มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....*

*ภูมินทร์ บุตรอินทร์***

บทคัดย่อ

เทคโนโลยีสารสนเทศ (Information Technology – IT) ได้ก่อให้เกิดการเปลี่ยนแปลงต่อสังคม เศรษฐกิจ วัฒนธรรม และความมั่นคง อย่างยิ่งในปัจจุบัน จนมีผู้กล่าวว่าปัจจุบันนั้นเป็นยุคของ “การปฏิวัติสารสนเทศ (Information revolution)” ที่สร้างความเปลี่ยนแปลงต่าง ๆ ให้แก่โลกเหมือนกับเมื่อครั้งของการปฏิวัติเกษตรกรรม และการปฏิวัติอุตสาหกรรมในอดีต อีกทั้งบทบาทของเทคโนโลยีสารสนเทศก็เข้ามามีส่วนในชีวิตประจำวันของมนุษย์มากขึ้นเรื่อย ๆ ในอีกด้านหนึ่งก็มีผู้ที่ใช้เทคโนโลยีสารสนเทศในทางที่คุกคามบุคคลอื่น ๆ ทั้งในระดับปัจเจกบุคคล ในระดับมวลชน จนถึงการคุกคามในระดับความมั่นคงของประเทศ ซึ่งในหลายประเทศได้มีการตรากฎหมายเพื่อรับมือกับภัยคุกคามประเภทต่าง ๆ เหล่านั้นแล้ว และประเทศไทยได้จัดทำ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... ซึ่งเป็นที่มาของประเด็นต่าง ๆ ในการศึกษาวิจัยนี้ เพื่อเสนอแนะและเติมเต็มสิ่งที่ขาดหายไปเพื่อให้กฎหมายว่าด้วยการป้องกันภัยคุกคามทางไซเบอร์มีมาตรฐานในระดับสากลที่นานาประเทศยอมรับ ตลอดจนการบังคับใช้กฎหมายที่มีประสิทธิภาพและได้รับการยอมรับจากทุกฝ่ายที่เกี่ยวข้อง

---

*บทความนี้เป็นบทสรุปของรายงานการวิจัยเรื่องมาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. .... โดยงบประมาณสนับสนุนจากโครงการวิจัยทางวิชาการนิติศาสตร์ ตามประกาศคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์

**ผู้ช่วยศาสตราจารย์ ประจำคณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์ลำปาง

ในการศึกษาวิจัยนี้ จึงต้องศึกษาหลักการและแนวคิดที่เกี่ยวข้องกับการรักษาความมั่นคงไซเบอร์ของประเทศสหรัฐอเมริกา ประเทศจีน และสหภาพยุโรป เพื่อนำผลที่ได้มาศึกษาเปรียบเทียบกับกฎหมายว่าด้วยความมั่นคงไซเบอร์ของประเทศไทย เพื่อค้นหาจุดเด่น จุดด้อย ข้อควรพิจารณาต่าง ๆ และแนวทางในการแก้ไข ปรับปรุง (ร่าง) กฎหมายให้มีประสิทธิภาพยิ่งขึ้น

คำสำคัญ สิทธิในความเป็นส่วนตัว, ข้อมูลส่วนบุคคล, ความมั่นคงไซเบอร์, สิทธิมนุษยชน

Abstract

Information technology (IT) has led to changes in society, economy, culture and national security. Moreover, it is said that today is the age of “Information revolution” that is leading to change many things in the world as important as the times of the agricultural revolution and the industrial revolution. The role of Information technology is increasingly influential in our daily lives. On the other hand, some people use information technology in a way that threatens others at individual and public levels. And sometimes national security has been directly threatened.

In this research, principles and concepts related to cybersecurity in the United States, China and the European Union will be studied to compare with Thai’s cybersecurity law and to find its strengths, weaknesses, considerations. And considerations how to amend (draft) the law to be more effective will also be proposed in this research.

Key words: privacy rights- personal data-cybersecurity- human rights

1. บทนำ

เนื่องด้วยบทความนี้เป็นบทสรุปของงานวิจัยเรื่อง “มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ....” โดยงานวิจัยดังกล่าวทำการศึกษากฎหมายว่าด้วยความมั่นคงทางไซเบอร์ของสหภาพยุโรป ประเทศสาธารณรัฐประชาชนจีน และประเทศสหรัฐอเมริกา เพื่อค้นหามุมมองของกฎหมายว่าด้วยความมั่นคงทางไซเบอร์ว่าเหมือนหรือแตกต่างกันอย่างไร ตลอดจนข้อกังวลต่าง ๆ ที่เกิดขึ้นกับกฎหมายดังกล่าว ซึ่งในส่วนท้ายของรายงานการวิจัยได้มีการนำเสนอในลักษณะของตารางเปรียบเทียบข้อมูลที่ได้ศึกษาและรวบรวมมาเพื่อให้ผู้อ่านเห็นได้ชัดเจนยิ่งขึ้นถึงรายละเอียดอันเป็นประเด็นสำคัญ ดังนั้น หากผู้อ่านสนใจในรายละเอียดเพิ่มเติม ก็สามารถเข้าไปอ่านเพิ่มเติมในรายงานการวิจัยฯ ดังกล่าวได้

เทคโนโลยีสารสนเทศ (Information Technology – IT) ได้ก่อให้เกิดการเปลี่ยนแปลงต่อสังคม เศรษฐกิจ วัฒนธรรม และความมั่นคง โดยเฉพาะอย่างยิ่งในปัจจุบัน จนมีผู้กล่าวว่าปัจจุบันนั้นเป็นยุคของ “การปฏิวัติสารสนเทศ (Information revolution)” ที่สร้างความเปลี่ยนแปลงต่าง ๆ ให้แก่โลกเหมือนกับเมื่อครั้งของการปฏิวัติเกษตรกรรม และการปฏิวัติอุตสาหกรรมในอดีต ซึ่งการกล่าวเช่นนี้ก็ไม่เป็นการกล่าวเกินเลยแต่อย่างใดเพราะในปัจจุบันเทคโนโลยีสารสนเทศเป็นสิ่งที่สามารถเข้าถึงได้ง่าย สามารถประยุกต์ใช้กับสิ่งต่าง ๆ ในชีวิตประจำวันได้อย่างสะดวก และไม่มีค่าใช้จ่ายหรือค่าบำรุงรักษาที่สูงมากเหมือนในอดีต

การประยุกต์ใช้เทคโนโลยีสารสนเทศทำให้มี “โลกเสมือนจริง” ขึ้นมาอีกใบหนึ่ง แยกออกจากโลกแห่งความจริงซึ่งมีลักษณะที่เป็นรูปธรรมจับต้องได้ และโลกเสมือนจริงเช่นว่านั้นก็มีมนุษย์เป็นองค์ประกอบเหมือนกับโลกแห่งความจริงทุกประการ เพราะมนุษย์ซึ่งอยู่ในโลกแห่งความจริงนั้นได้นำกิจกรรมในชีวิตประจำวันหรือปัจจัยบางอย่างที่เกี่ยวข้องกับการใช้ชีวิตประจำวันไปไว้บนโลกเสมือนจริง ซึ่งทำให้เกิดการเข้าถึง การแลกเปลี่ยน ข้อมูลต่าง ๆ ในโลกเสมือนจริงดังกล่าวขึ้น ยิ่งไปกว่านั้น ในปัจจุบันได้ปรากฏว่า “รัฐ” ได้นำองค์กรและข้อมูลบางส่วนของตนเข้าไปจัดเก็บไว้ในโลกเสมือนจริงเช่นเดียวกัน ทั้งนี้ก็เพื่อความสะดวกในการดำเนินกิจการของรัฐหรือเพื่อการจัดทำบริการสาธารณะแก่ประชาชน

