำให้แน่ใจว่าคำสั่ง NIS ถูกนำไปใช้ในลักษณะที่เคารพและส่งเสริมสิทธิมนุษยชน นอกจากนี้ยังมีความท้าทายอื่น ๆ เช่น ศักยภาพและความพร้อมของรัฐสมาชิกในการรับมือกับภัยคุกคามทางไซเบอร์ที่แตกต่างกัน เป็นต้น

3.1.3 องค์การสนธิสัญญาแอตแลนติกเหนือ (North Atlantic Treaty Organisation - NATO) ก่อตั้งขึ้นโดยการรวมตัวกันของประเทศต่าง ๆ 12 ประเทศ ได้แก่ สหรัฐอเมริกา สหราชอาณาจักร แคนาดา เบลเยียม เดนมาร์ก ฝรั่งเศส ไอซ์แลนด์ อิตาลี ลักเซมเบิร์ก เนเธอร์แลนด์ นอร์เวย์ และโปรตุเกส ร่วมกันลงนามในสนธิสัญญาแอตแลนติกเหนือ (The North Atlantic Treaty) ก่อตั้งองค์การสนธิสัญญาแอตแลนติกเหนือขึ้น ในช่วงหลังสงครามโลกครั้งที่สอง โดยมีผลบังคับใช้เมื่อวันที่ 24 สิงหาคม ค.ศ. 1949 โดยมีวัตถุประสงค์เพื่อจัดตั้งระบบพันธมิตรทางทหารในการถ่วงดุลอำนาจกับฝ่ายคอมมิวนิสต์ (สหภาพโซเวียต) และให้ความช่วยเหลือประเทศสมาชิกในกรณีที่ประเทศสมาชิกถูกคุกคามจากภายนอก ตลอดจนส่งเสริมความมั่นคงในทางเศรษฐกิจ โดยล่าสุด เมื่อวันที่ 4 เมษายน ค.ศ. 2023 ประเทศฟินแลนด์ ได้กลายเป็นชาติที่ 31 ที่เข้าเป็นสมาชิกใหม่ของ NATO

---

[13] (70) Large-scale cybersecurity incidents and crises at Union level require coordinated action to ensure a rapid and effective response because of the high degree of interdependence between sectors and Member States. The availability of cyber-resilient network and information systems and the availability, confidentiality and integrity of data are vital for the security of the Union and for the protection of its citizens, businesses and institutions against incidents and cyber threats, as well as for enhancing the trust of individuals and organisations in the Union’s ability to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

3.1.3.1 Tallinn Manual

NATO ได้จัดตั้งศูนย์ความเป็นเลิศนาโต้ด้านความร่วมมือในการป้องกันไซเบอร์ (NATO Cooperative Cyber Defense Centre of Excellence: NATO CCDCOE) ขึ้นที่กรุงทาลลินน์ ประเทศเอสโตเนีย โดย CCDCOE จัดทำเอกสารที่เรียกว่า “Tallinn Manual” ขึ้น

Tallinn Manual เป็นเอกสารที่กล่าวถึงการบังคับใช้กฎหมายระหว่างประเทศกับสงครามไซเบอร์ (cyber warfare) และปฏิบัติการทางไซเบอร์ (cyber operations) เผยแพร่ครั้งแรกในปี 2013 โดยกลุ่มผู้เชี่ยวชาญด้านกฎหมายที่รู้จักกันในชื่อ Tallinn Manual Project และตั้งชื่อเอกสารตามชื่อเมือง Tallinn ในเอสโตเนีย ซึ่งเป็นที่ตั้งของ CCDCOE โดย Tallinn Manual 1.0 ตีพิมพ์ครั้งแรกในปี 2013 โดยมุ่งเน้นที่กฎหมายระหว่างประเทศที่มีอยู่ เช่น กฎบัตรสหประชาชาติและกฎหมายจารีตประเพณีระหว่างประเทศ ที่บังคับใช้กับสงครามไซเบอร์และความขัดแย้งทางไซเบอร์ โดยกล่าวถึงประเด็นต่าง ๆ รวมถึงคำจำกัดความของการโจมตีทางไซเบอร์ ที่มาของปฏิบัติการทางไซเบอร์ ความชอบด้วยกฎหมายของการตอบสนองของรัฐต่อการโจมตีทางไซเบอร์ และการจำแนกประเภทของปฏิบัติการทางไซเบอร์ระหว่างการสู้รบ และ Tallinn Manual 2.0 ซึ่งตีพิมพ์ในปี 2017 ขยายความฉบับพิมพ์ครั้งแรกโดยกล่าวถึงประเด็นทางกฎหมายเพิ่มเติมที่เกี่ยวข้องกับไซเบอร์สเปซ เช่น การควบคุมกิจกรรมของรัฐในยามสงบในไซเบอร์สเปซ การจารกรรมทางไซเบอร์ และสถานะของผู้มีบทบาทที่ไม่ใช่รัฐในไซเบอร์สเปซ[14]

Tallinn Manual เป็นแนวทางสำหรับการประยุกต์ใช้กฎหมายระหว่างประเทศกับกิจกรรมทางไซเบอร์ รวมถึงประเด็นต่าง ๆ เช่น อำนาจอธิปไตย ความรับผิดชอบของรัฐ กฎหมายความขัดแย้งทางอาวุธ สิทธิมนุษยชน และกฎหมายทะเล เป็นต้น โดยมีจุดมุ่งหมายเพื่อให้ความชัดเจนและคำแนะนำแก่รัฐ ผู้ปฏิบัติงานทางทหาร ที่ปรึกษากฎหมาย และนักวิชาการเกี่ยวกับการใช้กฎหมายระหว่างประเทศในโลกไซเบอร์ ทั้งนี้ Tallinn Manual ไม่ใช่เอกสารอย่างเป็นทางการขององค์กรระหว่างประเทศหรือสนธิสัญญาที่มีผลผูกพัน อย่างไรก็ตาม ได้รับการยอมรับและอ้างอิงอย่างกว้างขวางจากรัฐบาล ผู้เชี่ยวชาญด้านกฎหมาย และผู้ปฏิบัติงานทางทหารทั่วโลก ถือเป็นแหล่งข้อมูลที่เชื่อถือได้ในด้านกฎหมายไซเบอร์และมีอิทธิพลในการสร้างการอภิปรายระหว่างประเทศเกี่ยวกับแง่มุมทางกฎหมายของการดำเนินการทางไซเบอร์ จัดทำกรอบความเข้าใจว่ากฎหมายระหว่างประเทศที่มีอยู่นำไปใช้กับไซเบอร์สเปซอย่างไร และช่วยผู้กำหนดนโยบาย ผู้ปฏิบัติงานด้านกฎหมาย และนักวิชาการในการรับมือกับความท้าทายทางกฎหมายที่ซับซ้อนที่เกิดจากกิจกรรม

[14] Eric Talbot Jensen, ‘The Tallinn Manual 2.0: Highlights and Insights’ (2017) 48 Georgetown Journal of International Law, 735, 735-737.

ทางไซเบอร์ และมีส่วนสนับสนุนการอภิปรายอย่างต่อเนื่องเกี่ยวกับการพัฒนาบรรทัดฐานและกฎระเบียบในไซเบอร์สเปซ

สำหรับประเด็นสิทธิมนุษยชน Tallinn Manual แสดงให้เห็นว่ากิจกรรมทางไซเบอร์ไม่ได้ตกอยู่ภายใต้กฎหมายระหว่างประเทศเพียงเรื่องใดเรื่องหนึ่ง แต่ยังอยู่ภายใต้กฎหมายระหว่างประเทศด้านอื่น ๆ รวมถึงกฎหมายสิทธิมนุษยชนด้วย ซึ่งตระหนักดีว่ารัฐมีหน้าที่ต้องเคารพและปกป้องสิทธิมนุษยชนในโลกไซเบอร์ เช่นเดียวกับในโลกทางกายภาพ เอกสารนี้เน้นย้ำว่าหลักการของความจำเป็น และความได้สัดส่วน จะต้องได้รับการพิจารณาเมื่อดำเนินการทางไซเบอร์ที่อาจส่งผลกระทบต่อสิทธิมนุษยชน[15] แม้ว่า Tallinn Manual จะไม่ได้ให้การวิเคราะห์เชิงลึกเกี่ยวกับกรอบกฎหมายสิทธิมนุษยชน แต่อ้างอิงถึงตราสารสิทธิมนุษยชนที่สำคัญ เช่น ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน (Universal Declaration of Human Rights: UDHR) กติการะหว่างประเทศว่าด้วยสิทธิพลเมืองและสิทธิทางการเมือง (International Covenant on Civil and Political Rights: ICCPR) และกติการะหว่างประเทศว่าด้วยสิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม (International Covenant on Economic, Social and Cultural Rights: ICESCR) ตราสารเหล่านี้คุ้มครองสิทธิมนุษยชนขั้นพื้นฐาน รวมถึงสิทธิในความเป็นส่วนตัว เสรีภาพในการแสดงออก และสิทธิที่จะเป็นอิสระจากการแทรกแซงโดยพลการต่อการติดต่อสื่อสาร ซึ่งรัฐมีภาระผูกพันในการปกป้องสิทธิเหล่านี้ในโลกไซเบอร์ และการจำกัดสิทธิเหล่านี้ต้องชอบด้วยกฎหมาย จำเป็น และได้สัดส่วน

3.1.4 สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations: ASEAN)

อาเซียนเป็นองค์การระหว่างประเทศระดับภูมิภาคที่ให้ความสำคัญและตื่นตัวกับปัญหาภัยคุกคามทางไซเบอร์เป็นอย่างมาก และมีความพยายามในการดำเนินการต่าง ๆ ด้านความมั่นคงปลอดภัยทางไซเบอร์มาเป็นระยะ โดยอาศัยความร่วมมือระหว่างประเทศสมาชิก มีกลไกความร่วมมือผ่านการประชุมในระดับรัฐมนตรี คือ การประชุมรัฐมนตรีอาเซียนว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ (AMCC) นอกจากนี้ ประเด็นความมั่นคงปลอดภัยทางไซเบอร์ยังเป็นวาระสำคัญในการประชุมรัฐมนตรีอาเซียนด้านดิจิทัล (ADGMIN) การประชุมรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (AMMTC) การประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (SOMTC) และการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (ARF) ซึ่งล้วนเน้นย้ำความสำคัญของความมั่นคงปลอดภัยทางไซเบอร์ในภูมิภาคอาเซียน ในห้วงหลายปีที่

---

[15] See Michael N. Schmitt editor, *Tallinn manual 2.0 on the international law applicable to cyber operations'*, (New York: Cambridge University Press 2016) 179-208.

ผ่านมาอาเซียนออกตราสารหลายฉบับ เพื่อตอกย้ำความมุ่งมั่นของอาเซียนที่จะร่วมมือกันในการเตรียมความพร้อมให้แก่ประเทศสมาชิกในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

3.1.4.1 ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ ปี 2017 (ASEAN Declaration to Prevent and Combat Cybercrime)

ในการประชุมสุดยอดผู้นำอาเซียน ครั้งที่ 31 ระหว่างวันที่ 13 - 14 พฤศจิกายน ค.ศ. 2017 ณ กรุงมะนิลา สาธารณรัฐฟิลิปปินส์ ผู้นำอาเซียนได้ตระหนักถึงความจำเป็นในการเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรมทางไซเบอร์ โดยมุ่งเน้นไปที่การป้องกันสังคมของภูมิภาคอาเซียน รวมถึงการริเริ่มวิธีการในระดับภูมิภาคที่มั่นคงและมีประสิทธิภาพ โดยในการประชุมสุดยอดอาเซียนในครั้งดังกล่าว ผู้นำอาเซียนทั้ง 10 ประเทศได้รับรองปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์[16] ซึ่งให้ความสำคัญกับการปรับปรุงกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์และหลักฐานทางอิเล็กทรอนิกส์ รวมทั้งสนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกัน และต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรต่าง ๆ ที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ นอกจากนี้ ยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกัน และความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ และเพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้าง และพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์อีกด้วย เป็นการแสดงเจตนารมณ์ร่วมกันระหว่างประเทศสมาชิกในการสร้างความร่วมมือระหว่างกัน ในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ในภูมิภาคอาเซียน โดยในทางกฎหมายระหว่างประเทศแล้ว การจัดทำปฏิญญาในลักษณะนี้ไม่ก่อให้เกิดพันธกรณีระหว่างประเทศที่ร่วมรับรองปฏิญญา อย่างไรก็ตาม ปฏิญญาฯ ก็ได้วางแนวปฏิบัติสำหรับประเทศสมาชิกเพื่อให้เกิดความร่วมมือในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์อย่างเป็นรูปธรรม

3.1.4.2 แถลงการณ์ร่วมของผู้นำอาเซียนว่าด้วยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ ปี 2018

การประชุมสุดยอดอาเซียน ครั้งที่ 32 (32nd ASEAN Summit) จัดขึ้นระหว่างวันที่ 25 - 28 เมษายน ค.ศ. 2018 โดยมีสาธารณรัฐสิงคโปร์เป็นประธานในการจัดการ

---

[16] ASEAN, 'ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME' <https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf> สืบค้นเมื่อ 19 สิงหาคม 2565.

ประชุม ภายใต้แนวคิด “Resilient and Innovative” ซึ่งให้ความสำคัญกับการเสริมสร้างความเข้มแข็งและส่งเสริมการใช้นวัตกรรมเพื่อขับเคลื่อนอาเซียน ในการนี้ได้มีการลงนามในวิสัยทัศน์ผู้นำอาเซียน (ASEAN Leaders Vision) เพื่อรองรับการเปลี่ยนแปลงทางภูมิรัฐศาสตร์และภูมิทัศน์ทางเศรษฐกิจ และยังคงยืนยันหลักการพื้นฐานในกฎบัตรอาเซียน (ASEAN Charter) สนธิสัญญามิตรภาพและความร่วมมือในภูมิภาคเอเชียตะวันออกเฉียงใต้ (The Treaty of Amity and Cooperation in Southeast Asia) และวิสัยทัศน์ประชาคมอาเซียน 2025 (ASEAN Community Vision 2025) และเพื่อเป็นการยกระดับความเป็นอยู่ของประชากรในอาเซียนผ่านการใช้นวัตกรรมและเทคโนโลยี จึงได้ริเริ่มแนวคิดเครือข่ายเมืองอัจฉริยะ (ASEAN Smart Cities Network) ขึ้น โดยมุ่งหวังให้เกิดการทำงานร่วมกัน การแบ่งปันแนวทางการปฏิบัติ รวมถึงการสร้างขีดความสามารถและการพัฒนาอย่างยั่งยืน สำหรับความก้าวหน้าของประชาคมการเมืองและความมั่นคง ผู้นำประเทศสมาชิกอาเซียนได้ร่วมลงนามในแถลงการณ์ว่าด้วยความร่วมมือด้านความมั่นคงทางไซเบอร์ (ASEAN Leaders Statement on Cybersecurity Cooperation)[17] โดยมีเป้าหมายเพื่อให้อาเซียนเป็นภูมิภาคที่มีความปลอดภัย ยกระดับการเชื่อมต่อและมาตรฐานการครองชีพที่ดีขึ้นในภูมิภาค เน้นย้ำถึงความตระหนักต่อภัยคุกคามทางไซเบอร์ที่เป็นปัญหาที่มีความเร่งด่วนและมีความซับซ้อนเป็นทวีคูณในปัจจุบัน ท่ามกลางการเปลี่ยนแปลงทางเศรษฐกิจที่เข้าสู่ยุคของระบบดิจิทัลทั่วอาเซียน ซึ่งประเด็นความมั่นคงปลอดภัยทางไซเบอร์ เป็นงานที่ต้องอาศัยความเชี่ยวชาญ ตลอดจนการประสานความร่วมมือกันของผู้มีส่วนได้ส่วนเสียหลายภาคส่วน เพื่อให้เกิดการจัดการอย่างมีประสิทธิภาพ

ผู้นำอาเซียนจึงได้เห็นร่วมกันที่จะส่งเสริมแนวบรรทัดฐานระหว่างประเทศแบบสมัครใจในด้านไซเบอร์ ว่าด้วยพฤติกรรมของรัฐที่มีความรับผิดชอบ อันจะเป็นเครื่องมือสำคัญในการสร้างความไว้เนื้อเชื่อใจซึ่งกันและกันระหว่างประเทศสมาชิก และยืนยันว่ากฎหมายระหว่างประเทศ โดยเฉพาะอย่างยิ่งกฎบัตรสหประชาชาติ มีผลบังคับใช้และจำเป็นต่อการรักษาสันติภาพและเสถียรภาพ รวมตลอดถึงการส่งเสริมสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสารที่เปิดกว้าง ปลอดภัย มั่นคง เข้าถึงได้ และสันติ โดยมุ่งเน้นการสร้างความร่วมมือและการประสานงานที่ใกล้ชิดมากยิ่งขึ้นระหว่างประเทศสมาชิกอาเซียน ในการพัฒนานโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์

---

[17] ASEAN, ‘ASEAN LEADERS’ STATEMENT ON CYBERSECURITY COOPERATION’ <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf> สืบค้นเมื่อ 19 สิงหาคม 2565.

นอกจากนี้ ในแถลงการณ์ดังกล่าว ประเทศสมาชิกอาเซียนยังยอมรับบรรทัดฐานพฤติกรรมของรัฐในเรื่องความรับผิดชอบบนพื้นที่ไซเบอร์ 11 ข้อ ของสหประชาชาติ[18] ซึ่งเป็นข้อเสนอแนะโดยสมัครใจและไม่มีผลผูกพัน เพื่อให้รัฐมีบรรทัดฐานในเรื่องความรับผิดชอบบนโลกไซเบอร์ และได้ผลักดันบรรทัดฐานดังกล่าวโดยดำเนินการจัดทำแผนงานระดับภูมิภาคในการแลกเปลี่ยนข้อมูลและเสริมสร้างความร่วมมือในภูมิภาค ซึ่งถือเป็นองค์การระหว่างประเทศระดับภูมิภาคองค์การแรกที่รับเอาบรรทัดฐานดังกล่าวของสหประชาชาติมาปรับใช้เป็นเครื่องมือในการสร้างความมั่นคงปลอดภัยทางไซเบอร์ในภูมิภาค[19]

อาเซียนได้จัดตั้งคณะกรรมการประสานงานอาเซียนด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อเสริมสร้างการประสานงานระดับภูมิภาคข้ามภาคส่วนด้านความมั่นคงปลอดภัยทางไซเบอร์ และอาเซียนยังร่วมมือกับประเทศอื่น เช่น การตั้งศูนย์สร้างขีดความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ อาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากร การจัดเวทีหารืออาเซียน-ญี่ปุ่นว่าด้วยอาชญากรรมไซเบอร์ ความร่วมมือในอาเซียนเป็นประตูสำคัญในการขับเคลื่อนความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสมาชิก ซึ่งต้องเริ่มจากปัจจัยแรกอย่างการผลักดันให้ประเทศสมาชิกมีกฎหมายที่ครอบคลุมและสอดคล้องกันในภูมิภาค และรัฐมีนโยบายที่ให้ความสำคัญมากเพียงพอ ปัจจัยที่สองคือการปฏิบัติ โดยบังคับใช้กฎหมายอย่างเคร่งครัด ดำเนินการตามกรอบนโยบายให้เกิดผลสัมฤทธิ์ พัฒนาเทคโนโลยีและความสามารถของบุคลากร รวมถึงสร้างความ

---

[18] ASEAN LEADERS' STATEMENT ON CYBERSECURITY COOPERATION " FURTHER TASK relevant Ministers from all ASEAN Member States to make progress on discussions by ASEAN ICT and Cybersecurity Ministers at the AMCC, TELMIN, as well as other relevant sectoral bodies such as the AMMTC, to identify a concrete list of voluntary, practical norms of State behaviour in cyberspace that ASEAN can work towards adopting and implementing, and to facilitate cross-border cooperation in addressing critical infrastructure vulnerabilities, as well as to encourage capacity-building and cooperative measures to address the criminal or terrorist use of cyberspace , taking reference from the voluntary norms recommended in 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 (UNGGE)."

[19] ZDNet, 'Asean champions regional efforts in cybersecurity, urges international participation' <https://www.zdnet.com/article/asean-champions-regional-efforts-in-cybersecurity-urges-international-participation/> สืบค้นเมื่อ 25 สิงหาคม 2565.

ตระหนักทั้งในภาครัฐ ภาคเอกชน และประชาชนปัจจัย สุดท้ายคือความร่วมมือระหว่างประเทศสมาชิกในการแลกเปลี่ยนประสบการณ์และแนวปฏิบัติและการประสานความร่วมมือทั้งในลักษณะการสนับสนุน การพัฒนา ไปจนถึงการช่วยเหลือ เพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ในอาเซียน ความร่วมมือกันด้านความมั่นคงปลอดภัยทางไซเบอร์จะเป็นพื้นฐานสำคัญของการเติบโตของเศรษฐกิจดิจิทัลในภูมิภาคนี้อย่างยั่งยืน

3.1.4.3 ยุทธศาสตร์ความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของอาเซียน (ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025))[20]

การประชุมรัฐมนตรีอาเซียนด้านดิจิทัล ครั้งที่ 2 ระหว่างวันที่ 27 - 28 มกราคม ค.ศ. 2023 จัดขึ้นภายใต้หัวข้อ การปรับเปลี่ยนไปสู่ดิจิทัลเพื่อเป็นพลังสำคัญในการฟื้นฟูเศรษฐกิจของภูมิภาคอาเซียนจากโรคโควิด – 19 (Digital Transformation: The Engine for ASEAN Economic Recovery from COVID – 19) โดยมุ่งเน้นการขับเคลื่อนภูมิภาคอาเซียนให้บรรลุวิสัยทัศน์ของประชาคมเศรษฐกิจอาเซียน และแผนแม่บทอาเซียนด้านดิจิทัล ค.ศ. 2025 รวมทั้งแนวทางการดำเนินงานของอาเซียนที่เกี่ยวข้องอย่างบูรณาการ ตลอดจนการสร้างความร่วมมือกับภาคีภายนอก และผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง เพื่อสนับสนุนการดำเนินความร่วมมือด้านดิจิทัลให้บรรลุการเป็นประชาคมชั้นนำด้านดิจิทัลและกลุ่มประเทศทางเศรษฐกิจที่ขับเคลื่อนด้วยเทคโนโลยีบริการดิจิทัล และระบบนิเวศที่มีความปลอดภัยและปรับเปลี่ยนได้ ซึ่งในที่ประชุมครั้งนี้มีการเปิดตัวยุทธศาสตร์ความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของอาเซียน ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025) ซึ่งเป็นการปรับปรุงยุทธศาสตร์ฉบับเดิม 2017 - 2020 กลยุทธ์ที่ได้รับการปรับปรุงนี้เป็นการตอบสนองต่อการพัฒนาทางไซเบอร์ที่ใหม่กว่าตั้งแต่ปี 2560 และต่อยอดจากกลยุทธ์ก่อนหน้าเพื่อให้แน่ใจว่าไม่มีการเชื่อมโยงที่อ่อนแอในความพยายามร่วมกันในการรักษาความปลอดภัยพื้นที่ไซเบอร์สำหรับเศรษฐกิจดิจิทัลของภูมิภาคและชุมชนที่จะเติบโต

---

[20] ASEAN, ‘ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025)’ <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf> สืบค้นเมื่อ 25 สิงหาคม 2565.

3.1.4.4 แถลงการณ์ของประธานการประชุมสุดยอดอาเซียน ครั้งที่ 42 (CHAIRMAN'S STATEMENT OF THE 42ND ASEAN SUMMIT 2023)[21]

ในการประชุมสุดยอดอาเซียน ครั้งที่ 42 และการประชุมที่เกี่ยวข้อง ณ เมืองลาบวน บาโจ อินโดนีเซีย ระหว่างวันที่ 9 - 11 พฤษภาคม ค.ศ. 2023 ประธานอาเซียนแถลงยินดีต่อความคืบหน้าในการดำเนินการตามยุทธศาสตร์ความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียนระหว่างปี 2021 - 2025 และข้อเสนอ ASEAN CERT ระดับภูมิภาคของอาเซียน ซึ่งอาเซียนตระหนักถึงบทบาทอย่างต่อเนื่องของกิจกรรมการรับรู้ด้านความปลอดภัยในโลกไซเบอร์ และโครงการเสริมสร้างศักยภาพของศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ (ASCCE) และศูนย์เสริมสร้างศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-ญี่ปุ่น (AJCCBC) ในการส่งเสริมความพยายามของอาเซียนที่มีอยู่ในการสร้างบทบาทด้านความปลอดภัยทางไซเบอร์ระดับภูมิภาค

สรุปได้ว่าในปัจจุบันยังไม่มีสนธิสัญญาหลักในระดับพหุภาคีที่มีค่าบังคับทางกฎหมายเพื่อใช้กับประเด็นความมั่นคงปลอดภัยทางไซเบอร์โดยตรง[22] ซึ่งเมื่อมีความตระหนักถึงความต้องการมาตรการทางกฎหมายระหว่างประเทศสำหรับความมั่งคงปลอดภัยในโลกไซเบอร์ อาจนำไปสู่ผลลัพธ์ที่แตกต่างกัน 3 ประการ ประการแรก การปฏิบัติของรัฐอาจพัฒนาไปในลักษณะที่ "แทรก" สิทธิมนุษยชนที่มีอยู่เข้ากับความปลอดภัยในโลกไซเบอร์ กล่าวอีกนัยหนึ่งคือวิธีการตีความกฎหมายที่มีอยู่ ประการที่สอง รัฐอาจตัดสินใจทำข้อตกลงทวิภาคีหรือพหุภาคีที่กำหนดกฎและหลักการที่ควบคุมกิจกรรมข้ามพรมแดนซึ่งได้รับการสนับสนุนโดยรัฐในพื้นที่ไซเบอร์ วิธีการดังกล่าวน่าจะมุ่งเน้นไปที่สิทธิและหน้าที่ของรัฐมากกว่าตัวบุคคล ประการที่สาม รัฐต่าง ๆ อาจตระหนักว่าจำเป็นต้องมีการแก้ไขกฎหมายสิทธิมนุษยชนระหว่างประเทศที่มีอยู่ และควรเพิ่มสิทธิมนุษยชนเข้าไปในประเด็นความมั่นคงปลอดภัยทางไซเบอร์ นอกเหนือจากสิทธิมนุษยชนที่มีอยู่ในสนธิสัญญาและกฎหมายจารีตประเพณีระหว่างประเทศต่าง ๆ[23]

---

[21] ASEAN, 'CHAIRMAN'S STATEMENT OF THE 42ND ASEAN SUMMIT LABUAN BAJO, INDONESIA, 10-11 MAY 2023' <https://asean.org/wp-content/uploads/2023/05/FINAL-Chairmans-Statement-42nd-ASEAN-Summit-1.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

[22] Matthias C. Kettemann, 'Ensuring Cybersecurity through International Law' (2017) 69 Revista Espanola de Derecho Internacional 281, 285.

[23] Ido Kilovaty, 'An Extraterritorial Human Rights to Cybersecurity' (2020) 10 Notre Dame Journal of International & Comparative Law 35, 54.

