

นโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์ของพลเมืองโลก

ปัญญาธิสาร องค์กรปรัชญากุล¹

วันที่รับบทความ: 30 มิถุนายน 2566

วันที่แก้ไขครั้งสุดท้าย: 1 พฤศจิกายน 2566

วันที่ตอบรับตีพิมพ์: 8 พฤศจิกายน 2566

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการศึกษานโยบายด้านกฎหมายของประเทศต่างๆ ที่ออกมาใช้กำกับ ดูแล ควบคุม ป้องกัน ความปลอดภัยทางไซเบอร์ให้กับพลเมืองของประเทศ และพลเมืองโลก ผลการศึกษาพบว่า วิวัฒนาการในโลกไซเบอร์ได้พัฒนาจนเป็นวัฒนธรรมไซเบอร์ ประเทศต่างๆ ทั่วโลก รวมทั้งประเทศมหาอำนาจ กลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศจีน รวมถึงประเทศไทย ได้หาหนทางในการแก้ไขปัญหาและอาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ มีการหามาตรการมาทำการควบคุม ดูแล ทั้งด้านนโยบายด้านกฎหมาย และด้านอื่นๆ ซึ่งนโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์นั้นทุกประเทศได้มีการกำหนดนโยบายความปลอดภัยไซเบอร์เป็นนโยบายหลักที่สำคัญ ด้านกฎหมายทุกประเทศได้มีการออกกฎหมายความปลอดภัยทางไซเบอร์ และกำหนดให้จัดตั้งองค์กรที่มาควบคุมดูแลด้านความปลอดภัยทางไซเบอร์เป็นการเฉพาะ โดยจะมีลักษณะหลักเกณฑ์ทางปฏิบัติคล้ายคลึงกัน จะแตกต่างกันบ้างเกี่ยวกับการมุ่งเน้นรักษาความมั่นคงอธิปไตยของแต่ละประเทศ และวิธีการนำไปบังคับใช้ที่ขึ้นอยู่กับบริบทการปกครองและสังคมของแต่ละประเทศ พลเมืองของประเทศไทยและพลเมืองโลกในยุคนี้ส่วนใหญ่เกี่ยวข้องอยู่ในโลกไซเบอร์ จึงควรศึกษาริบทด้านกฎหมายการดูแลรักษาความปลอดภัยไซเบอร์ของประเทศที่ต้องการทำธุรกรรมในโลกไซเบอร์ก่อนเพื่อลดความเสี่ยงภัยทางไซเบอร์

คำสำคัญ นโยบาย, กฎหมาย, ความปลอดภัย, ไซเบอร์, พลเมืองดิจิทัล

¹ อาจารย์ ดร. คณะนิติศาสตร์ มหาวิทยาลัยเกริก กรุงเทพฯ 10220 อีเมล: pantip2ong@gmail.com

Cyber Security Legal Policies for Global Citizens

Pannisa Ongprachayakul²

Received: 30 June 2023

Revised: 1 November 2023

Accepted: 8 November 2023

Abstract

This article aims to study the legal policies of various countries, which have been enacted to regulate, supervise, control, and protect the cyber security for citizens of the countries and citizens of the world. As the result of the study, it is found that the evolution in the cyberworlds has developed into a cyberculture; countries around the world, including superpowers, European Union countries, the United States of America, China, as well as Thailand, have found a way to solve problems and crimes that occur in the cyberworlds. Measures have been sought to control and regulate in terms of policy, law and other aspects. As for the cyber security legal policy, every country has set cyber security policy as an important main policy. In regard to the law, every country has enacted cyber security laws, and required the establishment of an organization to specifically supervise the cyber security, with similar principles of practice; certain differences lie on the focus on maintaining the security and sovereignty of each country and the method of enforcement, which depends on the administrative and social context of each country. Most of the citizens of Thailand and the world nowadays are involved in the cyberworlds; therefore, one should first study the cyber security legal context of the country where one wants to conduct transactions in the cyberworlds in order to reduce cyber risks.

Keywords Policy, Law, Security, Cyber, Digital Citizens

² Lecturer, Ph.D., Faculty of Law, Krirk University, Bangkok 10220. E-mail: pantip2ong@gmail.com

1. บทนำ

วิวัฒนาการของโลกไซเบอร์เกิดขึ้นมาหลายทศวรรษแล้ว เริ่มจากการที่มนุษย์มีการคิดค้นสร้างเทคโนโลยีขึ้นมาใช้อำนวยความสะดวกในการใช้ชีวิตประจำวันทั้งการผลิต คอมพิวเตอร์ โทรศัพท์ เครื่องมือสื่อสารต่างๆ ขยายการพัฒนาเทคโนโลยีสู่ระบบการทำงาน ชุมชน สังคม เพื่ออำนวยความสะดวกให้กับตัวเองและพลเมืองโลก พัฒนาจนเป็นการสื่อสารทางดิจิทัลในโลกไซเบอร์ที่พลเมืองโลกใช้ติดต่อกันได้ทั่วโลกทุกหนแห่งอย่างไร้พรมแดน ปัจจุบันนี้ประเทศต่างๆ และประเทศมหาอำนาจ ทั้งกลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศจีน ที่มีศักยภาพและเงินทุนต่างแข่งขันกันพัฒนาเทคโนโลยีและเครื่องมือสื่อสารต่างๆ ออกกันมาอย่างมากมายและรวดเร็วในด้านต่างๆ เช่น ด้านการพัฒนา เศรษฐกิจได้พัฒนาระบบการทำธุรกรรมทางการเงินเชื่อมต่อเป็นเครือข่ายดิจิทัลเป็นโลกไซเบอร์อย่างสมบูรณ์แบบ ด้านความมั่นคงได้นำเทคโนโลยีไปพัฒนาอาวุธยุทโธปกรณ์ที่มีประสิทธิภาพ การทำลายล้างสูงและรวดเร็ว ด้านสังคมการดำรงชีวิตประจำวันของพลเมืองได้พัฒนาเครื่องมือสื่อสารจนกลายเป็นการอำนวยความสะดวกในการใช้ชีวิตด้วยโทรศัพท์เพียงเครื่องเดียว เป็นต้น เพื่อแข่งขันกันทางเทคโนโลยีและใช้ประโยชน์จากพื้นที่ในโลกไซเบอร์

โลกไซเบอร์ในยุคดิจิทัลที่เทคโนโลยีเข้ามามีบทบาทสำคัญที่ทำให้การดำเนินชีวิต มีการเปลี่ยนแปลงอย่างรวดเร็ว สร้างความท้าทายให้กับคนในสังคมทุกช่วงวัย สังคมดิจิทัลเป็นสังคมที่ทำให้มนุษย์แลกเปลี่ยนเรียนรู้ เชื่อมโยง และผสมผสานกันด้วยเทคโนโลยีสารสนเทศ ทำให้เทคโนโลยีเป็นส่วนหนึ่งของชีวิตประจำวัน โดยเฉพาะการติดต่อสื่อสาร การแลกเปลี่ยนข้อมูล หรือแม้แต่การทำธุรกรรมการเงิน เทคโนโลยีสารสนเทศจึงมีส่วนในการขับเคลื่อนให้เกิดเป็นสังคมดิจิทัล

ความเป็นพลเมืองดิจิทัล (Digital Citizenship) เป็นพลเมืองที่มีความสามารถในการใช้อินเทอร์เน็ตในการบริหารจัดการ ควบคุม กำกับตน รู้ผิดรู้ถูก และรู้เท่าทัน เป็นบรรทัดฐานในการใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม มีความรับผิดชอบ เรียนรู้ที่จะใช้เทคโนโลยีอย่างชาญฉลาด และปลอดภัย พลเมืองดิจิทัลจึงต้องตระหนักถึงโอกาสและความเสี่ยงในโลกดิจิทัล เข้าใจถึงสิทธิและความรับผิดชอบในโลกออนไลน์ ความเป็นพลเมืองดิจิทัล นับเป็นมาตรฐานหนึ่งด้านเทคโนโลยีการศึกษาที่เสนอโดยสมาคมเทคโนโลยีการศึกษานานาชาติ (International Society for Technology in Education: ISTE) เพื่อให้ผู้เรียนสามารถแสดงความเข้าใจประเด็นทางสังคม วัฒนธรรม และความเป็นมนุษย์ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และปฏิบัติตนอย่างมีจริยธรรมและตามครรลองกฎหมายให้ใช้ข้อมูลข่าวสารได้อย่างปลอดภัย ถูกกฎหมาย

ซึ่งมีความสำคัญในทักษะแห่งการเรียนรู้ในศตวรรษที่ 21 แยกองค์ประกอบได้เป็น 4 มิติ (ฉัตรพงศ์ ชูแสงนิล, 2561) ดังนี้

(1) มิติการรักษาอัตลักษณ์และข้อมูลส่วนบุคคล การสร้างอัตลักษณ์ออนไลน์ถือเป็นปรากฏการณ์ใหม่ ที่ทำให้บุคคลสามารถแสดงออกถึงความเป็นตัวตนของตนเองต่อสังคมภายนอก ด้วยการอาศัยช่องทางการสื่อสารผ่านเว็บไซต์เครือข่ายสังคมเพื่ออธิบายรูปแบบใหม่ของการสื่อสารแบบมีปฏิสัมพันธ์ทางอินเทอร์เน็ตที่ทำให้เกิดการแสดงออกเกี่ยวกับตัวตนผ่านเว็บไซต์เครือข่ายสังคมต่างๆ เพื่อการสื่อสารและเชื่อมต่อความสัมพันธ์กับบุคคลอื่น การที่ผู้ใช้ปรับตัวให้เข้ากับเทคโนโลยีสื่อใหม่และการใช้กลยุทธ์ต่างๆ เพื่อนำเสนอตัวตนบนโลกออนไลน์ พลเมืองดิจิทัลจะต้องมีความตระหนักในความเท่าเทียมกันทางดิจิทัล การรักษาความปลอดภัยของข้อมูลตนเองในสังคมดิจิทัล ที่มีความจำเป็นจะต้องบริหารจัดการข้อมูลของตนเอง รู้ว่าข้อมูลใดควรเผยแพร่และข้อมูลใดไม่ควรเผยแพร่ การปกป้องข้อมูลส่วนบุคคล การจัดการกับความเสี่ยงของข้อมูลของตนในสื่อสังคมดิจิทัล

(2) มิติของกิจกรรมบนสื่อสังคมดิจิทัล พลเมืองดิจิทัล มีความจำเป็นต้องมีความสามารถในการจัดการธุรกรรมการเงินทางอินเทอร์เน็ต เช่น การซื้อขายสินค้าในอินเทอร์เน็ต บัตรเครดิต อิเล็กทรอนิกส์ การค้าแบบดิจิทัล การเมือง เศรษฐกิจ การมีส่วนร่วมวัฒนธรรมพลเมืองดิจิทัล ต้องรู้จักใช้ศักยภาพของอินเทอร์เน็ตในการมีส่วนร่วมทางการเมือง เศรษฐกิจ และสังคม อินเทอร์เน็ตเป็นได้ทั้งเครื่องมือเพิ่มการมีส่วนร่วมทางการเมืองในระบบ เช่น รัฐบาลใช้ อินเทอร์เน็ตในการรับฟังความเห็นของประชาชนก่อนออกกฎหมาย การลงคะแนนเสียง อิเล็กทรอนิกส์ หรือการยื่นคำร้องออนไลน์ อีกทั้งพลเมืองดิจิทัลจะต้องรักษาความสัมพันธ์ที่ดีกับคนในสังคมดิจิทัล มีน้ำใจการแสดงความเห็นอกเห็นใจ เสียใจ เห็นด้วย ไม่เห็นด้วย ยินดี สนุกสนาน เพื่อสานสัมพันธ์กับผู้คนในโลกออนไลน์ การสร้างความสัมพันธ์ระหว่างตนเองกับสังคมและสิ่งแวดล้อมเพื่อให้สามารถอยู่ในสังคมได้อย่างมีความสุข

(3) มิติทักษะและความสามารถในการสภาพแวดล้อมดิจิทัล พลเมืองดิจิทัลต้องมีความรู้ความสามารถในการเข้าถึง ใช้ สร้างสรรค์ ประเมิน สังเคราะห์ และสื่อสารข้อมูลข่าวสารผ่านเครื่องมือดิจิทัล ดังนั้น พลเมืองยุคใหม่จึงต้องมีความรู้ด้านเทคนิคในการเข้าถึงและใช้เครื่องมือดิจิทัล เช่น คอมพิวเตอร์ สมาร์ทโฟน แท็บเล็ต ได้อย่างเชี่ยวชาญ รวมถึงทักษะในการรู้คิดขั้นสูง เช่น ทักษะการคิดอย่างมีวิจารณญาณ ซึ่งจำเป็นต่อการเลือก จัดประเภท วิเคราะห์ ตีความ และเข้าใจข้อมูลข่าวสาร มีความรู้และทักษะในสภาพแวดล้อมดิจิทัล การรู้ดิจิทัลโดยมุ่งให้เป็นผู้ใช้ที่ดี เป็นผู้เข้าใจบริบทที่ดี และเป็นผู้สร้างเนื้อหาทางดิจิทัลที่ดี ในสภาพแวดล้อมสังคมดิจิทัล