อย่างไรก็ตามเมื่อ “สังคมมนุษย์” และ “รัฐ” เข้าไปอยู่ในโลกเสมือนจริงดังกล่าวแล้ว สิ่งหนึ่งที่ยังคงติดตามมาด้วยก็คือ “ภัยคุกคาม” ต่าง ๆ ไม่ว่าจะเป็นอาชญากรรมในรูปแบบต่าง ๆ หรือการโจมตีระหว่างรัฐต่อรัฐ ซึ่งปัจจุบันภัยคุกคามทางไซเบอร์นั้นเกิดขึ้นได้หลากหลายรูปแบบและมีการพัฒนาและปรับเปลี่ยนให้มีความซับซ้อนมากยิ่งขึ้นเรื่อย ๆ โดยในช่วงต้นปีที่ผ่านมาระหว่างวันที่ 13-17 กุมภาพันธ์ 2560 สถาบัน SANS Institute[1] ซึ่งเป็นสถาบันที่ใหญ่ที่สุดและ

[1]ข้อมูลเพิ่มเติมสืบค้นได้จาก “What is SANS?,” [Online], Available: https://www.sans.org/, Retrieved Aug 24, 2017.

ได้รับความไว้วางใจมากที่สุดในด้านการฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์และการออกประกาศนียบัตรรับรองให้แก่ผู้ประกอบวิชาชีพทั้งในภาครัฐและเอกชนทั่วโลก ได้จัดให้มีการประชุม RSA Conference 2017 ที่เมืองซานฟรานซิสโก ประเทศสหรัฐอเมริกา[2] โดยมีหัวข้อที่น่าสนใจหัวข้อหนึ่งที่กล่าวถึง 7 ภัยคุกคามทางไซเบอร์ที่อันตราย (The Seven Most Dangerous New Attack Techniques, and What's Coming Next)[3] โดยภัยดังกล่าวได้แก่ ภัยจาก Ransomware ซึ่งเป็นภัยที่พร้อมเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์และหากต้องการข้อมูลดังกล่าวจำเป็นต้องจ่ายเงินค่าไถ่เพื่อแลกกับกุญแจสำหรับปลดรหัสซึ่งในปัจจุบันมีการคุกคามลักษณะดังกล่าวแพร่กระจายไปทั่วโลก หรือภัยจากการโจมตีบน Internet of Things อันเป็นภัยที่อาจเกิดขึ้นเมื่อผู้บริโภคเชื่อมต่ออุปกรณ์กับอินเทอร์เน็ต หรือการใช้อุปกรณ์เชื่อมต่อระหว่างอุปกรณ์ด้วยกัน ซึ่งจะเปิดโอกาสให้แฮ็คเกอร์สามารถเข้าโจมตีได้โดยง่าย ดังเหตุการณ์ที่เกิดขึ้นเมื่อต้นปีที่ผ่านมา (มกราคม พ.ศ. 2560) โรงแรมแห่งหนึ่งในประเทศออสเตรียถูกแฮ็คระบบคีย์การ์ดอิเล็กทรอนิกส์ทำให้ไม่สามารถใช้งานคีย์การ์ดได้ทำให้แขกที่มาพักติดอยู่นอกห้องและในห้องโดยไม่สามารถเปิดหรือปิดประตูได้[4] เป็นต้น

ด้วยเหตุนี้จึงเป็นหน้าที่ของรัฐที่ต้องให้หลักประกันและรับรองว่าภัยคุกคามเช่นว่านั้นจะไม่สร้างผลกระทบต่อการประยุกต์ใช้เทคโนโลยีสารสนเทศของบุคคลต่าง ๆ จึงได้เกิดการตอบโต้ภัยคุกคามดังกล่าวนั้นขึ้นมา ในการตอบโต้ภัยคุกคามอันเกิดจากการประยุกต์ใช้เทคโนโลยีสารสนเทศหรือที่นิยมเรียกกันโดยทั่วไปว่าภัยคุกคามทางไซเบอร์ดังกล่าวนั้น กลไกหลักที่รัฐได้นำมาใช้ก็คือ “กลไกทางด้านกฎหมาย” จึงทำให้เกิด “กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์” ขึ้นในหลายประเทศ ในส่วนของประเทศไทยนั้นได้มีการตรากฎหมายที่เกี่ยวข้องกับการตอบโต้ภัยคุกคามไซเบอร์มาเป็นระยะเวลาหนึ่งแล้วแต่ในช่วงเวลาดังกล่าว ความตื่นตัวเกี่ยวกับการประยุกต์ใช้เทคโนโลยีสารสนเทศยังไม่เป็นที่แพร่หลายนักในประเทศไทยทำให้กฎหมายดังกล่าวถูกกล่าวถึงและมีบทบาทเฉพาะในส่วนของหน่วยงานหรือองค์กรที่เกี่ยวข้องเท่านั้น ต่อมาเมื่อเกิดการผลักดันนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม อันทำให้เกิดการวางแผนจัดทำ “ชุดร่างกฎหมายดิจิทัลการส่งเสริมเศรษฐกิจและสังคม” หรือเรียกโดยย่อว่า “ชุดกฎหมายเศรษฐกิจดิจิทัล” ขึ้น ซึ่งในชุดกฎหมายดังกล่าวก็ได้มีกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์โดยตรงฉบับหนึ่ง ก็คือ “(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์

---

[2]ข้อมูลเพิ่มเติมสืบค้นได้จาก “7 ภัยคุกคามไซเบอร์ที่น่ากลัวที่สุดในโลก จัดอันดับโดย SANS INSTITUTE,” [ออนไลน์], เข้าถึงได้จาก: https://www.techtalkthai.com/7-deadly-attacks-by-sans/, สืบค้น 24 สิงหาคม 2560.

[3]ข้อมูลเพิ่มเติมสืบค้นได้จาก “The Seven Most Dangerous New Attack Techniques, and What's Coming Next,” [Online], Available: https://www.rsaconference.com/events/us17/agenda/sessions/7582-The-Seven-Most-Dangerous-New-Attack-Techniques,-and-What's-Coming-Next, Retrieved Aug 24, 2017.

[4]ข้อมูลเพิ่มเติมสืบค้นได้จาก “Alpine hotel brings locks cyber hacking,” [Online], Available: http://www.dailymail.co.uk/news/article-4163886/Alpine-hotel-brings-locks-cyber-hacking.html#ixzz4wOQDx87i, Retrieved Aug 24, 2017.