3.2 กฎหมายต่างประเทศว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์

ในส่วนนี้เป็นการศึกษากฎหมายของต่างประเทศว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ ประเทศสหรัฐอเมริกา ประเทศจีน และประเทศสิงคโปร์ โดยประเทศสหรัฐอเมริกาและประเทศจีน เป็นประเทศที่มีบทบาทสำคัญในระบบเศรษฐกิจของโลกในปัจจุบัน และในส่วนของประเทศสิงคโปร์นั้น เป็นประเทศที่มีความก้าวหน้าในการบุกเบิกและพัฒนาเทคโนโลยี และอยู่ในภูมิภาคเอเชียตะวันออกเฉียงใต้เช่นเดียวกับประเทศไทย เพื่อมองหาแนวคิดที่แตกต่างกันในการสร้างและใช้กฎหมายของแต่ละประเทศ

ทั้งนี้ จะทำการศึกษากฎหมายของทั้ง 3 ประเทศในประเด็น ดังต่อไปนี้

1. โครงสร้างของกฎหมาย
2. สาระสำคัญของกฎหมาย
   2.1 วัตถุประสงค์ของกฎหมาย
   2.2 หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย
   2.3 มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์
3. มิติด้านสิทธิมนุษยชนในกฎหมาย

3.2.1 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา

สหรัฐอเมริกามีระบอบการปกครองในแบบสหพันธรัฐ (Federal Republic) ประกอบด้วย 50 รัฐ และ 1 เขตปกครองพิเศษ การปกครองแบ่งเป็นระดับรัฐบาลกลางและระดับมลรัฐ ดังนั้น กฎหมายที่ตราขึ้นโดยฝ่ายนิติบัญญัติจึงมีสองระดับเช่นเดียวกัน คือ กฎหมายของรัฐบาลกลาง ซึ่งควบคุมกิจการระหว่างมลรัฐ และเรื่องที่เกี่ยวกับการต่างประเทศ ในขณะที่กฎหมายมลรัฐควบคุมกิจกรรมที่ดำเนินการภายในมลรัฐ ซึ่งการศึกษากฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสหรัฐอเมริกาจึงศึกษาเฉพาะกฎหมายระดับรัฐบาลกลาง ซึ่งมีผลผูกพันกับทุกมลรัฐในประเทศสหรัฐอเมริกา

3.2.1.1 โครงสร้างของกฎหมาย

กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2015 (Cybersecurity Act of 2015: CSA)[24] ประกาศเป็นกฎหมายเมื่อวันที่ 18 ธันวาคม 2015 ในสมัยประธานาธิบดี บารัค โอบามา ประกอบด้วย 4 หมวด (Title) ได้แก่

หมวดที่ 1 การแบ่งปันข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ (TITLE I—CYBERSECURITY INFORMATION SHARING ACT of 2015: CISA) Sec. 101 – 111

หมวดที่ 2 การเพิ่มศักยภาพในการป้องกันความมั่นคงปลอดภัยทางไซเบอร์ของรัฐบาลกลาง (TITLE II—NATIONAL CYBERSECURITY ADVANCEMENT ACT of 2015)

หมวดย่อย A ศูนย์บูรณาการความปลอดภัยทางไซเบอร์และการสื่อสารแห่งชาติ (Subtitle A—National Cybersecurity and Communications Integration Center) Sec. 201 - 211

หมวดย่อย B การปรับปรุงความปลอดภัยทางไซเบอร์ของรัฐบาลกลาง (Subtitle B—Federal Cybersecurity Enhancement) Sec. 221 - 229

หมวดที่ 3 การประเมินทีมปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ของรัฐบาลกลาง (TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT ACT of 2015) Sec. 301 - 305

หมวดที่ 4 บททั่วไปอื่น ๆ ที่เกี่ยวข้องกับประเด็นทางไซเบอร์ (TITLE IV—OTHER CYBER MATTERS) Sec. 401 - 407

กฎหมายฉบับนี้เป็นการนำเอากฎหมายต่าง ๆ ที่เกี่ยวข้องกับประเด็นความมั่นคงปลอดภัยทางไซเบอร์เข้ามารวมไว้ด้วยกันเป็นฉบับเดียวในทำนองเดียวกับประมวลกฎหมาย เพื่อให้การใช้บังคับกฎหมายมีความสอดคล้องและบูรณาการเข้าด้วยกัน โดยส่วนสำคัญที่สุดของกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2015 ฉบับนี้ คือส่วนของหมวดที่ 1 การแบ่งปันข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ โดยบทอื่น ๆ เป็นส่วนสนับสนุนการดำเนินการที่เกี่ยวข้อง

3.2.1.2 สาระสำคัญของกฎหมาย

(1) วัตถุประสงค์ของกฎหมาย เป็นการสร้างระบบสมัครใจสำหรับการแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์และมาตรการป้องกัน เพื่อร่วมมือกันสร้างความปลอดภัย

---

[24] US Senate, 'CYBERSECURITY ACT OF 2015' <https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

ทางไซเบอร์ระหว่างรัฐบาลกลางและหน่วยงานที่มิใช่รัฐบาลกลาง โดยมีสององค์ประกอบหลัก ประการแรก อนุญาตให้บริษัทตรวจสอบและใช้มาตรการป้องกันบนระบบข้อมูลของตนเองเพื่อตอบโต้ภัยคุกคามทางไซเบอร์ ประการที่สอง CISA ให้ความคุ้มครองบางประการเพื่อส่งเสริมให้บริษัทต่าง ๆ สมัครใจที่จะแบ่งปันข้อมูล โดยเฉพาะข้อมูลเกี่ยวกับ “ตัวบ่งชี้ภัยคุกคามทางไซเบอร์” และ “มาตรการป้องกัน” กับรัฐบาลกลาง หน่วยงานของรัฐและท้องถิ่น ตลอดจนบริษัทและหน่วยงานเอกชนอื่น ๆ การคุ้มครองเหล่านี้รวมถึงการคุ้มครองจากความรับผิด และการคุ้มครองจากการเปิดเผยข้อมูลที่สำคัญ และเพื่อให้มีคุณสมบัติในการคุ้มครองเหล่านี้ การแบ่งปันข้อมูลต้องเป็นไปตามข้อกำหนดของ CISA รวมถึงการลบข้อมูลส่วนบุคคล

(2) หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย ได้แก่ กระทรวงความมั่นคงแห่งมาตุภูมิ (Department of Homeland Security: DHS) โดยร่วมกับกระทรวงกลาโหม (Department of Defense) สำนักงานข่าวกรองแห่งชาติ (National Intelligence) และสำนักงานอัยการสูงสุด (Office of Secretary General) ในการพัฒนาและออกระเบียบปฏิบัติเพื่ออำนวยความสะดวกและสงเสริมการแบ่งปันตัวบ่งชี้ภัยคุกคามทางไซเบอร์อย่างทันท่วงที และมาตรการป้องกันในความครอบครอบของรัฐบาลกลาง กับตัวแทนของหน่วยงานรัฐที่เกี่ยวข้อง รวมถึงหน่วยงานที่มิใช่ของรัฐที่มีความปลอดภัยที่เหมาะสม นอกจากนั้น กฎหมายฉบับนี้ยังกำหนดให้ศูนย์บูรณาการความปลอดภัยทางไซเบอร์และการสื่อสารแห่งชาติ (National Cybersecurity & Communications Integration Center: NCCIC) ซึ่งอยู่ภายใต้กระทรวงความมั่นคงแห่งมาตุภูมิ ทำหน้าที่อำนวยความสะดวกในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ ประเมินและตอบสนองต่อความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ และตัวบ่งชี้ภัยคุกคาม โดยกฎหมายยังให้อำนาจประธานาธิบดีในการโอนอำนาจและความรับผิดชอบในการรวบรวมและเผยแพร่ข้อมูลภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ให้แก่หน่วยงานอื่นนอกเหนือจาก NCCIC รวมถึงหน่วยงานภายนอก DHS

(3) มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์

3.1 ตรวจสอบและปกป้องระบบสารสนเทศ (Monitor and Defend Information Systems) ภายใต้ข้อกำหนดบางประการ บริษัทได้รับอนุญาตให้ตรวจสอบและดำเนินมาตรการป้องกันในระบบข้อมูลของบริษัทเอง หรือระบบของบุคคลอื่นเมื่อได้รับอนุญาตเป็นลายลักษณ์อักษร เพื่อวัตถุประสงค์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (มาตรา 104(a)(1)(A)-(C), (b)(1)(A)-(C))[25]

---

[25] SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

3.2 การคุ้มครองจากความรับผิด กล่าวคือเมื่อองค์กรหรือบริษัทต่าง ๆ ได้ดำเนินการตรวจสอบและปกป้องระบบสารสนเทศ ตามที่บัญญัติไว้ใน มาตรา 104 และเป็นไปตามมาตรฐานที่ CISA กำหนดไว้ จะไม่มีความรับผิดและไม่ถูกดำเนินคดี (มาตรา 106(a))[26]

---

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

[26] SEC. 106. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information under section 104(a) that is conducted in accordance with this title.

3.3 แบ่งปันหรือรับข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์หรือมาตรการป้องกันภายใต้ข้อกำหนดบางประการ บริษัทได้รับอนุญาตให้แบ่งปันหรือได้รับข้อมูลจากรัฐบาลกลาง มลรัฐ และรัฐบาลท้องถิ่น รวมถึงบริษัทและหน่วยงานเอกชนอื่น ๆ เกี่ยวกับตัวบ่งชี้ภัยคุกคามทางไซเบอร์และมาตรการป้องกัน สำหรับวัตถุประสงค์ด้านความปลอดภัยทางไซเบอร์ (มาตรา 104(c)(1))[27] โดยกฎหมายได้ให้นิยามคำสำคัญไว้ดังนี้

ตัวบ่งชี้ภัยคุกคามทางไซเบอร์ (Cyber Threat Indicator) หมายถึง ข้อมูลที่จำเป็นในการอธิบายหรือระบุภัยคุกคามต่าง ๆ รวมถึงการสอดแนมที่เป็นอันตราย และวิธีการใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัย หรือทำให้ผู้ใช้โดยชอบด้วยกฎหมายเปิดใช้งานการแสวงหาประโยชน์ดังกล่าวโดยไม่เจตนา รวมถึงข้อมูลเกี่ยวกับอันตรายที่เกิดขึ้นจริงหรืออาจเกิดขึ้นจากเหตุการณ์

มาตรการป้องกัน (Defensive Measure) หมายถึง สิ่งที่ใช้กับระบบข้อมูล หรือกับข้อมูลในระบบนั้น ๆ เพื่อตรวจจับ ป้องกัน หรือบรรเทาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์หรือช่องโหว่ด้านความปลอดภัยที่ทราบหรือสงสัยว่ามีอยู่ แต่ทั้งนี้ไม่รวมถึงมาตรการทำลาย ทำให้ใช้งานไม่ได้ ให้การเข้าถึงโดยไม่ได้รับอนุญาต หรือทำอันตรายต่อระบบข้อมูลของบุคคลที่สามอย่างร้ายแรง

วัตถุประสงค์ด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Purpose) หมายถึง วัตถุประสงค์ในการปกป้องระบบข้อมูลหรือข้อมูลจากภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ หรือช่องโหว่ด้านความปลอดภัย

การแบ่งปันข้อมูลเป็นหัวใจสำคัญของกฎหมายฉบับนี้ ซึ่งเน้นระบบสมัครใจ ไม่ได้กำหนดให้เป็นหน้าที่ ซึ่งจำเป็นต้องทำความเข้าใจกับเอกชนถึงความสำคัญในการร่วมมือซึ่งกันและกันให้เกิดการแบ่งปันข้อมูลที่มีความทันท่วงที และมีการประมวลผลเพื่อใช้แก้ไขปัญหาได้อย่างแม่นยำ ซึ่งข้อมูลที่แบ่งปันภายใต้ CISA ได้รับการยกเว้นจากการเปิดเผยภายใต้ Freedom of

---

[27] (c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, a non-Federal entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-Federal entity or the Federal Government a cyber threat indicator or defensive measure.

Information Act (5 U.S.C. 552) รวมถึงภายใต้บทบัญญัติของรัฐหรือท้องถิ่นที่กำหนดให้เปิดเผยข้อมูลหรือบันทึกอีกด้วย

3.2.1.3 มิติด้านสิทธิมนุษยชนในกฎหมาย

กฎหมายฉบับนี้ได้กำหนดไว้ว่า รัฐบาลอาจใช้ข้อมูลที่แบ่งปันเพื่อวัตถุประสงค์เหล่านี้เท่านั้น อันได้แก่ เพื่อระบุวัตถุประสงค์ด้านความปลอดภัยในโลกไซเบอร์ ระบุแหล่งที่มาของภัยคุกคามความปลอดภัยทางไซเบอร์หรือช่องโหว่ด้านความปลอดภัย ระบุภัยคุกคามความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับการใช้ระบบข้อมูลโดยศัตรูต่างชาติหรือผู้ก่อการร้าย ป้องกันหรือบรรเทาภัยคุกคามที่จวนเจียนจะถึงแก่ชีวิต การทำร้ายร่างกายอย่างร้ายแรง หรือความเสียหายทางเศรษฐกิจอย่างร้ายแรง รวมถึงการกระทำของผู้ก่อการร้ายหรือการใช้อาวุธที่มีอานุภาพทำลายล้างสูง ป้องกันหรือบรรเทาภัยคุกคามร้ายแรงต่อผู้เยาว์ รวมถึงการแสวงประโยชน์ทางเพศและการคุกคามต่อความปลอดภัยทางร่างกาย ป้องกัน ตรวจสอบ ขัดขวาง หรือดำเนินคดีกับความผิดที่เกิดขึ้นจากภัยคุกคาม เช่น อาชญากรที่มีความร้ายแรง หรือที่เกี่ยวข้องกับการฉ้อโกงและการโจรกรรมข้อมูลส่วนตัว

นอกจากนี้ยังมีการบัญญัติเพื่อคุ้มครองความเป็นส่วนตัว (Privacy Protection) โดยกฎหมายมาตรา 104(d)(2)[28] กำหนดให้หน่วยงานเอกชนระบุและลบข้อมูลส่วน

---

[28] (d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—A non-Federal entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—A non-Federal entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information

that identifies a specific individual and remove such information; or

(B) implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the non-Federal

บุคคลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ก่อนที่จะแบ่งปันข้อมูลภายใต้กฎหมาย และมาตรา 103(b)(1)(E) กำหนดให้มีการพัฒนาขั้นตอนเพื่อระบุและลบข้อมูลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ที่หน่วยงานของรัฐบาลกลางทราบในขณะที่แบ่งปันว่าเป็นข้อมูลส่วนบุคคลของบุคคลหรือข้อมูลที่เฉพาะเจาะจง นอกจากนี้ยังต้องมีขั้นตอนในการแจ้งบุคคลซึ่งทราบข้อมูลส่วนตัว หรือพิจารณาแล้วว่าถูกแบ่งปันโดยละเมิดกฎหมาย ดังนั้น กฎหมายนี้จึงสร้างกระบวนการตรวจสอบสองครั้งและการแจ้งเตือนเพื่อป้องกันการเปิดเผยข้อมูลส่วนบุคคลที่ไม่สำคัญต่อวัตถุประสงค์ด้านความปลอดภัยในโลกไซเบอร์ รวมถึงยังได้กำหนดกลไกการกำกับดูแลอีกหลายอย่าง และภายในสามปีจะต้องมีการจัดทำรายงานเสนอต่อสภาคองเกรสโดยประกอบด้วยข้อมูลเกี่ยวกับการประเมินความเพียงพอของนโยบาย ขั้นตอน และแนวปฏิบัติ ที่เกี่ยวข้องกับความเป็นส่วนตัวและเสรีภาพ

แต่ยังคงมีข้อกังวลหลักประการหนึ่งที่ผู้วิพากษ์วิจารณ์ต่างหยิบยกขึ้นมาคือผลกระทบที่อาจเกิดขึ้นกับสิทธิความเป็นส่วนตัว เนื่องจาก CISA รวมถึงบทบัญญัติที่อนุญาตให้มีการแบ่งปันตัวบ่งชี้ภัยคุกคามทางไซเบอร์และมาตรการป้องกันระหว่างหน่วยงานเอกชนและหน่วยงานของรัฐ โดยหลักแล้วเพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม การแบ่งปันข้อมูลนี้อาจส่งผลต่อสิทธิความเป็นส่วนตัวของแต่ละบุคคล เนื่องจากข้อมูลส่วนบุคคลอาจถูกรวบรวมและแบ่งปันโดยไม่ได้รับความยินยอมอย่างชัดแจ้งหรือการป้องกันที่เพียงพอ และกฎหมายดังกล่าวยังให้ความคุ้มครองความรับผิดบางประการแก่หน่วยงานเอกชนที่แบ่งปันข้อมูลความปลอดภัยทางไซเบอร์โดยสุจริต โดยตั้งใจที่จะสนับสนุนให้มีการแบ่งปันข้อมูล อย่างไรก็ดี การคุ้มครองความรับผิดส่วนนี้ถูกวิพากษ์วิจารณ์ว่ากว้างขวางเกินไป ซึ่งอาจเป็นการคุ้มกันให้กับหน่วยงานที่จัดการหรือใช้ข้อมูลที่แบ่งปันในทางที่ผิด ซึ่งอาจละเมิดสิทธิของบุคคล จึงจำเป็นอย่างยิ่งที่จะต้องสร้างความสมดุลระหว่างการรับรองความปลอดภัยทางไซเบอร์และการปกป้องสิทธิและเสรีภาพขั้นพื้นฐานของแต่ละบุคคล

---

entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

3.2.2 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของจีน

กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีนถูกวิพากษ์วิจารณ์อย่างกว้างขวางจากหลายประเทศทั่วโลก ในเรื่องการใช้มาตรการที่อาจละเมิดสิทธิมนุษยชนในการควบคุมการใช้อินเทอร์เน็ต การเข้าถึงและเก็บรวบรวมข้อมูลของประชาชน และเอกชน โดยการให้อำนาจรัฐในการควบคุม กำกับดูแล การไหลเวียนของข้อมูลข่าวสารและเพิ่มมาตรการตรวจสอบเทคโนโลยีต่าง ๆ ที่มาจากต่างประเทศ

3.2.2.1 โครงสร้างของกฎหมาย

กฎหมายด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2017 (中华人民共和国网络安全法- Cybersecurity Law of the People's Republic of China)[29] ผ่านการพิจารณาจากสภาประชาชนแห่งชาติเมื่อวันที่ 7 พฤศจิกายน 2016 และมีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2017 ประกอบด้วย 7 หมวด (Chapter) 79 มาตรา[30] ได้แก่

หมวดที่ 1 บทบัญญัติทั่วไป (Chapter I: General Provisions) มาตรา 1 – 14

หมวดที่ 2 การสนับสนุนและส่งเสริมความปลอดภัยทางไซเบอร์ (Chapter II: Support and Promotion of Cybersecurity) มาตรา 15 – 20

หมวดที่ 3 ความปลอดภัยของการดำเนินงานเครือข่าย (Chapter III: Network Operations Security) แบ่งเป็น 2 บทย่อย

บทที่ 1 บทบัญญัติทั่วไป (Section 1: General Provisions) มาตรา 21 – 30

บทที่ 2 การรักษาความปลอดภัยการดำเนินงานสำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Section 2: Operations Security for Critical Information Infrastructure) มาตรา 31 – 39

---

[29] The State Council of the People's Republic of China, '中华人民共和国网络安全法' <https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm> สืบค้นเมื่อ 25 มีนาคม 2566.

[30] Rogier Creemers, Graham Webster, and Paul Triolo, 'Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)' Stanford University <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> accessed on 25 March 2023.

หมวดที่ 4 ความปลอดภัยของข้อมูลเครือข่าย (Chapter IV: Network Information Security) มาตรา 40 – 50

หมวดที่ 5 การตรวจสอบ การเตือนล่วงหน้า และการตอบสนองเหตุฉุกเฉิน (Chapter V: Monitoring, Early Warning, and Emergency Response) มาตรา 51 – 58

หมวดที่ 6 ความรับผิดชอบทางกฎหมาย (Chapter VI: Legal Responsibility) มาตรา 59 – 75

หมวดที่ 7 บทบัญญัติเพิ่มเติม (Chapter VII: Supplementary Provisions) มาตรา 76 - 79

3.2.2.2 สาระสำคัญของกฎหมาย

(1) วัตถุประสงค์ของกฎหมาย บัญญัติไว้ในหมวดที่ 1 บทบัญญัติทั่วไป โดยกฎหมายฉบับนี้ตราขึ้นเพื่อรับรองความปลอดภัยทางไซเบอร์ ปกป้องอธิปไตยในโลกไซเบอร์และความมั่นคงของชาติ และผลประโยชน์ทางสังคมและสาธารณะ ปกป้องสิทธิและผลประโยชน์โดยชอบด้วยกฎหมายของพลเมือง นิติบุคคล และองค์กรอื่น ๆ และส่งเสริมการพัฒนาสุขภาพของข้อมูลข่าวสารของเศรษฐกิจและสังคม[31] โดยบังคับใช้กับการสร้าง การดำเนินการ การบำรุงรักษา และการใช้เครือข่าย ตลอดจนการกำกับดูแลและการจัดการความมั่นคงปลอดภัยทางไซเบอร์ภายในดินแดนแผ่นดินใหญ่ของสาธารณรัฐประชาชนจีน[32] นอกจากนี้ยังบัญญัติว่ารัฐยังคงให้ความสำคัญกับความปลอดภัยทางไซเบอร์และการพัฒนาข้อมูลอย่างเท่าเทียมกัน และปฏิบัติตามหลักการของการใช้งานเชิงรุก การพัฒนาทางวิทยาศาสตร์ การจัดการตามกฎหมาย และการรับประกันความปลอดภัย[33] รัฐ

---

[31] Article 1: This Law is formulated in order to: ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the information of the economy and society.

[32] Article 2: This Law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China.

[33] Article 3: The State persists in equally stressing cybersecurity and information development, and abides by the principles of active use, scientific development, management in accordance with law, and ensuring security. The State advances the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technology, supports the cultivation of qualified

เดินหน้าสร้างโครงสร้างพื้นฐานเครือข่ายและการเชื่อมต่อระหว่างกัน ส่งเสริมนวัตกรรมและการประยุกต์ใช้เทคโนโลยีเครือข่าย สนับสนุนการพัฒนาบุคลากรด้านความปลอดภัยทางไซเบอร์ที่มีคุณภาพ สร้างระบบที่สมบูรณ์เพื่อป้องกันความปลอดภัยทางไซเบอร์ และเพิ่มขีดความสามารถในการปกป้องความปลอดภัยทางไซเบอร์[34] ใช้มาตรการในการติดตาม ป้องกัน และจัดการกับความเสี่ยงและภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นทั้งภายในและนอกอาณาเขตแผ่นดินใหญ่ของสาธารณรัฐประชาชนจีน ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศจากการถูกโจมตี การบุกรุก การแทรกแซง และการทำลายล้าง ลงโทษกิจกรรมทางไซเบอร์ที่ผิดกฎหมายและเป็นอาชญากรรมตามกฎหมาย รักษาความปลอดภัยและความสงบเรียบร้อยของโลกไซเบอร์[35] รวมถึงสนับสนุนพฤติกรรมออนไลน์ที่จริงใจ ซื่อสัตย์ ดีต่อสุขภาพและมีอารยธรรม ส่งเสริมการเผยแพร่ค่านิยมหลักของสังคมนิยม ใช้มาตรการเพื่อยกระดับการรับรู้และระดับความปลอดภัยทางไซเบอร์ของทั้งสังคมและกำหนดสภาพแวดล้อมที่ดีสำหรับทั้งสังคมในการมีส่วนร่วมในการพัฒนาความปลอดภัยทางไซเบอร์[36]

(2) หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2017 ได้กำหนดอำนาจหน้าที่ของ “สำนักงานบริหารไซเบอร์

---

cybersecurity personnel, establishes a complete system to safeguard cybersecurity, and raises capacity to protect cybersecurity.

[34] Article 4: The State formulates and continuously improves cybersecurity strategy, clarifies the fundamental requirements and primary goals of ensuring cybersecurity, and puts forward cybersecurity policies, work tasks, and procedures for key sectors.

[35] Article 5: The State takes measures for monitoring, preventing, and handling cybersecurity risks and threats arising both within and without the mainland territory of the People’s Republic of China. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction; the State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace.

[36] Article 6: The State advocates sincere, honest, healthy and civilized online conduct; it promotes the dissemination of core socialist values, adopts measures to raise the entire society’s awareness and level of cybersecurity, and formulates a good environment for the entire society to jointly participate in advancing cybersecurity.

สเปซของจีน” (Cyberspace Administration of China - 国家网信部门)[37] เรียกโดยย่อว่า CAC รวมถึงสำนักงานสาขา ในการวางแผนและประสานงานการรักษาความปลอดภัยทางไซเบอร์และประเด็นที่เกี่ยวข้องอย่างครอบคลุม กำกับดูแลและบริหารจัดการกับหน่วยงานหลายแห่งที่มีเขตอำนาจทับซ้อนกันหรือเสริมกัน รวมถึงทำหน้าที่ประสานงานโดยรวมเกี่ยวกับความปลอดภัยของข้อมูลออนไลน์และกฎระเบียบที่เกี่ยวข้อง และให้อำนาจควบคุมการส่งออกข้อมูลสำคัญร่วมกับหน่วยงานรัฐที่เกี่ยวข้อง นอกจากนั้น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของจีนปี 2021 (Personal Information Protection Law 2021: PIPL) ยังได้ให้อำนาจ CAC สำหรับการวางแผน การประสานงาน และการกำกับดูแลงานคุ้มครองข้อมูลส่วนบุคคลอย่างครอบคลุมอีกด้วย นอกเหนือจาก CAC แล้ว ยังมีหน่วยงานรัฐอื่น ๆ ที่มีหน้าที่ในการร่วมดำเนินการเพื่อบังคับใช้กฎหมายฉบับนี้ด้วย ได้แก่ กระทรวงความมั่นคงสาธารณะ (Ministry of Public Security: MPS) และสำนักงานความมั่นคงสาธารณะในพื้นที่ กระทรวงอุตสาหกรรมและเทคโนโลยีสารสนเทศ (Ministry of Industry and Information Technologies: MIIT)) และสำนักงานโทรคมนาคมในพื้นที่ รวมทั้งหน่วยงานกำกับดูแลอื่น ๆ เช่น กระทรวงวิทยาศาสตร์และเทคโนโลยี (Ministry of Science and Technology: MOST) หน่วยงานบริหารพลังงานแห่งชาติ (National Energy Administration: NEA) และคณะกรรมการกำกับดูแลการธนาคารและการประกันภัยของจีน (China Banking and Insurance Regulatory Commission: CBIRC)

(3) มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์ ในขณะที่กฎหมายมีผลบังคับใช้แล้ว แต่ยังมีบทบัญญัติอีกหลายส่วนที่เว้นช่องให้ CAC สามารถเพิ่มเติมบทบัญญัติเองได้ ทำให้เกิดความคลุมเครือและปล่อยให้รายละเอียดของกฎหมายรวมถึงการนำมาใช้อยู่ในดุลยพินิจของ CAC สำหรับรูปแบบการรักษาความปลอดภัยทางไซเบอร์ของกฎหมายฉบับนี้ ใช้ระบบการคุ้มครองหลายลำดับชั้น (Multi-Level Protection Scheme: MLPS)[38] ซึ่งเป็นระบบการจำแนกเครือข่ายทั้งหมดในประเทศจีน ยกเว้นเครือข่ายสำหรับใช้ส่วนบุคคลและครัวเรือน และข้อกำหนดสำหรับการป้องกันและกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์แบบ MLPS จะไม่

---

[37] Jamie P. Horsley, ‘Behind the Facade of China’s Cyber Super-Regulator’ <https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/> สืบค้นเมื่อ 25 มีนาคม 2566.

[38] Government of Canada, ‘China’s cybersecurity regime’ <https://www.tradecommissioner.gc.ca/china-chine/cyber-security_cyber-securite_china-chine.aspx?lang=eng> สืบค้นเมื่อ 25 มีนาคม 2566.

ใช้กับเครือข่ายที่มีเซิร์ฟเวอร์อยู่นอกประเทศจีน โดย MLPS แบ่งประเภทเครือข่ายตามระดับของอันตรายที่ระบบสามารถก่อให้เกิดได้หากถูกบุกรุกหรือถูกทำให้เสียหาย มี 5 ระดับ ดังนี้[39]

ระดับ	ประเภทของเครือข่าย	วัตถุที่ตกอยู่ในอันตรายเมื่อถูกบุกรุก	ระดับของความเสียหาย
ระดับ 1	เครือข่ายพื้นฐาน	- สิทธิและผลประโยชน์โดยชอบด้วยกฎหมายของพลเมือง นิติบุคคล และองค์กรอื่นๆ ที่เกี่ยวข้อง	- ความเสียหายทั่วไป
ระดับ 2	เครือข่ายพื้นฐาน	- สิทธิและผลประโยชน์โดยชอบด้วยกฎหมายของพลเมือง นิติบุคคล และองค์กรอื่นๆ ที่เกี่ยวข้อง - ความสงบเรียบร้อยและสาธารณประโยชน์	- ความเสียหายร้ายแรง - ความเสียหายทั่วไป
ระดับ 3	เครือข่ายสำคัญ	- สิทธิและผลประโยชน์โดยชอบด้วยกฎหมายของพลเมือง นิติบุคคล และองค์กรอื่นๆ ที่เกี่ยวข้อง - ความสงบเรียบร้อยและสาธารณประโยชน์ - ความมั่นคงของชาติ	- ความเสียหายวิกฤต - ความเสียหายร้ายแรง - ความเสียหายทั่วไป
ระดับ 4	เครือข่ายสำคัญอย่างยิ่ง	- ความสงบเรียบร้อยและสาธารณประโยชน์ - ความมั่นคงของชาติ	- ความเสียหายวิกฤต - ความเสียหายร้ายแรง
ระดับ 5	เครือข่ายสำคัญสูงสุด	- ความมั่นคงของชาติ	- ความเสียหายวิกฤต

ตารางที่ 3.1 ประเภทเครือข่ายตามระดับของอันตรายที่ระบบสามารถก่อให้เกิดได้หากถูกบุกรุกหรือถูกทำให้เสียหาย

[39] AppInChina, 'What is an MLPS Filing and who needs one?' <https://www.appinchina.co/what-is-an-mlps-filing-and-who-needs-one> สืบค้นเมื่อ 31 มีนาคม 2566.

ระดับที่ 1 มีความสำคัญน้อยที่สุดและเป็นไปตามข้อกำหนดด้านความปลอดภัยน้อยที่สุด ในขณะที่ระดับที่ 5 มีความสำคัญสูงสุดและอยู่ภายใต้ข้อกำหนดด้านความปลอดภัยสูงสุด

โดยกฎหมายบัญญัติให้ผู้ให้บริการเครือข่ายทั้งหมด โดยไม่คำนึงถึงการจัดประเภท MLPS จะต้องดำเนินมาตรการรักษาความปลอดภัยทางไซเบอร์ทั่วไป ดังต่อไปนี้[40]

- การบริหารงานบุคคลและการฝึกอบรมเกี่ยวกับมาตรการรักษาความปลอดภัยทางไซเบอร์
- การจัดการห้องข้อมูล เซิร์ฟเวอร์ และอุปกรณ์
- การป้องกันมัลแวร์และการโจมตีทางไซเบอร์
- การตรวจสอบและบันทึกสถานะเครือข่าย
- การสำรองข้อมูล
- การรายงานเหตุการณ์ด้านความปลอดภัย

นอกจากนี้ มีข้อกำหนดเพิ่มเติมสำหรับเครือข่ายที่จำแนกเป็น MLPS ระดับสามขึ้นไป เช่น

- ตรวจสอบสถานะเครือข่าย การรับส่งข้อมูลเครือข่าย พฤติกรรมผู้ใช้ เหตุการณ์ด้านความปลอดภัย และการเชื่อมต่อเครือข่ายการตรวจสอบกับเครือข่าย CAC
- จัดทำแผนฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์และดำเนินการฝึกซ้อมรับมือเหตุฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ
- การใช้ผลิตภัณฑ์และบริการของเครือข่ายที่ตรงกับระดับการจัดประเภทโดยการจัดหาผลิตภัณฑ์และบริการที่ได้รับการรับรองจาก CAC
- การใช้เทคโนโลยีการเข้ารหัส ผลิตภัณฑ์และบริการที่ได้รับอนุมัติจาก State Cryptography Administration (SCA)
- ดำเนินการบำรุงรักษาทางเทคนิคของเครือข่ายภายในประเทศจีน หากจำเป็น ต้องทำการบำรุงรักษาระยะไกลนอกประเทศจีนด้วยเหตุผลทางธุรกิจ การดำเนินการประเมินความปลอดภัยทางไซเบอร์และใช้มาตรการจัดการความเสี่ยงที่สำคัญ

การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งหมายถึง สิ่งอำนวยความสะดวกเครือข่ายและระบบข้อมูลที่สำคัญในจีน ซึ่งในกรณีที่เกิดความเสียหาย สูญเสียการทำงาน หรือข้อมูลรั่วไหล อาจสร้างความเสียหายอย่างร้ายแรงต่อความมั่นคงของชาติ เศรษฐกิจของประเทศ การดำรงชีวิตของประชาชน หรือ

---

[40] Government of Canada (เชิงอรรถ 59).