(4) มิติจริยธรรมทางดิจิทัล พลเมืองดิจิทัล จะต้องเป็นผู้รู้กฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์ การกระทำความผิดทางคอมพิวเตอร์ การใช้เทคโนโลยีอย่างรู้จริยธรรม รู้จักคุณค่าและจริยธรรมจากการใช้เทคโนโลยี มีความรู้ในงานลิขสิทธิ์และเคารพทรัพย์สินทางปัญญาของผู้อื่น และการปกป้องตนเองและชุมชน มีความรับผิดชอบทางดิจิทัล รู้จักสิทธิเสรีภาพให้เกียรติในการพูดการกระทำในสังคมดิจิทัล มารยาททางดิจิทัล เข้าใจถึงการรับความเสี่ยงและการบริหารจัดการความเสี่ยงในโลกออนไลน์ เช่น การไม่ไปรังแกและสามารถจัดการกับการถูกรังแกบนโลกไซเบอร์ (Cyberbullying) รวมไปถึงการเกี่ยวพาราสี การเหยียดผิว-เหยียดชนชั้น รวมไปถึงเนื้อหาต่างๆ ที่สุ่มเสี่ยง เช่น เนื้อหาที่มีความรุนแรง ไปเบียดเบียนลามกหายาเสพติด

พลเมืองดิจิทัลที่ดีจะต้องมีทักษะทางดิจิทัลมีชุดทักษะและความรู้ทั้งในเชิงเทคโนโลยีและการคิดขั้นสูง ในการรักษาอัตลักษณ์และข้อมูลส่วนบุคคลของตนเอง เคารพสิทธิเสรีภาพการใช้ข้อมูลทั้งของตนเองและผู้อื่น สามารถบริหารจัดการกิจกรรมบนสื่อสังคมดิจิทัล รวมถึงการสร้างความสัมพันธ์ระหว่างตนเองกับสังคมและสิ่งแวดล้อม มีความรู้ด้านเทคนิคในการเข้าถึงและใช้เครื่องมือดิจิทัล มีทักษะการคิดอย่างมีวิจารณญาณ รู้จักคุณค่าและจริยธรรมจากการใช้เทคโนโลยี มีความรู้ในงานลิขสิทธิ์และเคารพทรัพย์สินทางปัญญาของผู้อื่น การปกป้องตนเองและชุมชน และเกิดความรับผิดชอบต่อทางดิจิทัล

แต่เมื่อโลกไซเบอร์มีการพัฒนาขึ้นอย่างรวดเร็วและรวดเร็วในยุคดิจิทัล ก็มีปัญหาดังกล่าว ในโลกไซเบอร์เกิดขึ้นตามมาด้วยเช่นกัน ดังปัญหาการโจมตีทางไซเบอร์กันระหว่างรัฐชาติยุคแรกนั้นย้อนกลับไปเมื่อเดือนกันยายน ค.ศ. 2007 กลุ่มอาครแห่งหนึ่งทางตะวันออกของซีเรีย ซึ่งเป็นอาคารที่กำลังก่อสร้างโดยใช้คนงานเกาหลีเหนือถูกฝูงบินอิสราเอลโจมตี แต่รัฐบาลซีเรียเป็นฝ่ายที่ตกเป็นเป้าโจมตีกลับนิ่งเงียบ แต่เมื่อเรื่องทราบถึงสื่อสหรัฐอเมริกาและอังกฤษ ก็เริ่มมีเรื่องนี้ออกมามากขึ้นซึ่งรายละเอียดในหนังสือแตกต่างกันออกไปส่วนใหญ่แล้วที่อ้างแหล่งข่าวของรัฐบาลอิสราเอลจะระบุว่า สถานที่ที่ถูกโจมตีเป็นโรงงานผลิตอาวุธนิวเคลียร์ที่ออกแบบโดยเกาหลีเหนือ ซีเรียใช้งบประมาณหลายพันล้านดอลลาร์จัดหาระบบป้องกันทางอากาศ เครื่องบินที่ลอดผ่านเข้ามาในซีเรียทางตุรกีคือเครื่องบินฟอลคอน และอีเกิล ออกแบบสร้างครั้งแรกตั้งแต่ ค.ศ. 1970 ยังห่างไกลศักยภาพการหลบหลีกเรดาร์มากนัก เป็นเรื่องที่น่าเจ็บปวดสำหรับซีเรียคือ ระบบป้องกันทางอากาศราคาแพงของทางการเมืองตามัสกัส ซึ่งเป็นเมืองหลวงของซีเรีย ถูกครอบครองโดยอิสราเอล สิ่งที่ปรากฏบนจอเรดาร์คือความว่างเปล่า จรวดนำวิถีต่อต้านอากาศยานเพื่อป้องกันทางอากาศไม่สามารถระดมยิงได้ ฝูงบินป้องกันน่านฟ้าของซีเรียไม่สามารถขึ้นปฏิบัติการได้ ซึ่งระบบนี้ของซีเรียสร้างโดยรัสเซีย เมื่อนั้นกระทรวงกลาโหมรัสเซียจึงมีโทรศัพท์ดังขึ้นโดยซีเรียต้องการคำตอบว่าระบบนี้ผิดพลาดได้อย่างไร เรื่องนี้อาจทำให้อิหร่านที่กำลังจะซื้อระบบจากรัสเซียต้องตกตะลึงเหมือนกัน

แม้ว่าในความเป็นจริงแล้วอุตสาหกรรมการทหารรัสเซียก็มีดีระดับหนึ่ง และไม่ได้ถึงกับใช้ประชาสัมพันธ์ผลิตภัณฑ์ตัวเองอย่างหนักขนาดนั้น แต่บรรดาเหล่านักรบไซเบอร์แล้วน่าจะไม่ต้องประหลาดใจกับเรื่องนี้ นี่คือตัวอย่าง “สงครามไซเบอร์” การดำเนินการโดยรัฐชาติหนึ่งเพื่อแทรกซึมคอมพิวเตอร์หรือเครือข่ายของอีกรัฐชาติ เพื่อสร้างความเสียหายหรือรบกวนขัดขวางการดำเนินงาน (คลาร์ก และเคนเนด, 2555)

หรือภัยคุกคามทางไซเบอร์ซึ่งเป็นปัญหาที่ไร้พรมแดนและกระทบต่อความปลอดภัยในภาคการเงินทั่วโลกด้วย แม้เทคโนโลยีดิจิทัล จะช่วยให้เราใช้ชีวิตประจำวันสะดวกสบายขึ้น ทั้งการใช้สื่อโซเชียล และการซื้อสินค้าหรือการโอนเงินออนไลน์ แต่ความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์ ทั้งการโจรกรรมข้อมูล การลักยอกเงินจากอินเทอร์เน็ตแบงก์กิ้ง และเงินดิจิทัลกลับเพิ่มมากขึ้น และเป็นความเสี่ยงสำคัญของระบบการเงินโลก ภัยคุกคามทางไซเบอร์เป็นปัญหาที่ไร้พรมแดนและกระทบต่อความปลอดภัยในภาคการเงินทั่วโลก แม้เทคโนโลยีดิจิทัลจะช่วยให้มนุษย์ใช้ชีวิตประจำวันสะดวกสบายขึ้น ทั้งการใช้สื่อโซเชียล และการซื้อสินค้าหรือการโอนเงินออนไลน์ แต่ความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์กลับเพิ่มมากขึ้น และเป็นความเสี่ยงสำคัญของระบบการเงินโลก World Economic Forum จัดเรื่องภัยคุกคามทางไซเบอร์เป็น 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลก ซึ่งภาคการเงินเป็นเป้าหมายหลักของการถูกโจมตี เช่น กรณีธนาคารยักษ์ใหญ่แห่งหนึ่งในสหรัฐอเมริกา ถูกขโมยข้อมูลลูกค้ากว่า 83 ล้านบัญชี เมื่อปี พ.ศ. 2557 ไม่เว้นแม้แต่ธนาคารกลางแห่งหนึ่งในเอเชียใต้ที่ถูกลักยอกเงินสำรองระหว่างประเทศกว่า 81 ล้านดอลลาร์สหรัฐ จากการถูกเจาะเข้าระบบการเงินเมื่อปี พ.ศ. 2559 เช่นเดียวกับอีกธนาคารกลางหนึ่งในอาเซียนที่ประสบเหตุคล้ายกันเมื่อต้นปี แต่โชคดีที่พบความผิดปกติได้ทันเวลา และเมื่อปลายกรกฎาคมที่ผ่านมา ข้อมูลของลูกค้าบางส่วนของสถาบันการเงินในไทย 2 แห่ง ถูกโจรกรรมแต่ไม่พบความเสียหาย (อนุภาค มาตรมุล และอิศราวุฒิ เอี่ยมวิริยะกุล, 2561)

หรือจากข้อมูลขององค์การยูนิเซฟ (UNICEF) ได้รวบรวมผู้เชี่ยวชาญจากยูนิเซฟ และผู้เชี่ยวชาญด้านการป้องกันการกระทำความผิดทางไซเบอร์และเด็กระหว่างประเทศ (International cyberbullying and child protection experts) พร้อมร่วมมือกับเฟซบุ๊ก (Facebook) อินสตาแกรม (Instagram) และทวิตเตอร์ (Twitter) เพื่อสำรวจปัญหาการถูกระรานทางไซเบอร์ (Cyberbully) ของเด็กๆ ทั่วโลก และให้คำแนะนำเกี่ยวกับวิธีการรับมือกับการกลั่นแกล้งทางโลกออนไลน์ พบว่า บ่อยครั้งที่เด็กๆ บอกไม่ได้ว่าสิ่งที่เพื่อนทำกับพวกเขาอยู่คือการแกล้งกันเล่นๆ หรือการพยายามทำร้ายพวกเขาอยู่กันแน่ โดยเฉพาะบนโลกออนไลน์ เพราะพวกเขามักหยอกกันแรงๆ แล้วหัวเราะพร้อมทั้งท้ายด้วยประโยคที่ว่า “แค่ล้อเล่นน่า” หรือ “อย่าคิดมากน่า” เอาไว้ ผู้เชี่ยวชาญจึงให้ข้อสังเกตไว้ว่า หากเมื่อไรเราเริ่มรู้สึกว่

การล่อเล่นนั้นเลยเกิดไปไกลถึงขนาดที่เริ่มทำร้ายจิตใจเราแล้ว นั่นอาจเป็นการ Cyberbully (สำนักงานกองทุนสนับสนุนการสร้างเสริมสุขภาพ, 2563) เป็นต้น

เมื่อโลกไซเบอร์เข้ามาเป็นส่วนหนึ่งของดำรงชีวิตของพลเมืองโลกอย่างรวดเร็วและเห็นได้ชัดเจนมากขึ้นทั่วโลกทั้งในประเทศใหญ่และประเทศเล็ก โลกไซเบอร์เป็นเครือข่ายไร้พรมแดนที่มีการนำมาใช้ประโยชน์ในด้านต่างๆ ดังเช่น ความมั่นคงปลอดภัย ธุรกรรมทางการเงิน สังคมความเป็นอยู่ของพลเมือง ทั้งภายในประเทศเฉพาะกลุ่มเฉพาะเรื่อง รวมทั้งใช้เชื่อมโยงข้ามชาติติดต่อกันระหว่างประเทศ การเปลี่ยนแปลงสู่โลกไซเบอร์ที่สำคัญในด้านมหภาคมีวิวัฒนาการการทำสงครามระหว่างประเทศที่เปลี่ยนแปลงไปทำสงครามระหว่างประเทศกันในโลกไซเบอร์ การทำธุรกรรมทางการเงินเชื่อมต่อเป็นเครือข่ายดิจิทัลในโลกไซเบอร์อย่างไร้พรมแดน ด้านจุลภาคโลกไซเบอร์ได้เข้ามามีบทบาทในการดำรงชีวิตประจำวันของสังคมพลเมืองโลกทุกเพศทุกวัย โดยเฉพาะในวัยเยาว์