พ.ศ. ....” ซึ่งก่อให้เกิดความสนใจและตระหนักถึงการใช้กฎหมายเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นอย่างมากหากเทียบกับเมื่อครั้งในอดีต

ในอีกมุมหนึ่งความสนใจและความตระหนักเช่นว่านั้นกลับถูกแสดงออกมาในลักษณะที่ค่อนข้างเป็นปฏิปักษ์และต่อต้านกฎหมายดังกล่าว เพราะโดยลักษณะอันเป็นธรรมชาติของกฎหมายความมั่นคงต่าง ๆ มักจะมีลักษณะเป็นการก้าวล่วงเข้าไปในแดนแห่งสิทธิและเสรีภาพของประชาชน จึงทำให้เกิดการวิพากษ์วิจารณ์และโต้แย้งจากภาคประชาชนเกี่ยวกับเนื้อหาของบทบัญญัติกฎหมายดังกล่าวในหลายประเด็นด้วยกัน จึงเกิดเป็นปัญหาข้อพิพาทระหว่าง “ความมั่นคงของรัฐ และสิทธิเสรีภาพของประชาชน” ขึ้นอีกครั้งหนึ่ง และด้วยเหตุนี้จึงทำให้ “(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....” จึงยังอยู่ระหว่างการพิจารณาและยังไม่สามารถนำมาประกาศเพื่อบังคับใช้ได้

ความกังวลและความไม่เห็นด้วยกับเนื้อหาของ “(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....” นั้น ดังความคิดเห็นของภาคประชาชนที่ปรากฏในการจัดสัมมนารับฟังความคิดเห็นและที่ปรากฏตามสื่อต่าง ๆ[5] ส่วนหนึ่งเกิดมาจากความซับซ้อนของหลักการ ทฤษฎี และนิติวิธี ที่อยู่ในร่างกฎหมายดังกล่าว เพราะการรักษาความมั่นคงไซเบอร์เป็นกระบวนการที่มีความเป็น “สหวิทยาการ” เกี่ยวข้องกับวิทยาศาสตร์และสังคมศาสตร์หลายแขนงด้วยกัน ไม่ว่าจะเป็นหลักการทางด้านเทคโนโลยีสารสนเทศ กฎหมาย และความมั่นคงของรัฐ เป็นต้น จึงทำให้ (ร่าง) พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... มีเนื้อหาที่ยากต่อการทำความเข้าใจไปโดยปริยาย จึงอาจกล่าวได้ว่าปัญหาที่เป็นข้อพิพาทอยู่ในสังคม ณ ขณะนี้เกิดจากความเข้าใจอย่างไม่ตรงกันระหว่างหน่วยงานของรัฐกับประชาชนในหลายส่วนของกฎหมายดังกล่าว โดยเฉพาะอย่างยิ่ง “การใช้คำ” หรือ “นิยาม” ต่าง ๆ ที่ปรากฏในกฎหมายฉบับนี้ตลอดจนความคิดเห็นที่แตกต่างกันในเรื่องของหลักการต่าง ๆ นั่นเอง

ท้ายที่สุด ปัญหาดังกล่าวจะก่อให้เกิดผลกระทบกับความรู้สึกของภาคประชาชนว่าเป็นการตีความและปรับใช้ร่างกฎหมายฯ ดังกล่าวในแง่ที่เป็นปฏิปักษ์ต่อสิทธิและเสรีภาพของประชาชน ซึ่งความเข้าใจผิดของประชาชนและความรู้สึกไม่ดีระหว่างภาครัฐกับภาคประชาชนย่อมไม่ก่อให้เกิดผลดีต่อทั้งรัฐและประชาชน เพราะหากกฎหมายฉบับดังกล่าวถูกคัดค้านหรือโต้แย้งมากจนไม่อาจบังคับใช้ได้ ประเทศไทยและประชาชนก็จะตกอยู่ในสภาวะที่เสี่ยงต่อการถูกคุกคามจากภัยคุกคามทางไซเบอร์ได้ง่าย

จากเหตุปัจจัยและปัญหาในด้านต่าง ๆ จึงมีความจำเป็นอย่างยิ่งที่ประชาชนทุกคน เจ้าหน้าที่ของรัฐ และหน่วยงานองค์กรต่าง ๆ ทั้งภาครัฐและภาคเอกชนควรจะได้ทราบถึงหลักการและทฤษฎี ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ทั้งทางด้านกฎหมาย และด้านความมั่นคง เพื่อให้ได้ทราบถึงหลักการที่แท้จริงของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเพื่อจะได้นำมา

---

[5]ข้อมูลเพิ่มเติมสืบค้นได้จาก ASTV ผู้จัดการรายวัน, ““พ.ร.บ.ความมั่นคงไซเบอร์” เมื่อรัฐบาลรู้ทุกความลับของคุณได้,” [ออนไลน์], เข้าถึงได้จาก: http://www.manager.co.th/daily/ViewNews.aspx?News ID=9580000008653 [2558]. สืบค้น 24 สิงหาคม 2560.

เปรียบเทียบถึงข้อดีและข้อเสียของการจัดทำ “(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....” อันจะทำให้ประเทศมีกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์บังคับใช้ต่อไป

2. ความทั่วไปว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์

โดยที่ได้กล่าวไว้ในตอนต้นว่าเทคโนโลยีสารสนเทศมีอิทธิพลอย่างยิ่งในการดำรงชีวิตประจำวัน และมีแนวโน้มเพิ่มมากขึ้นเรื่อย ๆ จนอาจกล่าวได้ว่าในการดำรงชีวิตในแต่ละวัน จะต้องมีความเกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างหลีกเลี่ยงไม่ได้ อาทิ การซื้อของทางออนไลน์ การอ่านหนังสือพิมพ์หรือการดูภาพยนตร์ผ่านทางเว็บไซต์ต่าง ๆ การสนทนาโต้ตอบระหว่างกันโดยผ่านทางแอพพลิเคชั่นไลน์ หรือการโพสต์รูปถ่ายลงบนเฟซบุ๊ค เป็นต้น และในขณะเดียวกันก็มักจะมีผู้ไม่หวังดีที่อาศัยเทคโนโลยีสารสนเทศที่บุคคลใช้ในชีวิตประจำวันมาปรับใช้ในการแสวงหาผลประโยชน์ในทางไม่สุจริตเพื่อตนเองเช่นเดียวกัน