ผลประโยชน์สาธารณะ เช่น หน่วยงานบริการสื่อสารและสารสนเทศสาธารณะ หน่วยงานด้านพลังงาน การขนส่ง การอนุรักษ์น้ำ การเงิน การจัดทำบริการสาธารณะ รัฐบาลอิเล็กทรอนิกส์ อุตสาหกรรมเทคโนโลยีการป้องกันประเทศ และอุตสาหกรรมสาขาอื่น ๆ ที่สำคัญ โดยหน่วยงาน Chinese sectoral regulators มีหน้าที่ระบุ CII โดยคำนึงถึงปัจจัยกว้าง ๆ สามประการต่อไปนี้ คือ 1) ความสำคัญของสิ่งอำนวยความสะดวกเครือข่ายและระบบข้อมูลต่อธุรกิจหลักของอุตสาหกรรมหรือสาขา 2) ระดับอันตรายที่อาจเกิดขึ้นหากเครือข่ายและระบบสารสนเทศเสียหาย ปิดใช้งาน หรือข้อมูลรั่วไหล 3) ผลกระทบที่อาจเกิดขึ้นกับอุตสาหกรรมและสาขาอื่น ๆ เมื่อมีการกำหนดหน่วยงาน CII แล้ว ให้แจ้งผลไปยังผู้ดำเนินการซึ่งจะต้องปฏิบัติตามข้อกำหนดด้านความปลอดภัยทางไซเบอร์ที่เข้มงวด และดำเนินกิจกรรมการป้องกันความปลอดภัยทางไซเบอร์ที่คล้ายคลึงกับข้อกำหนดของเครือข่ายที่จำแนกตาม MLPS ระดับสามขึ้นไป นอกจากนี้ ผู้ประกอบการต้องปฏิบัติตามข้อกำหนดต่าง ๆ เช่น จัดตั้งสำนักงานจัดการความปลอดภัยพิเศษเพื่อรับผิดชอบการป้องกันความปลอดภัยของ CII ทำการประเมินความปลอดภัยสำหรับระบบและซอฟต์แวร์ที่พัฒนาโดยบุคคลที่สามก่อนที่เครือข่ายจะออนไลน์ จัดเก็บข้อมูลส่วนบุคคลและข้อมูลสำคัญที่รวบรวมและ/หรือผลิตขึ้นในระหว่างการดำเนินการในประเทศจีน หากจำเป็นต้องถ่ายโอนข้อมูลดังกล่าวข้ามพรมแดนด้วยเหตุผลทางธุรกิจ ผู้ประกอบการจะต้องผ่านการประเมินความปลอดภัยภาคบังคับโดย CAC ผ่านการตรวจสอบความปลอดภัยทางไซเบอร์ก่อนที่ผู้ให้บริการจะจัดหาผลิตภัณฑ์และบริการเครือข่ายที่หลากหลายซึ่งอาจส่งผลเสียต่อความมั่นคงของจีน ข้อตกลงการจัดซื้อจัดจ้างของผู้ประกอบการต้องระบุไว้อย่างชัดเจนว่าซัพพลายเออร์จะช่วยเหลือในการตรวจสอบความปลอดภัยทางไซเบอร์และมุ่งมั่นที่จะไม่มีส่วนร่วมในกิจกรรมที่ผิดกฎหมาย และต้องลงนามในข้อตกลงการรักษาความลับด้านความปลอดภัยกับการจัดหาผลิตภัณฑ์และบริการเครือข่าย และข้อตกลงดังกล่าวจะต้องระบุภาระผูกพันของซัพพลายเออร์ในการสนับสนุนทางเทคนิคและการรักษาความลับด้านความปลอดภัย

ทั้งนี้ จะมีการทบทวนการกำหนดหน่วยงานที่เป็น CII เป็นระยะ โดยไม่ได้กำหนดระยะเวลา

โดยเมื่อฝ่าฝืนบทบัญญัติตามกฎหมายฉบับนี้จะมีบทลงโทษ ดังนี้

มาตรา	ฐานความผิด	ค่าปรับและบทลงโทษ
มาตรา 59 มาตรา 60 มาตรา 61 และมาตรา 62	ฝ่าฝืนมาตรา 21 มาตรา 22 วรรค 1 และวรรค 2 มาตรา 23 มาตรา 24 วรรค 1 มาตรา 25 มาตรา 26 มาตรา 28 มาตรา 33 มาตรา 34 มาตรา 36 และมาตรา 38 (มาตรา 21 ถึง 28 เกี่ยวข้องกับข้อกำหนดความปลอดภัยทางไซเบอร์	ค่าปรับ 10,000 หยวน ถึง 100,000 หยวน หรือ 50,000 หยวน ถึง 500,000 หยวน สำหรับการฝ่าฝืนที่มีผล "ร้ายแรง" และปรับ 10,000 หยวน ถึง 100,000 หยวน สำหรับผู้รับผิดชอบ

มาตรา	ฐานความผิด	ค่าปรับและบทลงโทษ
	ของผู้ให้บริการเครือข่ายทั่วไป ในขณะที่มาตรา 33 ถึง 38 เกี่ยวข้องกับภาระหน้าที่ในการป้องกันความปลอดภัยทางไซเบอร์ของหน่วยงานที่เป็น CII)	
มาตรา 63 และมาตรา 67	ฝ่าฝืนมาตรา 27 และ มาตรา 46 (มาตรา 27 ห้ามบุคคลและบริษัทมีส่วนร่วมในขั้นตอนหรือใช้เครื่องมือที่เป็นอันตรายต่อกิจกรรมความปลอดภัยทางไซเบอร์ มาตรา 46 กำหนดให้บุคคลและองค์กรต้องรับผิดชอบต่อวิธีใช้เครือข่าย และห้ามมิให้สร้างเว็บไซต์หรือกลุ่มสื่อสารสำหรับกิจกรรมที่ผิดกฎหมายและเป็นอาชญากรรม)	ค่าปรับ 10,000 หยวน ถึง 100,000 หยวน และกักขังไม่เกิน5 วัน หรือปรับตั้งแต่ 50,000 หยวน ถึง 500,000 หยวน และกักขังตั้งแต่ 5 ถึง 15 วันสำหรับการฝ่าฝืนอย่างร้ายแรง (สำหรับการฝ่าฝืนมาตรา 46)
มาตรา 64	ฝ่าฝืนมาตรา 35 ซึ่งกำหนดให้ผลิตภัณฑ์และบริการเครือข่ายซึ่งจัดหามาโดยหน่วยงานที่เป็น CII ที่อาจส่งผลกระทบต่อความมั่นคงของชาติต้องผ่านการตรวจสอบด้านความมั่นคงแห่งชาติที่กำหนดโดย CAC	ค่าปรับ 1-10 เท่าของยอดซื้อ และค่าปรับ 10,000 ถึง 100,000 หยวน สำหรับผู้รับผิดชอบ
มาตรา 68 และ 69	ฝ่าฝืนมาตรา 47 มาตรา 48 และมาตรา 49 ซึ่งกำหนดให้ผู้ให้บริการเครือข่ายต้องจัดการเนื้อหาที่ตีพิมพ์และเผยแพร่โดยบุคคลหรือองค์กรผ่านเครือข่ายของตน และรับผิดชอบหากผู้ใช้เผยแพร่เนื้อหาที่ต้องห้าม	ปรับ 100,000 ถึง 500,000 หยวน และปรับ 10,000 ถึง 100,000 หยวน สำหรับผู้รับผิดชอบ
มาตรา 70	ฝ่าฝืนมาตรา 12 ซึ่งกำหนดว่าบุคคลหรือองค์กรใด ๆ ที่ใช้อินเทอร์เน็ตต้องปฏิบัติตามรัฐธรรมนูญและกฎหมายของจีนในการรักษาความสงบเรียบร้อยของประชาชน และเคารพศีลธรรมทางสังคม นอกจากนี้ ยังห้ามการใช้	ได้รับโทษตามบทบัญญัติแห่งกฎหมายและระเบียบบริหารราชการแผ่นดินที่เกี่ยวข้อง

มาตรา	ฐานความผิด	ค่าปรับและบทลงโทษ
	อินเทอร์เน็ตเพื่อมีส่วนร่วมในกิจกรรมที่บ่อนทำลายอำนาจอธิปไตย ความมั่นคงของชาติ และเสถียรภาพของจีน เช่น การยุยงให้เกิดการโค่นล้มอำนาจรัฐ การล้มล้างระบบสังคมนิยม และอื่น ๆ	

ตาราง 3.2 บทกำหนดโทษของ Cybersecurity Law of the People's Republic of China

นอกจากค่าปรับข้างต้นแล้ว บริษัทที่พบว่าฝ่าฝืนมาตราที่ระบุไว้อาจต้องรับผิดในการลงโทษอื่น ๆ ด้วย ซึ่งรวมถึงการระงับธุรกิจที่เกี่ยวข้อง การปิดเว็บไซต์หรือบริการอื่น ๆ การเพิกถอนใบอนุญาตประกอบธุรกิจ และการลงโทษทางปกครองอื่น ๆ บุคคลที่มีหน้าที่รับผิดชอบโดยตรงต่อการฝ่าฝืนอาจถูกห้ามไม่ให้ดำรงตำแหน่งระดับสูงในบริษัทหรืออุตสาหกรรม หรือถูกห้ามไม่ให้ทำงานในอุตสาหกรรมอีก หากการละเมิดนั้นถือว่าร้ายแรงเป็นพิเศษ

3.2.2.3 มิติด้านสิทธิมนุษยชนในกฎหมาย

กฎหมายฉบับนี้ได้รับเสียงวิจารณ์จากนอกประเทศว่า อาจปิดกั้นบริษัทเทคโนโลยีไม่ให้ทำธุรกิจในบางกิจการที่สำคัญ และไม่เห็นด้วยที่กำหนดให้มีการตรวจสอบด้านความปลอดภัย รวมทั้งกำหนดให้เก็บข้อมูลบนเซิร์ฟเวอร์ซึ่งอยู่ในประเทศจีน องค์กรธุรกิจระดับโลกกว่า 40 แห่งยื่นหนังสือถึงนายกรัฐมนตรีหลี่เค่อเฉียง เรียกร้องให้รัฐบาลจีนปรับปรุงร่างในส่วนที่ถูกวิจารณ์ อย่างไรก็ดี บทบัญญัติที่ถูกโต้แย้งเหล่านั้นยังคงปรากฏในกฎหมายฉบับนี้

สำหรับประเด็นที่เห็นได้อย่างชัดเจนในกฎหมายฉบับนี้ คือการใช้ถ้อยคำที่ค่อนข้างกว้าง และกำกวม ซึ่งหน่วยงานรัฐที่บังคับใช้กฎหมายอาจตีความได้กว้างขวางและละเมิดสิทธิมนุษยชน ซึ่งจะยิ่งปิดกั้นเสรีภาพทางออนไลน์มากขึ้น เช่น ในมาตรา 12 ที่บัญญัติว่า[41]

[41] Article 12: The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information.

Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering

“รัฐคุ้มครองสิทธิของพลเมือง นิติบุคคล และองค์กรอื่น ๆ ในการใช้เครือข่ายตามกฎหมาย ส่งเสริมการเข้าถึงเครือข่ายอย่างกว้างขวาง ยกระดับบริการเครือข่ายให้บริการเครือข่ายที่ปลอดภัยและสะดวกสบายแก่สังคม และรับประกันการเผยแพร่ข้อมูลเครือข่ายที่ถูกต้องตามกฎหมาย เป็นระเบียบเรียบร้อย และฟรี

บุคคลและองค์กรใดที่ใช้เครือข่ายจะต้องปฏิบัติตามรัฐธรรมนูญและกฎหมาย รักษาความสงบเรียบร้อยของประชาชน และเคารพศีลธรรมของสังคม ต้องไม่เป็นอันตรายต่อความปลอดภัยทางไซเบอร์ และต้องไม่ใช้อินเทอร์เน็ตเพื่อมีส่วนร่วมในกิจกรรมที่เป็นอันตรายต่อความมั่นคงของชาติ เกียรติยศของชาติ และผลประโยชน์ของชาติ ต้องไม่ยุยงปลุกปั่นล้มล้างอธิปไตยของชาติ ล้มล้างระบบสังคมนิยม ปลุกปั่นแบ่งแยกดินแดน ทำลายเอกภาพของชาติ สนับสนุนการก่อการร้ายหรือลัทธิสุดโต่ง สนับสนุนการเกลียดชังชาติพันธุ์และการเลือกปฏิบัติทางชาติพันธุ์ เผยแพร่ความรุนแรง ลามกอนาจาร หรือข้อมูลทางเพศ สร้างหรือเผยแพร่ข้อมูลเท็จเพื่อขัดขวางระเบียบทางเศรษฐกิจหรือสังคม หรือข้อมูลที่ละเมิดต่อชื่อเสียง ความเป็นส่วนตัว ทรัพย์สินทางปัญญา หรือสิทธิและผลประโยชน์ตามกฎหมายอื่น ๆ ของผู้อื่น และการกระทำอื่น ๆ ดังกล่าว”

ซึ่งจะเห็นว่ามีหลายถ้อยคำที่กำกวม เช่น “กิจกรรมที่เป็นอันตรายต่อความมั่นคงของชาติ” “เกียรติยศของชาติ” “ผลประโยชน์ของชาติ” “เอกภาพของชาติ” เป็นต้น ซึ่งแนวคิดเรื่องอำนาจอธิปไตยทางไซเบอร์ของจีน (Chinese Cyber Sovereignty Concept) เป็นแนวคิดที่แตกต่างจากคำว่า "ความมั่นคงปลอดภัยทางไซเบอร์" โดยทั่วไปที่เข้าใจกัน กล่าวคือ รัฐบาลมีการปกป้องโครงสร้างพื้นฐานและกระบวนการที่เชื่อมต่อกับอินเทอร์เน็ต อำนาจอธิปไตยทางไซเบอร์มุ่งเน้นไปที่ข้อมูลและเนื้อหาที่อยู่บนอินเทอร์เน็ต ทั้งนี้ แนวคิดอธิปไตยทางไซเบอร์ของจีนตั้งอยู่บนหลักการสำคัญ คือ ปิดกั้นข้อมูลที่มีอิทธิพลที่ไม่ต้องการในพื้นที่ข้อมูลของประเทศ ซึ่งจะส่งผลช่วยให้รัฐบาลสามารถป้องกันไม่ให้พลเมืองของตนแสดงความคิดเห็นที่รัฐบาลถือว่าเป็นอันตราย รวมถึงเปลี่ยนการกำกับดูแลอินเทอร์เน็ตที่อนุญาตให้รัฐบาลเพิ่มการควบคุมทางอินเทอร์เน็ต

---

national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

สำหรับประเด็นการคุ้มครองความเป็นส่วนตัว กฎหมายฉบับนี้ได้กำหนดให้ผู้ให้บริการเครือข่ายจะต้องรวบรวมหรือใช้ข้อมูลส่วนบุคคลอย่างถูกกฎหมาย เหมาะสม และเท่าที่จำเป็น และจะต้องเปิดเผยวัตถุประสงค์ วิธีการ และขอบเขตในการรวบรวมข้อมูล โดยได้รับความยินยอมจากเจ้าของข้อมูลก่อนที่จะทำการเก็บข้อมูล เจ้าของข้อมูลยังมีสิทธิในการเปลี่ยนแปลงแก้ไขหรือลบข้อมูลนั้นด้วย และหากข้อมูลส่วนตัวใดที่ไม่เกี่ยวข้องกับการให้บริการ ห้ามให้ผู้ให้บริการเก็บข้อมูลเหล่านั้น รวมถึงห้ามเปิดเผยข้อมูลให้กับบุคคลอื่น เว้นแต่ เจ้าของข้อมูลให้ความยินยอมแล้ว หรือข้อมูลนั้นถูกแปลงสภาพจนไม่สามารถทราบได้ว่าหมายถึงบุคคลใดโดยเฉพาะเจาะจง และหากมีการฝ่าฝืนบทบัญญัติในส่วนนี้ ผู้ให้บริการจะถูกออกหนังสือตักเตือน และสั่งให้ทำการแก้ไข อาจถูกยึดทรัพย์ หรือปรับไม่เกิน 1 ล้านหยวน และปรับผู้รับผิดชอบโดยตรงและผู้บังคับบัญชาตั้งแต่ 10,000 หยวน แต่ไม่เกิน 100,000 หยวน แต่ในกรณีที่เกิดความเสียหายร้ายแรงอาจถูกสั่งระงับการให้บริการ ปิดเว็บไซต์ หรือระงับการประกอบกิจการ รวมถึงระงับใบอนุญาตประกอบกิจการชั่วคราวหรือถาวร

อย่างไรก็ดี แม้ดูเหมือนว่ากฎหมายฉบับนี้จะคุ้มครองความเป็นส่วนตัวของประชาชน โดยเป็นหน้าที่ของผู้ให้บริการ แต่เจ้าหน้าที่รัฐไม่ตกอยู่ภายใต้บังคับของหน้าที่นี้ ซ้ำยังเป็นเครื่องมือให้เจ้าหน้าที่รัฐใช้ในการควบคุมและสอดแนมข้อมูลส่วนบุคคลโดยโยนภาระต่าง ๆ ให้กับผู้ประกอบการ ที่จะต้องให้ความช่วยเหลือทางเทคนิคแก่เจ้าหน้าที่รัฐในการรักษาความมั่นคงชองชาติ ดังนั้น เจ้าหน้าที่รัฐจึงสามารถเข้าถึงข้อมูลส่วนบุคคลได้โดยชอบด้วยกฎหมาย รวมถึงการบังคับให้ผู้ใช้งานต้องแสดงตัวตนก่อนเข้าใช้งานอินเทอร์เน็ต โดยอ้างว่าเพื่อต่อต้านข่าวปลอม การใช้คำไม่สุภาพ สื่อลามกอนาจาร ซึ่งแท้ที่จริงแล้วเป็นการใช้กฎหมายเป็นเครื่องมือโดยรัฐบาลไม่ต้องการให้ประชาชนที่ใช้งานอินเทอร์เน็ตวิพากษ์วิจารณ์รัฐบาล ซึ่งเป็นการขัดขวางเสรีภาพในการแสดงความคิดเห็น (Freedom of Expression) และกระทบต่อสิทธิมนุษยชนบนโลกดิจิทัล

3.2.3 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสิงคโปร์

ความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยี ทำให้สิงคโปร์ได้รับยกย่องให้เป็นต้นแบบของประเทศแห่งอนาคตที่วางแผนพัฒนาประเทศและยกระดับคุณภาพชีวิตของประชาชนด้วยการเชื่อมโยงโครงสร้างพื้นฐานต่างๆ เข้ากับเครือข่ายเทคโนโลยีที่ทันสมัย การขับเคลื่อนสังคมและเศรษฐกิจด้วยเทคโนโลยีดิจิทัลภายใต้แนวคิดอินเตอร์เน็ตของสรรพสิ่ง (Internet of Things) ทำให้ความมั่นคงไซเบอร์กลายเป็นประเด็นที่รัฐบาลสิงคโปร์ต้องให้ความสำคัญเป็นพิเศษ เนื่องจากจำเป็นต้องรับมือความเสี่ยงที่จะถูกโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์ที่เพิ่มจำนวนขึ้น ด้วยเหตุนี้ รัฐบาลสิงคโปร์จึงทยอยออกมาตรการเพื่อรับมือกับความท้าทายในโลกไซเบอร์อย่างต่อเนื่อง เช่น การก่อตั้งหน่วยงานความมั่นคงไซเบอร์ (Cyber Security Agency-CSA) เพื่อกำกับ

ดูแลงานด้านความมั่นคงไซเบอร์ในภาพรวมโดยให้ขึ้นตรงต่อสำนักนายกรัฐมนตรี และมีกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act 2018) มีผลบังคับใช้เมื่อวันที่ 2 มีนาคม 2018

3.2.3.1 โครงสร้างของกฎหมาย

กฎหมายด้วยความมั่นคงปลอดภัยทางไซเบอร์ 2018 (Cybersecurity Act 2018) ผ่านการพิจารณาของรัฐสภาเมื่อวันที่ 5 กุมภาพันธ์ 2018 และประกาศใช้เมื่อวันที่ 2 มีนาคม 2018 ประกอบด้วย 6 ส่วน (Part) 51 มาตรา ได้แก่

ส่วนที่ 1 ความเบื้องต้น (PART 1 PRELIMINARY) มาตรา 1 – 3

ส่วนที่ 2 การบริหารจัดการ (PART 2 ADMINISTRATION) มาตรา 4 - 6

ส่วนที่ 3 โครงสร้างพื้นฐานของข้อมูลที่สำคัญ (PART 3 CRITICAL INFORMATION INFRASTRUCTURE) มาตรา 7 - 18

ส่วนที่ 4 การตอบสนองต่อภัยคุกคามความปลอดภัยทางไซเบอร์และเหตุการณ์ต่าง ๆ (PART 4 RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS) มาตรา 19 - 23

ส่วนที่ 5 ผู้ให้บริการความปลอดภัยทางไซเบอร์ (PART 5 CYBERSECURITY SERVICE PROVIDERS) มาตรา 24 - 35

ส่วนที่ 6 บททั่วไป (PART 6 GENERAL) มาตรา 36 – 51

3.2.3.2 สาระสำคัญของกฎหมาย

(1) วัตถุประสงค์ของกฎหมาย กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) ได้ประกาศใช้เมื่อวันที่ 2 มีนาคม ปี ค.ศ. 2018 ซึ่งเป็นกรอบกฎหมายในการควบคุมการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ โดยมีวัตถุประสงค์หลัก 4 ประการ[42] ได้แก่

1) เสริมสร้างการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) จากการโจมตีทางไซเบอร์ ซึ่ง CII คือระบบคอมพิวเตอร์ที่เกี่ยวข้องโดยตรงกับการให้บริการที่จำเป็น การโจมตีทางไซเบอร์ต่อ CII อาจส่งผลกระทบร้ายแรงต่อเศรษฐกิจและสังคม กฎหมายฉบับนี้ยังกำหนดกรอบการทำงานสำหรับการกำหนด CII และให้ความชัดเจนแก่เจ้าของ CII เกี่ยวกับภาระหน้าที่ในการปกป้อง CII จากการโจมตีทางไซเบอร์ในเชิงรุก สร้างความยืดหยุ่นให้กับ CII ปกป้องเศรษฐกิจของสิงคโปร์และวิถีชีวิตพลเมือง หน่วยงานกลุ่ม CII

[42] Cyber Security Agency of Singapore, ‘Cybersecurity Act’ <https://www.csa.gov.sg/legislation/cybersecurity-act> สืบค้นเมื่อ 31 มีนาคม 2566.

ได้แก่ พลังงาน น้ำ การเงินการธนาคาร ระบบบริการสุขภาพ การขนส่ง (ซึ่งรวมถึงการขนส่งทางบก ทางเรือ และทางอากาศ) การสื่อสารข้อมูล สื่อ บริการด้านการรักษาความปลอดภัยและเหตุฉุกเฉิน และรัฐบาล

2) อนุญาตให้ CSA มีอำนาจในการป้องกันและตอบสนองต่อภัยคุกคามและเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ กฎหมายนี้ยังให้อำนาจแก่ผู้บัญชาการความปลอดภัยทางไซเบอร์ในการตรวจสอบภัยคุกคามและเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ เพื่อกำหนดผลกระทบและป้องกันไม่ให้เกิดอันตรายหรือเหตุการณ์ด้านความปลอดภัยทางไซเบอร์เพิ่มเติม โดยใช้อำนาจได้ตามระดับความรุนแรงของภัยคุกคามความปลอดภัยทางไซเบอร์หรือเหตุการณ์ และมาตรการที่จำเป็นสำหรับการตอบสนอง ซึ่งจะทำให้ชาวสิงคโปร์มั่นใจได้ว่ารัฐบาลสามารถตอบสนองต่อภัยคุกคามความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ และทำให้ประเทศสิงคโปร์และชาวสิงคโปร์ปลอดภัย

3) กำหนดกรอบสำหรับการแบ่งปันข้อมูลความปลอดภัยทางไซเบอร์ เพื่ออำนวยความสะดวกในการแบ่งปันข้อมูลซึ่งมีความสำคัญ เนื่องจากข้อมูลที่ทันท่วงทีช่วยให้รัฐบาลและเจ้าของระบบคอมพิวเตอร์สามารถระบุช่องโหว่และป้องกันเหตุการณ์ทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้น กฎหมายกำหนดกรอบการทำงานสำหรับ CSA ในการขอข้อมูล และสำหรับการคุ้มครองและการแบ่งปันข้อมูลดังกล่าว

4) กำหนดกรอบการให้สิทธิ์การใช้งานแบบ light-touch สำหรับผู้ให้บริการความปลอดภัยทางไซเบอร์ ซึ่ง CSA ใช้วิธีการแบบ light-touch เพื่อออกใบอนุญาตผู้ให้บริการเพียง 2 ประเภทในปัจจุบัน ได้แก่ บริการทดสอบการเจาะระบบ และการตรวจสอบศูนย์ปฏิบัติการด้านความปลอดภัยที่มีการจัดการ บริการทั้งสองนี้ได้รับการจัดลำดับความสำคัญเนื่องจากผู้ให้บริการดังกล่าวสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนจากลูกค้าของตนได้ ดังนั้นจึงมีผลกระทบอย่างมากต่อภูมิทัศน์ด้านความปลอดภัยโดยรวม กรอบการออกใบอนุญาตพยายามที่จะสร้างสมดุลระหว่างความต้องการด้านความปลอดภัยและการพัฒนาระบบนิเวศความปลอดภัยทางไซเบอร์

(2) หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย

กฎหมายฉบับนี้ บัญญัติให้รัฐมนตรี แต่งตั้ง “ผู้บัญชาการความปลอดภัยทางไซเบอร์” ซึ่งมีอำนาจหน้าที่ต่าง ๆ เช่น ดูแลภาพรวมและส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ของคอมพิวเตอร์และระบบคอมพิวเตอร์ในประเทศสิงคโปร์ ให้คำแนะนำแก่รัฐบาลหรือหน่วยงานของรัฐในความต้องการและนโยบายระดับชาติด้านความปลอดภัยทางไซเบอร์ เฝ้าระวังภัยคุกคามทางไซเบอร์ ไม่ว่าภัยคุกคามนั้นจะเกิดขึ้นภายในหรือภายนอกประเทศสิงคโปร์ ตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่คุกคามความมั่นคงของประเทศ การป้องกันประเทศ เศรษฐกิจ ความสัมพันธ์ระหว่างประเทศ สาธารณสุข ความเป็นระเบียบเรียบร้อยและความปลอดภัย

สาธารณะ หรือบริการพื้นฐานของประเทศ กำหนดหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) และกำกับดูแลผู้รับผิดชอบหน่วยงานดังกล่าวให้ดำเนินการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ ร่วมมือกับทีมตอบโต้เหตุฉุกเฉินทางคอมพิวเตอร์ (Computer Emergency Response Teams: CERTs) ของประเทศหรือดินแดนอื่น ๆ ในกรณีเกิดเหตุการณ์ความปลอดภัยทางไซเบอร์ วางหลักเกณฑ์ มาตรฐาน การออกใบอนุญาตต่าง ๆ ที่เกี่ยวข้อง[43]

---

[43] Duties and functions of Commissioner

5. The Commissioner has the following duties and functions:

(a) to oversee and promote the cybersecurity of computers and computer systems in Singapore;

(b) to advise the Government or any other public authority on national needs and policies in respect of cybersecurity matters generally;

(c) to monitor cybersecurity threats, whether such cybersecurity threats occur in or outside Singapore;

(d) to respond to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services, of Singapore, whether such cybersecurity incidents occur in or outside Singapore;

(e) to identify and designate critical information infrastructure, and to regulate owners of critical information infrastructure with regard to the cybersecurity of the critical information infrastructure;

(f) to establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure;

(g) to represent the Government on cybersecurity issues internationally;

(h) to cooperate with computer emergency response teams (CERTs) of other countries or territories on cybersecurity incidents;

(i) to develop and promote the cybersecurity services industry in Singapore;

(j) to license and establish standards in relation to cybersecurity service providers;

นอกจากนี้รัฐมนตรียังแต่งตั้งรองผู้บัญชาการความปลอดภัยทางไซเบอร์จำนวน 1 คน และแต่งตั้งผู้ช่วยผู้บัญชาการฯ ได้ตั้งแต่ 1 คนขึ้นไป เพื่อทำงานสนับสนุนผู้บัญชาการฯ ในการปฏิบัติตามอำนาจหน้าที่ ปัจจุบันผู้บัญชาการความปลอดภัยทางไซเบอร์ของสิงคโปร์ คือ Mr David Koh ซึ่งยังดำรงตำแหน่งเป็น CEO ของสำนักงานความมั่นคงปลอดภัยไซเบอร์แห่งสิงคโปร์อีกด้วย โดยสำนักงานดังกล่าวเป็นหน่วยงานระดับชาติที่รับผิดชอบความมั่นคงปลอดภัยไซเบอร์ของประเทศ สังกัดกระทรวงการสื่อสารและสารสนเทศ (Ministry of Communications and Information: MCI) มีภารกิจหลัก 4 ด้าน คือ 1) ปกป้อง (Protect) ระบบสำคัญของประเทศให้ปลอดภัยจากภัยคุกคามไซเบอร์ 2) ตรวจจับ (Detect) ภัยคุกคามไซเบอร์ที่จะเป็นอันตรายต่อระบบสำคัญของประเทศ 3) ตอบสนองหรือรับมือ (Respond) เมื่อเกิดภัยคุกคามไซเบอร์ขึ้นกับระบบสำคัญของประเทศ และ 4) ดำเนินการฟื้นฟูหรือกู้คืน (Recover) ระบบสำคัญให้สามารถกลับมาทำงานได้ตามปกติโดยเร็วที่สุดหลังจากถูกโจมตีจากภัยคุกคามไซเบอร์[44] หน้าที่ของสำนักงานฯ ยังรวมถึงการขับเคลื่อนยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของสิงคโปร์ 2021 (Singapore's Cybersecurity Strategy 2021) ซึ่งประกอบด้วยเสาหลักเชิงยุทธศาสตร์ 3 ประการ และปัจจัยพื้นฐาน 2 ประการ ได้แก่

เสาหลักยุทธศาสตร์ที่ 1: สร้างโครงสร้างพื้นฐานที่ยืดหยุ่น

เสาหลักยุทธศาสตร์ที่ 2: เปิดใช้งานไซเบอร์สเปซที่ปลอดภัยยิ่งขึ้น

(k) to establish standards within Singapore in relation to cybersecurity products or services, and the recommended level of cybersecurity of computer hardware or software, including certification or accreditation schemes;

(l) to promote, develop, maintain and improve competencies and professional standards of persons working in the field of cybersecurity;

(m) to support the advancement of technology, and research and development relating to cybersecurity;

(n) to promote awareness of the need for and the importance of cybersecurity in Singapore;

(o) to perform such other functions and discharge such other duties as may be conferred on the Commissioner under any other written law.