ซึ่งวิวัฒนาการพัฒนาการของโลกไซเบอร์ทำให้เกิดปัญหาต่อพลเมืองโลกในทุกด้านด้วยเช่นกัน ทำให้ประเทศต่างๆ ทั่วโลก รวมทั้งประเทศมหาอำนาจ กลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศจีน รวมถึงประเทศไทยด้วย จึงหาหนทางในการแก้ไขปัญหาที่เกิดขึ้นในโลกไซเบอร์ มีการออกมาตรการและกฎหมายต่างๆ ภายในประเทศ รวมกลุ่มประเทศในระดับภูมิภาคทำความตกลงร่วมกันจัดตั้งองค์กรร่วมและออกกฎหมายต่างๆ มาทำการดูแลควบคุมการใช้เครือข่ายในโลกไซเบอร์ทั้งด้านนโยบาย ด้านกฎหมาย และด้านอื่นๆ

ดังนั้น ผู้เขียนจึงสนใจศึกษา นโยบายด้านกฎหมายของประเทศต่างๆ และประเทศไทย กฎหมายสากล และการเชื่อมโยงกฎหมายของกลุ่มประเทศที่ทำความร่วมมือกันที่ออกมาใช้กำกับ ดูแล ควบคุม ป้องกัน ความปลอดภัยทางไซเบอร์ให้กับพลเมืองของประเทศไทยและพลเมืองโลก อันจะเป็นประโยชน์ทำให้ทราบสภาพปัญหาที่เกิดขึ้นในโลกไซเบอร์ การพัฒนานโยบายด้านกฎหมายมาใช้กำกับ ดูแล ควบคุม ป้องกันความปลอดภัยทางไซเบอร์ให้พลเมืองโลกในยุคปัจจุบันอะไรบ้าง และจะมีแนวทางพัฒนาต่อไปในอนาคตอย่างไร

2. ความเป็นมา วิวัฒนาการ และปัญหาของโลกไซเบอร์

ความเป็นมาของโลกไซเบอร์ที่เกิดขึ้นมาหลายทศวรรษแล้วนั้น ประวัติศาสตร์ที่สะท้อนการพัฒนาของวัฒนธรรมไซเบอร์ (Cyber Culture) ในเชิงนวัตกรรมเกิดขึ้นเพราะการพัฒนาเทคโนโลยีคอมพิวเตอร์และการสื่อสารในแต่ละยุคสมัย Macek (2003) อธิบายไว้ว่า ในยุคแรกวัฒนธรรมโลกไซเบอร์กำเนิดมาจากวัฒนธรรมกลุ่มย่อยในกลุ่มแฮกเกอร์ชาวอเมริกันที่ประกอบด้วยนักศึกษา โปรแกรมเมอร์ นักวิจัย นักวิชาการกลุ่มที่ศึกษาวิทยาศาสตร์

คอมพิวเตอร์ ที่มีจุดเริ่มต้นครั้งสำคัญของกลุ่มแฮกเกอร์ที่สถาบันเทคโนโลยีแมสซาชูเซตส์ ในปี ค.ศ. 1959 ต่อมาในปี ค.ศ. 1960 มีแนวคิดการสร้างจักรกลกึ่งสิ่งมีชีวิตกึ่งหุ่นยนต์ (Cyborg) ข้อความไฮเปอร์เท็กซ์ (Hypertext) รวมทั้งยุคเริ่มต้นของเครือข่ายคอมพิวเตอร์ ในปี ค.ศ. 1963 จนถึงสิ้นสุดปี ค.ศ. 1968 ยุคที่สองอยู่ในช่วงปี ค.ศ. 1970-1978 เป็นช่วงที่วัฒนธรรมการพัฒนาโลกไซเบอร์เกิดขึ้นนอกสถาบันการศึกษาหรือมหาวิทยาลัย เหตุการณ์สำคัญในยุคนี้คือการเติบโตครั้งใหญ่ของเทคโนโลยีและคอมพิวเตอร์ที่มีไมโครโพรเซสเซอร์ เป็นหน่วยประมวลผลกลาง (Microcomputer) เริ่มมีกลุ่มคนที่พัฒนาโปรแกรมคอมพิวเตอร์ที่บ้าน ไม่ได้จำกัดแค่ในองค์กรใหญ่ ต่อมาเกิดการใช้คอมพิวเตอร์ที่มีผู้ใช้รายบุคคลขึ้น ในครั้งแรก ยุคที่สามเป็นการปฏิวัติวัฒนธรรมโลกไซเบอร์ที่กลายเป็นการใช้คอมพิวเตอร์เพื่อการทำงานในสำนักงานและเพื่อการบันเทิงทั่วไปที่บ้าน เกิดการพัฒนาเครือข่ายกันอย่างแพร่หลาย และยุคที่สี่เป็นยุคที่เทคโนโลยีคอมพิวเตอร์กลายเป็นเครื่องมือจำเป็นพื้นฐานเกิดขึ้น ตั้งแต่ปี ค.ศ. 1980-1990 เป็นต้นมา (ปองกมล สุรัตน์, 2561)

วิวัฒนาการของโลกไซเบอร์มีการพัฒนาเป็นการสื่อสารทางดิจิทัลกลายเป็นโลกไซเบอร์ที่พลเมืองโลกได้ติดต่อกันได้ทั่วโลกทุกหนแห่งอย่างไร้พรมแดน ประเทศต่างๆ มีการพัฒนาเทคโนโลยีเพื่อใช้ประโยชน์ในการสื่อสารทางดิจิทัลในด้านต่างๆ ทั้งด้านความมั่นคงปลอดภัย ด้านธุรกรรมทางการเงิน ด้านสังคม และด้านอื่นๆ จนเรียกได้ว่าครอบคลุมทุกด้าน

เมื่อโลกไซเบอร์มีการพัฒนาและใช้กันอย่างแพร่หลายและรวดเร็วก็มีปัญหาเกิดขึ้นตามมามากมายด้วยเช่นกัน ซึ่งเกิดจากมนุษย์ด้วยกันเองเป็นผู้ทำให้เกิดปัญหา เช่น คนบางกลุ่มนำเทคโนโลยีไปพัฒนาใช้ในการแสตงหาประโยชน์ในทางที่ผิดหรือก่อคดีอาชญากรรมต่างๆ จนกลายเป็นอาชญากรรมทางไซเบอร์ที่เกิดขึ้นทั้งเรื่องเล็กๆ ภายในประเทศ จนถึงเรื่องใหญ่ที่แพร่ขยายเครือข่ายการกระทำผิดในโลกไซเบอร์อย่างไร้พรมแดน โดย K. Jaishankar นักอาชญาวิทยาชาวอินเดีย ผู้คิดค้นทฤษฎีการเปลี่ยนพื้นที่ ได้นิยามคำว่า อาชญากรรมไซเบอร์ หมายถึง ความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มปัจเจกบุคคล ด้วยมูลเหตุจูงใจทางอาญา ซึ่งผู้กระทำมีเจตนาทำให้เหยื่อเสียชื่อเสียง ทำร้ายร่างกาย หรือจิตใจของเหยื่อไม่ว่าทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่เป็นเครื่องมือ (Halder & Jaishankar, 2011) ความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์ที่เกิดขึ้นในโลก เช่น สงครามทางไซเบอร์ การโจรกรรมข้อมูล การยักยอกเงินจากอินเทอร์เน็ตแบงก์กิ้งและเงินดิจิทัลเพิ่มมากขึ้นอย่างต่อเนื่อง เช่น กรณีของกลุ่มอาคารแห่งหนึ่งทางตะวันออกของซีเรียซึ่งเป็นอาคารที่กำลังก่อสร้างโดยใช้คนงานเกาหลีเหนือถูกฝูงบินอิสราเอลโจมตี ระบบป้องกันทางอากาศราคาแพงของทางเมืองดามัสกัส เมืองหลวงของซีเรียถูกรอบครอบโดยอิสราเอล สิ่งที่ปรากฏบนจอเรดาร์คือความว่างเปล่า จรวดนำวิถีต่อต้านอากาศยานเพื่อป้องกันทางอากาศ

ไม่สามารถระดมยิงได้ ฝูงบินป้องกันน่านฟ้าของซีเรียไม่สามารถขึ้นปฏิบัติการได้ ซึ่งระบบของซีเรียสร้างโดยรัสเซีย หรือสงครามเว็บครั้งที่ 1 (Web War One) ระหว่างเอสโตเนียกับรัสเซีย คืออีกตัวอย่างของสงครามไซเบอร์ที่เกิดขึ้นมานานแล้ว ไม่ว่าจะเป็นสิ่งที่เกิดกับเอสโตเนียที่ขัดแย้งทางความคิดเรื่องอนุสาวรีย์กองทัพแดงที่ตั้งอยู่ในทาลลินน์ (Tallinn) เมืองหลวงของเอสโตเนีย อันเป็นอนุสาวรีย์ที่รำลึกถึงกองทัพแดงที่ปลดแอกสาธารณรัฐริมทะเลบอลติกจากการยึดครองของนาซีในช่วงเวลาที่ชาวรัสเซียเรียกว่า “มหาสงครามรักชาติ” ขณะที่เอสโตเนียถูกบีบบังคับให้เป็นส่วนหนึ่งของสหภาพโซเวียต หลังจากเอสโตเนียได้รับเอกราชแล้วหลายปี เอสโตเนียพยายามหาทางลบล้างสัญลักษณ์ที่บ่งบอกถึงการถูกบีบบังคับให้เป็นส่วนหนึ่งของโซเวียต ขณะที่คนเชื้อสายรัสเซียก็ประกาศปกป้องอนุสาวรีย์จึงเกิดความขัดแย้งกันอย่างรุนแรง ภายหลังความขัดแย้งเคลื่อนย้ายไปสู่โลกไซเบอร์ เอสโตเนียโดนโจมตีด้วยคำสั่ง ดิ Distributed Denial of Service: DDOS) หรือการโจมตีด้วยการระดมคำสั่งจันเซิร์ฟเวอร์ไม่สามารถให้บริการได้ในช่วงปี ค.ศ. 2007 ชาวเอสโตเนียไม่สามารถใช้บริการธนาคารออนไลน์ เว็บไซต์สื่อต่างๆ หรือบริการอิเล็กทรอนิกส์ของรัฐบาลได้ ภายหลังเอสโตเนียโดนโจมตี นาโต้จัดตั้งศูนย์กลางกลาโหมเพื่อป้องกันภัยไซเบอร์ โดยดำเนินการอย่างเป็นทางการเมื่อ ค.ศ. 2008 (คลาร์ก และเคนค, 2555)

นอกจากปัญหาสงครามไซเบอร์แล้ว ภัยคุกคามทางไซเบอร์ซึ่งเป็นปัญหาที่ไร้พรมแดนและกระทบต่อความปลอดภัยในภาคการเงินทั่วโลกด้วย ความเสี่ยงในการเกิดอาชญากรรมทางไซเบอร์ ทั้งการโจรกรรมข้อมูล การยักยอกเงินจากอินเทอร์เน็ตแบงก์กิ้งและเงินดิจิทัลเพิ่มขึ้นอย่างรวดเร็วมากขึ้น ซึ่งเป็นความเสี่ยงสำคัญของระบบการเงินโลก เช่น กรณีธนาคารยักษ์ใหญ่แห่งหนึ่งในสหรัฐอเมริกาถูกขโมยข้อมูลลูกค้ากว่า 83 ล้านบัญชี เมื่อปี พ.ศ. 2557 และปัญหาโลกไซเบอร์ที่เกิดขึ้นด้านสังคมด้วยดังตามที่องค์การยูนิเซฟ (UNICEF) ได้มีการรวบรวมข้อมูลการระรานกลั่นแกล้งทางไซเบอร์ในกลุ่มเด็กๆ ที่มีการล้อเล่นกันเลวเลวไปไกลถึงขนาดที่เริ่มทำร้ายจิตใจนั้นอาจเป็นการ Cyberbully ดังที่กล่าวไว้ก่อนแล้ว

สังคมปัจจุบันนี้มีสองสถานะที่ชัดเจนและเด่นชัด สถานะหนึ่งเป็นสังคมจริง สังคมบนโลกกายภาพ (Physical World) อีกสถานะหนึ่งอยู่ในโลกออนไลน์ไซเบอร์ (Cyber World) ที่เรียกว่าเสมือนจริง (Virtual) จนมีปัญหาใหม่เกิดขึ้นอยู่เสมอ เช่น เด็กติดเกม การรังแกบนโลกไซเบอร์ การหลอกลวงแบบใหม่ในไซเบอร์ เป็นต้น พัฒนาการทางดิจิทัลทำให้มีความหลากหลายทางด้านผลิตภัณฑ์ เครื่องมือสมัยใหม่ เทคโนโลยีดิจิทัลมีพลานุภาพมากขึ้น มีพัฒนาการอยู่ตลอดเวลา หากเปรียบเทียบผลิตภัณฑ์เหล่านี้เป็นเผ่าพันธุ์ดิจิทัล หรือสายพันธุ์ดิจิทัล ที่เรียกว่า ดิจิทัลสปีชีส์ (Digital Species) เหมือนเผ่าพันธุ์ของสิ่งมีชีวิต ผลิตภัณฑ์ดิจิทัลมีวิวัฒนาการ มีความก้าวหน้าทางด้านการพัฒนา มีการสร้างผลิตภัณฑ์ออกมาให้มากมาย