ในด้านภารกิจของรัฐ รัฐได้นำเทคโนโลยีสารสนเทศมาใช้ในภารกิจของตนในหลายด้าน อาทิ การใช้เทคโนโลยีสารสนเทศในภารกิจด้านการบริหารราชการแผ่นดิน โดยมุ่งเน้นให้การจัดทำบริการสาธารณะและกิจการอื่น ๆ ของรัฐแปรเข้าสู่ระบบอิเล็กทรอนิกส์มากขึ้น ซึ่งในขณะนี้ประเทศไทยยังอยู่ในระยะที่กำลังพัฒนาและวางแผนเกี่ยวกับการเข้าสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ โดยเริ่มมีการขยายตัวและเป็นรูปเป็นร่างขึ้นทุกขณะ ทั้งการใช้เทคโนโลยีสารสนเทศในภารกิจด้านเศรษฐกิจ หรือการใช้เทคโนโลยีสารสนเทศในภารกิจด้านการศึกษา (การจัดให้มีการศึกษาผ่านระบบออนไลน์ (E-learning) ระบบหนังสือและตำราอิเล็กทรอนิกส์ (E-book)) หรือการใช้เทคโนโลยีสารสนเทศในภารกิจด้านการทหารหรือการป้องกันประเทศ เป็นต้น

ยิ่งไปกว่านั้น ปัจจุบันได้มีแนวคิดในการ “บูรณาการข้อมูลประชาชนให้เป็นภาพเดียว” (Single View of Citizen)[6] โดยเชื่อมโยงข้อมูลของประชาชนจากฐานข้อมูลของหน่วยงานทุกส่วนเข้าไว้เป็นหนึ่งเดียว เพื่อที่หน่วยงานต่าง ๆ ของรัฐจะได้สามารถนำข้อมูลมาใช้ได้ในทันที และประชาชนไม่ต้องทำการยื่นเอกสารหรือให้ข้อมูลแก่รัฐในลักษณะซ้ำซ้อน กล่าวคือ หากนาย ก. ได้ยื่นสำเนาทะเบียนบ้านแก่หน่วยงานรัฐแห่งใดแห่งหนึ่งไปแล้ว ต่อมาหากหน่วยงานของรัฐหน่วยงานใดต้องการสำเนาทะเบียนบ้านของ นาย ก. อีกก็ไม่ต้องแจ้งให้ นาย ก. ยื่นสำเนาทะเบียนบ้านอีก เพราะสำเนาทะเบียนบ้านเมื่อได้ยื่นให้แก่หน่วยงานรัฐใด ๆ ก็ตามแล้วก็จะถูกบันทึกอยู่ในฐานข้อมูลส่วนกลางเมื่อหน่วยงานรัฐใดมีความต้องการใช้ก็เพียงเรียกข้อมูลดังกล่าวมาใช้ได้ในทันที อันก่อให้เกิดความสะดวกและรวดเร็วในการจัดทำบริการสาธารณะของรัฐ ทว่า การที่รัฐหันมาพึ่งพาเทคโนโลยีสารสนเทศมากเท่าใด หากระบบเทคโนโลยีสารสนเทศเกิดความเสียหายและไม่สามารถ

[6] ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ ฝ่ายนโยบายและยุทธศาสตร์ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.), แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ระยะ 3 ปี (พ.ศ. 2559-2561), (กรุงเทพฯ: บริษัท ไอดี ออล ดิจิตอล พริ้นท์ จำกัด (สำนักงานใหญ่), 2559), น.18-19.

ใช้การได้ ย่อมเกิดผลกระทบต่อการทำงานของรัฐอย่างหลีกเลี่ยงไม่ได้ และย่อมเกิดผลกระทบโดยตรงต่อความปลอดภัยและการดำรงชีวิตโดยปกติสุขของประชาชนตามไปด้วย ดังนั้น จึงอาจกล่าวได้ว่าภัยคุกคามไซเบอร์หรือความมั่นคงทางไซเบอร์เป็นสิ่งสำคัญและถือเป็นภารกิจลำดับต้น ๆ ที่รัฐจะต้องให้ความสำคัญ

การนำระบบเทคโนโลยีสารสนเทศมาใช้กับการดำรงชีวิตประจำวัน ตลอดจนการดำเนินนโยบายภาครัฐ อาจนำมาสู่การคุกคามทางไซเบอร์เพิ่มขึ้น แต่ภัยคุกคามไซเบอร์นั้นมีความหมายที่กว้างมาก และเป็นคำที่กินความหมายรวมกับทุกการกระทำที่ส่งผลกระทบต่อการประยุกต์ใช้เทคโนโลยีสารสนเทศทุกประเภท ซึ่งอาจจำแนกภัยคุกคามทางไซเบอร์ได้สามประเภท ดังนี้ 1. อาชญากรรมทางไซเบอร์ (Cyber Crime) 2. สงครามไซเบอร์ (Cyber Warfare) และ 3. การก่อการร้ายไซเบอร์ (Cyber Terrorism) โดยมีรายละเอียด ดังต่อไปนี้

1. อาชญากรรมทางไซเบอร์ (Cyber Crime) เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือใช้คอมพิวเตอร์เป็นอุปกรณ์ในการกระทำความผิด ไม่ว่าจะเป็นการใช้คอมพิวเตอร์เพื่อเข้าถึงระบบคอมพิวเตอร์ของบุคคลอื่นโดยมิชอบ หรือเป็นการเข้าถึงคอมพิวเตอร์ของบุคคลอื่นเพื่อทำให้เสียหาย แก้ไข เปลี่ยนแปลงข้อมูล หรือเข้าถึงข้อมูลของผู้อื่นโดยไม่ชอบ นอกจากนี้ยังรวมถึงการกระทำใด ๆ ต่อระบบคอมพิวเตอร์ไม่ว่าจะเป็นการกระทำทางกายภาพ หรือเทคโนโลยีอื่น[7] ดังนั้น จึงอาจสรุปได้ว่าคอมพิวเตอร์นั้นอาจจะอยู่ในฐานะที่เป็นเป้าหมาย (Computer as a target) และอาจจะอยู่ในฐานะเป็นเครื่องมือในการกระทำความผิดได้ (Computer as a tool)

ความแตกต่างระหว่างอาชญากรรมทางคอมพิวเตอร์ (Computer crime) กับอาชญากรรมทางไซเบอร์ (Cyber Crime) นั้น อยู่ที่ว่าการกระทำความผิดนั้นได้ดำเนินการผ่านระบบอินเทอร์เน็ตหรือไม่ กล่าวคือหากเป็นการกระทำความผิดโดยใช้คอมพิวเตอร์หรือกระทำความผิดต่อคอมพิวเตอร์โดยมิได้มีการเชื่อมโยงกับระบบอินเทอร์เน็ต จะเรียกว่า “อาชญากรรมทางคอมพิวเตอร์” (Computer crime) ทว่า หากการกระทำความผิดนั้น มีการใช้คอมพิวเตอร์เชื่อมต่อกับระบบอินเทอร์เน็ต จะเรียกว่า “อาชญากรรมทางไซเบอร์” (Cyber Crime) หรือ “อาชญากรรมทางอินเทอร์เน็ต” (Internet crime)[8] ทว่า ในทางปฏิบัติมีการกล่าวอ้างและนำไปใช้อย่างทับซ้อนกัน โดยจะกล่าวถึงอาชญากรรมทางไซเบอร์ในความหมายที่ครอบคลุมอาชญากรรมทางคอมพิวเตอร์[9]

อาชญากรรมทางไซเบอร์ (Cyber Crime) เป็นการดำเนินการโดยบุคคลหรือกลุ่มบุคคลที่อาจจะมีมูลเหตุจูงใจทางด้านการเงิน ด้านการก่อกวน ด้านอุดมการณ์ทางการเมือง ก็ได้ แต่ความเสียหายจะอยู่ในระดับปัจเจกบุคคลและยังมิได้เป็นการโจมตีระบบโครงข่าย ดังนั้น ผลกระทบที่

---

[7]วัชระ เนติวาณิชย์, คู่มือกฎหมายการสื่อสารและเทคโนโลยีสารสนเทศ, (กำแพงเพชร: ห้างหุ้นส่วนจำกัดศรีสวัสดิ์การพิมพ์ 1994, ม.ป.ป.), น.199.