[44] Cyber Security Agency of Singapore, 'The Singapore Cybersecurity Strategy 2021' <https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021> สืบค้นเมื่อ 19 เมษายน 2566.

เสาหลักยุทธศาสตร์ที่ 3: ยกระดับความร่วมมือทางไซเบอร์ระหว่างประเทศ

ปัจจัยพื้นฐานที่ 1: พัฒนาระบบนิเวศความปลอดภัยทางไซเบอร์ที่มีชีวิตชีวา

ปัจจัยพื้นฐานที่ 2: ขยายช่องทางผลิตบุคลากรที่มีทักษะด้านไซเบอร์ที่แข็งแกร่ง

ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ 2021 เป็นเครื่องมือสำคัญในการสำรวจการขยายขอบเขตการกำกับดูแลของรัฐบาลภายใต้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ เพื่อรวมหน่วยงานและระบบนอกเหนือจากโครงสร้างพื้นฐานสำคัญทางสารสนเทศซึ่งสนับสนุนการให้บริการที่จำเป็นใน 11 ภาคส่วนขณะเดียวกันยุทธศาสตร์ฉบับนี้ จะสนับสนุนให้องค์กรต่าง ๆ ลงทุนในความปลอดภัยทางไซเบอร์และรวมความปลอดภัยทางไซเบอร์ไว้เป็นส่วนหนึ่งของกรอบการจัดการความเสี่ยง

(3) มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์

มาตรการสำคัญที่ใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์ของกฎหมายฉบับนี้แบ่งออกเป็น 3 เรื่องหลัก กล่าวคือ 1) การกำหนดหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) และหน้าที่ของเจ้าของหรือผู้รับผิดชอบหน่วยงานเหล่านั้น ที่จะต้องปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์ 2) การใช้มาตรการเพื่อป้องกัน จัดการ และตอบสนองต่อภัยคุกคามและเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ในสิงคโปร์ 3) การออกใบอนุญาตของผู้ให้บริการความปลอดภัยทางไซเบอร์สำหรับประเภทบริการที่สามารถขอใบอนุญาตได้

หน่วยงานหรือองค์กรที่ถูกระบุว่าเป็น CII จะต้องดำเนินมาตรการต่าง ๆ เช่น ป้องกัน จัดการ และตอบสนองต่อภัยคุกคามและเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) จัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร ตรวจสอบความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่ระบุเป็นประจำ และดำเนินการตามนโยบาย มาตรฐาน และแนวปฏิบัติเพื่อจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ดำเนินการหรือมีสิทธิ์เข้าถึง CII รวมถึงแบ่งปันข้อมูลกับ Cyber Security Agency of Singapore (CSA) ในกรณีที่มีการโจมตีทางไซเบอร์

สำหรับการสอบสวนความผิดที่เกิดจากผู้ประกอบการ กฎหมายให้อำนาจผู้บัญชาการฯ ในการแต่งตั้งเจ้าหน้าที่สืบสวนสอบสวน ซึ่งมีอำนาจเรียกเอกสารและข้อมูลในความครอบครองของบุคคลที่เกี่ยวข้อง หรือเรียกบุคคลเข้าให้ข้อมูลหรือให้ปากคำ เพื่อประโยชน์ในการสืบสวนสอบสวน หากขัดขืนคำสั่งเรียกของเจ้าหน้าที่ฯ จะรายงานไปยังศาลเพื่อขอให้ศาลออก

หมายเรียก นอกจากนี้ หากผู้ใดขัดขวางเจ้าพนักงานในการดำเนินการสืบสวนสอบสวน หรือทำให้เกิดความล่าช้าในการดำเนินการ ปฏิเสธที่จะให้ข้อมูลหรือเอกสารที่เจ้าหน้าที่มีคำสั่งเรียก รวมถึงไม่ให้ความร่วมมือในการสืบสวนสอบสวน ถือว่ามีความผิดและต้องระวางโทษปรับไม่เกิน 20,000 ดอลลาร์ หรือจำคุกไม่เกิน 12 เดือน หรือทั้งจำทั้งปรับ

โดยการค้นสถานประกอบการกฎหมายบัญญัติให้ออกหมายค้นโดยศาล ซึ่งเจ้าหน้าที่สืบสวนสอบสวนต้องให้เหตุผลจนศาลเชื่อได้ว่าสถานประกอบการนั้นมีการกระทำฝ่าฝืนกฎหมายฉบับนี้ หรือจะมีการปกปิด เคลื่อนย้าย หรือทำลายพยานหลักฐาน หรือมีหลักฐานว่ามีเอกสารหลักฐานที่เกี่ยวข้องกับการสืบสวนสอบสวน โดยหมายค้นให้อำนาจแก่เจ้าหน้าที่ในการเข้าตรวจค้น ยึดเอกสารหรือสำเนา ทั้งหมดหรือบางส่วน เรียกให้ผู้เกี่ยวข้องกับสถานที่นั้นให้ข้อมูล เรียกเอกสารที่เกี่ยวข้องเพิ่มเติมซึ่งเก็บไว้ในรูปแบบอิเล็กทรอนิกส์และสามารถเข้าถึงได้จากสถานที่นั้น ซึ่งอยู่ในรูปแบบที่สามารถนำออกไปได้ และสามารถอ่านได้ ทั้งนี้ หมายศาลดังกล่าวมีอายุ 1 เดือนนับแต่วันออกหมาย และหากในวันที่ทำการตรวจค้นไม่มีผู้ใดอยู่ในสถานที่นั้น ต้องแจ้งให้เจ้าของสถานประกอบการทราบในการเข้าตรวจค้น หากไม่สามารถแจ้งให้เจ้าของทราบได้ เมื่อได้ดำเนินการตรวจค้นตามหมายค้นแล้ว ให้แสดงสำเนาหมายค้นไว้ในจุดที่สามารถมองเห็นได้ในสถานที่นั้น

ในกรณีเกิดเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ เจ้าหน้าที่สืบสวนสอบสวน หรือเจ้าหน้าที่ตอบโต้เหตุการณ์ฉุกเฉินทางไซเบอร์ มีอำนาจเรียกเอกสาร บุคคล และให้บุคคลให้ข้อมูลหรือให้ปากคำเพื่อประโยชน์ในการสืบสวนสอบสวนเหตุการณ์ที่เกิดขึ้น และหากไม่ได้รับความร่วมมือในขั้นต้น ก็มีการบัญญัติให้ดำเนินการขอหมายเรียกที่ออกโดยศาลเช่นเดียวกัน และเมื่อมีกรณีฝ่าฝืนหมายศาลก็จะมีความผิดและมีโทษต่าง ๆ กันไปตามแต่ความหนักเบาแห่งกรณีที่ฝ่าฝืน

3.2.3.3 มิติด้านสิทธิมนุษยชนในกฎหมาย

กฎหมายความมั่นคงปลอดภัยไซเบอร์ของสิงคโปร์ มีการตรวจสอบถ่วงดุลโดยศาลก่อนการตรวจค้นสถานประกอบการจะต้องมีหลักฐานที่แสดงต่อศาลจนเชื่อได้ว่าสถานประกอบการนั้นมีการกระทำฝ่าฝืนกฎหมายฉบับนี้ หรือจะมีการปกปิด เคลื่อนย้าย หรือทำลายพยานหลักฐาน หรือมีหลักฐานว่ามีเอกสารหลักฐานที่เกี่ยวข้องกับการสืบสวนสอบสวน นอกจากนี้กฎหมายเปิดช่องให้ผู้ที่ได้รับคำสั่งจากผู้บัญชาการความปลอดภัยทางไซเบอร์ให้ดำเนินการต่าง ๆ สามารถอุทธรณ์คำสั่งไปยังรัฐมนตรีได้ และหากมีกฎหมายอื่นให้ความคุ้มครองไว้ ผู้ได้รับคำสั่งสามารถปฏิเสธการดำเนินการโดยอ้างเหตุผลอันสมควรภายใต้การคุ้มครองของกฎหมายอื่น ๆ ได้ เช่น การปฏิเสธไม่ให้ข้อมูลส่วนบุคคลของโดยผู้ให้บริการที่เก็บรวบรวมข้อมูลของผู้ใช้ ภายใต้ความคุ้มครองของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

อนึ่ง ยังมีบทบัญญัติบางส่วนที่ตีความได้อย่างกว้างขวาง และอาจกระทบต่อสิทธิของประชาชนได้ เช่น มาตรา 19 ในกรณีที่ผู้บัญชาการได้รับข้อมูลเกี่ยวกับภัยคุกคามหรือเหตุการณ์

ด้านความปลอดภัยทางไซเบอร์ ผู้บัญชาการอาจใช้หรืออาจมอบอำนาจให้รองผู้บัญชาการ ผู้ช่วยผู้บัญชาการ เจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ แล้วแต่กรณี ในการตรวจสอบภัยคุกคามหรือเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ ... โดยนิยามในมาตรา 2 คำว่า “ภัยคุกคามความปลอดภัยทางไซเบอร์” หมายถึง การกระทำหรือกิจกรรม (ไม่ว่าจะทราบหรือสงสัยว่า) กระทำบนหรือผ่านคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดอันตรายหรือส่งผลกระทบในทางลบอย่างฉับพลันต่อความปลอดภัยทางไซเบอร์ของคอมพิวเตอร์หรือระบบคอมพิวเตอร์เครื่องนั้นหรือเครื่องอื่นโดยไม่มีอำนาจตามกฎหมาย ซึ่งหมายความว่า แม้เป็นเพียงความสงสัยก็สามารถใช้อำนาจในการสืบสวนสอบสวนได้ โดยไม่คำนึงถึงระดับความเสียหายที่เกิดขึ้นว่ามากน้อยเพียงใด ซึ่งอาจกระทบต่อสิทธิและเสรีภาพของประชาชน

บทที่ 4
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562

ก่อนที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 จะเดินทางมาถึงวันที่มีการบังคับใช้ ได้ผ่านการแก้ไขมาหลายต่อหลายครั้งในขณะที่เป็นร่างพระราชบัญญัติ ด้วยมีเสียงวิพากษ์วิจารณ์มากมายทั้งจากภาคประชาสังคม นักกฎหมาย นักวิชาการ นักสิทธิมนุษยชน และประชาชน ที่กังวลว่าบทบัญญัติหลายส่วนในกฎหมายฉบับนี้จะใช้เป็นช่องทางให้รัฐใช้อำนาจละเมิดต่อสิทธิเสรีภาพของประชาชนได้ โดยเฉพาะเสรีภาพในการแสดงความคิดเห็นและสิทธิความเป็นส่วนตัว เนื่องจากความไม่ชัดเจนของถ้อยคำในกฎหมาย การใช้อำนาจที่ขาดการตรวจสอบถ่วงดุล และข้อห่วงกังวลอีกหลายประการ การศึกษาในบทนี้จึงเน้นศึกษาถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เพื่อพิจารณาว่าบทบัญญัติของกฎหมายฉบับนี้มีความสมดุลระหว่างมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสิทธิมนุษยชนหรือไม่ รวมถึงหากเปรียบเทียบกับแนวทางในระดับระหว่างประเทศ หรือกฎหมายต่างประเทศ มีความเหมือนหรือแตกต่างกันอย่างไร

4.1 ความเป็นมาของกฎหมาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เสนอโดยคณะรัฐมนตรีชุดที่มี พลเอก ประยุทธ์ จันทร์โอชา เป็นนายกรัฐมนตรี ต่อประธานสภานิติบัญญัติแห่งชาติ เมื่อวันที่ 27 ธันวาคม 2561 เพื่อให้สภานิติบัญญัติแห่งชาติพิจารณาตามบทบัญญัติรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557 โดยที่ประชุมสภานิติบัญญัติแห่งชาติ ครั้งที่ 91/2561 วันศุกร์ที่ 28 ธันวาคม 2561 ได้ลงมติรับหลักการแห่งร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... ไว้พิจารณา และมีมติมอบหมายให้คณะกรรมาธิการวิสามัญพิจารณาร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. .... เป็นผู้พิจารณาร่างพระราชบัญญัตินี้อีกฉบับหนึ่ง ซึ่งคณะกรรมาธิการวิสามัญ ประกอบด้วยกรรมาธิการจำนวน 19 คน ต่อมาในคราวประชุมสภานิติบัญญัติแห่งชาติ ครั้งที่ 19/2562 เป็นพิเศษ วันพฤหัสบดีที่ 28 กุมภาพันธ์ 2562 ที่ประชุมได้พิจารณาร่างพระราชบัญญัติฯ ซึ่งคณะกรรมาธิการวิสามัญพิจารณาเสร็จแล้ว และมีมติเห็นชอบให้ประกาศใช้เป็นกฎหมาย โดยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ประกาศในราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก วันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป กล่าวคือ มีผลบังคับใช้ในวันที่ 28 พฤษภาคม 2562

4.2 โครงสร้างของกฎหมาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มีจำนวน 83 มาตรา แบ่งออกเป็น

มาตรา 1 ชื่อพระราชบัญญัติ

มาตรา 2 วันที่มีผลบังคับใช้

มาตรา 3 นิยามคำสำคัญ

มาตรา 4 ผู้รักษาการกฎหมาย

หมวด 1 คณะกรรมการ

ส่วนที่ 1 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา 5 – มาตรา 11

ส่วนที่ 2 คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

มาตรา 12 – มาตรา 19

หมวด 2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา 20 – มาตรา 40

หมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ 1 นโยบายและแผน มาตรา 41 – มาตรา 44

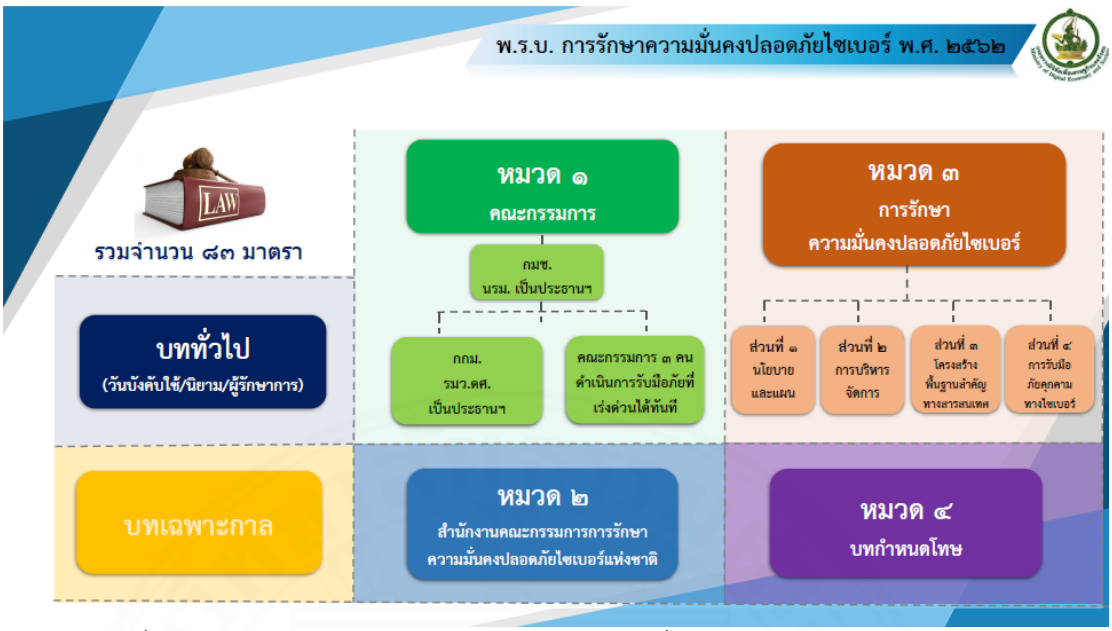
ส่วนที่ 2 การบริหารจัดการ มาตรา 45 – มาตรา 47

ส่วนที่ 3 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตรา 48 – มาตรา 57

ส่วนที่ 4 การรับมือกับภัยคุกคามทางไซเบอร์ มาตรา 58 – มาตรา 69

หมวด 4 บทกำหนดโทษ มาตรา 70 – มาตรา 77

บทเฉพาะกาล มาตรา 78 – มาตรา 83



ภาพที่ 4.1 โครงสร้างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ที่มา : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

4.3 สาระสำคัญของกฎหมาย

4.3.1 วัตถุประสงค์ในการบังคับใช้

โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที จึงควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ[1]

---

[1] ‘หมายเหตุท้ายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562’ (ราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก).

4.3.2 หน่วยงานหรือองค์กรที่ทำหน้าที่หลักภายใต้กฎหมาย

กฎหมายฉบับนี้ได้กำหนดให้มีคณะกรรมการที่สำคัญขึ้น 3 คณะ ได้แก่ มาตรา 5 กำหนดให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” มาตรา 12 กำหนดให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” นอกจากนี้ยังกำหนดให้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กมช. และ กกม. และมาตรา 25 กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน

ภาพ 4.2 คณะกรรมการในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประกอบด้วย

1) นายกรัฐมนตรี เป็นประธานกรรมการ

2) กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ และเลขาธิการสภาความมั่นคง

3) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรม ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสี่ปี และได้รับการแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

โดยให้เลขาธิการ เป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงาน เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ ตามที่กำหนดไว้ในมาตรา 9 ดังต่อไปนี้[2]

(1) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 42 และมาตรา 43 ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา 42

(2) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(3) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

(4) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(5) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของ

---

[2] สกมช., ‘คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)’ <https://www.ncsa.or.th/ncsc.html> สืบค้นเมื่อ 18 เมษายน 2565.

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(6) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(7) แต่งตั้งและถอดถอนเลขาธิการ

(8) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนดวัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

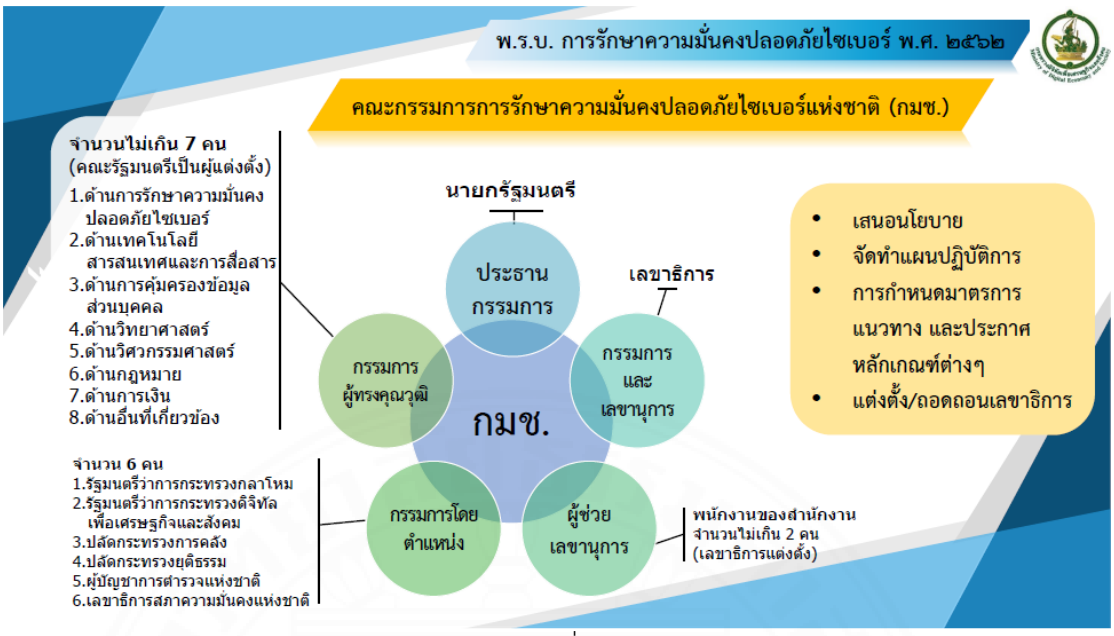
(9) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(10) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(11) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(12) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(13) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย



ภาพ 4.3 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

1) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

2) กรรมการโดยตำแหน่ง ได้แก่ ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงสาธารณสุข ผู้บัญชาการตำรวจแห่งชาติ ผู้บัญชาการทหารสูงสุด เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

3) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกิน 4 คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยกรรมการผู้ทรงคุณวุฒิมีวาระการดำรงตำแหน่งคราวละสี่ปี และได้รับการแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกิน 2 คน

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีหน้าที่และอำนาจตามที่กำหนดไว้ในมาตรา 13 ดังต่อไปนี้[3]

(1) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา 9 (1) และมาตรา 42

(2) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา 61 มาตรา 62 มาตรา 63 มาตรา 64 มาตรา 65 และมาตรา 66

(3) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(4) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(5) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(6) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการ

(7) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น

ในการกำหนดกรอบมาตรฐานตาม ข้อ (4) ให้คำนึงถึงหลักการบริหารความเสี่ยงโดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

---

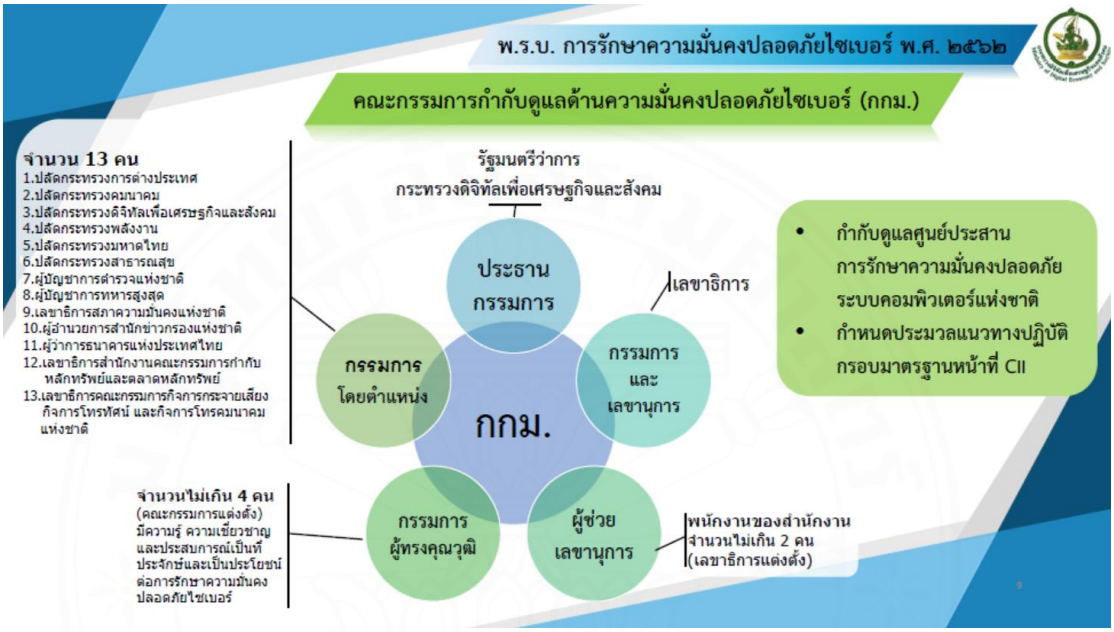
[3] สกมช., 'คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)' <https://www.ncsa.or.th/ncsc2.html> สืบค้นเมื่อ 18 เมษายน 2565.

(2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์



ภาพ 4.4 คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

1) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกิน 6 คน เป็นกรรมการ

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกิน 2 คน

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ มีหน้าที่และอำนาจ ตามที่กำหนดไว้ในมาตรา 27 ดังต่อไปนี้

(1) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน

(2) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน

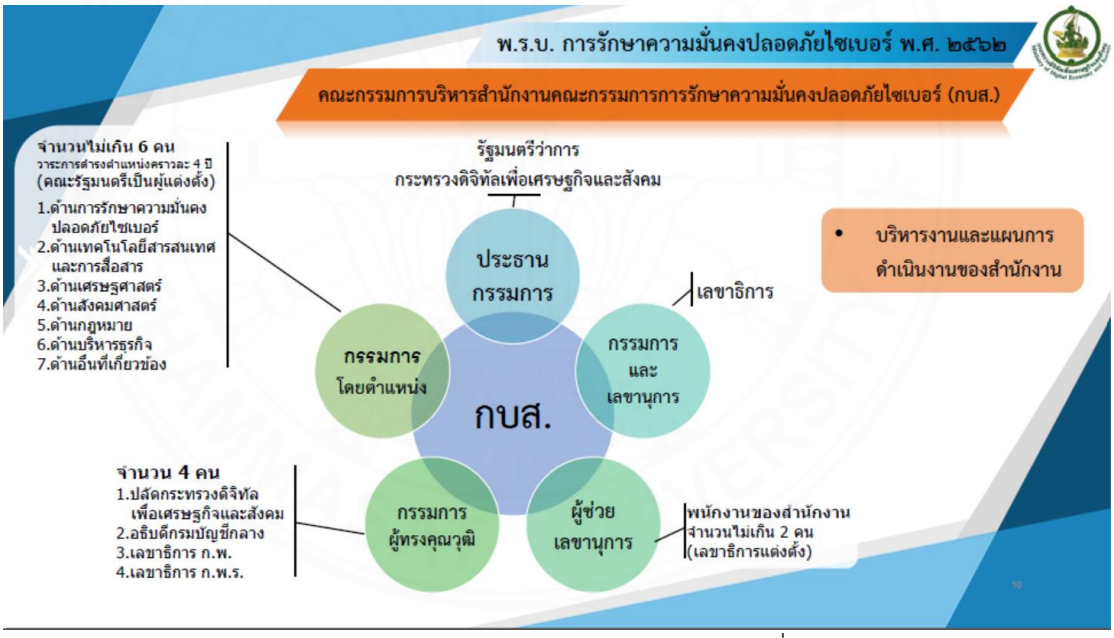
(3) อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน

(4) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง

(5) วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน

(6) ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ

(7) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของ กบส. หรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย



ภาพ 4.5 คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทำหน้าที่เป็นหน่วยธุรการของคณะกรรมการทั้ง 3 คณะ ปฏิบัติหน้าที่ส่งเสริม สนับสนุน งานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติการ ประสานงานเฝ้าระวัง แจ้งเตือน ให้ความช่วยเหลือ ตลอดจนจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน ศึกษาและวิจัยข้อมูลที่จำเป็น ดำเนินการอบรมและฝึกซ้อมการรับมือภัยคุกคามให้แก่หน่วยงานที่เกี่ยวข้อง และเจ้าหน้าที่ให้มีทักษะความเชี่ยวชาญ รวมถึงรายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

4.3.3 มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์

มาตรการสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกฎหมายฉบับนี้ได้แก่

1) นโยบายและแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) จัดทำเสนอต่อคณะรัฐมนตรีตามมาตรา 9 (1) (2) และ (3) และมาตรา 43 เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวม โดยสอดคล้องกับยุทธศาสตร์ชาติด้านความมั่นคง การป้องกันและแก้ไขปัญหาที่กระทบต่อความมั่นคง ซึ่งคณะกรรมการ กมช. ได้ออก “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)[4]” ประกาศในราชกิจจานุเบกษา เล่ม 139 ตอนพิเศษ 288 ง วันที่ 9 ธันวาคม 2565 และมีผลบังคับใช้ในวันถัดจากวันประกาศในราชกิจจานุเบกษา คือวันที่ 10 ธันวาคม 2565 โดยมีกรอบการดำเนินงานมุ่งเน้นไปในเรื่องของความมั่นคง เช่น การสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งในด้านบุคลากร องค์ความรู้ และเทคโนโลยี การบูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ การสร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ และการสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน

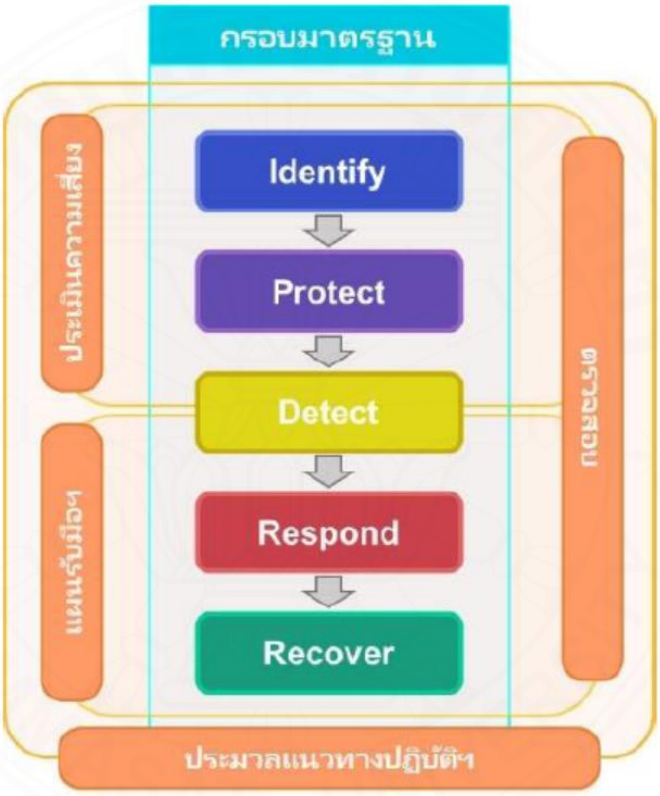
ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) ตามมาตรา 13 วรรคหนึ่ง (4) และวรรคสอง และมาตรา 54 เพื่อเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือภัยคุกคามทางไซเบอร์ ทั้งนี้ คณะกรรมการ กกม. ได้ออก “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษา

---

[4] ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)’ <https://ratchakitcha.soc.go.th/documents/17236495.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

ความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564[5]” ประกาศในราชกิจจานุเบกษา เล่ม 138 ตอนพิเศษ 208 ง วันที่ 6 กันยายน 2564 โดยให้มีผลบังคับใช้เมื่อพ้นกำหนดหนึ่งปีนับแต่วันประกาศในราชกิจจานุเบกษา คือ วันที่ 6 กันยายน 2565

ประมวลแนวทางฯ ดังกล่าว มีองค์ประกอบ 3 ประการ ได้แก่ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์



ภาพ 4.6 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ที่มา: คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

[5] ‘ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17176753.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

สำหรับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 5 หัวข้อหลัก ได้แก่ 1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) 2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) 3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) 4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) 5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

ทั้งนี้ มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว โดยใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานที่ออกโดยคณะกรรมการ กกม. เป็นแนวทางตัวอย่างในการจัดทำสำหรับหน่วยงานของตน และในกรณีที่หน่วยงานยังไม่มีประมวลฯ หรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้อง ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานฉบับของ กกม. ไปใช้บังคับ

2) การกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) โดยมาตรา 49 บัญญัติให้เป็นอำนาจของคณะกรรมการ กมช. ที่จะประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านต่าง ๆ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งกำหนดไว้ 7 ด้าน และด้านอื่น ๆ ที่อาจกำหนดเพิ่มเติมในภายหลัง

ภาพ 4.7 โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

คณะกรรมการ กมช. ได้ออก “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564[6]” ประกาศในราชกิจจานุเบกษา เล่ม 138 ตอนพิเศษ 194 ง วันที่ 23 สิงหาคม 2564 โดยมีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา คือวันที่ 24 สิงหาคม 2564 ประกาศฉบับดังกล่าวได้วางหลักเกณฑ์สำหรับหน่วยงานที่มีลักษณะหรือภารกิจหรือให้บริการในด้านต่าง ๆ ที่เข้าลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 7 หมวด โดยกำหนดลักษณะหน่วยงาน ภารกิจหรือการให้บริการ และหน่วยงานที่ควบคุมหรือกำกับดูแล ซึ่งปัจจุบันมี CII จำนวน 54 องค์กร แต่ไม่สามารถเปิดเผยรายชื่อได้ เพราะเกรงว่าจะเป็นเป้าหมายความท้าทายของแฮกเกอร์[7] เมื่อได้กำหนดหน่วยงานที่เป็น CII แล้ว ยังมีการกำหนดหน้าที่ของหน่วยงานที่เป็น CII ต้องแจ้งรายชื่อผู้ติดต่อประสานงานของหน่วยงาน และดำเนินการต่าง ๆ ให้เป็นไปตามมาตรฐานขั้นต่ำ มีการประเมินความเสี่ยง และซักซ้อมการรับมือภัยคุกคามทางไซเบอร์ รวมถึงต้องรายงานต่อสำนักงานคณะกรรมการ กมช. และหน่วยงานควบคุมหรือกำกับดูแล ในกรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น

3) การกำหนดระดับของภัยคุกคามทางไซเบอร์ ในมาตรา 60 ได้กำหนดภัยคุกคามทางไซเบอร์ออกเป็น 3 ระดับ ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ซึ่งการแบ่งระดับของภัยคุกคามนั้นเป็นการใช้ถ้อยคำที่ตีความได้อย่างกว้างขวาง เช่น ความมั่นคงของรัฐ ความสงบเรียบร้อยของประชาชน ประเทศตกอยู่ในภาวะคับขัน เป็นต้น โดยให้คณะกรรมการ กมช. ออกกฎหมายลำดับรองเพื่อกำหนดรายละเอียด โดย กมช. ได้ออก “ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564[8]” ประกาศใน

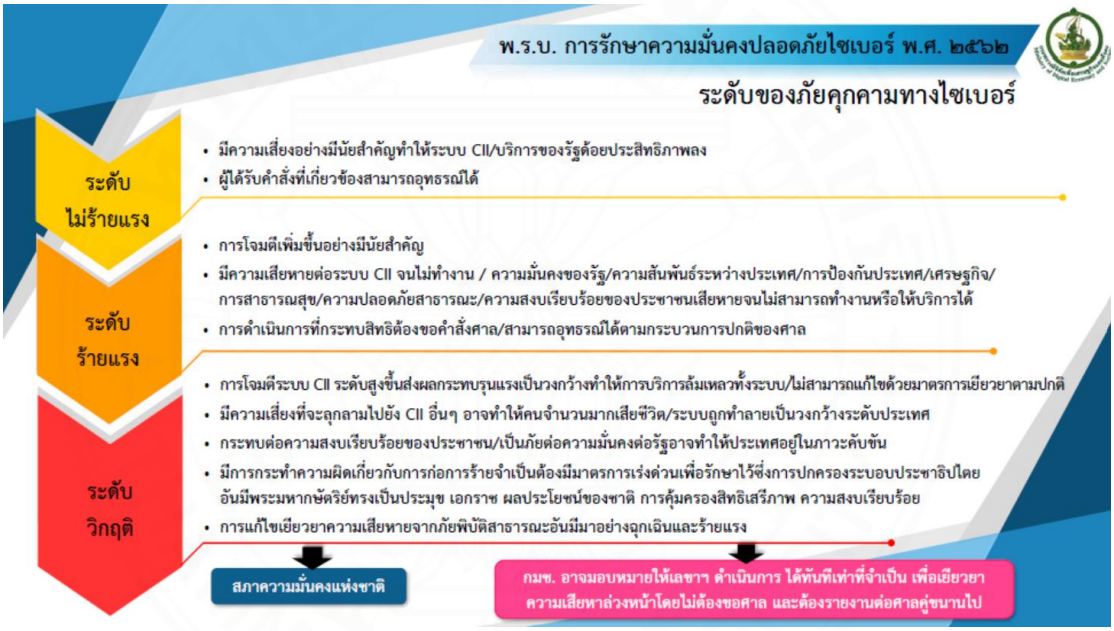
---

[6] ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17175301.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

[7] MGR Online, ‘สกมช.เร่งหน่วยงาน CII สร้างมาตรฐานขั้นต่ำป้องภัยไซเบอร์ ก่อนบังคับใช้ 6 ก.ย.นี้’ <https://mgronline.com/cyberbiz/detail/9650000064474> สืบค้นเมื่อ 25 กรกฎาคม 2565.

[8] ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์

ราชกิจจานุเบกษา เล่ม 138 ตอนพิเศษ 303 ง วันที่ 11 ธันวาคม 2564 โดยมีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา คือวันที่ 12 ธันวาคม 2564 ประกาศฉบับนี้แบ่งเป็น 2 ส่วน คือ ลักษณะและการประเมินภัยคุกคามทางไซเบอร์ในแต่ละระดับ โดยพิจารณาจากปัจจัยที่ใช้ในการประเมิน 4 ปัจจัย ได้แก่ ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน ลักษณะผลกระทบต่อข้อมูลในระบบ แนวโน้มในการกู้คืนระบบ และลักษณะผลกระทบต่อลูกค้าหรือผู้ให้บริการ แต่เมื่อพิจารณาแล้วพบว่ายังคงใช้ถ้อยคำลักษณะเดียวกับมาตรา 60 กล่าวคือมีคำที่สามารถตีความได้อย่างกว้างขวาง โดยเฉพาะในกรณีภัยคุกคามระดับวิกฤติ เช่น ส่งผลหรืออาจส่งผลกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ เป็นต้น



ภาพ 4.8 ระดับของภัยคุกคามทางไซเบอร์

ที่มา: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำหรับประกาศอีกส่วนหนึ่ง ว่าด้วยมาตรการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดยแบ่งขั้นตอนการดำเนินการออกเป็น 4 ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ได้แก่

แต่ละระดับ พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17190586.pdf> สืบค้นเมื่อ 25 กรกฎาคม 2565.

ขั้นตอนที่ 1 การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

ขั้นตอนที่ 3 การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

ขั้นตอนที่ 4 การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

4) การพิจารณาใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ จะแบ่งตามระดับความร้ายแรงของภัยคุกคาม หากเป็นภัยคุกคามในระดับร้ายแรงจะเป็นหน้าที่และอำนาจของคณะกรรมการ กกม. ในการดำเนินการ โดย กกม. มีอำนาจสั่งให้หน่วยงานของรัฐให้ข้อมูลสนับสนุน บุคลากรในสังกัดหรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามและดำเนินมาตรการที่จำเป็น อีกทั้งมีอำนาจออกคำสั่งให้บุคคลผู้เกี่ยวข้องหรือได้รับผลกระทบ ดำเนินการเฝ้าระวัง ตรวจสอบ ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์ รักษาสถานะของข้อมูล หรือในกรณีมีความจำเป็นต้องเข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดครองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เพื่อการตรวจสอบวิเคราะห์ กกม. ต้องยื่นคำร้องต่อศาล โดยระบุเหตุอันควรเชื่อได้ว่าบุคคลกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

สำหรับกรณีภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หน้าที่และอำนาจในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์จะเป็นของสภาความมั่นคงแห่งชาติตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง ตามที่กำหนดไว้ในมาตรา 67 นอกจากนี้มาตรา 68 กำหนดว่าหากเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติและมีเหตุจำเป็นเร่งด่วน คณะกรรมการ กมช. อาจมอบหมายให้เลขาธิการ สกมช. ดำเนินการได้ทันทีเพื่อป้องกันความเสียหาย โดยไม่ต้องยื่นคำร้องต่อศาล แต่ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบในภายหลัง

ทั้งนี้ มาตรา 69 บัญญัติว่า *“ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น”* กล่าวคือ หากเป็นคำสั่งอันเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและในระดับวิกฤติจะไม่สามารถอุทธรณ์คำสั่งได้ และต้องปฏิบัติตามเท่านั้น มิเช่นนั้นอาจมีโทษตามแต่กรณี

5) มีการกำหนดโทษสำหรับการฝ่าฝืนหรือไม่ปฏิบัติตามพระราชบัญญัติฉบับนี้ โดยมีโทษทางอาญาทั้งในส่วนที่เป็นโทษสำหรับพนักงานเจ้าหน้าที่ โทษสำหรับบุคคล และโทษสำหรับ

องค์กรและหน่วยงานที่มีหน้าที่ดูแลปกป้องระบบที่มีความสำคัญ หรือองค์กรที่เกี่ยวข้องที่จำเป็นต้องช่วยเหลือดูแลระบบ แต่ละเลยการปฏิบัติหน้าที่ หรือไม่ให้ความร่วมมือในกรณีที่มีภัยคุกคามในระดับร้ายแรง

กลุ่มความผิด	ผู้กระทำผิด	ฐานความผิด	บทกำหนดโทษ
ความรับผิดชอบของผู้ใช้อำนาจตามกฎหมาย	- พนักงานเจ้าหน้าที่ (ม.70)	- เปิดเผยหรือส่งมอบข้อมูลให้แก่บุคคลใด	- จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ
	(ม.71)	- กระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลที่ได้มาจากการปฏิบัติตามหน้าที่	- จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ
	- ผู้ใด (ม.72)	- ล่วงรู้ข้อมูลฯ ที่พนักงานเจ้าหน้าที่ได้มาแล้วนำไปเปิดเผยต่อผู้หนึ่งผู้ใด	- จำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ
ความผิดต่อหน้าที่ทั่วไป	- หน่วยงาน CII (ม.73)	- ไม่รายงานเหตุภัยคุกคามทางไซเบอร์โดยไม่มีเหตุอันสมควร	- ปรับไม่เกิน 200,000 บาท
ไม่ให้ความร่วมมือในการรวบรวมข้อมูล	- ผู้ใด (ม.74)	- ไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่ หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่โดยไม่มีเหตุอันสมควร	- ปรับไม่เกิน 100,000 บาท
ขัดขวางหรือไม่ให้ความร่วมมือในการรับมือภัยคุกคามในระดับร้ายแรง	- ผู้ใด (ม.75 วรรคหนึ่ง)	- ไม่เฝ้าระวัง/ไม่ตรวจสอบหาข้อบกพร่อง ที่กระทบต่อการรักษาความมั่นคงปลอดภัยตามคำสั่งของ กกม. โดยไม่มีเหตุอันสมควร	- ปรับไม่เกิน 300,000 บาท หากไม่ปฏิบัติตามคำสั่งที่ให้ปฏิบัติ ปรับเป็นรายวันอีกไม่เกินวันละ 10,000 บาท นับแต่วันที่ครบกำหนดตามคำสั่ง
	(ม.75 วรรคสอง)	- ไม่ดำเนินการแก้ไขภัยคุกคาม/ไม่รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามคำสั่งของ กกม.หรือไม่	- จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

กลุ่มความผิด	ผู้กระทำผิด	ฐานความผิด	บทกำหนดโทษ
	(ม.76)	ปฏิบัติตามคำสั่งศาลเพื่อเข้าถึงข้อมูลเท่าที่จำเป็น - ขัดขวาง ไม่ปฏิบัติตามคำสั่ง ของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติตามคำสั่งของ กกม. (ตรวจสอบสถานที่/เข้าถึงข้อมูล/ทดสอบการทำงาน/ยึดหรืออายัดเพื่อตรวจวิเคราะห์) โดยไม่มีเหตุอันสมควร	- จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ
	นิติบุคคล (ม.77)	ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย	

ตาราง 4.1 สรุปบทกำหนดโทษของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

4.4 ปัญหาบทบัญญัติของกฎหมายที่อาจกระทบต่อสิทธิมนุษยชน

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่รัฐตราขึ้น เพื่อใช้รักษาความมั่นคงปลอดภัยให้แก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งหากประสบกับภัยคุกคามจะทำให้ประชาชนที่ต้องพึ่งพิงระบบโครงสร้างพื้นฐานต่าง ๆ ได้รับความเดือดร้อน จึงตรากฎหมายในลักษณะเป็นกรอบกว้าง ๆ สำหรับให้เจ้าหน้าที่ได้ใช้ดุลพินิจอย่างยืดหยุ่น ในการแก้ไขสถานการณ์แต่ละครั้งที่เกิดขึ้นโดยอันมีรายละเอียดของเหตุการณ์ที่แตกต่างกัน แต่อย่างไรก็ตาม การบังคับใช้กฎหมายโดยให้ดุลพินิจอย่างกว้างขวางแก่เจ้าหน้าที่อาจเป็นดาบสองคม จึงเกิดข้อกังวลจากผู้สนับสนุนด้านสิทธิมนุษยชนและองค์กรต่าง ๆ ซึ่งเน้นย้ำถึงความสำคัญของการสร้างสมดุลระหว่างความต้องการด้านความมั่นคงปลอดภัยในโลกไซเบอร์และการคุ้มครองสิทธิขั้นพื้นฐาน ซึ่งการสร้างสมดุลระหว่างมาตรการรักษาความปลอดภัยทางไซเบอร์และการปกป้องสิทธิมนุษยชนอาจเป็นงานที่ซับซ้อน แม้ว่าการจัดการกับภัยคุกคามความปลอดภัยทางไซเบอร์จะมีความสำคัญ แต่ก็ไม่ควรทำให้สิทธิส่วนบุคคล เสรีภาพในการแสดงออก และสิทธิมนุษยชนอื่น ๆ สูญเสียไป สิ่งสำคัญสำหรับรัฐคือ

ต้องแน่ใจว่ากฎหมายความมั่นคงปลอดภัยทางไซเบอร์ ได้รับการตราขึ้นและนำไปบังคับใช้ในลักษณะที่สนับสนุนและเคารพมาตรฐานสิทธิมนุษยชน รวมถึงการป้องกันที่แข็งแกร่ง กลไกการกำกับดูแลที่เป็นอิสระ และกระบวนการที่โปร่งใสเพื่อป้องกันการใช้อำนาจในทางที่ผิด ซึ่งพระราชบัญญัติฉบับนี้อาจกระทบต่อสิทธิมนุษยชนด้านต่าง ๆ ดังที่ได้จำแนกไว้ในบทที่ 2 ดังนี้

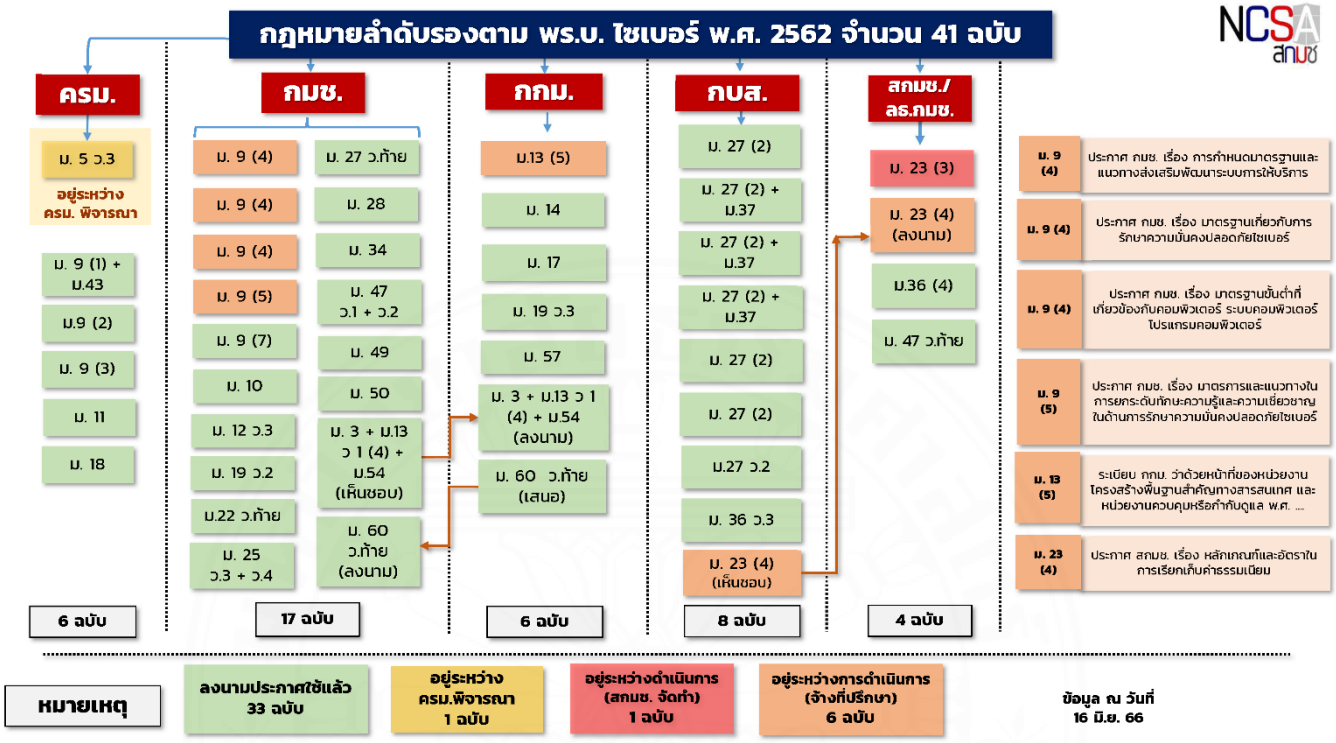
4.4.1 สิทธิในความเป็นส่วนตัว (Right to Privacy) และเสรีภาพในการแสดงออก (Freedom of Expression) เนื่องจากขอบเขตการบังคับใช้และนิยามของคำสำคัญกว้างขวางเกินไป ขาดความชัดเจน อาจเกิดการตีความที่ไม่ตรงกัน โดยในมาตรา 3 บัญญัติว่า

""การรักษาความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ"

ขอบเขตที่กว้างขวางของคำว่า "ความมั่นคงของรัฐ" "ความมั่นคงทางเศรษฐกิจ" "ความมั่นคงทางทหาร" และ "ความสงบเรียบร้อยภายในประเทศ" ไม่มีการให้นิยามอย่างชัดเจน ทำให้เกิดช่องว่างในการตีความมากเกินไป เขตอำนาจของกฎหมายฉบับนี้ คำสำคัญที่ให้นิยามเพื่อการบังคับใช้กฎหมาย วิธีการบังคับใช้ และอีกหลายส่วนของกฎหมายมีเนื้อหากว้างขวางไม่คำนึงถึงสัดส่วนความสมดุลกับสิทธิมนุษยชน สิทธิส่วนบุคคล หรือมาตรฐานระหว่างประเทศ ทำให้เห็นว่าผู้ร่างกฎหมายมุ่งเน้นให้ความมั่นคงปลอดภัยทางไซเบอร์ในกฎหมายฉบับนี้ ให้ความสำคัญกับผลกระทบที่เกิดต่อการดำเนินงานของรัฐและเสถียรภาพของรัฐเป็นหลัก โดยไม่ได้ให้ความสำคัญกับความปลอดภัยและสิทธิของบุคคล นอกจากนี้ในกรณีของ "ความมั่นคงของรัฐ" อาจถูกนำไปตีความและบังคับโดยมิชอบ นำไปสู่การละเมิดสิทธิมนุษยชนได้ และกระบวนการดำเนินมาตรการต่าง ๆ ไม่ได้ให้รายละเอียดที่ชัดเจนไว้ในพระราชบัญญัติฉบับนี้ แต่ต้องพิจารณาจากกฎหมายลำดับรองอีกหลายฉบับซึ่งให้อำนาจแก่คณะกรรมการต่าง ๆ ที่พระราชบัญญัติฉบับนี้ตั้งขึ้นเป็นผู้กำหนด อันหมายความว่ารายละเอียดของการดำเนินการต่าง ๆ เหล่านั้น จะเป็นกฎหมายที่ไม่ต้องผ่านการพิจารณาของรัฐสภา โดยพระราชบัญญัติเป็นเพียงกรอบที่กว้างขวางและให้อำนาจแก่คณะกรรมการต่าง ๆ ในการกำหนดรายละเอียดโดยอาจขาดการตรวจสอบถ่วงดุล ซึ่งจนถึงปัจจุบันมีกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562[9] ที่ดำเนินการแล้วเสร็จ จำนวน 33 ฉบับ

[9] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 'รายงานผลการจัดทำกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562' (การประชุมคณะรัฐมนตรี, 18 กรกฎาคม 2566) 1.

อยู่ระหว่างดำเนินการ 7 ฉบับ และอยู่ระหว่างเสนอคณะรัฐมนตรีเพื่อพิจารณามีมติเห็นชอบ 1 ฉบับ รวมกฎหมายลำดับรองทั้งสิ้น 41 ฉบับ[10]



ภาพ 4.9 กฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
ที่มา: สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีการให้อำนาจอย่างกว้างขวางกับหน่วยงานของรัฐ ซึ่งคณะกรรมการ กมช. สามารถใช้ดุลพินิจเพื่อจำแนกว่าหน่วยงานใดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งส่งผลให้หน่วยงานเหล่านั้นถูกควบคุมอย่างเข้มงวดโดยหน่วยงานกำกับดูแลของรัฐที่ได้รับมอบหมาย และอาจมีการนำบทบัญญัตินี้ไปใช้อย่างขัดต่อหลักประชาธิปไตย เช่น บังคับใช้กับหน่วยงานซึ่งรัฐมองว่าเป็นภัยคุกคามต่อการรักษาอำนาจของตน ดังนั้นการกำหนดหน่วยงานที่เป็น CII ควรมีการรับฟังความเห็นจากผู้มีส่วนได้ส่วนเสียเกี่ยวกับหลักเกณฑ์การจำแนกประเภทของหน่วยงาน ให้มีโอกาสมีส่วนร่วมอย่างอิสระเพื่อทบทวนหลักเกณฑ์เหล่านี้

ปัญหาสำคัญอีกประการหนึ่งคือการแทรกแซงอย่างกว้างขวางของรัฐ ซึ่งกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการรายงานภัยคุกคาม

[10] รายชื่อกฎหมายลำดับรอง โปรดดู ภาคผนวก ก.

ทางไซเบอร์ให้หน่วยงานของรัฐทราบทุกครั้ง จึงเป็นปัญหาสำหรับภาคเอกชนที่จะต้องคอยติดตามและรายงานเมื่อเกิดภัยคุกคาม ทว่าสถานการณ์ของภัยคุกคามที่เปลี่ยนแปลงไป ข้อมูลที่ส่งให้แก่รัฐอาจเป็นข้อมูลลับ หรือในบางกรณีอาจไม่สามารถจำแนกได้ว่าสถานการณ์ใดถือเป็นภัยคุกคามจนกระทั่งเกิดการโจมตีทางไซเบอร์ขึ้นแล้ว การรายงานมากเกินความจำเป็น รวมถึงการรายงานที่ไม่มีความเสี่ยงที่พิสูจน์ได้ อาจส่งผลให้หน่วยงานนั้น ๆ ไม่สามารถดำเนินงานอย่างเหมาะสมเมื่อเกิดภัยคุกคามที่แท้จริงขึ้น แต่เพื่อหลีกเลี่ยงการได้รับโทษทางอาญาจากการไม่รายงาน อาจทำให้หน่วยงานเอกชนตัดสินใจผิดพลาด ยอมสูญเสียความเป็นส่วนตัว ตลอดจนสิทธิมนุษยชนของตนและผู้รับบริการ

นอกจากนี้ บทบัญญัติที่สำคัญไม่มีความชัดเจน ในเรื่องการแบ่งระดับภัยคุกคามทางไซเบอร์ 3 ระดับ ตามมาตรา 60 ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ ซึ่งการจำแนกความเสี่ยงที่จะเกิดภัยคุกคามมีทั้งในลักษณะที่เป็นเชิงรุก และเชิงรับ ทั้งนี้เพื่อให้สามารถป้องกันก่อนที่จะสร้างความเสียหายให้กับประเทศและโครงสร้างพื้นฐานสำคัญได้ โดยรวมถึงภัยคุกคามที่แท้จริงหรือภัยคุกคามที่พิสูจน์ได้ ภัยคุกคามที่เกิดขึ้นหรือสิ่งที่อาจเป็นภัยคุกคามและภัยคุกคามเท็จ กรณีภัยคุกคามในระดับวิกฤติ เป็นกรณีที่มีความเสี่ยงอย่างแท้จริงที่จะเกิดภัยคุกคาม หรือได้มีการจำแนกว่าได้เกิดภัยคุกคามขึ้นแล้ว หรือกรณีภัยคุกคามระดับร้ายแรงเป็นกรณีที่จำแนกว่าได้เกิดภัยคุกคามแท้จริงขึ้น อันมีเป้าหมายเพื่อโจมตีหรือมีเจตนาที่ชัดเจนและก่อให้เกิดผลกระทบที่เป็นรูปธรรม มีความเสียหายเกิดขึ้นกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แต่ภัยคุกคามเท็จ อาจเกิดได้กับภัยคุกคามทั้ง 3 ระดับ เนื่องจากอำนาจในการจำแนกระดับภัยคุกคามเป็นของคณะกรรมการ กมช. มาตรการเพื่อการรับมือภัยคุกคามทางไซเบอร์จึงไม่ควรส่งผลให้ต้องทำลายหลักประกันเพื่อคุ้มครองสิทธิของบุคคล โดยเฉพาะภัยคุกคามในระดับวิกฤติ ซึ่งกฎหมายให้เป็นอำนาจของสภาความมั่นคงแห่งชาติ ที่จะสามารถใช้ดุลพินิจในการประกาศให้หน่วยงานของรัฐดำเนินการใด ๆ ก็ได้เพื่อแก้ไขสถานการณ์ภัยคุกคาม โดยที่ไม่สามารถคาดเดาได้ว่าจะเกิดผลกระทบต่อสิทธิความเป็นส่วนตัว ตลอดจนเสรีภาพในการแสดงความคิดเห็นมากน้อยเพียงใด จึงควรมีบทบัญญัติที่ให้ความคุ้มครองสิทธิมนุษยชน ที่สอดคล้องกับรัฐธรรมนูญและมาตรฐานสิทธิมนุษยชนระหว่างประเทศที่เกี่ยวข้อง

ต้องมีการคุ้มครองสิทธิความเป็นส่วนตัวของบุคคลในการดำเนินการตามมาตรา 65 และมาตรา 66 ในแง่ของความเสียหายที่เกิดขึ้นระหว่างการดำเนินการเพื่อป้องกัน รับมือหรือลดผลกระทบจากภัยคุกคามในระดับร้ายแรง กรณีเจ้าพนักงานต้องเข้าถึงคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เพื่อให้ได้มาและเพื่อทำสำเนาข้อมูล จึงต้องมีการแจ้งให้บุคคลที่ได้รับผลกระทบจากการเก็บข้อมูลนี้ทราบ และต้องมีมาตรการควบคุมที่เคร่งครัดในการแง่ของการนำข้อมูลไปใช้เพื่อเป็นหลักประกันในการคุ้มครองข้อมูลส่วนบุคคลทุกประการ

การใช้คำว่า “ภัยคุกคามที่อาจเกิดขึ้น” ไม่มีมาตรฐานการพิสูจน์เพื่อจำแนกโอกาสที่จะเกิดภัยคุกคามอย่างแท้จริง ไม่มีการขยายความที่เหมาะสมที่จะใช้จำแนกความร้ายแรงของ “ภัยคุกคามที่อาจเกิดขึ้น” ควรสร้างมาตรฐานในการจำแนกระดับภัยคุกคามโดยใช้ “หลักฐานที่เชื่อได้ว่าอาจมีความเสี่ยงที่จะเกิดภัยคุกคามที่ส่งผลสอดคล้องกับการจำแนกภัยคุกคามในระดับต่าง ๆ”

4.4.2 สิทธิในการเข้าถึงข้อมูลและความเหลื่อมล้ำทางดิจิทัล (Right of Access to Information and Digital Divide) และสิทธิในการศึกษา (Right to Education) สิทธิทั้งสองประการที่อาจถูกกระทบจากพระราชบัญญัติฉบับนี้ เป็นสิทธิเกี่ยวเนื่องกัน ในกรณีที่เกิดภัยคุกคามตามที่ระบุในมาตรา 60 หน่วยงานรัฐจะต้องดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 โดยแนวปฏิบัติพื้นฐาน (Security Control Baselines) สำหรับการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)[11] ระบุว่า

“(1) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง

(1.1) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ...”