ขยายตัวอย่างรวดเร็ว จนปัจจุบันมนุษย์ต้องเกี่ยวข้องอยู่ร่วมกัน พึ่งพาอาศัยผลิตภัณฑ์ อุปกรณ์ดิจิทัลเหล่านี้ หากพิจารณาด้วยหลักการของการอยู่ร่วมกันกับดิจิทัล วิถีชีวิตใหม่มีการดำเนินชีวิตแบบใหม่ที่พึ่งพาดิจิทัลมากขึ้น ก่อให้เกิดระบบนิเวศทางด้านดิจิทัลที่เรียกว่า ดิจิทัล-อีโคซิสเต็ม (Digital Eco-system) มีผลิตภัณฑ์ ของใช้ เฝ้ามั่นรู้ดิจิทัลเกิดขึ้นมากมาย การอยู่รวมของคนกับเฝ้ามั่นรู้ดิจิทัลจึงเกิดขึ้น ทำให้วิถีชีวิตใหม่ ความเป็นอยู่ การเรียน การเล่น การเข้าสู่สังคมเปลี่ยนไป (ยง ภูววรรณ, 2564)

โลกไซเบอร์เกิดขึ้นหลายทศวรรษมีวิวัฒนาการเริ่มยุคแรกจากวัฒนธรรมกลุ่มย่อยในกลุ่มแฮกเกอร์ชาวอเมริกันร่วมกันพัฒนาเครือข่ายคอมพิวเตอร์จนในยุคปัจจุบันนี้เข้ามาเป็นส่วนหนึ่งของดำรงชีวิตของพลเมืองโลกที่เห็นชัดเจนมากขึ้นและยังมีการพัฒนาอย่างต่อเนื่องต่อไป ทั้งในด้านมหภาคที่มีวิวัฒนาการการทำสงครามระหว่างประเทศที่เปลี่ยนแปลงไปในการทำสงครามระหว่างประเทศกันในโลกไซเบอร์ การทำธุรกรรมทางการเงินเชื่อมต่อเป็นเครือข่ายดิจิทัลเป็นโลกไซเบอร์ ส่วนในด้านจุลภาคโลกไซเบอร์ได้เข้ามามีบทบาทในการดำรงชีวิตประจำวันของพลเมืองโลกทุกเพศทุกวัย โดยเฉพาะในเด็กวัยเยาว์ ซึ่งทำให้เกิดปัญหาต่อพลเมืองโลกตามมาในทุกด้านด้วยเช่นกัน การทำสงครามใช้เทคโนโลยีทำสงครามในโลกไซเบอร์ทำให้เกิดปัญหาการทำลายล้างที่เสียหายรุนแรง การก่ออาชญากรรมทางการเงินเปลี่ยนรูปแบบไปสู่โลกไซเบอร์ การใช้สื่อเทคโนโลยีออนไลน์ทำร้ายรังแกกันโดยเฉพาะเด็กๆ เปลี่ยนรูปแบบไปสู่โลกไซเบอร์เช่นกัน อันจะทำให้พลเมืองโลกได้รับความเสียหายทั้งแก่ชีวิตและทรัพย์สินมากมาย

3. นโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์เพื่อคุ้มครองพลเมืองโลก

จากการรวบรวมแนวคิดเรื่องอำนาจอธิปไตยซึ่งเป็นพื้นฐานในการวิเคราะห์อำนาจอธิปไตยทางไซเบอร์ พบว่าลักษณะพิเศษบางอย่างของโลกไซเบอร์เป็นอุปสรรคต่อการกำหนดเขตแดนอธิปไตย ไม่ว่าจะเป็นการเปลี่ยนแปลงอย่างรวดเร็ว ความไร้ตัวตนไร้ซึ่งพรมแดน จะไม่สามารถกำหนดได้ว่าอำนาจอธิปไตยที่แท้จริงของแต่ละรัฐชาตินั้นเป็นอย่างไร และจากอุปสรรคดังกล่าวจึงเป็นที่มาของการค้นคว้า พัฒนาคำนิยามในการใช้อำนาจอธิปไตยไซเบอร์ของรัฐให้สอดคล้องตามยุคสมัย โดยรัฐจะต้องใช้อำนาจอธิปไตยอย่างพอดี ไม่มากเกินไปจนละเมิดความเป็นส่วนตัวของประชาชน และไม่น้อยเกินไปเพื่อที่จะยังคงซึ่งอำนาจอธิปไตยไว้แม้แต่ในโลกที่ไร้พรมแดน การใช้อำนาจอธิปไตยในโลกไซเบอร์ที่แท้จริงจะผ่านการกำหนดกฎหมายและนโยบายต่างๆ ที่ไม่ให้รัฐอื่นสามารถแทรกแซงรัฐของตนได้ แต่เมื่อใดที่มีการแทรกแซงรัฐจำเป็นจะต้องมีเครือข่ายสำรองทุกภาคส่วนเพื่อรับมือการโจมตีทางไซเบอร์ที่เกิดขึ้น ในกรณี

ที่สัญญาณอินเทอร์เน็ตของรัฐถูกโจมตีจากภายนอก เครือข่ายสำรองจากภาคเอกชนจะถูกนำมาใช้แทนทันทีเพื่อไม่ให้เกิดความชะงักงันในการใช้ชีวิตของประชาชน และสุดท้ายการใช้แนวทางด้านการทูตเพื่อเป็นเครื่องมือในการต่อรองในเวทีโลก ประเทศจีนและประเทศรัสเซียที่มีความต้องการในการสนับสนุนการใช้อำนาจอิปไตในโลกลิเบอร์อย่างชัดเจน เพราะไม่ต้องการให้ประเทศอื่นๆ เข้ามาละเมิดอำนาจของรัฐตนได้ ทั้งสองประเทศได้เสนอแนวคิดผ่านองค์กรสหประชาชาติ เพื่อแสดงจุดยืนของตนอย่างชัดเจนเพื่อไม่ให้รัฐอื่นเข้ามาแทรกแซงประการสุดท้าย การกำหนดนโยบายสอดคล้องกับรูปแบบการปกครองในโลกความเป็นจริงที่คู่ขนานกับโลกลิเบอร์จึงมีแนวโน้มว่าประเทศเสรีประชาธิปไตยอย่างประเทศสหรัฐอเมริกาหรือประเทศอังกฤษจะมีท่าทีที่จะกำหนดอำนาจอิปไตทางลิเบอร์ของตนอิงตามรูปแบบการปกครองทางการเมือง เศรษฐกิจมนุษยชนของประชาชนในประเทศตน และพยายามจะใช้วิธีการทางทูตในการแก้ไขปัญหาการละเมิดอำนาจอิปไตของตน (นัทธมน เพชรกล้า และ สมุนทิพย์ จิตสว่าง, 2566)

กฎหมายระหว่างประเทศเป็นกฎหมายที่ถูกนำมาใช้เมื่อเกิดปัญหากระทบกระทั่งระหว่างรัฐชาติ โดยที่ไม่สามารถใช้กฎหมายภายในจัดการได้ กฎหมายต่างประเทศถึงจะถือเป็นเสาหลักในการแก้ปัญหาในระดับสากล แต่ไม่สามารถนำมาใช้กับปัญหาที่เกิดขึ้นในโลกแห่งลิเบอร์ได้ เพราะลักษณะความพิเศษที่เปลี่ยนแปลงอย่างรวดเร็วเกิดขึ้นภายในโลกลิเบอร์ การขาดซึ่งความเชื่อมโยงทางภูมิศาสตร์ การแบ่งลักษณะตัวตน บั๊กเจกหรือองค์กรในคราวเดียวกัน ทำให้ปัญหาที่เกิดขึ้นในโลกลิเบอร์มีความซับซ้อนมากขึ้น การกำหนดนิยามของอิปไตลิเบอร์จึงไม่สามารถเกิดขึ้นได้อย่างเป็นเอกฉันท์ในปัจจุบัน (Corn & Taylor, 2017; Brown, 2013) ซึ่งทำให้ปัญหาในการนิยามอิปไตลิเบอร์ยังคงเป็นข้อถกเถียงอยู่ในปัจจุบัน (Hare, 2009)

อาชญากรรมลิเบอร์ หรือการโจมตีทางลิเบอร์ แบ่งเป็นสามประเภทหลักคือ (1) ตัวแสดง (2) เป้าหมายในการก่อความเสียหายทางลิเบอร์ (3) ระดับความรุนแรง อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมลิเบอร์ ค.ศ. 2001 (Convention on Cybercrime Budapest, 23.XI.2001) ได้กำหนดลักษณะการกระทำความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ข้ามชาติไว้เกี่ยวข้องกับการสร้างความเสียหายต่อระบบคอมพิวเตอร์และข้อมูลในคอมพิวเตอร์ การหลอกลวงและการปลอมแปลง สื่อลามกเด็ก และการละเมิดลิขสิทธิ์ (Council of Europe, 2001)

ภัยลิเบอร์ที่มีแนวโน้มจะเกิดมากขึ้น หน่วยงานกำกับดูแลและองค์กรทั่วโลกจึงตื่นตัวกับการเร่งยกระดับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางลิเบอร์อย่างจริงจัง มีการออกกฎหมายและแนวทางการกำกับดูแลเพื่อลดความเสี่ยงดังกล่าว เช่น สหภาพยุโรป

ออกกรอบการดูแลความปลอดภัยไซเบอร์ของภาคอุตสาหกรรมในยุโรป (Directive on Security of Network and Information Systems) และกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป (General Data Protection Regulation) ขณะที่ประเทศสหรัฐอเมริกาได้จัดทำกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (National Institute of Standards and Technology Cybersecurity Framework) ซึ่งเป็นกรอบมาตรฐานสากลที่ถูกนำมาใช้อย่างแพร่หลายในองค์กรต่างๆ ทั่วโลก รวมถึงประเทศไทยด้วย โดยกรอบนี้วางแนวปฏิบัติที่ดีที่ครอบคลุมถึงการระบุและเข้าใจถึงบริบทต่างๆ เพื่อบริหารจัดการความเสี่ยง (Identify) การวางมาตรฐานควบคุมเพื่อป้องกัน (Protect) การตรวจจับ (Detect) การรับมือต่อภัยคุกคาม (Respond) และการฟื้นฟูระบบในเวลาที่เหมาะสม (Recover) (อนุภาคมาตรฐาน และอิสรารุณี เอี่ยมวิริยะกุล, 2561)

สหภาพยุโรปได้ออกกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรปหรืออียู (EU Cybersecurity Act) เริ่มมีผลบังคับวันที่ 27 มิถุนายน พ.ศ. 2562 เป็นต้นไป ภายหลังจากที่ทีมเจรจาคณะมนตรีแห่งยุโรปและสภายุโรปสามารถบรรลุข้อตกลงร่วมกันได้เมื่อปลายปี พ.ศ. 2561 ที่ผ่านมา โดยกฎหมายดังกล่าวเป็นก้าวแรกในการจัดให้มีระบบตรวจสอบและรับรองมาตรฐานความปลอดภัยทางไซเบอร์ (Cybersecurity Certification) สำหรับอียู (Europe Wide) ของสินค้าและบริการ ตลอดจนการประมวลผลทางไอทีต่างๆ ตามเกณฑ์ที่กำหนดก่อนจะสามารถจัดจำหน่ายหรือให้บริการในอียูได้ อีกทั้งยังเป็นกฎหมายโดยตรงที่จะรับรองบทบาทและหน้าที่ของศูนย์ Cybersecurity Agency ของอียู หรือที่เรียกว่า ENISA (European Agency for Network and Information Security) ในการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์และจัดสรรงบประมาณในการดำเนินการใดๆ ของหน่วยงานดังกล่าว (thaieurope, 2562)

ต่อมาสหภาพยุโรปได้เสนอให้เพิ่มมิติของความปลอดภัยทางไซเบอร์ในทุกภาคส่วนของห่วงโซ่อุปทาน รวมถึงอุปกรณ์เชื่อมต่ออินเทอร์เน็ตต่างๆ โดยเสนอให้มีการปรับปรุงและออกกฎหมายใหม่ ส่งเสริมการลงทุน และริเริ่มร่างนโยบายใหม่ควบคู่ไปกับการบูรณาการเครื่องมือของสหภาพยุโรป เช่น ตลาดภายใน กฎหมาย ช่องทางการทูต และช่องทางการกลาโหม เพื่อเตรียมพร้อมในการรับมือกับการโจมตีออนไลน์และสร้างกลไกด้านการรักษาความปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพมากขึ้น โดยสรุปสาระสำคัญดังนี้