[8]ข้อมูลเพิ่มเติมสืบค้นได้จาก “COMPUTER CRIMES/CYBER CRIMES,” [Online], Available: http://www.salzmanattorney.com/federal-crimes/computer-crimescyber-crimes/. Retrieved Aug 24, 2017.

[9]ITU, “The Phenomena,” Understanding cybercrime: Phenomena, challenges and legal response, (2012): p.11, [Online], Available: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Retrieved Aug 24, 2017.

เกิดขึ้นจึงยังไม่ถึงระดับการทำสงครามทางไซเบอร์ ซึ่งกรณีอาชญากรรมทางไซเบอร์ (Cyber Crime) นี้จะมีกฎหมายอาญากำหนดลักษณะความผิดและองค์ประกอบความผิดไว้อย่างชัดเจน

2. สงครามไซเบอร์ (Cyber Warfare) หมายถึง การดำเนินการใด ๆ ในลักษณะของการก่อวินาศกรรมหรือการโจรกรรม ซึ่งอาจจะมีวัตถุประสงค์เพื่อได้มาซึ่งข้อมูลอันเป็นความลับ การก่อกวน หรือการทำลายเป้าหมาย เป็นต้น ซึ่งการโจมตีในระดับนี้มักจะเป็นภัยคุกคามชั้นสูง (An advanced persistent threat หรือ APT)[10] หรือเป็นการโจมตีโครงข่ายซึ่งอาจจะเป็นการจารกรรมข้อมูล หรือการทำลายโครงข่ายก็ได้ โดยมีรูปแบบตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด อาทิ การโจมตีเว็บไซต์ หรือปิดกั้นเว็บไซต์ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลและแนวติดด้านการเมืองผ่านอินเทอร์เน็ต การเจาะข้อมูลลับโดยแฮ็คเกอร์ (Hacker) การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐานที่มีความสำคัญอย่างยิ่ง (Critical Infrastructure) เป็นต้น[11]

3. การก่อการร้ายไซเบอร์ (Cyber Terrorism) หมายถึง “การดำเนินการอันมีวัตถุประสงค์เพื่อก่อการร้าย โดยมีระบบดิจิทัลเป็นเป้าหมายในการโจมตี หรือการใช้ระบบดิจิทัลเป็นเครื่องมือในการกระทำความผิดเกี่ยวกับการก่อการร้าย”

อย่างไรก็ตาม นิยามดังกล่าวก็ยังมิใช่นิยามที่เป็นสากลและได้รับการยอมรับร่วมกันในระดับนานาชาติ และหลายกรณียังมีความสับสนระหว่างการก่อการร้ายไซเบอร์ (Cyber Terrorism) กับสงครามไซเบอร์ (Cyber Warfare) เพราะองค์ประกอบของการกระทำความผิดและลักษณะของการกระทำความผิดโดยทั่วไปนั้น มีความคล้ายคลึงกัน อีกทั้งยังคงเป็นสิ่งที่มีข้อถกเถียงในทางวิชาการอยู่มาก ทั้งในวงวิชาการ และในวงผู้ปฏิบัติงาน จึงอาจกล่าวได้ว่าในปัจจุบัน ยังคงมีปัญหาในเรื่องของการให้คำนิยามของถ้อยคำต่าง ๆ เหล่านี้อย่างมาก

จึงอาจกล่าวได้ว่านิยามของ “การก่อการร้ายไซเบอร์” ยังคงเป็นปัญหาในทำนองเดียวกันกับการให้คำนิยามของคำว่า “การก่อการร้าย” ซึ่งเป็นถ้อยคำที่ยังคงไม่มีบทนิยามที่เป็นหนึ่งเดียวและเป็นที่ยอมรับร่วมกัน[12] และสถานการณ์ปัจจุบันนั้น อยู่ในสภาวการณ์ที่มีปัญหาในเรื่องของการให้คำนิยามของถ้อยคำต่าง ๆ เหล่านี้อย่างมาก[13]

---

[10]Margaret Rouse, “advanced persistent threat (APT),” [Online], Available: http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT. Retrieved Sep 11, 2016.

[11]โรงเรียนนายเรือ, “สงครามไซเบอร์ (Cyber Warfare),” [ออนไลน์], เข้าถึงได้จาก: http://www.rtna.ac.th/download/cyberwar.pdf. สืบค้น 15 กันยายน 2559.

[12]ปกป้อง ศรีสนิท, คำอธิบายกฎหมายอาญาระหว่างประเทศ, พิมพ์ครั้งที่ 1, (กรุงเทพมหานคร: โรงพิมพ์เดือนตุลา, 2556), น.111.

[13]ในรายงานพิเศษของสถาบันสันติวิธีสหรัฐอเมริกา (United States Institute of Peace) ได้มีการกล่าวถึงคำนิยามของการก่อการร้ายไซเบอร์ซึ่งได้ถูกนิยามโดย ศาสตราจารย์ทางด้านวิทยาศาสตร์คอมพิวเตอร์ Dorothy Denning ไว้ดังนี้

“การก่อการร้ายไซเบอร์ คือ การรวมกันของโลกเทคโนโลยีสารสนเทศและการก่อการร้ายมันหมายถึงการโจมตีที่ไม่ชอบด้วยกฎหมายหรือภัยของการโจมตีต่อคอมพิวเตอร์ เครือข่าย และข้อมูลข่าวสารที่ถูกเก็บไว้ภายใน อันกระทำไปเพื่อข่มขู่ ทำให้กลัว หรือ บีบบังคับ รัฐบาลหรือประชาชนด้วยวัตถุประสงค์ทางการเมืองหรือทางสังคม นอกจากนี้การใดจะเป็น

2.1 กฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์ในต่างประเทศ

วัตถุประสงค์ในการศึกษากฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์ในต่างประเทศ ตามที่ปรากฏในรายงานการวิจัย เรื่อง “มาตรการที่เหมาะสมในการรักษาความมั่นคงปลอดภัยไซเบอร์: ศึกษา ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ....” นั้น เพื่อต้องการทราบถึงแนวคิดพื้นฐานในการปรับใช้กฎหมายฯ บทบัญญัติทางกฎหมายที่สำคัญ และข้อกังวลของภาคประชาชนในการนำกฎหมายฯ ดังกล่าวมาบังคับใช้ ที่เกิดขึ้นในต่างประเทศ เนื่องจากภัยคุกคามทางไซเบอร์เป็นการคุกคามในรูปแบบใหม่ มีความหลากหลาย และมีลักษณะของการคุกคามที่แตกต่างกัน ดังนั้น การนำเอา “กลไกทางด้านกฎหมาย” มาใช้ในการตอบโต้ภัยดังกล่าวในประเทศไทยนั้น จึงจำเป็นอย่างยิ่งที่จะต้องศึกษาถึงกฎหมายว่าด้วยความมั่นคงไซเบอร์ของต่างประเทศ