ซึ่งมาตรการเหล่านี้หากถูกนำมาใช้โดยไม่ได้สัดส่วน หรือใช้ดุลพินิจอย่างไม่ระมัดระวัง อาจส่งผลให้เกิดการจำกัดการไหลเวียนของข้อมูลอย่างเสรี ขัดขวางการเข้าถึงข้อมูลและโอกาส ตลอดจนอาจลดการเข้าถึงทรัพยากรทางการศึกษาได้

4.4.3 กระบวนการอันชอบธรรมและหลักนิติธรรม (Due Process and Rule of Law) พระราชบัญญัติฉบับนี้มีปัญหากลไกการควบคุมโดยหน่วยงานและองค์กรของรัฐ ที่ให้อำนาจอย่างกว้างขวาง ขาดความโปร่งใสและมาตรฐาน พระราชบัญญัติฉบับนี้ควรนำไปสู่สภาพแวดล้อมดิจิทัลที่สร้างความไว้วางใจให้แก่ประชาชนและภาคธุรกิจ ที่จะได้รับบริการที่ปลอดภัยผ่านหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งข้อท้าทายสำคัญสำหรับคณะกรรมการคณะต่าง ๆ ที่ได้รับการแต่งตั้งขึ้นตามกฎหมายฉบับนี้คือ แม้ว่าบุคลากรในคณะกรรมการ กมช. และ กกม. จะมีทักษะความเชี่ยวชาญ แต่เป็นความเชี่ยวชาญในการทำงานระดับสูง โดยอาจขาดความเข้าใจ

---

[11] เพิ่งอ้าง 13.

หรือไม่สามารถเป็นตัวแทนมุมมองของภาคประชาชนและภาคประชาสังคมที่ได้รับผลกระทบได้ ดังนั้น การกำหนดนโยบาย ประมวลแนวทางปฏิบัติและกรอบมาตรการต่าง ๆ มักเกิดขึ้นเพื่อประโยชน์ของรัฐเป็นหลัก โดยขาดการรับฟังความเห็นของภาคส่วนต่าง ๆ อย่างรอบด้าน เพื่อประกันให้มีการตรวจสอบได้ นอกจากนี้หากมีการตีความอย่างมิชอบของผู้มีอำนาจในการวางหลักเกณฑ์ระเบียบ ประกาศต่าง ๆ อาจก่อให้เกิดการกระทบต่อสิทธิขั้นพื้นฐานของประชาชนได้ นอกจากนี้ควรมีหลักประกันความเป็นธรรมในขั้นตอนการปฏิบัติ เช่น มีการแจ้งให้ผู้ใช้งานทราบถึงความเสี่ยง หากมีการเข้าถึงข้อมูลส่วนบุคคล ต้องปฏิบัติตามกระบวนการอันควรตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อดำเนินงานเฉพาะเท่าที่จำเป็นและได้สัดส่วนตามเป้าหมายที่ชอบธรรม ประกันว่าเป็นการดำเนินการเพื่อรับมือเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ที่ผ่านการจำแนกตามหลักเกณฑ์และการประเมินที่ชัดเจน ไม่ควรมีการบังคับจนเกิดการละเมิดสิทธิ และให้ความสำคัญกับผู้มีส่วนได้ส่วนเสียทุกกลุ่ม ทบทวนความชอบด้วยกฎหมายในระหว่างปฏิบัติหน้าที่อยู่เสมอ

นอกจากนี้ยังมีช่องว่างของการตรวจสอบถ่วงดุล พระราชบัญญัติฉบับนี้ขาดการตรวจสอบถ่วงดุลที่เข้มแข็ง ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง และระดับร้ายแรงจำเป็นต้องยื่นคำร้องต่อศาลเพื่อใช้อำนาจดำเนินการตามมาตรา 65 แต่ในกรณีเกิดภัยคุกคามระดับวิกฤติ กระบวนการรับมือที่มีอยู่ ไม่อยู่ภายใต้การตรวจสอบถ่วงดุลใด ๆ ทำให้ขาดการตรวจสอบได้และความโปร่งใส ขาดกลไกการติดตามผลหรือกำกับดูแลที่น่าเชื่อถือหรือเป็นอิสระ การรักษาความมั่นคงของพื้นที่ไซเบอร์โดยใช้กฎหมายความมั่นคง คือการให้ความสำคัญกับความมั่นคงของรัฐเหนือสิทธิส่วนบุคคล ไม่มีความโปร่งใสในแง่การรายงานข้อมูลต่อสาธารณะและการเข้าถึงได้

อีกทั้ง พระราชบัญญัตินี้ยังขาดบทบัญญัติที่ประกันให้มีการเยียวยากรณีได้รับความเสียหายจากการบังคับใช้กฎหมาย พระราชบัญญัติฉบับนี้ไม่กำหนดให้มีการเยียวยากรณีที่หน่วยงานกำกับดูแล คำสั่งของคณะกรรมการต่าง ๆ การดำเนินงานของเลขาธิการฯ ละเมิดสิทธิของบุคคลหรือองค์กร เนื่องจากขาดกลไกการตรวจสอบอย่างสิ้นเชิง

กรณีที่พนักงานเจ้าหน้าที่และบุคคลกระทำความผิดและมีโทษตามมาตรา 70 71 และ 72 แต่ผู้ได้รับผลกระทบจะไม่สามารถเข้าถึงการเยียวยา ไม่มีบทบัญญัติให้ได้รับการชดเชยความเสียหายที่เป็นธรรม สอดคล้องกับความเสียหายที่เกิดขึ้น

ในกรณีภัยคุกคามระดับร้ายแรง หรือระดับวิกฤติ ผู้ได้รับคำสั่งไม่สามารถอุทธรณ์คำสั่งได้ หากคำสั่งนั้นเป็นคำสั่งที่ทำให้เกิดการละเมิดสิทธิมนุษยชน ก็ไม่มีช่องทางให้ผู้ได้รับผลกระทบเข้าถึงการเยียวยาใด ๆ หากการประเมินเพื่อจำแนกระดับภัยคุกคามเกิดความผิดพลาดขึ้นจากการขาดกลไกการตรวจสอบ นั่นหมายถึงผู้ได้รับผลกระทบจะได้รับความไม่เป็นธรรมถึงสองชั้น

4.4.4 การเลือกปฏิบัติทางไซเบอร์ (Cyber Discrimination) ข้อกังวลในประเด็นนี้เนื่องจาก เมื่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นถูกจัดให้เป็นภัยคุกคามในระดับวิกฤติ การดำเนินมาตรการรับมือจะเข้าสู่อำนาจของพระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. 2559 ซึ่งมาตรา 19 วรรคแรก ระบุว่า

“มาตรา 19 ในกรณีที่มีสถานการณ์อันเป็นภัยคุกคามต่อความมั่นคงแห่งชาติ ให้สภาประกาศระดับความร้ายแรงของภัยคุกคามดังกล่าว พร้อมทั้งเสนอความเห็น แนวทาง มาตรการ หรือการดำเนินการอื่นที่จำเป็นต่อนายกรัฐมนตรีหรือคณะรัฐมนตรีเพื่อพิจารณาอนุมัติหรือสั่งการให้หน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐดำเนินการตามอำนาจหน้าที่ตามที่บัญญัติไว้ในกฎหมายเพื่อป้องกัน แก้ไข หรือระงับยับยั้งภัยคุกคามดังกล่าว”

ซึ่งการเฝ้าระวังในวงกว้างอาจกำหนดเป้าหมายไปยังบางกลุ่ม รัฐต้องตรวจสอบให้แน่ใจว่ามาตรการรับมือเหตุการณ์ภัยคุกคามนั้นไม่เลือกปฏิบัติ และมีพื้นฐานมาจากการประเมินความเสี่ยงตามหลักฐานที่เชื่อถือได้

4.5 เปรียบเทียบกฎหมายไทยกับบรรทัดฐานระหว่างประเทศและกฎหมายต่างประเทศ

กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์เป็นเครื่องมือสำคัญในการต่อสู้กับภัยคุกคามทางไซเบอร์ ปกป้องข้อมูลที่ละเอียดอ่อน และประกันความปลอดภัยของโครงสร้างพื้นฐานที่สำคัญ องค์การระหว่างประเทศตลอดจนประเทศต่าง ๆ ได้นำแนวทางที่แตกต่างกันไปใช้ในการกำกับดูแลความปลอดภัยทางไซเบอร์ ซึ่งสะท้อนถึงลำดับความสำคัญและข้อพิจารณาของแต่ละประเทศที่แตกต่างกัน ในขณะที่ภูมิทัศน์ทางดิจิทัลมีการพัฒนาอย่างต่อเนื่อง จึงเป็นเรื่องสำคัญที่รัฐบาลจะต้องปรับกฎหมายความปลอดภัยทางไซเบอร์เพื่อจัดการกับภัยคุกคามที่เกิดขึ้นใหม่และความก้าวหน้าทางเทคโนโลยี การอัปเดตอย่างสม่ำเสมอ ความร่วมมือระหว่างประเทศ และความร่วมมือระหว่างภาครัฐและเอกชนเป็นองค์ประกอบหลักในการสร้างกรอบความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ ซึ่งช่วยปกป้องทรัพย์สินทางดิจิทัลของประเทศต่าง ๆ ได้อย่างมีประสิทธิภาพและดำรงไว้ซึ่งสิทธิมนุษยชน รักษาความเป็นส่วนตัวและความปลอดภัยของปัจเจกบุคคล

เมื่อเปรียบเทียบกฎหมายไทยกับแนวบรรทัดฐานระหว่างประเทศและกฎหมายต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่ามีทั้งส่วนที่คล้ายคลึงกันและส่วนที่แตกต่างกัน ได้แก่

4.5.1 วัตถุประสงค์ของกฎหมาย กฎหมายของประเทศไทย และสิงคโปร์ มีความใกล้เคียงกันในเรื่องการมุ่งเน้นปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับประเทศจีนมีการขยายขอบเขตไปถึงการควบคุมการใช้อินเทอร์เน็ตด้วย โดยกฎหมายของทั้งไทย จีน และสิงคโปร์ มีลักษณะเป็นการบังคับให้ต้องปฏิบัติตามบทบัญญัติในกฎหมาย หากไม่ปฏิบัติตามจะมีความผิดและมีโทษแล้วแต่กรณี ในขณะที่กฎหมายของสหรัฐอเมริกา เป็นการสร้างระบบสมัครใจสำหรับการแบ่งปันข้อมูลตัวบ่งชี้ภัยคุกคามทางไซเบอร์ระหว่างหน่วยงานของรัฐและเอกชน สำหรับแนวบรรทัดฐานของสหประชาชาติ และอาเซียน เป็นแนวบรรทัดฐานที่ไม่มีสภาพบังคับ เน้นให้เกิดระบบสมัครใจที่ประเทศต่าง ๆ จะปฏิบัติร่วมกันซึ่งหากสามารถทำให้เกิดการยอมรับ นำไปปฏิบัติอย่างกว้างขวางและต่อเนื่อง อาจพัฒนาไปสู่การเป็นกฎหมายจารีตประเพณีได้ในอนาคต สำหรับสหภาพยุโรปเป็นกฎและระเบียบที่มุ่งเน้นการสร้างขีดความสามารถของประเทศสมาชิกและเพิ่มความร่วมมือระหว่างกันเพื่อให้เกิดการดำเนินการที่มีมาตรฐานเดียวกันทั่วทั้งภูมิภาค

4.5.2 หน่วยงานหรือองค์กรหลักที่ทำหน้าที่ภายใต้กฎหมาย สำหรับสหประชาชาติและอาเซียนไม่ได้มีหน่วยงานเพื่อกำกับดูแลการปฏิบัติตามแนวบรรทัดฐาน แต่ในการประชุมในระดับต่าง ๆ อาจมีการติดตามความคืบหน้าในการปฏิบัติหรือการดำเนินการของรัฐสมาชิกว่าได้นำเอาบรรทัดฐานต่าง ๆ ไปใช้มากน้อยเพียงใด เพื่อพัฒนาบรรทัดฐาน คำแนะนำ หรือแนวปฏิบัติให้เป็นที่ยอมรับอย่างกว้างขวางมากขึ้นต่อไป สำหรับสหภาพยุโรปมีกลไกของการบังคับใช้กฎหมายของสหภาพยุโรปซึ่งแตกต่างจากองค์การระหว่างประเทศของภูมิภาคอื่น ๆ อยู่แล้ว ดังนั้นเมื่อสหภาพยุโรปออกกฎหรือข้อบังคับที่มีผลต่อทุกประเทศสมาชิก ทุกประเทศก็จะต้องดำเนินการให้เป็นไปตามกฎหมายของสหภาพยุโรปด้วย และมี ENISA เป็นหน่วยงานหลักในการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์ สำหรับกฎหมายของประเทศสหรัฐอเมริกา หน่วยงานที่ทำหน้าที่หลักเป็นหน่วยงานที่มีอยู่เดิม เช่น กระทรวงความมั่นคงแห่งมาตุภูมิ กระทรวงกลาโหม สำนักงานข่าวกรองแห่งชาติ เป็นต้น ในขณะที่กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีน สิงคโปร์ และไทย มีการตั้งหน่วยงาน หรือคณะกรรมการขึ้นใหม่ โดยจีนมี สำนักงานบริหารไซเบอร์สเปซ หรือ CAC เป็นหน่วยงานหลักในการดำเนินงานด้านการรักษาความปลอดภัยทางไซเบอร์ ประเทศสิงคโปร์ มีการแต่งตั้งผู้บัญชาการความปลอดภัยทางไซเบอร์ และหน่วยงานความมั่นคงไซเบอร์ หรือ CSA เพื่อกำกับดูแลและดำเนินงานด้านความมั่นคงไซเบอร์ โดยให้ขึ้นตรงต่อสำนักนายกรัฐมนตรี และประเทศไทย มีการตั้งคณะกรรมการขึ้น 3 ชุด ได้แก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ กบส. นอกจากนี้ยังตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะ

เป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

ทั้งนี้ หน่วยงานของสิงคโปร์และของไทยมีหน้าที่และอำนาจที่คล้ายคลึงกัน กล่าวคือ กำหนดหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดหน้าที่ให้แก่หน่วยงานเหล่านั้น ตลอดจนหน่วยงานกำกับดูแล รวมถึงการวางแนวปฏิบัติและมาตรฐานต่าง ๆ

4.5.3 มาตรการที่สำคัญในการใช้รักษาความมั่นคงปลอดภัยทางไซเบอร์

ในแนวบรรทัดฐานของสหประชาชาติ และตราสารฉบับต่าง ๆ ของอาเซียนนั้น ไม่ได้มีมาตรการที่มุ่งเน้นในเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยเฉพาะ แต่เป็นบรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ เพื่อให้เกิดสันติภาพและความมั่นคงระหว่างประเทศ โดยมุ่งไปที่บทบาทของรัฐสมาชิกที่จะไม่กลายเป็นผู้ก่อให้เกิดภัยคุกคามทางไซเบอร์ หรือเป็นผู้สนับสนุนกิจกรรมที่เป็นอันตราย และการให้ความร่วมมือในการป้องกัน รับมือ ภัยคุกคาม รวมถึงการให้ความช่วยเหลือรัฐสมาชิกอื่น ๆ สำหรับสหภาพยุโรปมุ่งเน้นไปที่มาตรการเพื่อสร้างขีดความสามารถของรัฐสมาชิก และการสร้างระบบรับรองที่เป็นมาตรฐานเดียวกันทั่วภูมิภาค โดยการเปิดโอกาสให้รัฐสมาชิกนำเสนอแนวคิดใหม่ ๆ การทบทวนร่วมกัน และการแบ่งปันความรู้ระหว่างประเทศสมาชิก

มาตรการสำคัญของกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา คือการแบ่งปันข้อมูล โดยเน้นระบบสมัครใจ ไม่ได้กำหนดเป็นหน้าที่ ซึ่งอาศัยการทำความเข้าใจกับเอกชนถึงความสำคัญในการให้ความร่วมมือ เพื่อสามารถนำข้อมูลไปประมวลผลสำหรับใช้แก้ปัญหาได้อย่างทันท่วงทีและแม่นยำ ในขณะที่กฎหมายของจีนมีบทบัญญัติที่ค่อนข้างเข้มงวดและมีการเปิดช่องให้หน่วยงานที่ทำหน้าที่หลัก คือ CAC กำหนดกฎหมายเพิ่มเติมได้ ลักษณะเดียวกับการให้อำนาจคณะกรรมการต่าง ๆ ในกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของไทยสามารถใช้อำนาจและดุลพินิจกำหนดรายละเอียด และหลักเกณฑ์ในเรื่องต่าง ๆ ได้ แต่แตกต่างกันในเรื่องการแบ่งระดับความเสียหายของจีน ใช้ระบบการคุ้มครองหลายลำดับชั้น หรือ MLPS ซึ่งแบ่งเป็น 5 ระดับ ในขณะที่ประเทศไทยแบ่งระดับภัยคุกคามออกเป็น 3 ระดับ ส่วนประเทศสิงคโปร์มีการกำหนดอำนาจในการสอบสวนและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ใน 2 ระดับ คือ เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ในมาตรา 19 และเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์อย่างร้ายแรง ในมาตรา 20 ทั้งนี้ ทั้งประเทศจีน ไทย และสิงคโปร์ ต่างให้ความสำคัญกับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศเช่นเดียวกัน โดยมีการกำหนดมาตรฐานและหน้าที่ให้ผู้รับผิดชอบหน่วยงานเหล่านั้นต้องปฏิบัติตาม

สำหรับการกำหนดโทษผู้ที่ฝ่าฝืนหรือละเมิดกฎหมาย ในสหรัฐอเมริกากฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ เป็นการสร้างระบบสมัครใจในการแบ่งปันข้อมูลเป็นหลัก จึงไม่มี

บทกำหนดโทษในกฎหมาย ในขณะที่กฎหมายของจีน สิงคโปร์ และไทย มีการกำหนดโทษ โดยโทษในกฎหมายจีนจะเน้นไปที่โทษปรับมากกว่าโทษจำคุก แต่สิงคโปร์และไทย มีทั้งโทษจำคุกและโทษปรับ ซึ่งโทษจำคุกของสิงคโปร์ในบางฐานความผิดมีโทษสูงถึง 10 ปี เช่น การไม่ปฏิบัติตามมาตรการที่รัฐมนตรีสั่งโดยมีวัตถุประสงค์เพื่อป้องกัน ตรวจจับ หรือตอบโต้ ในกรณีเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างร้ายแรง ที่กระทบต่อการบริการพื้นฐาน หรือความมั่นคงของชาติ การป้องกันประเทศ ความสัมพันธ์ระหว่างประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของสิงคโปร์ ตามมาตรา 23

4.5.4 มิติด้านสิทธิมนุษยชนในกฎหมาย

บรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ ของสหประชาชาติ ข้อ 5 เน้นย้ำให้รัฐเคารพข้อมติคณะมนตรีสิทธิมนุษยชนที่ 20/8 และ 26/13 ว่าด้วยการส่งเสริม การคุ้มครองและการใช้สิทธิมนุษยชนบนอินเทอร์เน็ต เช่นเดียวกับมติสมัชชาใหญ่ที่ 68/167 และ 69/166 ว่าด้วยสิทธิในความเป็นส่วนตัวในยุคดิจิทัล เพื่อรับประกันการเคารพสิทธิมนุษยชนอย่างเต็มที่ ซึ่งอาเซียนเป็นองค์การระหว่างประเทศระดับภูมิภาคองค์การแรกที่รับเอาแนวบรรทัดฐานของสหประชาชาติมาปรับใช้ในภูมิภาค ดังนั้น ย่อมรวมถึงบรรทัดฐานข้อที่ 5 ในเรื่องการรับรองและเคารพสิทธิมนุษยชนดังกล่าวด้วย สำหรับการให้ความสำคัญด้านสิทธิมนุษยชนของสหภาพยุโรปในกฎหมาย กฎ ข้อบังคับต่าง ๆ ปรากฏให้เห็นผ่านกลไก และสถาบันด้านสิทธิมนุษยชนของสหภาพยุโรป รวมถึงในกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือ NIS Directive ได้เน้นย้ำความสำคัญของสิทธิมนุษยชนโดยกล่าวถึงในอารัมภบทของ NIS Directive ทั้งสองฉบับ

สำหรับกฎหมายความมั่นคงปลอดภัยไซเบอร์ของสหรัฐอเมริกา จีน สิงคโปร์ และไทย มีการให้ความคุ้มครองข้อมูลส่วนบุคคล โดยกฎหมายของสหรัฐอเมริกากำหนดให้หน่วยงานเอกชนระบุและลบข้อมูลส่วนบุคคลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ก่อนที่จะแบ่งปันข้อมูลภายใต้กฎหมาย รวมถึงกำหนดให้มีการพัฒนาขั้นตอนเพื่อระบุและลบข้อมูลที่ไม่เกี่ยวข้องโดยตรงกับภัยคุกคามความปลอดภัยทางไซเบอร์ที่หน่วยงานของรัฐบาลกลางทราบในขณะที่แบ่งปันข้อมูล ว่าเป็นข้อมูลส่วนบุคคลหรือข้อมูลที่เฉพาะเจาะจง นอกจากนี้ยังมีขั้นตอนการแจ้งบุคคลที่ได้รับทราบข้อมูลหรือพิจารณาแล้วว่าถูกแบ่งปันโดยละเมิดกฎหมาย แต่ไม่มีบทกำหนดโทษที่ประกันการเยียวยา กรณีเกิดความผิดพลาดในการจัดการข้อมูลส่วนบุคคล ในกฎหมายของประเทศจีน กำหนดให้ผู้ให้บริการเครือข่ายจะต้องรวบรวมหรือใช้ข้อมูลส่วนบุคคลอย่างถูกกฎหมายเหมาะสมและเท่าที่จำเป็น และจะต้องเปิดเผยวัตถุประสงค์ วิธีการ และขอบเขตในการรวบรวมข้อมูลโดยได้รับความยินยอมจากเจ้าของข้อมูลก่อน ห้ามเก็บข้อมูลที่ไม่เกี่ยวข้องกับการให้บริการ และห้ามเปิดเผยให้แก่บุคคลอื่น เว้นแต่เจ้าของข้อมูลให้ความยินยอม ซึ่งหากฝ่าฝืนจะมีโทษ ในส่วนกฎหมายของประเทศสิงคโปร์มีการกำหนดให้ผู้ได้รับคำสั่งจากผู้บัญชาการความมั่นคงปลอดภัยไซเบอร์

สามารถปฏิเสธการให้ข้อมูลส่วนบุคคลของผู้ใช้บริการได้ โดยได้รับความคุ้มครองจากกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงสามารถอุทธรณ์คำสั่งของผู้บัญชาการฯ ไปยังรัฐมนตรีได้อีกด้วย ในขณะที่ประเทศไทยมีการกำหนดโทษสำหรับเจ้าหน้าที่ที่เปิดเผยข้อมูลโดยเจตนาหรือโดยประมาท รวมถึงบุคคลที่ได้ทราบข้อมูลจากเจ้าหน้าที่และนำไปเผยแพร่ให้บุคคลอื่นทราบ แต่ไม่สามารถปฏิเสธหรืออุทธรณ์คำสั่งของคณะกรรมการได้ในกรณีภัยคุกคามระดับร้ายแรงและระดับวิกฤติ

อนึ่ง กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของทั้ง 4 ประเทศ ยังมีปัญหาคล้ายคลึงกันในเรื่องการมีบทบัญญัติบางส่วนที่มีความกำกวม อาจทำให้เกิดการตีความอย่างกว้างขวางจนกระทบต่อสิทธิมนุษยชน เช่น กฎหมายของประเทศจีน มาตรา 12 มีถ้อยคำกำกวมจำนวนมาก ได้แก่ “กิจกรรมที่เป็นอันตรายต่อความมั่นคงของชาติ” “เกียรติยศของชาติ” “ผลประโยชน์ของชาติ” “เอกภาพของชาติ” ซึ่งสะท้อนให้เห็นความไม่โปร่งใสของการตรากฎหมายที่เจตนาให้เกิดการตีความและใช้ดุลพินิจของรัฐ เพื่อปิดกั้นและกำกับดูแลการใช้อินเทอร์เน็ตของประชาชน ซึ่งเป็นการขัดขวางเสรีภาพในการแสดงความคิดเห็น กระทบต่อสิทธิมนุษยชน เช่นเดียวกับถ้อยคำที่สามารถตีความได้อย่างกว้างขวางในกฎหมายไทย เช่น “ความมั่นคงของรัฐ” “ความมั่นคงทางเศรษฐกิจ” “ความมั่นคงทางทหาร” และ “ความสงบเรียบร้อยภายในประเทศ” ซึ่งอาจหมิ่นเหม่ต่อการที่รัฐจะใช้กฎหมายเป็นเครื่องมือให้เกิดโทษต่อผู้ที่มีความเห็นขัดแย้งกับรัฐได้

การศึกษาในบทนี้พบว่าพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่วางกรอบในลักษณะกว้าง ๆ โดยให้อำนาจคณะกรรมการต่าง ๆ ที่ตั้งขึ้นตามพระราชบัญญัติฉบับนี้มีอำนาจในการกำหนดรายละเอียด ทำให้ถ้อยคำในพระราชบัญญัติมีลักษณะที่ตีความได้กว้างขวาง ไม่มีความชัดเจน การตั้งคณะกรรมการหลายชุดที่อาจมีการทำงานที่ซ้ำซ้อนและมีอำนาจมาก การกำหนดหลักเกณฑ์ ประมวลแนวปฏิบัติ กรอบมาตรฐาน ประเภทและระดับภัยคุกคาม ไม่ผ่านการรับฟังความคิดเห็นจากผู้มีส่วนได้ส่วนเสียอย่างกว้างขวาง ทำให้ขาดการตรวจสอบ ถ่วงดุล กฎหมายมุ่งไปที่ประเด็นด้านความมั่นคงเป็นหลัก โดยยังไม่ได้ให้ความสำคัญด้านสิทธิมนุษยชน การปกป้องสิทธิขั้นพื้นฐาน และการมีส่วนร่วมของประชาชนเท่าที่ควรจะเป็น นอกจากนี้แม้ว่าประเทศไทยจะเป็นสมาชิกอาเซียนซึ่งรับเอาแนวบรรทัดฐานของสหประชาชาติมาเป็นแนวปฏิบัติในภูมิภาค แต่ประเทศไทยยังไม่ได้ปฏิบัติให้สอดคล้องกับบรรทัดฐานดังกล่าว โดยเฉพาะในบรรทัดฐานข้อ 5 ในเรื่องที่ว่าด้วยสิทธิมนุษยชน รวมถึงปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ซึ่งเป็นกฎหมายจารีตประเพณีระหว่างประเทศด้านสิทธิมนุษยชนที่สำคัญ ซึ่งรับรองสิทธิความเป็นส่วนตัวและเสรีภาพในการแสดงออก

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

ในบทนี้จะเป็นการนำเสนอบทสรุปที่เกี่ยวกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กับความสมดุลระหว่างมิติด้านความมั่นคงและมิติด้านการคุ้มครองสิทธิมนุษยชน ความสอดคล้องกับมาตรฐานระหว่างประเทศ และอีกส่วนหนึ่งจะเป็นข้อเสนอแนะในการนำแนวทางฐานสิทธิมนุษยชนมาสร้างสมดุลในการพัฒนานโยบายและมาตรการทางกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงแนวทางในการพัฒนาและปรับปรุงกฎหมายดังกล่าว

5.1 บทสรุป

เป็นที่ยอมรับกันในปัจจุบันว่าภัยคุกคามทางไซเบอร์ได้ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศอย่างรุนแรงจนก่อให้เกิดความเสียหายทั้งในระดับบุคคล และระดับประเทศ ดังนั้น เพื่อปกป้อง คุ้มครอง ป้องกัน แก้ไข และรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ ตลอดจนเสริมสร้างความปลอดภัยต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประเทศต่าง ๆ จึงตรากฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยประเทศไทยเอง ได้มีการตราพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ด้วยเหตุผลหลัก ๆ เช่นเดียวกับนานาประเทศ

วาทกรรมเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ส่วนใหญ่มาจากแนวคิดเรื่องความมั่นคงของชาติ ซึ่งทำให้เสรีภาพของพลเมืองและสิทธิมนุษยชนอยู่ภายใต้แรงกดดันที่ลดคุณค่าลงหรือแม้แต่วางตำแหน่งให้เป็นสิ่งที่ตรงกันข้ามกับความมั่นคงของชาติ แม้จะมีการกล่าวถึงสิทธิมนุษยชนอยู่บ้าง แต่ความเข้าใจโดยทั่วไปเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ยังคงเน้นหนักไปที่รัฐอธิปไตย ดินแดน และโครงสร้างพื้นฐานมากกว่าตัวบุคคล[1] การใช้แนวทางสิทธิมนุษยชนเป็นศูนย์กลาง เป็นการเปลี่ยนจุดเน้นไปที่ความปลอดภัยและสิทธิมนุษยชนของผู้คน ไม่ทำให้เกิดการละเมิดจนเปลี่ยนพลเมืองจากผู้รับประโยชน์ทางเทคโนโลยีให้กลายเป็นเหยื่อ ยิ่งกว่านั้นยังช่วยให้

[1] Pavlina Pavlova,‘Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups’ (2020) 4(3) Peace Human Rights Governance, 391, 396-397.