(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)) เพื่อยกระดับความปลอดภัยให้ครอบคลุมอุตสาหกรรมและภาคส่วนอื่นๆ ที่ต้องการความยืดหยุ่น

นอกเหนือจากการคุ้มครองของ NIS เช่น ศูนย์จัดเก็บข้อมูลห้องปฏิบัติการเพื่อการวิจัยอุตสาหกรรมการผลิตยาและอุปกรณ์การแพทย์ และการไปรษณีย์บริการจัดส่งพัสดุ เป็นต้น โดยกฎหมายทั้งสองจะทำงานสอดคล้องกันและส่งเสริมกัน

(2) เพิ่มมาตรฐานความปลอดภัยทางไซเบอร์ในอุปกรณ์เชื่อมต่อกับอินเทอร์เน็ต สหภาพยุโรปเสนอให้มีการกำหนดหลักเกณฑ์สำหรับอุปกรณ์เชื่อมต่อที่จะวางขายในตลาดยุโรป เพื่อสร้าง “Internet of Secure Things”

(3) ใช้ AI ในการสร้าง “เกราะความปลอดภัยทางไซเบอร์” สหภาพยุโรปเสนอให้มีการจัดตั้งหน่วยงานด้านความปลอดภัย (Security Operations Centres) ในสหภาพยุโรป เพื่อพัฒนา European Cyber Shield หรือเกราะความปลอดภัยทางไซเบอร์ โดยใช้เทคโนโลยี AI ในการตรวจจับสัญญาณของการโจมตีออนไลน์ตั้งแต่เนิ่นๆ เพื่อให้สหภาพยุโรปสามารถตอบโต้ได้ทันก่อนจะเกิดความเสียหาย

(4) ตั้งเป้าหมายในการจัดหาเครือข่ายโทรคมนาคมในอนาคตที่ทันสมัยกว่าเทคโนโลยี 5G สหภาพยุโรปร่วมกับ ENISA หน่วยงานด้านความปลอดภัยทางไซเบอร์ ได้ออกคำแนะนำเพื่อสนับสนุนให้ประเทศสมาชิกดำเนินการตาม “EU 5G Toolbox” ซึ่งได้กำหนดแนวทางการนำเทคโนโลยี 5G และเครือข่ายโทรคมนาคมในอนาคตมาใช้อย่างปลอดภัย เช่น แนะนำให้ประเทศสมาชิกหลีกเลี่ยงผู้ให้บริการที่มีความเสี่ยงสูงและหรือการพึ่งพาซัพพลายเออร์ดังกล่าว เป็นต้น และแสวงหาแนวทางการพัฒนาเทคโนโลยี 6G

(5) จัดตั้งหน่วยงานไซเบอร์กลางของสหภาพยุโรปและการเสริมสร้างความร่วมมือด้านไซเบอร์ เสนอให้มีการจัดตั้ง Joint Cyber Unit เพื่อเสริมสร้างความร่วมมือระหว่างหน่วยงานของสหภาพยุโรปและประเทศสมาชิกในการรับมือการโจมตีออนไลน์ รวมถึงการจัดตั้งเครือข่ายองค์การประสานงานวิกฤตไซเบอร์ (Cyber Crisis Liaison Organisation Network: CyCLONE) ภายใต้ร่างกฎหมาย NIS2 เพื่อป้องกันและตอบโต้การโจมตีออนไลน์ขนาดใหญ่และวิกฤตไซเบอร์ในระดับอียู เช่น การโจมตีทางไซเบอร์ข้ามประเทศ โดยใช้ EU Cyber Diplomacy Toolbox เป็นเครื่องมือในการยกระดับความร่วมมือด้านการป้องกันทางไซเบอร์ระหว่างประเทศ และจัดตั้งหน่วยงาน European Cybersecurity Competence Centre ที่จะจัดตั้งขึ้นที่โรมาเนีย และเสริมสร้างความร่วมมือกับนานาชาติ รวมถึง NATO และองค์กรระหว่างประเทศอื่นๆ (กรมยุโรป กระทรวงการต่างประเทศ, 2564)

ประเทศสหรัฐอเมริกาเร่งผลักดันแนวคิดการรักษาความปลอดภัยระบบคอมพิวเตอร์แบบ Zero Trust เปิดเว็บไซต์ govinfosecurity.com ของทำเนียบประธานาธิบดีสหรัฐฯ ร่วมกับสำนักความมั่นคงโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity and Infrastructure Security Agency: CISA) และสำนักบริหารงบประมาณ

(Office of Management and Budget: OMB) ของสหรัฐอเมริกา กำลังผลักดันให้หน่วยงานของรัฐนำแนวคิดการออกแบบมาตรการรักษาความมั่นคงปลอดภัยแบบ "zero trust" มาใช้ภายในเดือนกันยายน ค.ศ. 2024 Zero trust เป็นแนวคิดการออกแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ การเข้าถึงทรัพยากรบนระบบเครือข่ายคอมพิวเตอร์หรือการอนุญาตให้อุปกรณ์คอมพิวเตอร์เชื่อมต่อในเครือข่ายจะต้องผ่านการตรวจสอบ (Verify) อย่างเข้มงวดทั้งการเชื่อมต่อจากภายในสำนักงานหรือภายนอกสำนักงาน และปฏิบัติในลักษณะเดียวกัน ไม่ว่าจะเป็นผู้บริหารระดับสูง ผู้ดูแลระบบไอที และพนักงาน

ประธานาธิบดีของสหรัฐอเมริกาออกคำสั่งเมื่อพฤษภาคม ค.ศ. 2021 ให้เร่งแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ในหลายประเด็นจากการโจมตีทางไซเบอร์จากกรณี SolarWinds กรณีข้อมูลของหน่วยงานรัฐบาลสหรัฐอเมริกาหลายแห่งรั่วไหลเมื่อเดือนธันวาคม ค.ศ. 2020 และหลายกรณีจากมัลแวร์เรียกค่าไถ่ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยหนึ่งในองค์ประกอบนั้นคือการนำแนวคิดสถาปัตยกรรมเครือข่ายแบบ Zero Trust มาประยุกต์ใช้ในหน่วยงานภาครัฐ และส่งเสริมให้หน่วยงานภาครัฐประยุกต์ใช้เทคโนโลยีการรักษาความปลอดภัยที่เข้มงวดขึ้น เช่น การใช้วิธีการพิสูจน์ยืนยันตัวบุคคลแบบหลายปัจจัย (Multiple factor authentication) ก่อนการเข้าถึงทรัพยากรบนเครือข่าย และการจัดหาระบบตรวจจับและตอบสนองภัยคุกคามปลายทาง (Endpoint Detection and Response) มาประยุกต์ใช้แทนการรักษาความปลอดภัยแบบดั้งเดิม หลังจาก OMB เผยแพร่เอกสารที่เกี่ยวข้องกับการออกแบบมาตรการรักษาความปลอดภัยแบบ Zero Trust แล้ว หน่วยงานภาครัฐจะต้องส่งแผนการนำนโยบาย Zero Trust ไปสู่การปฏิบัติระหว่างปี ค.ศ. 2022-2024 โดยหน่วยงานภาครัฐต้องประยุกต์ใช้สถาปัตยกรรมแบบ "Zero Trust" ซึ่งประกอบด้วย 5 เสาหลัก การพัฒนามาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ (สำนักข่าวกรองแห่งชาติ, 2564) ดังนี้

(1) การระบุยืนยันตัวตน (Identity) เจ้าหน้าที่ในหน่วยงานทุกคนจะต้องปฏิบัติตามแนวปฏิบัติที่ดี (Best Practices) เมื่อเชื่อมต่อและเข้าถึงแอปพลิเคชันที่ใช้ในการปฏิบัติงาน ซึ่งรวมถึงการใช้งาน multiple factor authentication เพื่อลดภัยคุกคามทางไซเบอร์ เช่น อีเมลหลอกลวง

(2) อุปกรณ์ (Devices) หน่วยงานภาครัฐจะต้องจัดทำทะเบียนทรัพย์สินสารสนเทศภายในเครือข่ายให้ครบถ้วนเพื่อช่วยในการตรวจจับและรับมือภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

(3) เครือข่าย (Networks) หน่วยงานภาครัฐต้องเข้ารหัสข้อมูลการติดต่อสื่อสารบนเครือข่ายอินเทอร์เน็ต เช่น ระบบ Domain Name และโปรโตคอล HTTP และแบ่งแยกเครือข่ายตามลำดับชั้นการรักษาความปลอดภัยข้อมูล รวมทั้งการใช้อีเมลเข้ารหัส

(4) แอปพลิเคชัน (Applications) หน่วยงานภาครัฐต้องทดสอบแอปพลิเคชันเพื่อตรวจสอบช่องโหว่และมั่นใจว่ามีมาตรการด้านการรักษาความมั่นคงปลอดภัยที่เหมาะสม รวมถึงพิจารณารายงานจากแหล่งข้อมูลภายนอกเกี่ยวกับช่องโหว่และข้อผิดพลาดของแอปพลิเคชันที่ใช้งานด้วย

(5) ข้อมูล (Data) หน่วยงานภาครัฐที่ใช้บริการความปลอดภัยผ่านระบบคลาวด์ จะต้องเผื่อตรวจตราการเข้าถึงข้อมูลสำคัญ และจัดทำระบบการบันทึกข้อมูลการจราจรคอมพิวเตอร์ การเข้าถึงข้อมูลในระบบต่างๆ ทั่วทั้งองค์กร

ประเทศจีนออกหนังสือปกขาวเผยแพร่โดยสำนักงานข้อมูลข่าวสารแห่งคณะรัฐมนตรีจีน ปี ค.ศ. 2010 ได้กล่าวถึงนโยบายของรัฐบาลในการปกป้องความปลอดภัยทางไซเบอร์ไว้ และประกาศความมุ่งหมายที่จะกำจัดเนื้อหาที่ “ต่อต้านหลักการสำคัญในรัฐธรรมนูญ เป็นอันตรายต่อความมั่นคงของรัฐ เปิดเผยความลับของชาติ บ่อนทำลายชาติและความสามัคคี ทำลายเกียรติหรือผลประโยชน์ของประเทศ ส่งเสริมให้เกิดความเกลียดชังหรือเหยียดหยาม ศีลธรรมอันดีของสังคม ฝ่าฝืนนโยบายของชาติว่าด้วยการนับถือศาสนา โฆษณาเนื้อหาลัทธิ นอกรีต กระจ่ายข่าวลือ สร้างความปั่นป่วนให้กับสังคม เผยแพร่สื่อลามกอนาจาร การพนัน ความรุนแรง การก่อการร้ายหรืออาชญากรรมอื่น การล้อเลียนเสียดสี ละเมิดสิทธิของผู้อื่น หรือเนื้อหาอื่นที่มีลักษณะต้องห้ามตามกฎหมายหรือระเบียบของฝ่ายบริหาร” (Information Office of the State Council the People's Republic of China, 2010) ข้อความนี้สะท้อนให้เห็นถึงมุมมองของประเทศจีนที่มีต่อความปลอดภัยทางไซเบอร์อย่างชัดเจนว่าให้ความสำคัญกับเสถียรภาพทางสังคม อำนาจอธิปไตย และความสามัคคีของคนในชาติ ภายใต้การบังคับใช้ของกฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศจีน ผู้ให้บริการทางโครงข่ายซึ่งประกอบด้วยกิจการอันเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญจะถูกบังคับให้มีส่วนร่วมในการปกป้องความมั่นคงปลอดภัยไซเบอร์ด้วย ประเทศจีนเชื่อมั่นในระบบบังคับและจะทดลองมาตรการต่างๆ เพื่อนำไปสู่การให้ความคุ้มครองระบบโครงสร้างพื้นฐานที่มีประสิทธิภาพและยั่งยืนสำหรับประเด็นเรื่องการเก็บรวบรวมข้อมูลในท้องถิ่นนั้น ก็จัดว่าเป็นอีกภาระหนึ่งที่ยุ่งยากสำหรับผู้ให้บริการเครือข่ายที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญ และไม่มีคำแนะนำว่ามาตรการดังกล่าวจะช่วยเสริมสร้างความแข็งแกร่งให้กับความปลอดภัยไซเบอร์ในระยะยาวได้จริง ทั้งนี้ มาตรการการเก็บรวบรวมข้อมูลในท้องถิ่นอาจทำให้ผู้ประกอบการธุรกิจได้รับความเสี่ยงจากการถูกสอดแนมโดยรัฐบาลท้องถิ่น และถึงแม้ว่ากฎหมายจะมีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเกิดขึ้นมาแล้วก็ตาม แต่กฎหมายความปลอดภัยไซเบอร์ก็ยังให้อำนาจในการเข้าถึงข้อมูลเหล่านั้น อันนำไปสู่การรั่วไหลของข้อมูลอยู่นั่นเอง (อาร์ม ตั้งนิรันดร, 2563)