การศึกษากฎหมายว่าด้วยการรักษาความมั่นคงไซเบอร์ในต่างประเทศที่จะกล่าวถึงในลำดับต่อไป ได้แก่ 1. กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์แห่งสหภาพยุโรป (EU) 2. กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ประเทศสาธารณรัฐประชาชนจีน และ 3. กฎหมายความมั่นคงปลอดภัยไซเบอร์ของประเทศสหรัฐอเมริกา ซึ่งการคัดเลือกกลุ่มประเทศข้างต้นในการศึกษา เนื่องจากแต่ละแห่งมีพัฒนาการเรื่องความมั่นคงปลอดภัยทางไซเบอร์ในระดับต้น ๆ ของโลก โดยในรายงานการวิจัยฯ ฉบับเต็ม จะนำเสนอให้ทราบถึงประเด็นสำคัญในด้านต่าง ๆ ตามลำดับ ได้แก่ วัตถุประสงค์ในการบังคับใช้กฎหมาย หน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามไซเบอร์ มาตรการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐาน ปัญหาและข้อกังวลในการบังคับใช้กฎหมาย และในส่วนท้ายจะมีการนำเสนอในรูปแบบของตารางเพื่อให้ผู้อ่านได้เห็นในเชิงเปรียบเทียบในประเด็นที่ได้ศึกษามาแล้ว

2.1.1 กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์แห่งสหภาพยุโรป (EU)

สหภาพยุโรปมีรัฐสมาชิกจำนวน 28 ประเทศ ซึ่งรัฐสภายุโรปได้ตรากฎหมายเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ขึ้นมาเพื่อใช้บังคับกับประเทศสมาชิก เรียกว่า “กฎว่าด้วยความปลอดภัยของเครือข่ายและระบบข้อมูลข่าวสารสนเทศ” หรือ “The Directive on security of network and information systems” (the NIS Directive) ลงวันที่ 6 กรกฎาคม 2016 โดยมี

การก่อการร้ายไซเบอร์หรือไม่นั้น การโจมตีควรจะส่งผลให้เกิดความรุนแรงต่อบุคคลหรือทรัพย์สิน หรือสร้างความเสียหายเพียงพอที่จะสร้างความกลัว การโจมตีที่นำมาซึ่งความตายหรือการบาดเจ็บทางกาย การระเบิด หรือทำให้เกิดความเสียหายทางเศรษฐกิจ เป็นตัวอย่างการก่อการร้ายไซเบอร์ การโจมตีอย่างรุนแรงต่อโครงสร้างพื้นฐานที่มีความสำคัญอย่างยิ่งอาจเป็นการกระทำของการก่อการร้ายไซเบอร์ ขึ้นอยู่กับผลกระทบของมัน ซึ่งการโจมตีที่ทำลายการบริการที่ไม่มีความสำคัญหรือทำให้เกิดเพียงความเดือดร้อนรำคาญย่อมไม่เป็นการก่อการร้ายไซเบอร์” ศึกษารายละเอียดเพิ่มเติมที่ Gabriel Weimann, “Cyberterrorism: How Real Is the Threat?”, [Online], Available: http://www.usip.org/ publications/ cyberterrorism-how-real-the-threat [2004]. Retrieved September 19, 2016.

วัตถุประสงค์เพื่อตอบสนองนโยบายในการสร้างความเชื่อมั่นสำหรับการสื่อสารให้มีความปลอดภัยมากที่สุด โดยกำหนดมาตรฐานความปลอดภัยขั้นต่ำที่นำมาใช้กับระบบสื่อสารและข้อมูลสารสนเทศทั้งหมดและมีการผลักดันนโยบาย การป้องกันภัยคุกคามทางไซเบอร์ผ่านยุทธศาสตร์ 3 ยุทธศาสตร์[14] ได้แก่ การสร้างความร่วมมือระหว่างประเทศสมาชิก การสร้างความพร้อมในการรับมือกับภัยคุกคามไซเบอร์สำหรับประเทศสมาชิก และการสร้างวัฒนธรรมในเชิงป้องกันและการใช้งานที่ปลอดภัยจากภัยคุกคามไซเบอร์ โดยมีหน่วยงานกลางที่ดำเนินการเชื่อมโยงและประสานการทำงานของประเทศสมาชิกของสหภาพยุโรปสำหรับการรับมือต่อภัยคุกคามไซเบอร์ที่เกิดขึ้นในสหภาพยุโรปหลายหน่วยงาน ดังนี้

ตัวอย่างหน่วยงานสำคัญทางด้านความมั่นคงปลอดภัยทางไซเบอร์

หน่วยงานทางด้านความมั่นคงปลอดภัยทางโครงข่ายและสารสนเทศแห่งสหภาพยุโรป (The European Union Agency for Network and Information Security หรือ ENISA)[15] ENISA เป็นหน่วยงานกลางสำหรับอำนวยความสะดวกและประสานงานการป้องกันและปราบปรามการคุกคามระบบโครงข่ายไซเบอร์ในสหภาพยุโรป โดยการทำงานของ ENISA จะมุ่งเน้นการลดช่องว่างด้านมาตรฐานการทำงานด้านความปลอดภัยของแต่ละประเทศสมาชิกที่แตกต่างกัน และมีบทบาทตามที่ปรากฏใน the new Basic Regulation of 2013 ซึ่งกำหนดให้เป็นผู้เชี่ยวชาญหลักในการให้คำแนะนำแก่คณะกรรมาธิการและรัฐสมาชิกเกี่ยวกับประเด็นข้อสงสัยของการบังคับใช้ “กฎว่าด้วยความปลอดภัยของโครงข่ายและระบบข้อมูลข่าวสารสนเทศ” หรือ The Directive on security of network and information systems (the NIS Directive) เพื่อทำหน้าที่ในการรวบรวมและวิเคราะห์ข้อมูลต่าง ๆ ที่ได้รับมาเพื่อระบุหรือประเมินความเสี่ยงที่เกิดขึ้น ตลอดจนส่งเสริมความร่วมมือระหว่างผู้มีส่วนได้เสียในภาคส่วนต่าง ๆ และประสานการทำงานร่วมกันระหว่างภาครัฐและภาคเอกชน

หน่วยงานตอบสนองเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์ (computer security incident response teams (CSIRT)) หรือ (computer emergency response team (CERT)) เป็นหน่วยงานที่จัดตั้งในภาครัฐหรือภาคเอกชนก็ได้ แต่ได้รับมอบหมายให้รับผิดชอบในการประสานงานและสนับสนุนการตอบสนองต่อเหตุการณ์คุกคาม หรือเพื่อสร้างความปลอดภัยของระบบคอมพิวเตอร์ หรือดำเนินการเพื่อลดและควบคุมความเสียหายที่เกิดจากเหตุการณ์ที่เกิดขึ้นหรือการกู้คืนข้อมูลที่ถูกทำลาย

---

[14]Europa, “The Directive on security of network and information systems (NIS Directive),” [Online], Available: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [n.d.] Retrieved Sep 11, 2017.