พวกเขาสามารถใช้สิทธิได้อย่างเต็มที่ การรักษาความปลอดภัยต้องปราศจากการคุกคามต่อคุณค่าหลักของมนุษย์ ในขณะที่อีกทางหนึ่งคือส่งเสริมความเข้าใจเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ในฐานะนโยบายและแนวปฏิบัติที่ปกป้องและทำให้ผู้คนสามารถใช้สิทธิของตนได้อย่างอิสระและปลอดภัย

ทั้งนี้ เมื่อพิจารณาจากการศึกษาในบทที่ 1-4 พบว่ากฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศที่นำมาศึกษา มีแนวคิดหลักใกล้เคียงกัน โดยเอนเอียงไปในด้านการให้ความสำคัญกับความมั่นคงเป็นหลัก และให้ความสำคัญกับสิทธิมนุษยชนเป็นลำดับรอง และในบางประเทศแทบจะไม่ให้ความสำคัญเลย หรือแม้กระทั่งหมิ่นเหม่ที่จะทำให้เกิดการละเมิดสิทธิมนุษยชนจากการบังคับใช้กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์อีกด้วย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีเจตนารมณ์ในการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของประเทศและปกป้องโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญให้พ้นจากภัยคุกคามทางไซเบอร์ แม้ว่ากฎหมายฉบับนี้จะตราขึ้นโดยมีเจตนาอันดีเพื่อความมั่นคงปลอดภัยโดยรวมของประเทศ ทว่าการตรากฎหมายในลักษณะกรอบกว้าง ๆ และให้อำนาจแก่คณะกรรมการ กมช. และ กกม. ในการออกกฎหมายลำดับรองเพื่อกำหนดรายละเอียดของหลักเกณฑ์ประมวลแนวทางปฏิบัติ กรอบมาตรฐานต่าง ๆ ตลอดจนประเภทของภัยคุกคามและระดับของภัยคุกคาม ทำให้พระราชบัญญัติที่ประกาศใช้มีลักษณะเป็นบทบัญญัติที่ไม่ชัดเจน มีถ้อยคำที่ตีความได้อย่างกว้างขวาง และเปิดโอกาสให้คณะกรรมการต่าง ๆ ใช้ดุลพินิจมากเกินไป นอกจากนี้กฎหมายลำดับรองต่าง ๆ ที่ออกโดยคณะกรรมการ ไม่มีการรับฟังความเห็นหรือเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียเข้ามามีส่วนร่วมในการจัดทำอย่างกว้างขวางและทั่วถึง อีกทั้งในพระราชบัญญัตินี้ยังไม่กำหนดบทบัญญัติที่เกี่ยวข้องกับการดำเนินการในกรณีภัยคุกคามระดับวิกฤติไว้ โดยให้ไปใช้พระราชบัญญัติสภาความมั่นคงแห่งชาติ พ.ศ. 2559 ซึ่งเป็นการแสดงให้เห็นอย่างชัดเจนว่ากฎหมายฉบับนี้มุ่งไปที่ประเด็นด้านความมั่นคงเป็นหลัก

เมื่อไปพิจารณานิยามในพระราชบัญญัติสภาความมั่นคงแล้ว พบว่าได้ให้ความหมายของคำว่า “ภัยคุกคาม” ไว้ดังนี้

“ภัยคุกคาม” หมายความว่า ภาวะหรือสถานการณ์ที่ก่อให้เกิดความไม่มั่นคงซึ่งเป็นปัญหาที่มีความรุนแรง สลับซับซ้อน หากไม่ดำเนินการแก้ไขจะเกิดผลกระทบในวงกว้างต่อความมั่นคงแห่งชาติ”

จะเห็นได้ว่าคำนิยามในพระราชบัญญัติสภาความมั่นคงยิ่งมีความกว้างขวางและไม่ชัดเจนยิ่งขึ้นไปอีก เมื่อใดที่ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นถูกประเมินว่าเป็นภัยคุกคามระดับวิกฤติจะถูกส่งไปยังสภาความมั่นคงและกลายเป็นภัยคุกคามตามนิยามของพระราชบัญญัติสภาความมั่นคง

ทันที ซึ่งจะรวบอำนาจจากคณะกรรมการ กมช. และกกม. กลับไปที่นายกรัฐมนตรี ซึ่งเป็นประธานของสภาความมั่นคงแห่งชาติ โดยไม่มีบทบัญญัติที่รับประกันการเยียวยากรณีมีการประเมินระดับของภัยคุกคามผิดพลาด จนทำให้เกิดการดำเนินการที่ละเมิดสิทธิมนุษยชนของประชาชนหรือเอกชนที่เกี่ยวข้อง รวมถึงการดำเนินการในกรณีภัยคุกคามระดับวิกฤติที่อ้างความจำเป็นเร่งด่วนดำเนินการได้โดยไม่ต้องร้องขอต่อศาล แต่เพียงรายงานการดำเนินงานให้ศาลทราบภายหลังเท่านั้น ซึ่งก็ไม่ได้บัญญัติว่าหากการดำเนินงานเหล่านั้นไม่ถูกต้องหรือก่อให้เกิดความเสียหาย จะต้องมีการเยียวยาแก้ไข หรือชดเชยให้กับผู้ได้รับผลกระทบอย่างไร

กฎหมายฉบับนี้มีบทกำหนดโทษในกรณีที่พนักงานเจ้าหน้าที่จงใจหรือประมาทเลินเล่อในการเปิดเผยข้อมูลหรือทำให้ผู้อื่นล่วงรู้ข้อมูลที่ได้จากการปฏิบัติหน้าที่ แต่ไม่มีบทบัญญัติที่ประกันการเยียวยาความเสียหายในกรณีอื่น ๆ หากการใช้ดุลพินิจหรือการปฏิบัติงานของพนักงานเจ้าหน้าที่ก่อให้เกิดความเสียหายทั้งต่อความเป็นส่วนตัว ทรัพย์สิน หรือสิทธิมนุษยชนด้านอื่น ๆ จะได้รับการคุ้มครองหรือให้การช่วยเหลือเยียวยาอย่างไร อีกทั้งยังมีปัญหาเกี่ยวกับการอุทธรณ์คำสั่ง ในกรณีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงและระดับวิกฤติ ตามที่บัญญัติไว้ในมาตรา 69 ให้ผู้ได้รับคำสั่งเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น ซึ่งการดำเนินการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหลายมาตราขาดพยานหลักฐานที่ชัดเจนเพียงพอในการจำกัดสิทธิเสรีภาพส่วนบุคคล เช่น มาตรา 66 การให้ กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยเข้าไปตรวจสอบสถานที่ เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทดสอบการทำงานของคอมพิวเตอร์ ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใดๆ แม้ว่าจะให้ยื่นคำร้องต่อศาลเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ แต่ใน (1) ซึ่งเป็นการเข้าตรวจสอบสถานที่ ไม่อยู่ในบังคับที่จะต้องยื่นคำร้องต่อศาลก่อนการปฏิบัติ ไม่ได้กำหนดให้มีหมายค้น เพียงให้มีหนังสือแจ้งเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น[2] ทำให้เห็นว่าสัดส่วนของมิติด้านสิทธิมนุษยชน

---

[2] มาตรา 66 ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่อง ดังต่อไปนี้

(1) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

มีน้ำหนักน้อยมากในกฎหมายฉบับนี้ เมื่อเทียบกับมิติด้านความมั่นคง ซึ่งอาจส่งผลกระทบต่อสิทธิมนุษยชนด้านต่าง ๆ ได้แก่

1) สิทธิในความเป็นส่วนตัว (Right to Privacy)

2) เสรีภาพในการแสดงออก (Freedom of Expression)

3) กระบวนการอันชอบธรรมและหลักนิติธรรม (Due Process and Rule of Law)

4) สิทธิในการเข้าถึงข้อมูลและความเหลื่อมล้ำทางดิจิทัล (Right of Access to Information and Digital Divide)

5) สิทธิในการศึกษา (Right to Education)

6) การเลือกปฏิบัติทางไซเบอร์ (Cyber Discrimination)

ทั้งนี้ พระราชบัญญัติหลักเกณฑ์การจัดทำร่างกฎหมายและการประเมินผลสัมฤทธิ์ของกฎหมาย พ.ศ. 2562 บัญญัติไว้ในมาตรา 34 ว่า

“มาตรา 34 การประเมินผลสัมฤทธิ์ให้กระทำอย่างน้อยทุกห้าปีนับแต่วันที่กฎหมายนั้นมีผลใช้บังคับ หรือทุกรอบระยะเวลาอื่นตามที่กำหนดในกฎกระทรวง หรือเมื่อมีกรณีใดกรณีหนึ่งดังต่อไปนี้

---

(2) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(3) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(4) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (2) (3) และ (4) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

(1) ได้รับหนังสือร้องเรียนหรือข้อเสนอแนะจากองค์กรที่เกี่ยวข้องหรือจากประชาชน และหน่วยงานของรัฐผู้รับผิดชอบการประเมินผลสัมฤทธิ์ เห็นว่าข้อร้องเรียนหรือข้อเสนอแนะนั้นมีเหตุผลอันสมควร

(2) ได้รับข้อเสนอแนะจากคณะกรรมการพัฒนากฎหมาย

(3) กรณีอื่นตามที่กำหนดในกฎกระทรวง

การประเมินผลสัมฤทธิ์ของพระราชกำหนดใดที่ตราขึ้นภายหลังพระราชบัญญัตินี้มีผลใช้บังคับเป็นครั้งแรก ให้กระทำภายในสองปีนับแต่วันที่พระราชกำหนดนั้นมีผลใช้บังคับส่วนครั้งต่อ ๆ ไป ให้กระทำตามวรรคหนึ่ง"

ซึ่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จะครบกำหนดที่จะต้องประเมินผลสัมฤทธิ์ในวันที่ 27 พฤษภาคม 2567 อันจะเป็นโอกาสให้ได้ทบทวนกฎหมายฉบับนี้และแก้ไขปรับปรุงให้เกิดความสมดุลระหว่างมิติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กับมิติด้านสิทธิมนุษยชน รวมถึงการทบทวนกฎหมายลำดับรองที่เกี่ยวข้อง โดยเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียทุกกลุ่มสามารถเข้ามามีส่วนร่วมได้อย่างกว้างขวาง โดยในการปรับปรุงแก้ไขผู้เขียนจะขอให้ข้อเสนอแนะในลำดับถัดไป

5.2 ข้อเสนอแนะ

ในการปรับปรุงแก้ไขพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งจากการศึกษาพบว่ามีบทบัญญัติหลายส่วนที่ยังขาดมิติในด้านการคุ้มครองสิทธิมนุษยชน และมุ่งเน้นเพียงด้านความมั่นคง ทำให้ข้อเสนอแนะในการปรับปรุงแก้ไขต้องนำแนวทางฐานสิทธิมนุษยชนเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (Human Rights-Based Approach to Cybersecurity) มาเป็นกรอบในการปรับปรุงกฎหมาย ซึ่งแนวทางดังกล่าวอยู่บนหลักการของข้อมติสหประชาชาติ The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/RES/26/13) ที่รับรองโดยสหประชาชาติในเดือนกรกฎาคม ค.ศ. 2014 โดยการปรับปรุงแก้ไขกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องมีหลักคิดในการเคารพสิทธิมนุษยชนตั้งแต่การเริ่มต้นออกแบบกฎหมาย เพื่อมิให้เกิดความไม่สมดุลในบทบัญญัติต่าง ๆ ระหว่างความมั่นคงปลอดภัยไซเบอร์กับสิทธิมนุษยชนดังเช่นกฎหมายฉบับปัจจุบัน รวมถึงนโยบาย ประมวลแนวทางปฏิบัติ กรอบมาตรฐาน และกฎหมายลำดับรองอื่น ๆ ตลอดจนกระบวนการใช้ดุลพินิจของพนักงานเจ้าหน้าที่ควรปกป้องและเคารพสิทธิมนุษยชน รวมทั้งต้องสอดคล้องกับกฎหมายระหว่างประเทศ กฎหมายสิทธิมนุษยชนระหว่างประเทศ และกฎหมายด้านมนุษยธรรมระหว่างประเทศ ซึ่งส่งเสริมความ

ปลอดภัยของบุคคลทั้งแบบออนไลน์และออฟไลน์ โดยคำนึงถึงภัยคุกคามที่ไม่เหมาะสมที่บุคคลและกลุ่มต่าง ๆ มีความเสี่ยงที่จะต้องเผชิญอยู่

กฎหมาย นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ควรสนับสนุนและปกป้องความมั่นคงปลอดภัยของอินเทอร์เน็ต และไม่ทำลายความสมบูรณ์ของโครงสร้างพื้นฐาน ฮาร์ดแวร์ ซอฟต์แวร์ และบริการเสียเอง รวมถึงสะท้อนให้เห็นความสำคัญของการเข้ารหัสและการไม่เปิดเผยตัวตน ซึ่งเป็นการปฏิบัติตามสิทธิมนุษยชน โดยเฉพาะในเรื่องเสรีภาพของการแสดงความคิดเห็น การสมาคม การชุมนุม และความเป็นส่วนตัว และข้อสำคัญอีกประการหนึ่งคือไม่ควรใช้กฎหมาย นโยบาย และแนวปฏิบัติเกี่ยวกับความปลอดภัยทางไซเบอร์เพื่อเป็นข้ออ้างในการละเมิดสิทธิมนุษยชน และไม่ควรเป็นอุปสรรคต่อการพัฒนาทางเทคโนโลยีที่นำไปสู่การคุ้มครองสิทธิมนุษยชน จึงควรปรับปรุงแก้ไขบทบัญญัติในพระราชบัญญัติฉบับนี้เพื่อให้เกิดการคุ้มครองสิทธิมนุษยชนด้านต่าง ๆ ดังที่ได้กล่าวไว้ในบทที่ 2 ดังต่อไปนี้[3]

1) การให้นิยามที่ชัดเจนของคำสำคัญเพื่อการบังคับใช้กฎหมายอย่างมีประสิทธิภาพและหลีกเลี่ยงการตีความที่กว้างขวางโดยเจ้าหน้าที่ผู้ปฏิบัติ โดยในมาตรา 3 มีคำสำคัญหลายคำที่ควรต้องปรับปรุง เช่น “การรักษาความมั่นคงปลอดภัยไซเบอร์” ซึ่งมิได้ให้ความหมายหรือขยายความคำว่า ความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ว่าหมายถึงสิ่งใดบ้าง “ภัยคุกคามทางไซเบอร์” ที่ให้ความหมายขยายไปถึง “ข้อมูลอื่นที่เกี่ยวข้อง” นอกเหนือจากความเสียหายที่เกิดกับการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่ง “ข้อมูลอื่นที่เกี่ยวข้อง” เป็นข้อความที่กว้าง และไม่สามารถระบุได้ว่าข้อมูลอย่างไรบ้างที่จัดว่าเกี่ยวข้อง โดยเมื่อเปรียบเทียบกับกฎหมายของสิงคโปร์ พบว่า มีการนิยามคำว่า “ภัยคุกคามความปลอดภัยทางไซเบอร์” หมายถึง การกระทำหรือกิจกรรม (ไม่ว่าจะทราบหรือสงสัยว่า) กระทำบนหรือผ่านคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจก่อให้เกิดอันตรายหรือส่งผลกระทบในทางลบอย่างฉับพลันต่อความปลอดภัยทางไซเบอร์ของคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น โดยไม่มีอำนาจตามกฎหมาย[4] ซึ่งมุ่งเน้นไปที่ภัยคุกคามอันเกิดต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์

---

[3] โดยที่บทบัญญัติในแต่ละมาตราอาจกระทบต่อสิทธิมนุษยชนหลายด้าน ผู้เขียนจึงให้ข้อเสนอแนะโดยยึดตัวบทเป็นหลัก เนื่องจากการแก้ไขบทบัญญัติแต่ละมาตรา จะสามารถแก้ไขปัญหาการกระทบสิทธิได้หลายประการในคราวเดียว

[4] “cybersecurity threat” means an act or activity (whether known or suspected) carried out on or through a computer or computer system, that may imminently

เท่านั้น นอกจากนี้ดังที่ได้กล่าวไว้ในบทก่อนหน้าถึงการแบ่งระดับภัยคุกคามไซเบอร์ออกเป็น 3 ระดับ คือระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ เป็นการเปิดช่องให้เกิดการขยายความ “ภัยคุกคามทางไซเบอร์” ให้กว้างขวางยิ่งขึ้นไปอีก รวมทั้งเปิดช่องให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. ขยายขอบเขตการตีความในการกำหนดรายละเอียดของภัยคุกคามแต่ละระดับ ซึ่งกฎหมายได้ให้อำนาจไว้ในมาตรา 13 (6) ให้ กกม. เป็นผู้กำหนดระดับภัยคุกคามทางไซเบอร์ ตลอดจนรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ เสนอต่อ กมช. เพื่อออกเป็นประกาศ ดังนั้น ควรตัดถ้อยคำที่กำกวมออก และเปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียทุกกลุ่มเข้าไปมีส่วนร่วมในการพิจารณากำหนดรายละเอียดภัยคุกคามรวมถึงมาตรการต่าง ๆ เพื่อหลีกเลี่ยงโอกาสที่จะทำให้เกิดการละเมิดสิทธิมนุษยชน

2) การใช้ดุลพินิจในกฎหมายต้องสอดคล้องกับพระราชบัญญัติหลักเกณฑ์การจัดทำร่างกฎหมายและการประเมินผลสัมฤทธิ์ของกฎหมาย พ.ศ. 2562 ด้วยการใช้อำนาจของเจ้าหน้าที่ของรัฐมีที่มาจากบทบัญญัติของกฎหมายเป็นพื้นฐานสำคัญ เมื่อใดที่กฎหมายที่ให้อำนาจแก่เจ้าหน้าที่ของรัฐโดยมิได้กำหนดองค์ประกอบหรือเงื่อนไขการใช้อำนาจไว้อย่างชัดเจนแล้ว ในการบังคับใช้กฎหมายย่อมจะทำให้เจ้าหน้าที่ของรัฐมีดุลพินิจในการใช้อำนาจในเรื่องนั้น ๆ ดังนั้น ดุลพินิจของเจ้าหน้าที่ของรัฐจึงเกิดขึ้นจากการที่ตัวบทกฎหมายเปิดโอกาสให้เจ้าหน้าที่ของรัฐ ใช้กฎหมายได้อย่างยืดหยุ่นและสอดคล้องกับข้อเท็จจริงเป็นการเฉพาะเรื่องเฉพาะราย เพื่อมิให้การใช้บทบัญญัติของกฎหมายแข็งกระด้างและเพื่อมุ่งหมายให้เกิดความยุติธรรมขึ้นแก่เฉพาะเรื่องเฉพาะรายนั้น ๆ อำนาจดุลพินิจสามารถแบ่งออกได้หลายประเภทตามการกระทำด้านต่าง ๆ ของรัฐ แต่ยังคงมีลักษณะร่วมกัน ได้แก่ การที่กฎหมายกำหนดให้อำนาจเจ้าหน้าที่ของรัฐโดยกำหนดถ้อยคำที่มีลักษณะไม่แน่นอนตายตัว หรือให้ทางเลือกในการใช้อำนาจหรือมาตรการได้หลายทางในขอบเขตที่กำหนด ซึ่งการยอมให้เจ้าหน้าที่ของรัฐมีดุลพินิจในเรื่องนั้น ๆ เพื่อให้มีการบริหารกฎหมายให้เป็นไปตามวัตถุประสงค์และมิให้เกิดการหยุดชะงักในการปฏิบัติหน้าที่หรือขาดประสิทธิภาพในการบังคับใช้กฎหมาย[5] ทั้งนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีบทบัญญัติ

---

jeopardise or affect adversely, without lawful authority, the cybersecurity of that or another computer or computer system;

[5] คณะทำงานศึกษาและยกร่างหลักเกณฑ์เกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ สำนักงานคณะกรรมการกฤษฎีกา, ‘ความเบื้องต้นเกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ’

จำนวนมากที่เปิดช่องให้คณะกรรมการคณะต่าง ๆ ในกฎหมาย เลขาธิการฯ ตลอดจนพนักงานเจ้าหน้าที่ใช้ดุลพินิจ ซึ่งมาตรา 23 แห่งพระราชบัญญัติหลักเกณฑ์การจัดทำร่างกฎหมายและการประเมินผลสัมฤทธิ์ของกฎหมาย พ.ศ. 2562 บัญญัติว่า

“มาตรา 23 ในกรณีที่ร่างกฎหมายกำหนดให้ออกกฎเพื่อกำหนดหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ กฎดังกล่าวต้องกำหนดให้การใช้ดุลพินิจเป็นไปตามหลักเกณฑ์ดังต่อไปนี้

(1) ไม่ขัดหรือแย้งต่อหลักการสำคัญที่รัฐธรรมนูญรับรอง

(2) สอดคล้องกับหลักการบริหารกิจการบ้านเมืองที่ดี

(3) สอดคล้องและปฏิบัติตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครอง

(4) ต้องยึดหลักความพอสมควรแก่เหตุ และหลักความได้สัดส่วนระหว่างประโยชน์ที่ส่วนรวมจะได้รับกับสิทธิและเสรีภาพและประโยชน์ที่บุคคลต้องเสียไป

(5) ต้องยึดหลักความเสมอภาคและต้องไม่เป็นการเลือกปฏิบัติโดยไม่เป็นธรรมต่อบุคคล”

เพื่อให้เป็นการใช้ดุลพินิจโดยชอบด้วยกฎหมายที่อยู่บนฐานข้อเท็จจริง ข้อกฎหมาย และการใช้เหตุผลประกอบการพิจารณาตัดสินอย่างเหมาะสม เนื่องจากการใช้อำนาจใด ๆ ของรัฐต้องผูกพันกับหลักการทางกฎหมาย เช่น หลักความเสมอภาค และหลักความได้สัดส่วน เป็นต้น[6] โดยมุ่งประสงค์ที่จะคุ้มครองสิทธิเสรีภาพของบุคคล ดังนั้น การกำหนดให้อำนาจในการใช้ดุลพินิจในเรื่องที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องคำนึงถึงหลักการทางกฎหมายที่สำคัญและการกำหนดเหตุหรือกรณีที่จะเปิดช่องให้เจ้าหน้าที่ของรัฐ มีอำนาจดุลพินิจโดยพิจารณาถึงความจำเป็นและสมควร ซึ่งแนวคิดดังกล่าวสะท้อนอยู่ในแนวนโยบายแห่งรัฐ ตามวรรคสามของมาตรา 77[7] ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ที่กำหนดให้รัฐพึงใช้ระบบอนุญาต และระบบ

<https://www.krisdika.go.th/data/article77/filenew/03-4-1.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

[6] สมยศ เชื้อไทย, ‘การกระทำทางปกครอง’ (2530) 3 วารสารนิติศาสตร์ 49, 58.

[7] มาตรา 77 รัฐพึงจัดให้มีกฎหมายเพียงเท่าที่จำเป็น และยกเลิกหรือปรับปรุงกฎหมายที่หมด ความจำเป็นหรือไม่สอดคล้องกับสภาพการณ์ หรือที่เป็นอุปสรรคต่อการดำรงชีวิตหรือการประกอบอาชีพโดยไม่ชักช้า เพื่อไม่ให้เป็นภาระแก่ประชาชน และดำเนินการให้ประชาชนเข้าถึงตัวบทกฎหมายต่าง ๆ ได้โดยสะดวกและสามารถเข้าใจ กฎหมายได้ง่ายเพื่อปฏิบัติตามกฎหมายได้อย่างถูกต้อง

คณะกรรมการในกฎหมายเฉพาะกรณีที่จำเป็น รวมถึงพึงกำหนดหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐและระยะเวลาในการดำเนินการตามขั้นตอนต่าง ๆ ที่บัญญัติไว้ในกฎหมายให้ชัดเจน เป็นต้น

3) กรณีที่กฎหมายบัญญัติให้เป็นการขอความร่วมมือ ไม่ควรมีโทษทางอาญา โดยในมาตรา 61 (1) บัญญัติว่า เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการรวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคาม[8] และมาตรา 62 (1) และ (2) บัญญัติว่า ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการมีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลา

รัฐพึงใช้ระบบอนุญาตและระบบคณะกรรมการในกฎหมายเฉพาะกรณีที่จำเป็น พึงกำหนดหลักเกณฑ์ การใช้ดุลพินิจของเจ้าหน้าที่ของรัฐและระยะเวลาในการดำเนินการตามขั้นตอนต่าง ๆ ที่บัญญัติไว้ในกฎหมายให้ชัดเจน และพึงกำหนดโทษอาญาเฉพาะความผิดร้ายแรง

[8] มาตรา 61 เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้

(1) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(2) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(3) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(4) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือและเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(5) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสมโดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(6) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชน เพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์ และมีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่น อันเป็นประโยชน์แก่การดำเนินการ[9] ดังจะเห็นได้ว่าบทบัญญัติของกฎหมายให้เลขาธิการมีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องมาให้ข้อมูล โดยในมาตรา 74 มีการกำหนดโทษของผู้ที่ไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา 62 (1) หรือ (2) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกิน 100,000 บาท ซึ่งบทบัญญัติในมาตรา 62 (1) เป็นการทำหนังสือขอความร่วมมือ จึงไม่ควรถูกลงโทษทางอาญาเป็นค่าปรับสูงถึง 100,000 บาท กรณีหากจะบังคับให้ต้องปฏิบัติตาม ควรบัญญัติให้เป็นคำสั่งเรียกให้บุคคลที่เกี่ยวข้องมาให้ข้อมูลโดยระบุเหตุผลความจำเป็นเพื่อประโยชน์แก่การดำเนินการวิเคราะห์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อไม่ให้เป็นการละเมิดสิทธิของบุคคลโดยไม่จำเป็น

4) การเข้าตรวจสอบสถานที่โดยไม่มีหมายค้น โดยในมาตรา 66(1) กำหนดให้พนักงานเจ้าหน้าที่โดยคำสั่งของ กกม. เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยมีข้อสังเกตคือ การเข้าตรวจสอบสถานที่ตามมาตรานี้ มีลักษณะเดียวกับ

---

[9] มาตรา 62 ในการดำเนินการตามมาตรา 61 เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการดังต่อไปนี้

(1) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสม และตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(2) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(3) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับภัยคุกคามทางไซเบอร์

(4) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

การค้นตามประมวลกฎหมายวิธีพิจารณาความอาญาหรือไม่ หากเป็นการเข้าไปในที่รโหฐานซึ่งมิใช่สถานที่ราชการ แต่เป็นสถานที่ของเอกชน ควรบัญญัติให้สอดคล้องกับกฎหมายวิธีพิจารณาความอาญา ซึ่งประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 92 วรรคหนึ่ง ห้ามมิให้ค้นในที่รโหฐานโดยไม่มีหมายค้นหรือคำสั่งศาล เว้นแต่พนักงานฝ่ายปกครองหรือตำรวจเป็นผู้ค้น ในกรณีตาม (1)–(5) นอกจากนั้นเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 66 (2) (3) และ (4) ซึ่งกำหนดให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง รวมถึงเพื่อให้ได้สัดส่วนกับบทกำหนดโทษในมาตรา 76 ที่บัญญัติว่า

“มาตรา 76 ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติการตามคำสั่งของ กกม. ตามมาตรา 66 (1) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา 66 (2) (3) หรือ (4) โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”

ซึ่งโทษที่จะลงแก่ผู้ไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติตามคำสั่งของ กกม. ตามมาตรา 66 (1) บัญญัติไว้เท่ากันกับโทษของการไม่ปฏิบัติตามคำสั่งศาลตามมาตรา 66 (2) (3) และ (4) ดังนั้น การใช้อำนาจของ กกม. ในมาตรา 66 (1) จึงควรได้รับการตรวจสอบถ่วงดุลโดยศาลด้วย อันจะเป็นการสร้างหลักประกันความยุติธรรมให้แก่ประชาชนอีกชั้นหนึ่ง และเป็นการคุ้มครองสิทธิความเป็นส่วนตัว มิให้ถูกแทรกแซงตามอำเภอใจในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัยหรือการสื่อสาร โดยต้องได้รับการคุ้มครองของกฎหมายจากการแทรกแซงสิทธิดังกล่าว

5) ปัญหาการอุทธรณ์คำสั่งในกรณีภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤติ โดยพระราชบัญญัตินี้บัญญัติไว้ในมาตรา 69 ว่า

“มาตรา 69 ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น”

ซึ่งควรแก้ไขเป็น “ผู้ที่ได้รับคำสั่งอันเกี่ยวกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งต่อรัฐมนตรีได้” เพื่อเป็นหลักประกันความชอบด้วยกฎหมายและให้สิทธิผู้ได้รับคำสั่งสามารถโต้แย้งคำสั่งทางปกครองนั้น ดังเช่นกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสิงคโปร์ที่

กฎหมายเปิดช่องให้ผู้ที่ได้รับคำสั่งจากผู้บัญชาการความปลอดภัยทางไซเบอร์ให้กระทำการใด ๆ สามารถอุทธรณ์คำสั่งไปยังรัฐมนตรีได้[10]

6) การเพิ่มบทบัญญัติที่มีการประกันการเยียวยา และการชดเชยความเสียหายจากการดำเนินการของพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ซึ่งประเด็นนี้เป็นประการสำคัญที่ขาดหายไปจากพระราชบัญญัติฉบับนี้ ด้วยเหตุการณ์ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์อาจเป็นกรณีเร่งด่วนและไม่อาจรอให้เนิ่นช้า หากเกิดการโจมตีหรือภัยคุกคามขึ้นจริง ก็อาจส่งผลให้เกิดความเสียหายอย่างร้ายแรงเป็นวงกว้างและยากต่อการกู้คืนมาได้ หากมีกรณีใดที่กฎหมายไม่อาจใช้วิธีการตรวจสอบถ่วงดุลโดยศาล หรือใช้วิธีขอความร่วมมือได้ อันเนื่องมาจากเหตุจำเป็นเร่งด่วนอย่างแท้จริง ก็อาจให้มีการดำเนินการเพื่อป้องกันสถานการณ์ โดยต้องมีบทบัญญัติขึ้นมารองรับความเสียหายที่อาจเกิดขึ้นต่อสิทธิเสรีภาพของบุคคล การเยียวยาความเสียหายจากผลกระทบที่อาจเกิดขึ้นจากการดำเนินการดังกล่าว เช่น กรณีการประเมินให้ภัยคุกคามเป็นระดับวิกฤติและมีการดำเนินการโดยไม่ได้ร้องขอต่อศาลในกรณีมีความจำเป็นเร่งด่วนตามมาตรา 68 วรรคแรก หากเกิดความผิดพลาดจากการประเมิน หรือเกิดความเสียหายต่อสิทธิเสรีภาพของบุคคลจากการดำเนินการนั้น นอกจากจะต้องรายงานการดำเนินการต่อศาลแล้ว ยังต้องมีการประกันการเยียวยาให้แก่ผู้ได้รับความเสียหาย รวมถึงต้องกำหนดความรับผิดของเจ้าหน้าที่ในกรณีอื่นที่มีการกระทำเกินกว่าเหตุ หรือประมาทเลินเล่อให้เกิดความเสียหาย หรือละเมิดสิทธิของบุคคลเกินจำเป็นด้วย นอกเหนือจากการกำหนดโทษในเรื่องการเก็บรักษาและเปิดเผยข้อมูลส่วนบุคคลในมาตรา 70 และ 71 เพื่อเป็นการคุ้มครองสิทธิเสรีภาพขั้นพื้นฐานอันเป็นของประชาชนทุกคน

จากการศึกษาพบว่าการประเมินความเหมาะสมและประสิทธิภาพของกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละประเทศจะขึ้นอยู่กับมุมมองและความเสี่ยงที่คำนึงถึง เนื่องจากแต่ละ

---

[10] Appeal to Minister

17.—(1) The owner of a critical information infrastructure who is aggrieved by —

(a) the decision of the Commissioner to issue the notice under section 7(1) designating the critical information infrastructure as such;

(b) a written direction of the Commissioner under section 12 or 16(2); or

(c) any provision in any code of practice or standard of performance issued or approved by the Commissioner that applies to the owner, or any amendment made to it, may appeal to the Minister against the decision, direction, provision or amendment in the manner prescribed.