ต่อมาการประชุมคณะกรรมการประจำสภาประชาชนแห่งชาติจีน ชุดที่ 13 ครั้งที่ 30 ได้ลงมติผ่านกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล โดยมีผลบังคับใช้ในวันที่ 1 พฤศจิกายน ค.ศ. 2021 ทั้งนี้ ในช่วงไม่กี่ปีที่ผ่านมาปัญหาต่างๆ เช่น การรวบรวมข้อมูลส่วนบุคคลมากเกินไป การขาดความคุ้นเคยกับข้อมูลขนาดใหญ่ การประมวลผลข้อมูลส่วนบุคคลที่ละเอียดอ่อนซึ่งได้กลายเป็นประเด็นร้อนในการปกป้องข้อมูลส่วนบุคคล และได้รับความสนใจอย่างมากจากโลกภายนอก การเกิดขึ้นของ “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” เป็นสัญลักษณ์ว่าหลังจากการบังคับใช้ “กฎหมายว่าด้วยการรักษาความปลอดภัยทางไซเบอร์” และ “กฎหมายว่าด้วยการรักษาความปลอดภัยของข้อมูล” ซึ่งเป็นระบบกฎหมายของจีนที่ทุนยุคสมัยนี้ให้ความสำคัญ (ไชยสิทธิ์ ตันตยกุล, 2564) กล่าวคือ

(1) หลังจากเกือบ 20 ปี ในที่สุดประเทศจีนมีกฎหมายที่สำคัญในสังคมดิจิทัล โดยได้ก่อตั้งระบบกฎหมายหลักว่าด้วย “กฎหมายว่าด้วยการรักษาความปลอดภัยทางไซเบอร์” “กฎหมายว่าด้วยการรักษาความปลอดภัยของข้อมูล” และ “กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล”

(2) หลังจากผ่านไปครึ่งศตวรรษ ระบบกฎหมายของประเทศจีนที่เกี่ยวข้องกับดิจิทัลได้ถูกสร้างขึ้น ปัจจุบัน 128 ประเทศ ได้ออกกฎหมายเพื่อปกป้องข้อมูลส่วนบุคคลและความเป็นส่วนตัว

(3) เป็นก้าวสำคัญในระบบการเข้าสู่สังคมดิจิทัลที่เน้นประชาชน โดยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศจีนที่ชี้แจงถึงการประมวลผลข้อมูลส่วนบุคคลต้องมีกฎหมายรองรับ

(4) เป็นไปตามหลักสากลทั่วไปอย่างสมบูรณ์

(5) เป็นส่วนช่วยในการกำกับดูแลทางดิจิทัลทั้งหมด โดยรักษาสมดุลระหว่างความสัมพันธ์ของการปกป้องสิทธิส่วนบุคคลและการส่งเสริมการใช้ข้อมูลนั้น เป็นประเด็นหลักของกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

ประเทศทั่วโลก รวมทั้งประเทศมหาอำนาจทั้งกลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศจีน ได้ให้ความสำคัญกับปัญหาที่เกิดขึ้นในโลกไซเบอร์เป็นอย่างมาก โดยกำหนดเป็นนโยบายหลักของประเทศในกำกับ ดูแล ป้องกัน แก้ไขปัญหาภัยคุกคามและอาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ มีการจัดตั้งศูนย์ หน่วยงาน องค์กร ขึ้นมากำกับดูแลโลกไซเบอร์ และออกกฎหมายความปลอดภัยทางไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง เพื่อต้องการรักษาอำนาจอธิปไตยของประเทศและกำกับดูแลคุ้มครองพลเมืองให้ใช้สื่อดิจิทัลในโลกไซเบอร์ให้ปลอดภัยและสามารถพัฒนาโลกไซเบอร์ให้เป็น

ประโยชน์ได้อย่างสร้างสรรค์ อันเป็นส่วนหนึ่งของนโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์เพื่อคุ้มครองพลเมืองโลก

4. นโยบายความปลอดภัยทางไซเบอร์ด้านกฎหมายของประเทศไทย

สำหรับประเทศไทยได้ให้ความสำคัญกับภัยคุกคามและอาชญากรรมทางไซเบอร์เป็นอย่างมากเช่นเดียวกับประเทศอื่นๆ โดยกำหนดเป็นนโยบายยุทธศาสตร์ชาติ ออกกฎหมายจัดตั้งหน่วยงานดูแลเรื่องนี้โดยตรง และกำหนดให้หน่วยงานองค์กรทั้งภาครัฐและภาคเอกชน นำนโยบายการกำกับดูแลความปลอดภัยทางไซเบอร์ไปปฏิบัติด้วย

กฎหมายที่ประเทศไทยออกมากำกับและดูแลความมั่นคงและปลอดภัยทางไซเบอร์ คือ พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม พ.ศ. 2562 เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่ในปัจจุบัน การให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกันหรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันทั่วทั้งที่สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่างๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้ (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

“ภัยคุกคามทางไซเบอร์” (Cyber Threats) เป็นภัยคุกคามที่ส่งผลกระทบในทุกภาคส่วน ทั้งทางเศรษฐกิจ หรือความมั่นคงของประเทศ โดยในปี พ.ศ. 2560 ประเทศไทยมีสถิติการคุกคามทางไซเบอร์ตลอดทั้งปี ผลโดยรวมทั้งหมด 3,237 ครั้ง ในปี พ.ศ. 2561 ตั้งแต่เดือนมกราคมถึงเดือนพฤศจิกายน มีการคุกคามทางไซเบอร์ ที่ได้บันทึกไว้ในสถิติแล้วจำนวนทั้งหมด 2,311 ครั้ง โดยการคุกคามที่มากที่สุดเป็นอันดับหนึ่งคือ “ความพยายามจะบุกรุกเข้าระบบ” (Intrusion Attempts) ที่บันทึกไว้ได้จำนวน 984 ครั้ง ซึ่งมากกว่าสถิติที่บันทึกได้ตลอดปี พ.ศ. 2560 ถึง 45 ครั้ง หรือเพิ่มขึ้นถึงร้อยละ 4.80 ปี พ.ศ. 2562 จะมีเทคนิค

การโจมตีแบบใหม่ที่เกิดขึ้นอีกมากมายและร้ายแรงกว่าที่เป็นอยู่ สถานการณ์ทางไซเบอร์ที่เกิดขึ้นทางรัฐบาลของประเทศไทย ได้ออกนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยได้จัดตั้ง “คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” หรือ National Cybersecurity Committee เมื่อเดือนเมษายน พ.ศ. 2561 ที่ผ่านมา ซึ่งเป็นหนึ่งในยุทธศาสตร์การพัฒนา ดิจิทัลเพื่อเศรษฐกิจและสังคมของรัฐบาล ควบคู่กับการเตรียมประกาศใช้ร่าง พระราชบัญญัติ รักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งจำเป็นต้องใช้มาตรการทั้งทางเทคนิคและทางกฎหมาย (เสมอ นิมะเงิน, 2563)

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 บัญญัติให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัตินี้ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ ในวาระเริ่มแรก กำหนดให้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จนกว่าจะจัดตั้งสำนักงานแล้วเสร็จ และให้ปลัดกระทรวงทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการตามมาตรา 79 วรรคสอง (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2566) โดยหน่วยงานภาครัฐที่มีการนำนโยบายการดูแลความปลอดภัยทางไซเบอร์ไปจัดทำแผนและปฏิบัติแล้ว ยกตัวอย่างเช่น

กระทรวงกลาโหมจัดทำแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม พ.ศ. 2566-2570 แบ่งออกเป็น 3 แนวทาง ในการดำเนินการพัฒนา คือ (1) การพัฒนาศักยภาพไซเบอร์ กท. โดยการเตรียมกำลังด้านไซเบอร์ (2) การปฏิบัติการไซเบอร์ของ กท. โดยการใช้กำลังด้านไซเบอร์ (3) ความร่วมมือด้านความมั่นคงไซเบอร์โดยการทำความร่วมมือในการขับเคลื่อนแผนการพัฒนาด้านไซเบอร์เพื่อความมั่นคงกท. พ.ศ. 2566-2570 ไปสู่เป้าหมายที่กำหนด โดยมุ่งเน้นการบริหารจัดการที่มีเอกภาพและประสิทธิภาพในทุกระดับ (กระทรวงกลาโหม, 2566) ดังนี้

สำนักงานปลัดกระทรวงกลาโหม เป็นหน่วยงานรับผิดชอบในการอำนวยความสะดวก ประสานงานกำกับดูแลและดำเนินการเกี่ยวกับนโยบายด้านไซเบอร์ของกระทรวงกลาโหม และความร่วมมือด้านไซเบอร์กับหน่วยงานที่เกี่ยวข้องทั้งในและต่างประเทศ สนับสนุนการดำเนินการด้านไซเบอร์ของหน่วยขึ้นตรงกระทรวงกลาโหม รวมทั้งรับผิดชอบการปฏิบัติการไซเบอร์ของสำนักงานปลัดกระทรวงกลาโหม

กองบัญชาการกองทัพไทย เป็นหน่วยงานรับผิดชอบในการอำนวยความสะดวก ประสานงานกำกับ ดูแล บูรณาการ และดำเนินการเกี่ยวกับการปฏิบัติการร่วมทางไซเบอร์ ตลอดจน

การพัฒนาศักยภาพในการปฏิบัติการร่วมทางไซเบอร์ของกองทัพไทยและกระทรวงกลาโหม ให้สอดคล้องกับนโยบายของกระทรวงกลาโหม และแผนป้องกันประเทศ

กองทัพบก เป็นหน่วยงานรับผิดชอบในการอำนวยความสะดวก ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการไซเบอร์และการพัฒนาศักยภาพด้านไซเบอร์ของกองทัพบก เพื่อรองรับการดำเนินการด้านไซเบอร์ของกระทรวงกลาโหม

กองทัพเรือ เป็นหน่วยงานรับผิดชอบในการอำนวยความสะดวก ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการไซเบอร์และการพัฒนาศักยภาพด้านไซเบอร์ของกองทัพเรือ เพื่อรองรับการดำเนินการด้านไซเบอร์ของกระทรวงกลาโหม

กองทัพอากาศเป็นหน่วยงานรับผิดชอบในการอำนวยความสะดวก ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับการปฏิบัติการไซเบอร์และการพัฒนาศักยภาพด้านไซเบอร์ของกองทัพอากาศ เพื่อรองรับการดำเนินการด้านไซเบอร์ของกระทรวงกลาโหม

สำนักงานพัฒนารัฐบาลดิจิทัล ได้กำหนดนโยบายความปลอดภัยทางไซเบอร์ โดยได้มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษา และการป้องกันให้เหมาะสมกับลักษณะการดำเนินกิจการ ซึ่งการดูแลรักษาและการป้องกันมุ่งหมายไปในทางความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่งการรักษาความลับของข้อมูล ความถูกต้องครบถ้วน และความสมบูรณ์พร้อมใช้ ดังนี้

การรักษาความลับ (Confidentiality) หมายถึง การป้องกันไม่ให้สินทรัพย์สามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงยังรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่าย ซึ่งสินทรัพย์นั้นด้วย ดังนั้น ในการรักษาความลับจำเป็นจะต้องมีการควบคุมทั้งทางกายภาพและทางเทคนิค โดยผู้ที่มีสิทธิจะต้องไม่สามารถเข้าถึงสินทรัพย์นั้นได้และสินทรัพย์จำเป็นจะต้องมีการจำแนกและกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ที่ถือครองสินทรัพย์ปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

ความถูกต้องครบถ้วน (Integrity) หมายถึง การป้องกันไม่ให้สินทรัพย์ถูกเปลี่ยนแปลงแก้ไขทั้งที่มีเจตนาหรือไม่ก็ตามจากผู้ไม่มีสิทธิที่จะแก้ไขสินทรัพย์เหล่านั้น ดังนั้น การควบคุมและป้องกันจึงต้องประกอบด้วยกำหนดสิทธิในการแก้ไข กำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีสินทรัพย์และทางเทคนิคประกอบด้วย