[15]ENISA, “About ENISA,” [Online], Available: https://www.enisa.europa.eu/about-enisa [n.d.]. Retrieved Sep 11, 2017.

ตัวอย่างมาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามทางไซเบอร์

สำหรับมาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามไซเบอร์นั้น สหภาพยุโรปได้กำหนดให้มีมาตรการหลายประการตามที่ปรากฏใน “กฎว่าด้วยความปลอดภัยของโครงข่ายและระบบข้อมูลข่าวสารสนเทศ” หรือ The Directive on security of network and information systems (the NIS Directive) เช่น การกำหนดให้มีการรวบรวมรายชื่อของผู้ประกอบการเอกชนในภาคส่วนต่าง ๆ ที่เป็นส่วนสำคัญต่อระบบเศรษฐกิจ และกำหนดให้ผู้ประกอบการเอกชนหรือหน่วยงานของรัฐต้องจัดเตรียมมาตรการสำหรับการป้องกันการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพ การกำหนดขั้นตอนการรับมือกับภัยคุกคามโดยยกระดับตามความร้ายแรงของภัยคุกคาม การกำหนดให้บริษัทเอกชนจะต้องแจ้งลักษณะของการคุกคามที่เกิดขึ้นต่อหน่วยงานของรัฐที่รับผิดชอบ และเมื่อหน่วยงานของรัฐเห็นว่าเป็นภัยคุกคามที่ร้ายแรง หน่วยงานของรัฐก็มีหน้าที่ในการแจ้งให้หน่วยงานป้องกันภัยคุกคามในระดับสหภาพยุโรปได้รับทราบ การส่งเสริมความร่วมมือและการแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิก การจัดตั้งกลุ่มความร่วมมือทางยุทธศาสตร์เพื่ออำนวยความสะดวกในการแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ดีที่สุดระหว่างประเทศสมาชิกสหภาพยุโรป และการจัดตั้งหน่วยงานตอบสนองเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์แห่งชาติ (National CSIRT) เพื่อเป็นจุดติดต่อระหว่างประเทศต่าง ๆ สำหรับหารือเกี่ยวกับเหตุการณ์ด้านความมั่นคงข้ามพรมแดนตลอดจนร่วมกันตอบโต้ภัยคุกคามโดยสมาชิกแห่งสหภาพยุโรป เป็นต้น

ตัวอย่างมาตรการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของประชาชน

ในด้านการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของประชาชนนั้น การทำงานใด ๆ ในสหภาพยุโรปโดยส่วนใหญ่จะให้ความสำคัญกับสิทธิมนุษยชนหรือสิทธิขั้นพื้นฐานอย่างยิ่ง เช่นเดียวกันกับ “กฎว่าด้วยความปลอดภัยของโครงข่ายและระบบข้อมูลข่าวสารสนเทศ” หรือ The Directive on security of network and information systems (the NIS Directive) ก็ระบุไว้อย่างชัดเจนใน อารัมภบท ข้อ 75 ว่าการดำเนินการตามกฎฯ นี้จะเคารพสิทธิขั้นพื้นฐานและจะปฏิบัติตามหลักการตามที่ได้รับการรับรองจากกฎบัตรสิทธิขั้นพื้นฐานของสหภาพยุโรป (the Charter of Fundamental Rights of the European Union) โดยเฉพาะอย่างยิ่ง การเคารพต่อสิทธิในชีวิตส่วนตัวและการสื่อสาร การคุ้มครองข้อมูลส่วนบุคคล เสรีภาพในการประกอบกิจการและการดำเนินธุรกิจ ตลอดจนสิทธิในทรัพย์สิน และสิทธิในการได้รับการเยียวยาความเสียหายจากศาล เป็นต้น

ข้อกังวลของภาคประชาชนในการบังคับใช้กฎหมาย

ปัญหาและข้อกังวลในการบังคับใช้กฎหมายของสหภาพยุโรป คือ ปัญหาในเรื่องความไม่ชัดเจน[16] กล่าวคือกฎหมายดังกล่าวได้รับการจัดทำขึ้นเพื่อใช้กับ “โครงข่ายโดยรวม” ทั้ง

[16]Mayer Brown, “A new EU framework on cybersecurity: the Network and Information Security Directive,” p.3, [Online], Available: https://www.mayerbrown.com/files/Publication/5da28c2 e-a8fd-4f19-

ด้านคมนาคม ด้านโทรคมนาคม ด้านการขนส่ง ด้านไฟฟ้า ด้านประปา เป็นต้น จึงอาจจะไม่สอดคล้องกับภาคส่วนที่มีลักษณะเฉพาะ อาทิ โครงข่ายพลังงานหรือโครงข่ายการคมนาคมขนส่งหรือโครงข่ายการเงินและการธนาคาร และกฎหมายดังกล่าวไม่ได้ระบุอย่างชัดเจนว่า “เหตุการณ์ลักษณะใดที่ถือว่าเป็นภัยคุกคาม” ที่มีความร้ายแรงถึงขนาดจะต้องแจ้งเหตุไปยังหน่วยงานที่เกี่ยวข้อง ซึ่งรัฐสมาชิกจะต้องให้คำจำกัดความและกำหนดมาตรฐานระดับชาติสำหรับการดำเนินการให้เป็นไปตามกฎหมายอีกทีหนึ่ง ปัญหาอีกประการคือ มาตรฐานความพร้อมสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละประเทศของสมาชิกสหภาพยุโรปแตกต่างกัน[17] อีกทั้งความเคร่งครัดในการดำเนินการตามกรอบของกฎหมายและระเบียบข้อบังคับก็ต่างกัน ดังนั้นประเทศสมาชิกจึงอาจจะมีปัญหาในการทำงานที่แต่ละประเทศจะต้องทำการเรียนรู้ร่วมกันและสร้างความไว้วางใจระหว่างกัน

อย่างไรก็ตาม กฎหมายดังกล่าวถือได้ว่าเป็นขั้นตอน (แรก) ที่สำคัญในการสร้างความร่วมมือการรักษาความปลอดภัยในโลกไซเบอร์ในสหภาพยุโรป และอาจใช้เป็นกรณีศึกษาสำหรับความร่วมมือในอนาคตในเรื่องความร่วมมือในโลกเสมือนที่ไม่มีพรมแดนอยู่จริงว่าควรจะดำเนินการอย่างไรต่อไป