ประเทศมีการให้ความสำคัญและเป้าหมายที่แตกต่างกันไปในด้านความปลอดภัยไซเบอร์ อีกทั้งยังขึ้นอยู่กับวิธีการปรับใช้และการปฏิบัติตามกฎหมายในแต่ละประเทศด้วย อย่างไรก็ตาม กฎหมาย นโยบาย มาตรการ กฎ ระเบียบ ด้านความมั่นคงปลอดภัยทางไซเบอร์ ก็ไม่สามารถละเลยการคุ้มครองสิทธิมนุษยชนขั้นพื้นฐานได้ โดยต้องตระหนักว่าบุคคลมีสิทธิโดยธรรมชาติบางประการที่ควรได้รับการเคารพและปกป้อง แม้ในบริบทของการจัดการกับภัยคุกคามและความท้าทายด้านความปลอดภัยทางไซเบอร์ ซึ่งแนวทางนี้เน้นความจำเป็นในการสร้างความสมดุลระหว่างความกังวลด้านความมั่นคงปลอดภัยกับการคุ้มครองสิทธิและเสรีภาพส่วนบุคคล (Security and Privacy) โดยการมีกฎหมายความมั่นคงทางไซเบอร์ที่สามารถแก้ไขข้อกังวลด้านความปลอดภัยได้อย่างมีประสิทธิภาพ ในขณะเดียวกันก็รักษาสิทธิขั้นพื้นฐานและเสรีภาพของบุคคล ทำให้เห็นว่าความปลอดภัยและสิทธิมนุษยชนไม่ได้ถูกแยกออกจากกัน แต่สามารถส่งเสริมซึ่งกันและกันได้ เพื่อให้เกิดแนวทางที่สมดุลและเป็นประชาธิปไตยมากขึ้นในการกำกับดูแลความปลอดภัยในโลกไซเบอร์

บรรณานุกรม

หนังสือ

ภาษาต่างประเทศ

Frederick Wamala, *The ITU National Cybersecurity Strategy Guide*, (Geneva : International Telecommunication Union 2012).

Michael N. Schmitt editor, *Tallinn manual 2.0 on the international law applicable to cyber operations*', (New York: Cambridge University Press 2016).

บทความ

ภาษาไทย

คณะทำงานศึกษาและยกร่างหลักเกณฑ์เกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ สำนักงานคณะกรรมการกฤษฎีกา, 'ความเบื้องต้นเกี่ยวกับการใช้ดุลพินิจของเจ้าหน้าที่ของรัฐ' <https://www.krisdika.go.th/data/article77/filenew/03-4-1.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

สมยศ เชื้อไทย, 'การกระทำทางปกครอง' (2530) 3 วารสารนิติศาสตร์.

ภาษาต่างประเทศ

Adrian Cristian Moise, 'Cybersecurity and Human Rights' (2016) Revista Universal Juridic 162.

Daniel Marius Morar, Mihaela Senia Costinescu, 'Constitutional Court of Romania: National Cybersecurity versus Fundamental Rights and Freedoms' (2015) 9 Vienna Journal on International Constitutional Law.

Eric Talbot Jensen, 'The Tallinn Manual 2.0: Highlights and Insights' (2017) 48 Georgetown Journal of International Law 735-737.

Ido Kilovaty, 'An Extraterritorial Human Rights to Cybersecurity' (2020) 10 Notre Dame Journal of International & Comparative Law 54.

Ilona Stadnik, 'What Is an International Cybersecurity Regime and How We Can Achieve It?' (2017) 11 Masaryk University Journal of Law and Technology 145.

Jacqueline Van De Velde, ‘The Law of Cyber Interference in Elections’ 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043828> สืบค้นเมื่อ 11 กุมภาพันธ์ 2562.

Marvin Ammori & Keira Poellet, ‘“Security versus Freedom”’ the internet: Cybersecurity and Net Neutrality’ (2010) 30 SAIS Review of International Affairs 63.

Matthias C. Kettemann, ‘Ensuring Cybersecurity through International Law’ (2017) Revista Española de Derecho Internacional 285.

Pavlina Pavlova,‘Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups’ (2020) 4(3) Peace Human Rights Governance 396-397.

Valentina Pavel Burloiu, ‘Romania: Another Episode in Trying to Adopt Cybersecurity Regulation, Another (Possible) Failure for Human Rights’ (2016) 2 European Data Protection Law Review 117-120.

Valentina Pavel Burloiu, ‘The Aftermath of Digital Rights Ireland: Romanian Constitutional Court Declares Overarching Cybersecurity Law Unconstitutional’ (2015) 2 European Data Protection Law Review.

เอกสารอิเล็กทรอนิกส์

ภาษาไทย

Blognone, ‘[IGF 2014] รู้จักกับ Internet Governance Forum เวทีประชุมด้านนโยบายของอินเทอร์เน็ตระดับนานาชาติ’ <https://www.blognone.com/node/59436> สืบค้นเมื่อ 24 พฤษภาคม 2562.

MGR Online, ‘สกมช.เร่งหน่วยงาน CII สร้างมาตรฐานขั้นต่ำป้องภัยไซเบอร์ ก่อนบังคับใช้ 6 ก.ย.นี้’ <https://mgronline.com/cyberbiz/detail/9650000064474> สืบค้นเมื่อ 25 กรกฎาคม 2565.

กระทรวงการต่างประเทศ, ‘ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน - Universal Declaration of Human Rights’ <https://humanrights.mfa.go.th/th/humanrights/obligation/index.php> สืบค้นเมื่อ 16 พฤษภาคม 2565.

ขวัญเรียม แก้วสุวรรณ, ‘โดนล้วงอื้อ! ย้อนรอย 3 เหตุการณ์คนไทยโดน แฮกเกอร์ ออนไลน์’ <https://www.komchadluek.net/quality-life/well-structured/546508> สืบค้นเมื่อวันที่ 9 กรกฎาคม 2567.

ธีรภัทร เจริญสุข, ‘พยัคฆ์ทะยาน โครงการก้าวกระโดดแบบเอสโตเนีย จิตวิญญาณสตาร์ทอัพระดับประเทศ’ <https://www.the101.world/estonia-startup-country> สืบค้นเมื่อวันที่ 24 พฤษภาคม 2562.

ราชกิจจานุเบกษา, ‘ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559’ <https://ictlawcenter.etda.or.th/files/law/file/78/e37c4fe15bbaeee06907537bdd4a7795.pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

ราชกิจจานุเบกษา, ‘พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562’ <http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF> สืบค้นเมื่อ 27 พฤษภาคม 2562.

สกมช., ‘คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)’ <https://www.ncsa.or.th/ncsc.html> สืบค้นเมื่อ 18 เมษายน 2565.

--, ‘คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)’ <https://www.ncsa.or.th/ncsc2.html> สืบค้นเมื่อ 18 เมษายน 2565.

สำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน), ‘ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)’ <https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf> สืบค้นเมื่อ 18 มีนาคม 2562.

--, ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)’ <https://ratchakitcha.soc.go.th/documents/17236495.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

--, ‘ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17176753.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

--, ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17175301.pdf> สืบค้นเมื่อ 18 เมษายน 2565.

--, ‘ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564’ <https://ratchakitcha.soc.go.th/documents/17190586.pdf> สืบค้นเมื่อ 25 กรกฎาคม 2565.

ภาษาต่างประเทศ

AppInChina, ‘What is an MLPS Filing and who needs one?’ <https://www.appinchina.co/what-is-an-mlps-filing-and-who-needs-one> สืบค้นเมื่อ 31 มีนาคม 2566.

ASEAN, ‘ASEAN CYBERSECURITY COOPERATION STRATEGY (2021 – 2025)’ <https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf> สืบค้นเมื่อ 25 สิงหาคม 2565.

--, ‘ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME’ <https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf> สืบค้นเมื่อ 19 สิงหาคม 2565.

--, ‘ASEAN LEADERS’ STATEMENT ON CYBERSECURITY COOPERATION’ <https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf> สืบค้นเมื่อ 19 สิงหาคม 2565.

--, ‘CHAIRMAN’S STATEMENT OF THE 42ND ASEAN SUMMIT LABUAN BAJO, INDONESIA, 10-11 MAY 2023’ <https://asean.org/wp-content/uploads/2023/05/FINAL-Chairmans-Statement-42nd-ASEAN-Summit-1.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

Council of the European Union, ‘Regulation of the European Parliament and of the Council on ENISA (The European Union Agency for Cybersecurity) and on Information and Communication Technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (EU Cybersecurity Act)’ <https://data.consilium.europa.eu/doc/document/PE-86-2018-REV-1/en/pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

Cyber Security Agency of Singapore, ‘Cybersecurity Act’ <https://www.csa.gov.sg/legislation/cybersecurity-act> สืบค้นเมื่อ 31 มีนาคม 2566.

--, ‘The Singapore Cybersecurity Strategy 2021’ <https://www.csa.gov.sg/Tips-Resource/publications/2021/singapore-cybersecurity-strategy-2021> สืบค้นเมื่อ 19 เมษายน 2566.

European Commission, ‘New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient’ <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391> สืบค้นเมื่อ 31 มีนาคม 2565.

EURONEWS, ‘EU reveals new cybersecurity strategy with plans for a joint unit and an AI-enabled Cyber Shield’ <https://www.euronews.com/my-europe/2020/12/16/eu-reveals-new-cybersecurity-strategy-with-plans-for-a-joint-unit-and-an-ai-enabled-cyber-> สืบค้นเมื่อ 19 สิงหาคม 2565.

European Parliament, ‘LEGISLATIVE TRAIN SCHEDULE: EU CYBERSECURITY AGENCY AND THE CYBERSECURITY ACT’ <http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-eu-cybersecurity-agency-and-cybersecurity-act> สืบค้นเมื่อ 19 พฤษภาคม 2562.

European Union, ‘Directive on Security of Network and Information Systems 2016’ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016L1148&from=EN> สืบค้นเมื่อ 25 มีนาคม 2565.

--, ‘EU Cyber Security Strategy’ <https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie> สืบค้นเมื่อ 15 พฤษภาคม 2565.

--, ‘EU Cyber Security Act 2018’ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881> สืบค้นเมื่อ 25 มีนาคม 2565.

European Union Agency for Cybersecurity, ‘Main incidents in the EU and worldwide’ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport> สืบค้นเมื่อ 19 สิงหาคม 2565.

--, ‘Supporting the implementation of Union policy and law regarding cybersecurity’ <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new> สืบค้นเมื่อ 19 สิงหาคม 2565.

Freedom Online Coalition, ‘Recommendations for human rights based approaches to cybersecurity’ <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/FOC-WG1-Recommendations-discussion-draft-IGF-20151.pdf> สืบค้นเมื่อ 22 พฤษภาคม 2562.

Government of Canada, ‘China’s cybersecurity regime’ <https://www.tradecommissioner.gc.ca/china-chine/cyber-security_cyber-securite_china-chine.aspx?lang=eng> สืบค้นเมื่อ 25 มีนาคม 2566.

Jamie P. Horsley, ‘Behind the Facade of China’s Cyber Super-Regulator’ <https://digichina.stanford.edu/work/behind-the-facade-of-chinas-cyber-super-regulator/> สืบค้นเมื่อ 25 มีนาคม 2566.

International Telecommunication Union, ‘SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security: Overview of cybersecurity Recommendation ITU-T X.1205’ 2 <https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items.> สืบค้นเมื่อ 19 พฤษภาคม 2562.

National Institute of Standards and Technology, ‘Cybersecurity Framework Manufacturing Profile’ <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf> สืบค้นเมื่อ 19 พฤษภาคม 2562.

National People's Congress of the People's Republic of China, ‘中华人民共和国网络安全法’ (The People's Republic of China Cyber Security Law) <http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm> สืบค้นเมื่อ 19 พฤษภาคม 2562.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), ‘WannaCry Campaign: Potential State Involvement Could Have Serious Consequences’ <https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/> สืบค้นเมื่อ 16 พฤษภาคม 2562.

NCCIC, Department of Homeland Security, ‘Cyber Threat Source Descriptions’ <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions> สืบค้นเมื่อ 15 พฤษภาคม 2562.

Rogier Creemers, Graham Webster, and Paul Triolo, ‘Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017)’ Stanford University <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> สืบค้นเมื่อ 25 มีนาคม 2566.

Russell Brandom, ‘A new ransomware attack is infecting airlines, banks, and utilities across Europe’ <https://www.theverge.com/2017/6/27/15879480/petrwrap-virus-ukraine-ransomware-attack-europe-wannacry> สืบค้นเมื่อ 19 พฤษภาคม 2562.

The State Council of the People's Republic of China, ‘中华人民共和国网络安全法’ <https://www.gov.cn/xinwen/2016-11/07/content_5129723.htm> สืบค้นเมื่อ 25 มีนาคม 2566.

Thomas Brewster, ‘Another Massive Ransomware Outbreak Is Going Global Fast’ <https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/#1fe143c37abd> สืบค้นเมื่อ 19 พฤษภาคม 2562.

‘UN Internet Governance Forum Charter of Human Rights and Principles for the Internet’ <https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf> สืบค้นเมื่อ 17 พฤษภาคม 2562.

UNDP, ‘Indicators for Human Rights Based Approaches to Development in UNDP Programming: A Users’ Guide 2006’ <http://www.undp-aciac.org/publications/other/undp/hr/humanrights-indicators-06e.pdf> สืบค้นเมื่อ 29 พฤษภาคม 2562.

United Nations, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ <https://dig.watch/wp-content/uploads/2022/08/UN-GGE-2015-report.pdf> สืบค้นเมื่อ 22 พฤษภาคม 2562.

United Nations, ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security’ <https://undocs.org/A/70/174> สืบค้นเมื่อ 25 มีนาคม 2564.

US Senate, ‘CYBERSECURITY ACT OF 2015’ <https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf> สืบค้นเมื่อ 31 สิงหาคม 2565.

ZDNet, ‘Asean champions regional efforts in cybersecurity, urges international participation’ <https://www.zdnet.com/article/asean-champions-regional-efforts-in-cybersecurity-urges-international-participation/> สืบค้นเมื่อ 25 สิงหาคม 2565.

เอกสารประกอบการประชุม

ภาษาไทย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, ‘รายงานผลการจัดทำกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562’ (การประชุมคณะรัฐมนตรี, 18 กรกฎาคม 2566).

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), ‘Critical Infrastructures (CI) และ Critical Information Infrastructures (CII) ความจำเป็นที่ต้องให้ความสำคัญและต้องทบทวน การประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานที่สำคัญของประเทศ’ (2561).

ภาคผนวก

ภาคผนวก ก
รายงานผลการจัดทำกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ข้อมูล ณ วันที่ ๑ มิ.ย. ๖๖

รายงานผลการจัดทำกฎหมายลำดับรอง
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีแผนกฎหมายลำดับรองตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ทั้งสิ้นจำนวน ๔๑ ฉบับ ในการนี้ สกมช. ได้ดำเนินการจัดทำกฎหมายลำดับรองไปแล้ว โดยมีรายละเอียดการดำเนินการ ดังนี้

ตารางสรุปผลการดำเนินการจัดทำกฎหมายลำดับรอง
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ลำดับที่	สถานะการดำเนินการ	จำนวน (ฉบับ)	หมายเหตุ
๑.	ดำเนินการแล้วเสร็จ	๓๓	
๒.	อยู่ระหว่างดำเนินการ	๗	
๓.	อยู่ระหว่างเสนอคณะรัฐมนตรีเพื่อพิจารณามีมติเห็นชอบ	๑	
	รวมกฎหมายลำดับรองทั้งสิ้น	๔๑	

หมายเหตุ : กฎหมายลำดับรองที่อยู่ระหว่างดำเนินการ จำนวน ๗ ฉบับดังกล่าวมีสถานะเป็นกฎ

๑. การจัดทำกฎหมายลำดับรองที่ได้ดำเนินการแล้วเสร็จ จำนวน ๓๓ ฉบับ ดังนี้

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะการดำเนินการ
๑	มาตรา ๙ (๗)	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์การแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	กมช.	ประธาน กมช.ลงนามและประกาศใช้แล้ว วันที่ ๖มิถุนายน๒๕๖๓
๒	มาตรา ๑๐	ระเบียบ	ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการประชุม พ.ศ. ๒๕๖๔	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้ววันที่ ๑๙ พฤศจิกายน ๒๕๖๔
๓	มาตรา ๑๑	มติ ครม.	หลักเกณฑ์การได้รับเบี้ยประชุมและค่าตอบแทนอื่นของประธานกรรมการและกรรมการในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	ครม.	คณะรัฐมนตรีมีมติเห็นชอบหลักเกณฑ์ดังกล่าวแล้วเมื่อวันที่ ๑๓ สิงหาคม ๒๕๖๓
๔	มาตรา ๑๒ วรรคสาม	ระเบียบ	ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยหลักเกณฑ์การสรรหากรรมการผู้ทรงคุณวุฒิในคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๓	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๓
๕	มาตรา ๓ ประกอบ	ประกาศ	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคง	กกม.	ประกาศในราชกิจจานุเบกษา เล่ม ๑๓๘ ตอนพิเศษ ๒๐๘ ง

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะการดำเนินการ
	มาตรา ๑๓ วรรคหนึ่ง (๔) มาตรา ๑๓ วรรคสองและ มาตรา ๕๔		ปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ พ.ศ. ๒๕๖๔		เมื่อวันที่ ๖ กันยายน ๒๕๖๔
๖	มาตรา ๑๔	ระเบียบ	ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคง ปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจให้ ปฏิบัติการแทนคณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕	กกม.	ประกาศในราชกิจจา นุเบกษา เล่มที่ ๑๓๙ ตอนพิเศษ ๒๕๔ ง ลงวันที่ ๒๖ ตุลาคม ๒๕๖๕
๗	มาตรา ๑๗	ระเบียบ	ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคง ปลอดภัยไซเบอร์ ว่าด้วยการประชุมของ คณะกรรมการกำกับดูแลด้านความมั่นคง ปลอดภัยไซเบอร์ และอนุกรรมการ พ.ศ. ๒๕๖๕	กกม.	ประธาน กกม. ลงนามและประกาศ ใช้แล้วเมื่อวันที่ ๑๕ มีนาคม ๒๕๖๕
๘	มาตรา ๑๘	มติ ครม.	หลักเกณฑ์การได้รับเบี้ยประชุมและ ค่าตอบแทนอื่นของประธานกรรมการและ กรรมการ ประธานอนุกรรมการและ อนุกรรมการ ที่ กกม. แต่งตั้ง	ครม.	คณะรัฐมนตรีมีมติ เห็นชอบหลักเกณฑ์ ดังกล่าวแล้ว เมื่อวันที่ ๑๓ สิงหาคม ๒๕๖๓
๙	มาตรา ๑๙ วรรคสอง	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนด ระดับความรู้ความชำนาญด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงาน เจ้าหน้าที่ พ.ศ. ๒๕๖๔	กมช.	ประกาศในราชกิจจา นุเบกษา เล่มที่ ๑๓๘ ตอนพิเศษ ๒๙๙ ง ลงวันที่ ๗ ธันวาคม ๒๕๖๔
๑๐	มาตรา ๑๙ วรรคสาม	ประกาศ	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคง ปลอดภัยไซเบอร์ เรื่อง บัตรประจำตัว พนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔	กกม.	ประธาน กกม. ลงนามและประกาศ ใช้แล้วเมื่อวันที่ ๑๒ ตุลาคม ๒๕๖๔
๑๑	มาตรา ๒๒ วรรคท้าย	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษา ความมั่นคงปลอดภัยระบบคอมพิวเตอร์ แห่งชาติ พ.ศ. ๒๕๖๔	กมช.	ประกาศในราชกิจจา นุเบกษา เล่มที่ ๑๓๘ ตอนพิเศษ ๑๙๔ ง ลงวันที่ ๒๓ สิงหาคม ๒๕๖๔
๑๒	มาตรา ๒๕ วรรคสาม และวรรคสี่	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์ และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการบริหารสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์	กมช.	ประธาน กมช. ลงนามและ ประกาศใช้แล้ว เมื่อวันที่ ๒๑ กุมภาพันธ์ ๒๕๖๓
๑๓	มาตรา ๒๗ วรรคหนึ่ง (๒)	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์ ว่าด้วยการบริหารงานบุคคล พ.ศ. ๒๕๖๓	กบส.	ประธาน กบส. ลงนามและประกาศ ใช้แล้วเมื่อวันที่ ๒๙ ธันวาคม ๒๕๖๓
๑๔	มาตรา ๒๗ วรรคหนึ่ง (๒)	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงาน คณะกรรมการการรักษาความมั่นคงปลอดภัย	กบส.	ประธาน กบส. ลงนามและประกาศ

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะการดำเนินการ
	ประกอบ มาตรา ๓๗		ไซเบอร์ ว่าด้วยการเงิน บัญชี และงบประมาณ พ.ศ. ๒๕๖๓		ใช้แล้วเมื่อวันที่ ๒๙ ธันวาคม ๒๕๖๓
๑๕	มาตรา ๒๗ วรรคหนึ่ง (๒) ประกอบ มาตรา ๓๗	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยงานสารบรรณ และระบบสารบรรณอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๑ กุมภาพันธ์ ๒๕๖๔
๑๖	มาตรา ๒๗ วรรคหนึ่ง (๒) ประกอบ มาตรา ๓๗	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการจัดองค์กร การกำหนดระดับตำแหน่งและชื่อตำแหน่ง ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๑ กุมภาพันธ์ ๒๕๖๔
๑๗	มาตรา ๒๗ วรรคหนึ่ง (๒)	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๒๙ มิถุนายน ๒๕๖๔
๑๘	มาตรา ๒๗ วรรคหนึ่ง (๒)	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยสวัสดิการและสิทธิประโยชน์อื่นสำหรับพนักงาน พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑ มิถุนายน ๒๕๖๔
๑๙	มาตรา ๒๗ วรรคสอง	ระเบียบ	ระเบียบคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการปฏิบัติงานและการประชุมของคณะอนุกรรมการ พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๒๕ สิงหาคม ๒๕๖๔
๒๐	มาตรา ๒๗ วรรคท้าย	ระเบียบ	ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการแต่งตั้งที่ปรึกษาของคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๙ กันยายน ๒๕๖๕
๒๑	มาตรา ๒๘	ประกาศ	ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยเบี้ยประชุม ค่าตอบแทนอื่น ของประธานกรรมการและกรรมการ ประธานอนุกรรมการและอนุกรรมการ ที่คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แต่งตั้ง พ.ศ. ๒๕๖๓	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๗ สิงหาคม ๒๕๖๓
๒๒	มาตรา ๓๔	ระเบียบ	ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยหลักเกณฑ์การประเมินผลการปฏิบัติงานของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๔	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๙ พฤศจิกายน ๒๕๖๔
๒๒ (ต่อ)			ระเบียบคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยหลักเกณฑ์		ประธาน กมช.

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะการดำเนินการ
			การประเมินผลการปฏิบัติงานของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๖ (ฉบับแก้ไขเพิ่มเติม)		ลงนามและประกาศใช้แล้วเมื่อวันที่ ๒๘ มกราคม ๒๕๖๖
๒๓	มาตรา ๓๖ วรรคสาม	ข้อบังคับ	ข้อบังคับคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๔	กบส.	ประธาน กบส. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๑ กุมภาพันธ์ ๒๕๖๔
๒๔	มาตรา ๔๗ วรรคหนึ่งและวรรคสอง	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง คุณสมบัติหรือประสบการณ์ของผู้เชี่ยวชาญ พ.ศ. ๒๕๖๔	กมช.	ประธาน กมช. ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๓ กรกฎาคม ๒๕๖๔
๒๕	มาตรา ๔๗ วรรคท้าย	ประกาศ	ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง บัตรประจำตัวผู้เชี่ยวชาญ พ.ศ. ๒๕๖๔	สกมช.	เลขาธิการ ลงนามและประกาศใช้แล้วเมื่อวันที่ ๑๒ ตุลาคม ๒๕๖๔
๒๖	มาตรา ๔๙	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔	กมช.	ประกาศในราชกิจจานุเบกษา เล่มที่ ๑๓๘ ตอนพิเศษ ๑๙๔ ง ลงวันที่ ๒๓ สิงหาคม ๒๕๖๔
๒๗	มาตรา ๕๐	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔	กมช.	ประกาศในราชกิจจานุเบกษา เล่มที่ ๑๓๘ ตอนพิเศษ ๑๙๔ ง ลงวันที่ ๒๓ สิงหาคม ๒๕๖๔
๒๘	มาตรา ๖๐ วรรคท้าย	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔	กมช.	ประกาศในราชกิจจานุเบกษา เล่มที่ ๑๓๘ ตอนพิเศษ ๓๐๓ ง ลงวันที่ ๑๑ ธันวาคม ๒๕๖๔
๒๙-๓๑	มาตรา ๙ (๑) (๒) (๓) ประกอบ มาตรา ๔๓	ประกาศ	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐)	กมช.	ประกาศในราชกิจจานุเบกษา เล่มที่ ๑๓๙ ตอนพิเศษ ๒๘๘ ง ลงวันที่ ๙ ธันวาคม ๒๕๖๕
๒๙	มาตรา ๙(๑) ประกอบ มาตรา ๔๓	นโยบายและแผน	นโยบายและแผนรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐	ครม.	คณะรัฐมนตรีมีมติเห็นชอบนโยบาย

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะการดำเนินการ
๓๐	มาตรา ๙ (๒)	นโยบายการบริหาร	นโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์	ครม.	และแผนดังกล่าวเมื่อวันที่ ๒๐ กันยายน ๒๕๖๕
๓๑	มาตรา ๙ (๓)	แผนปฏิบัติการ	แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐	ครม.	
๓๒	มาตรา ๓๖ (๔)	ประกาศ	ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการสรรหารองเลขาธิการและผู้ช่วยเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๖	สกมช.	ลธ.กมช.ลงนามและประกาศใช้แล้วเมื่อวันที่ ๔ เมษายน ๒๕๖๖
๓๓	มาตรา ๕๗	ประกาศ	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖	กกม.	ประกาศในราชกิจจานุเบกษา เล่มที่ ๑๔๐ ตอนพิเศษ ๑๐๗ ง ลงวันที่ ๙ พฤษภาคม ๒๕๖๖

๒. การจัดทำกฎหมายลำดับรองที่อยู่ระหว่างดำเนินการ จำนวน ๗ ฉบับ ดังนี้

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะดำเนินการ
๑	มาตรา ๙ (๔)	ประกาศ (มีสถานะเป็นกฎ)	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.	กมช.	อยู่ระหว่างดำเนินการ
๒	มาตรา ๙ (๔)	ประกาศ (มีสถานะเป็นกฎ)	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน พ.ศ.	กมช.	อยู่ระหว่างดำเนินการ
๓	มาตรา ๙ (๔)	ประกาศ (มีสถานะเป็นกฎ)	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานเอกชน พ.ศ.	กมช.	อยู่ระหว่างดำเนินการ
๔	มาตรา ๙ (๕)	ประกาศ (มีสถานะเป็นกฎ)	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคง	กมช.	อยู่ระหว่างดำเนินการ

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะดำเนินการ
			ปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.		
๕	มาตรา ๑๓ (๕)	ระเบียบ (มีสถานะเป็นกฎ)	ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ.	กกม.	อยู่ระหว่างดำเนินการ
๖	มาตรา ๒๓ (๓)	ระเบียบ (มีสถานะเป็นกฎ)	ระเบียบสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ว่าด้วยการให้ทุนส่งเสริมและสนับสนุนการดำเนินกิจการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.	สกมช.	อยู่ระหว่างดำเนินการ
๗	มาตรา ๒๓ (๔)	ประกาศ (มีสถานะเป็นกฎ)	ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์และอัตราในการเรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.	สกมช. โดยความเห็นชอบของ กบส.	อยู่ระหว่างดำเนินการ

๓. การจัดทำกฎหมายลำดับรองที่อยู่ระหว่างเสนอ ครม. เพื่อพิจารณามีมติเห็นชอบ จำนวน ๑ ฉบับ ดังนี้

ลำดับ	มาตรา	ประเภท	เรื่อง	ผู้ตรา	สถานะดำเนินการ
๑	มาตรา ๕ วรรคสาม	ระเบียบ	ระเบียบ ว่าด้วยหลักเกณฑ์และวิธีการสรรหากรรมการผู้ทรงคุณวุฒิในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.	ครม.	อยู่ระหว่างเสนอ ครม. พิจารณา (สกมช. เสนอเรื่องตั้งแต่วันที่ ๙ ตุลาคม ๒๕๖๕)

หมายเหตุ : ครม. หมายถึง คณะรัฐมนตรี
กมช. หมายถึง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม. หมายถึง คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
กบส. หมายถึง คณะบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ประวัติผู้เขียน

ชื่อ	อมรรัตน์ อินนุมาตร
วุฒิการศึกษา	ปีการศึกษา 2566: นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์

ผลงานทางวิชาการ

อมรรัตน์ อินนุมาตร, ‘กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์กับการคุ้มครองสิทธิมนุษยชน : ศึกษากรณีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยธรรมศาสตร์ 2566).