ความสมบูรณ์พร้อมใช้ (Availability) หมายถึง การที่ผู้ที่มีสิทธิสามารถเข้าใช้งานสินทรัพย์นั้นได้เมื่อยามต้องการใช้งาน ซึ่งมีทั้งในทางกายภาพและทางเทคโนโลยี ได้แก่ การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้งานต้องการจะรับหรือส่ง ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลา เป็นต้น (สำนักงานพัฒนารัฐบาลดิจิทัล, 2563)

ธนาคารแห่งประเทศไทยให้ความสำคัญกับเรื่องไซเบอร์เป็นอย่างมาก โดยดำเนินการตามนโยบายความปลอดภัยทางไซเบอร์ใน 3 มิติ ดังนี้

มิติแรก คือการวางแผนทางและกรอบกติกา ทำแผนยุทธศาสตร์ 3 ปี ด้านการรับมือภัยคุกคามไซเบอร์ปี พ.ศ. 2560-2562 เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของภาคการเงิน และมีการประเมินความพร้อมของธนาคารพาณิชย์ สถาบันการเงินเฉพาะกิจ และผู้ให้บริการชำระเงินในไทย รวมถึงธนาคารแห่งประเทศไทยเอง

มิติที่สอง คือการหาพันธมิตรเพื่อแลกเปลี่ยนข้อมูลข่าวสาร การสร้างความร่วมมือกับหน่วยงานอื่นๆ ในภาคการเงิน ขณะนี้ได้ร่วมมือกับ 4 องค์กร ได้แก่ สมาคมธนาคารไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานคณะกรรมการการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย ภาคการธนาคารได้มีการร่วมมือกันจัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือที่เรียกว่า “ไทยแบงก์กิ้งเซิร์ต” (Thailand Banking Sector-CERT: TB-CERT) เพื่อให้ภาคธนาคารมีการแลกเปลี่ยนข้อมูลภัยคุกคามและรับมือภัยไซเบอร์ ระหว่างกันอย่างเป็นระบบและมีประสิทธิภาพ รวมถึงมีแนวทางการติดตามแก้ไขปัญหา และมาตรฐานความปลอดภัยโดยศูนย์ดังกล่าวยังเชื่อมโยงไปยัง “ไทยเซิร์ต” (Thai-CERT) ของภาครัฐ และ CERT ของกลุ่มตลาดทุน กลุ่มประกันภัย และอาจขยายเครือข่ายไปยังธนาคารสาขาต่างประเทศ นอกจากนี้ ธนาคารแห่งประเทศไทยอยู่ระหว่างการเข้าร่วมกลุ่ม Central Banks, Regulators and Supervisory Entities (CERES) Forum เป็นกลุ่มความร่วมมือแรกที่มีขึ้นสำหรับหน่วยงานกำกับดูแลทางการเงินในภูมิภาคที่จะมีการขยายไปเชื่อมต่อกับทั่วโลก เพื่อแลกเปลี่ยนข้อมูล เหตุการณ์ภัยคุกคาม รวมถึงข้อมูลเชิงนโยบาย และกรอบการกำกับดูแลภัยไซเบอร์อย่างเป็นระบบ

มิติสุดท้าย คือการสร้างความเข้าใจที่ถูกต้องเกี่ยวกับการใช้เทคโนโลยีทางการเงินให้กับประชาชน รวมถึงการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ ธนาคารแห่งประเทศไทยได้ร่วมกับสถาบันการศึกษาจัดกิจกรรม Cybersecurity Bootcamp ให้นักศึกษาฝึกปฏิบัติกับภัยไซเบอร์จากสถานการณ์จำลอง เพื่อเตรียมความพร้อม รวมถึงสร้างเครือข่ายการสรรหาบุคลากรที่มีความเชี่ยวชาญดังกล่าว และเมื่อต้นปี พ.ศ. 2564 สพธอ. ได้จัดตั้ง ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ขึ้นในประเทศไทย โดยมีเป้าหมายที่จะฝึกอบรมบุคลากรในอาเซียนกว่าพันคน (อนุภาค มาตรฐาน และอิสรารุฒิ เอี่ยมวิริยะกุล, 2561)

จะเห็นว่าประเทศไทยได้ให้ความสำคัญในการกำกับดูแลรักษาความปลอดภัยทางไซเบอร์เช่นเดียวกับประเทศทั่วโลก โดยกำหนดเป็นนโยบายยุทธศาสตร์ชาติ โดยออกกฎหมาย

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มากำกับและดูแลความมั่นคง และปลอดภัยทางไซเบอร์ จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัตินี้ หน่วยงานองค์กรภาครัฐ และภาคเอกชนได้นำนโยบายยุทธศาสตร์ชาติและพระราชบัญญัติฉบับนี้ไปปฏิบัติโดยจัดทำ เป็นนโยบายและแผนงานของหน่วยงาน ดังเช่น กระทรวงกลาโหมนำมาจัดทำเป็นนโยบาย ในการกำกับ ดูแล ป้องกันด้านความมั่นคงของประเทศ ธนาคารแห่งประเทศไทยนำมาจัดทำ เป็นแผนงานในการกำกับ ดูแล ป้องกันด้านการทำธุรกรรมทางการเงินของประเทศ เป็นต้น

5. บทสรุป

ความเป็นมาของโลกไซเบอร์ที่ก่อเกิดเป็นวัฒนธรรมไซเบอร์ (Cyber Culture) เริ่มจากการที่มนุษย์เราในกลุ่มแฮกเกอร์ที่เป็นนักวิชาการนักโปรแกรมเมอร์นักศึกษาที่ศึกษา วิทยาศาสตร์คอมพิวเตอร์ คิดค้นประดิษฐ์โปรแกรมในการสร้างจักรกลในสถาบันการศึกษา และพัฒนาโปรแกรมใช้ในระบบคอมพิวเตอร์ขนาดใหญ่ออกไปภายนอกสถาบันการศึกษา ต่อมา พัฒนาเป็นเครือข่ายดิจิทัลแพร่ขยายไปทุกระบบทุกด้านทุกประเทศทั่วโลกอย่างไร้พรมแดน เพื่อตอบสนองความต้องการของพลเมืองโลก จึงทำให้ได้รับความสนใจอย่างรวดเร็วกว้างขวาง วิวัฒนาการพัฒนาระบบคอมพิวเตอร์และระบบการสื่อสารทางเทคโนโลยีดิจิทัลในโลก

ไซเบอร์ในทุกด้านเป็นไปอย่างรวดเร็ว ดังเช่นด้านมหภาคที่มีวิวัฒนาการการทำ สงครามระหว่างประเทศ การทำธุรกรรมทางการเงินเชื่อมต่อเป็นเครือข่ายดิจิทัล ด้านจุลภาค โลกไซเบอร์ได้เข้ามามีบทบาทในการดำรงชีวิตประจำวันของพลเมืองโลกทุกเพศทุกวัย จึงเห็น ว่าการพัฒนาโลกไซเบอร์ที่รวดเร็วนี้เป็นการแข่งขันกันของผู้พัฒนาระบบคอมพิวเตอร์และ เทคโนโลยีของกลุ่มคนและองค์กรต่างๆ ทั้งระดับประเทศและระหว่างประเทศ ต่างทำการสร้าง และพัฒนาระบบโดยมุ่งหมายคิดสร้างสรรค์เพื่อนำวิทยาการเทคโนโลยีและเครือข่ายดิจิทัล ใหม่ๆ ออกมาใช้ประโยชน์ในการตอบสนองความต้องการของมนุษย์ด้วยกันและองค์กร ในระดับประเทศและระหว่างประเทศทั้งในด้านความมั่นคง ด้านธุรกรรมทางการเงิน ด้านสังคม และด้านอื่นๆ แต่ไม่ได้มีการวางแผน กรอบแนวคิด ทิศทาง นโยบาย ในการกำกับ ดูแล ควบคุม จัดระเบียบการใช้งานระบบการสื่อสารและป้องกันความปลอดภัยทางไซเบอร์ตั้งแต่เริ่มเกิด โลกไซเบอร์ขึ้นมา จึงทำให้เกิดปัญหาตามมามากมาย และเกิดการกระทำผิดก่ออาชญากรรม ทางไซเบอร์เพิ่มขึ้นอย่างรวดเร็ว เช่น การใช้เทคโนโลยีทำสงครามในโลกไซเบอร์ทำให้เกิด ปัญหาการทำลายล้างที่เสียหายรุนแรง การก่ออาชญากรรมทางการเงินเปลี่ยนรูปแบบไปสู่

โลกไซเบอร์ การใช้สื่อเทคโนโลยีออนไลน์ทำร้ายรังแกกันโดยเฉพาะเด็กๆ เปลี่ยนรูปแบบไปสู่โลกไซเบอร์เช่นกัน อันจะทำให้พลเมืองโลกได้รับความเสียหายทั้งแก่ชีวิตและทรัพย์สินมากมาย

นโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์เพื่อคุ้มครองพลเมืองโลกนั้นประเทศต่างๆ ได้พยายามหาแนวทางวิธีการในการแก้ไขปัญหาและป้องกันความปลอดภัยทางไซเบอร์ ซึ่งมาตรการด้านกฎหมายถือเป็นมาตรการสำคัญประการหนึ่งที่ประเทศต่าง ๆ นำมาใช้ในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์และป้องกันความปลอดภัยทางไซเบอร์ ประเทศมหาอำนาจล้วนเป็นผู้นำและแข่งขันกันใช้เทคโนโลยีและดิจิทัลในพื้นที่ในโลกไซเบอร์ และมีการกำหนดนโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์เพื่อคุ้มครองพลเมือง เช่น

กลุ่มประเทศสหภาพยุโรปได้ร่วมกันออกกรอบการดูแลความปลอดภัยไซเบอร์ของภาคอุตสาหกรรมในยุโรป (Directive on Security of Network and Information Systems) ของสินค้าและบริการ การประมวลผลทางไอทีต่างๆ และเป็นกฎหมายที่จะรับรองบทบาทและหน้าที่ของศูนย์ Cybersecurity Agency ของอียู หรือเรียกย่อว่า European Agency for Network and Information Security (ENISA) ในการต่อต้านภัยคุกคามด้านความมั่นคงทางไซเบอร์และจัดสรรงบประมาณในการดำเนินการใดๆ ของหน่วยงาน และออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป (General Data Protection Regulation) และเสนอร่างกฎหมายด้านความยืดหยุ่นทางไซเบอร์ของหน่วยงานที่จำเป็น (Directive on Cyber Resilience of Critical Entities: CER) เพื่อยกระดับความปลอดภัยให้ครอบคลุมอุตสาหกรรมและภาคส่วนอื่นๆ ที่ต้องการความยืดหยุ่น จึงเห็นได้ว่า กลุ่มประเทศสหภาพยุโรปนั้นเป็นบริบทสถานะของการรวมตัวกันเป็นกลุ่มประเทศ จึงออกมาตราการกฎหมายการดูแลความปลอดภัยทางไซเบอร์มุ่งเน้นในด้านการทำความร่วมมือทางเศรษฐกิจการค้าและสิทธิส่วนบุคคลพลเมืองในการใช้สื่อในโลกไซเบอร์ติดต่อสื่อสารกันในกลุ่ม EU

ประเทศสหรัฐอเมริกา ทำเนียบประธานาธิบดีสหรัฐฯ ร่วมกับสำนักความมั่นคงโครงสร้างพื้นฐานและการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity and Infrastructure Security Agency: CISA) และสำนักบริหารงบประมาณ (Office of Management and Budget: OMB) ออกนโยบายผลักดันให้หน่วยงานของรัฐนำแนวคิดการออกแบบมาตรการรักษาความมั่นคงปลอดภัยแบบ "zero trust" ซึ่งเป็นแนวคิดการออกแบบระบบรักษาความปลอดภัยอย่างเข้มงวดบนพื้นฐานความไว้วางใจเป็นศูนย์ การเข้าถึงทรัพยากรบนระบบเครือข่ายคอมพิวเตอร์หรือการอนุญาตให้อุปกรณ์คอมพิวเตอร์เชื่อมต่อในเครือข่ายจะต้องผ่านการตรวจสอบอย่างเข้มงวดทั้งการเชื่อมต่อจากภายในสำนักงานหรือภายนอกสำนักงาน และปฏิบัติในลักษณะเดียวกัน จึงเห็นได้ว่า ประเทศสหรัฐอเมริกานั้นเป็นประเทศเสรีประชาธิปไตยปกครองแบบมลรัฐ จึงสร้างแนวคิด "zero trust" กำหนดเป็นนโยบายมาทำ

การวางกรอบการบังคับให้ปฏิบัติและออกกฎหมายให้องค์กรของมลรัฐและภาคเอกชนนำไปบังคับปรับใช้ในการปฏิบัติการดูแลความปลอดภัยทางไซเบอร์ของพลเมืองและองค์กร

ประเทศจีน รัฐบาลออกนโยบายในการปกป้องความปลอดภัยทางไซเบอร์ไว้ และประกาศความมุ่งหมายที่จะกำจัดเนื้อหาที่ต่อต้านหลักการสำคัญในรัฐธรรมนูญ เป็นอันตรายต่อความมั่นคงของรัฐ เปิดเผยความลับของชาติ บ่อนทำลายชาติและความสามัคคี ทำลายเกียรติหรือผลประโยชน์ของประเทศฯ โดยประเทศจีนให้ความสำคัญกับเสถียรภาพทางสังคม อำนาจอธิปไตยและความสามัคคีของคนในชาติ ภายใต้การบังคับใช้ของกฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศจีน ผู้ให้บริการทางโครงข่ายซึ่งประกอบด้วยกิจการอันเกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญจะถูกบังคับให้มีส่วนร่วมในการปกป้องความมั่นคงปลอดภัยไซเบอร์ด้วย ประเทศจีนมีกฎหมายหลักที่สำคัญในสังคมดิจิทัลคือ กฎหมายว่าด้วยการรักษาความปลอดภัยทางไซเบอร์ กฎหมายว่าด้วยการรักษาความปลอดภัยของข้อมูล และ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล จึงเห็นได้ว่า ประเทศจีนซึ่งปกครองโดยระบอบสังคมนิยมรัฐเดี่ยว ดังนั้น รัฐบาลจีนจึงออกนโยบายและกฎหมายนำไปใช้บังคับควบคุมดูแลความปลอดภัยทางไซเบอร์และมุ่งเน้นความปลอดภัยของอำนาจอธิปไตยรัฐเป็นหลักสำคัญก่อน ประชาชนและองค์กรภาคเอกชนต้องปฏิบัติตามอย่างเคร่งครัด

ประเทศทั่วโลก รวมทั้งกลุ่มประเทศสหภาพยุโรป ประเทศสหรัฐอเมริกา ประเทศจีน ได้กำหนดนโยบายการดูแลความปลอดภัยทางไซเบอร์เป็นนโยบายหลักของประเทศในกำกับดูแล ป้องกัน แก้ไขปัญหาภัยคุกคามและอาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ จัดตั้งหน่วยงานกำกับดูแลโลกไซเบอร์ และออกกฎหมายความปลอดภัยทางไซเบอร์และกฎหมายคุ้มครองข้อมูลส่วนบุคคล เพื่อต้องการรักษาอำนาจอธิปไตยของประเทศและกำกับดูแลคุ้มครองพลเมืองให้ใช้สื่อดิจิทัลในโลกไซเบอร์ให้ปลอดภัย แต่การนำนโยบายและกฎหมายไปบังคับใช้ของแต่ละประเทศและกลุ่มประเทศจะมีความแตกต่างกันตามระบอบการปกครองและการบริบทของการรวมตัวกันของกลุ่มประเทศ ส่วนความร่วมมือระหว่างประเทศในการรักษาความปลอดภัยทางไซเบอร์นั้นจะเป็นการทำความร่วมมือในระดับพหุภาคีประเทศ ยังไม่ค่อยรวมประเทศเป็นกลุ่มใหญ่หรือในองค์การระดับโลก อาจเนื่องจากแต่ละประเทศมุ่งหมายที่จะป้องกันคุ้มครองอธิปไตยของรัฐให้ความปลอดภัยจากสงครามการถูกประเทศอื่นโจมตีทางไซเบอร์

นโยบายความปลอดภัยทางไซเบอร์ด้านกฎหมายของประเทศไทยก็ให้ความสำคัญในการกำกับดูแลรักษาความปลอดภัยทางไซเบอร์เช่นเดียวกับประเทศทั่วโลก โดยกำหนดเป็นนโยบายยุทธศาสตร์ชาติ โดยออกกฎหมาย พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มากำกับ รับมือ และลดความเสี่ยงภัยคุกคามทางไซเบอร์ ได้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบ

งานตามพระราชบัญญัตินี้ บูรณาการความร่วมมือหน่วยงานองค์กรภาครัฐและภาคเอกชน ได้นำนโยบายยุทธศาสตร์ชาติและพระราชบัญญัติฉบับนี้ไปปฏิบัติโดยจัดทำเป็นนโยบายและแผนงานของหน่วยงาน ดังตัวอย่างของกระทรวงกลาโหม สำนักงานพัฒนารัฐบาลดิจิทัล ธนาคารแห่งประเทศไทย เป็นต้น ซึ่งพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นี้จะบัญญัติบังคับให้หน่วยงานของรัฐต้องปฏิบัติตาม แต่ในส่วนของภาคเอกชนจะเป็นการขอความร่วมมือให้ปฏิบัติ เปรียบได้ดังการนำนโยบายและกฎหมายของประเทศสหรัฐอเมริกา กับประเทศจีนมาปรับผสมผสานให้เข้ากับบริบทของสังคมไทย แต่อาจมีช่องว่างในส่วนของ การกำกับควบคุมดูแลองค์กรภาคเอกชนซึ่งมีตั้งแต่ขนาดเล็กจนถึงขนาดใหญ่เป็นจำนวนมาก เนื่องจากเป็นการขอความร่วมมือให้ปฏิบัติอาจได้รับการตอบรับจากองค์กรขนาดใหญ่เท่านั้น แต่ในองค์กรขนาดเล็กอาจเป็นองค์กรที่ทำให้เกิดปัญหาทางไซเบอร์ได้มากก็ได้

ซึ่งจากการศึกษานโยบายด้านกฎหมายความปลอดภัยทางไซเบอร์นั้นถือได้ว่าประเทศต่างๆ ทั่วโลกได้ดำเนินการกำหนดนโยบายและออกกฎหมาย รวมถึงการจัดตั้งองค์กร ควบคุมดูแลเรื่องความปลอดภัยทางไซเบอร์เป็นการเฉพาะที่เห็นได้เป็นรูปธรรมแล้ว จะมีลักษณะหลักเกณฑ์ทางปฏิบัติคล้ายคลึงกัน จะแตกต่างกันบ้างเกี่ยวกับการมุ่งเน้นรักษาความ มั่นคงอธิปไตยของแต่ละประเทศ และวิธีการนำไปบังคับใช้ที่ขึ้นอยู่กับบริบทการปกครองและ สังคมของแต่ละประเทศ พลเมืองของประเทศไทยและพลเมืองโลกในยุคนี้ส่วนใหญ่เกี่ยวข้องอยู่ใน โลกไซเบอร์ จึงควรศึกษาบริบทด้านกฎหมายการดูแลรักษาความปลอดภัยไซเบอร์ของ ประเทศที่ต้องการทำธุรกรรมในโลกไซเบอร์ก่อนเพื่อลดความเสี่ยงภัยทางไซเบอร์ และติดตาม ต่อไปว่าประเทศต่างๆ จะมุ่งมั่นปฏิบัติตามนโยบายและการบังคับใช้กฎหมายขององค์กรต่างๆ ที่เกี่ยวข้องในอนาคตต่อไปให้ได้อย่างมีประสิทธิภาพและต่อเนื่องหรือไม่ จะทำความร่วมมือกัน เพิ่มมากขึ้นช่วยกันแก้ไขปัญหาลงโลกไซเบอร์ให้มีความปลอดภัยเป็นประโยชน์กับพลเมืองโลก ได้หรือไม่ นั่น ยังคงเป็นเรื่องที่น่าสนใจติดตามต่อไป

เอกสารอ้างอิง

ภาษาไทย

- Thaieurope. (2562). *กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของอียูมีผลใช้บังคับแล้ว*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก https://appdb.tisi.go.th/tis_devs/regulate/eu/pdf/Cybersecurity.pdf
- กรมยุโรป กระทรวงการต่างประเทศ. (2564). *สหภาพยุโรปเสนอแผนยุทธศาสตร์ด้านความปลอดภัยทางไซเบอร์ เสริมเกราะป้องกันการโจมตีออนไลน์*. สืบค้นเมื่อ 26 มิถุนายน 2566, จาก <https://europetouch.mfa.go.th/th/content>
- กระทรวงกลาโหม. (2566). *แผนพัฒนาด้านไซเบอร์เพื่อความมั่นคง กระทรวงกลาโหม (พ.ศ. 2566-2570)*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://dist.mod.go.th/PDF/actplancyber63-65.aspx>
- กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2566). *เกี่ยวกับ สกมช*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://www.mdes.go.th/mission/detail/2481>
- คลาร์ก, ริชาร์ด เอ, และเคนเนดี, โรเบิร์ต เค. (2555). *สงครามไซเบอร์ [Cyber War]* (ไพรัตน์ พงศ์พานิชย์, ผู้แปล). กรุงเทพฯ: มติชน.
- ฉัตรพงศ์ ชูแสงนิล. (2561). *ยุคแห่งพลเมืองดิจิทัล*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://www.scimath.org/article-technology/item/8659-2018-09-11-07-58-08>
- ไชยสิทธิ์ ตันตยกุล. (2564). *กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลของจีน*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <http://www.vijachina.com/articles/2366>
- นัทธมน เพชรกล้า, และสมนทิพย์ จิตสว่าง. (2566). *การใช้อำนาจอธิปไตยในโลกไซเบอร์. วารสารสหวิทยาการมนุษยศาสตร์และสังคมศาสตร์, 6(2), 899-914.*
- ปองกมล สุรัตน์. (2561). *การรังแกผ่านโลกไซเบอร์ในมิติสังคมวัฒนธรรม: กรณีศึกษาเยาวชนไทย เจเนอเรชัน Z (วิทยานิพนธ์ปรัชญาดุษฎีบัณฑิต)*, สาขาวิชาการวิจัยพฤติกรรมศาสตร์ประยุกต์ บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ.
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก*.
- ยง ภู่วรรณ. (2564). *ชีวิตวิถีใหม่เกี่ยวกับดิจิทัล*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://learningdq-dc.ku.ac.th/course/?c=1&l=6>
- สำนักข่าวกรองแห่งชาติ. (2564). *สหรัฐฯ ยกระดับมาตรการรักษาความปลอดภัยทางไซเบอร์หน่วยงานด้านการคมนาคม*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://www.nia.go.th/cyber/cyberpage/565/>

- สำนักงานกองทุนสนับสนุนการส่งเสริมสุขภาพ. (2563). *Cyberbully คืออะไร? ส่งผลอย่างไร? และเราควรรับมือกับมันอย่างไรดี?*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://resourcecenter.thaihealth.or.th/article/cyberbully>.
- สำนักงานพัฒนารัฐบาลดิจิทัล. (2563). *นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://www.dga.or.th>
- เสมอ นิ่มเงิน. (2563). *ภัยคุกคามทางไซเบอร์กับกฎหมายไซเบอร์ไทย*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก <https://www.prd.go.th/th/file/get/file/2020122193f1c24f1221ab701e6cd1f075693b68110106.pdf>
- อนุกาต มาตรมูล, และอิสราวุฒิ เอี่ยมวิริยะกุล. (2561). *เตรียมพร้อมภาคการเงินเพื่อรับมือภัยทางไซเบอร์*. สืบค้นเมื่อ 20 มิถุนายน 2566, จาก https://www.bot.or.th/th/research-and-publications/articles-and-publications/articles/Article_17Oct201.html
- อาร์ม ตั้งนิรันดร. (2563). *กฎหมายความปลอดภัยทางไซเบอร์กับการกำกับดูแลเศรษฐกิจดิจิทัลของประเทศไทย: ถอดบทเรียนสำหรับเศรษฐกิจดิจิทัลในยุคไทยแลนด์ 4.0*. กรุงเทพฯ: สำนักงานการวิจัยแห่งชาติ (วช.).

ภาษาอังกฤษ

- Corn, G., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, 1(111), 207-212.
- Council of Europe. (2001). *Convention on Cybercrime*. Retrieved June 26, 2023, from <https://www.refworld.org/docid/47fdfb202.html>
- Halder, D., & Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Law, Right and Regulations*. Hershey, PA: IGI Global (USA).
- Hare, F. (2009). *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*. Retrieved October 22, 2022, from https://ccdcoe.org/uploads/2018/10/06_HARE_Borders-in-Cyberspace.pdf
- Information Office of the State Council the People's Republic of China. (2010). *Govt. White Papers – The Internet In China*. Retrieved 29 June 2023, from http://www.china.org.cn/government/whitepaper/2010-06/08/content_20208007.htm
- Macek, J. (2003). *Defining Cyberculture*. Retrieved November 31, 2023, from https://www.researchgate.net/publication/268629704_Defining_Cyberculture_Konzept_rane_kyberkultury