2.1.2 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีน

ประธานาธิบดี สี จิ้น ผิง เคยดำริในปี ค.ศ. 2014 ว่าการพัฒนาของอินเทอร์เน็ตจะเกิดความท้าทายใหม่ ๆ ต่อความมั่นคงด้านอธิปไตยของชาติ ทั้งในด้านความมั่นคง และผลประโยชน์ของชาติในโลกไซเบอร์[18] และในเวลาต่อมาท่านก็มีดำริว่า “อินเทอร์เน็ตมิได้หมายถึงดินแดนที่อยู่นอกกฎหมาย” และนับตั้งแต่นั้นเป็นต้นมา ก็ได้มีการจัดทำกฎหมายความมั่นคงปลอดภัยไซเบอร์[19] และกฎหมายความมั่นคงปลอดภัยไซเบอร์กลายเป็นเครื่องมือในการปกป้อง “อธิปไตยทางไซเบอร์” ของชาติ (网络空间主权) โดยมีการประกาศใช้กฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ เมื่อวันที่ 7 พฤศจิกายน 2016 โดยให้มีผลบังคับ ตั้งแต่วันที่ 1 มิถุนายน

---

bdc2-d62d6fc27f0b/Presentation/PublicationAttachment/2b75998a-2615-4e9d-828b-ee9b6e8e96e3/cybersecurity-update_jul2616.pdf [2016]. Retrieved Sep 11, 2017.

[17]Tom Reeve, “New EU directive requires critical infrastructure to improve cyber-security,” [Online], Available: https://www.scmagazineuk.com/updated-new-eu-directive-requires-critical-infrastructure-to-improve-cyber-security/article/530778/ [2016]. Retrieved Sep 11, 2017.

[18]Scott D. Livingston, “Beijing Touts ‘Cyber-Sovereignty’ In Internet Governance,” [Online], Available: http://www.chinafile.com/reporting-opinion/viewpoint/beijing-touts-cyber-sovereignty-inter net-governance [2015]. Retrieved Sep 11, 2017.

[19]Reed Smith, “The new Cybersecurity Law of China: What does it mean for the International Market?,” [Online], Available: http://www.lexology.com/library/detail.aspx?g=f4b2a415-9874-430d-9481-513215158660 [2017]. Retrieved Sep 11, 2017.

2017 เป็นต้นไป[20] โดยวัตถุประสงค์ของกฎหมายฉบับนี้ถูกบัญญัติอยู่ในมาตรา 1 ซึ่งได้กำหนดว่า “...กฎหมายนี้ตราขึ้นเพื่อประโยชน์แห่งการรักษาไว้ซึ่งความมั่นคงปลอดภัยเครือข่าย ปกป้องอธิปไตยของโลกเทคโนโลยีสารสนเทศ ความมั่นคงแห่งชาติ และประโยชน์สาธารณะ ปกป้องสิทธิทางกฎหมายและประโยชน์ของพลเมือง สร้างความร่วมมือกับองค์กรอื่น และเสริมสร้างการพัฒนาที่สร้างสรรค์ของเทคโนโลยีสารสนเทศในส่วนของเศรษฐกิจและสังคม...” ดังนั้น พึงคาดหมายได้ว่ากฎหมายฉบับนี้เป็นกฎหมายที่รัฐบาลจีนมุ่งหวังให้เป็นรากฐานสำคัญในการดูแลความมั่นคงปลอดภัยไซเบอร์ในประเทศจีน

ตัวอย่างหน่วยงานสำคัญทางด้านความมั่นคงปลอดภัยทางไซเบอร์

ประธานาธิบดี สี จิ้น ผิง ได้จัดตั้งองค์กรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยเฉพาะ กล่าวคือ “สำนักงานสารสนเทศทางอินเทอร์เน็ตของสภาแห่งรัฐ” หรือ “the State Council Internet Information Office” (国务院新闻办公室)[21] โดยหน่วยงานดังกล่าวเป็นหน่วยงานสำคัญและมีบทบาททางด้านความมั่นคงปลอดภัยทางไซเบอร์เป็นหลัก (หน่วยงานดังกล่าวอยู่ภายใต้การทำงานของสภาแห่งรัฐ) และบทบาทของหน่วยงานดังกล่าวมีอิทธิพลอย่างยิ่งในการกำหนดนโยบายอินเทอร์เน็ตในประเทศจีน

ตัวอย่างมาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามทางไซเบอร์

หากพิจารณาบทบัญญัติว่าด้วยกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของประเทศจีน อาจจำแนกมาตรการรักษาความมั่นคงไซเบอร์ได้เป็น 2 ส่วน กล่าวคือ[22]

1. มาตรการที่ปรากฏในบทบัญญัติทั่วไปอันเป็นการกำหนดกฎเกณฑ์กว้าง ๆ ของการรักษาความมั่นคงไซเบอร์ โดยบังคับใช้กับผู้ประกอบการในหลายส่วน อาทิ ผู้ให้บริการโครงข่ายและผู้ใช้บริการ เป็นต้น ซึ่งมาตรการเหล่านี้จะปรากฏอยู่ในหมวด 2 ของกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์[23]

2. มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่มุ่งเน้นรักษาความมั่นคงปลอดภัยในโครงสร้างพื้นฐานด้านข้อมูลข่าวสารที่มีความสำคัญ (critical infrastructure network operators) ซึ่งเน้นการคุ้มครองและปกป้องโครงสร้างพื้นฐานทางด้านสารสนเทศที่สำคัญของประเทศ และผู้ให้บริการโครงข่าย (Network operators) โดยมาตรการที่กำหนดขึ้นนี้หากมีการฝ่า

---

[20]Baker Mckenzie, “Final Passage of China's Cybersecurity Law,” [Online], Available: http://www.bakermckenzie.com/en/insight/publications/2016/11/final-passage-of-chinas-cybersecuri ty-law/ [2016]. Retrieved Sep 11, 2017.

[21]Rogier Creemers, “Is China’s Cybersecurity Law Visionary?,” [Online], Available: http://www.chinausfocus.com/peace-security/is-chinas-cybersecurity-law-visionary [2017]. Retrieved Jan 17, 2017.

[22]Infosec Institute, “China’s New Cyber Security Law,” [Online], Available: http://resources.infosecinstitute.com/chinas-new-cyber-security-law/#gref [n.d.] Retrieved Jan 17, 2017.

[23]*Ibid.* Retrieved Apr 19, 2017.

ฝืนหรือไม่ปฏิบัติตามกฎหมายจะมีบทลงโทษตามแต่ละกรณี อาทิ มาตรการลงโทษทางแพ่ง (โทษปรับ) มาตรการลงโทษทางปกครอง และมาตรการลงโทษทางอาญา เป็นต้น[24]

ตัวอย่างมาตรการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของประชาชน

กฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ได้ให้ความสำคัญกับการคุ้มครองสิทธิส่วนบุคคลเช่นเดียวกัน กล่าวคือ การกำหนดลักษณะของข้อมูลส่วนบุคคลที่ผู้ให้บริการสามารถจัดเก็บได้ การกำหนดข้อจำกัดในการถ่ายโอนข้อมูลส่วนบุคคล หรือการให้สิทธิ์แต่ละบุคคลในการขอให้ลบข้อมูลส่วนบุคคลทิ้ง หากมีการนำไปใช้ในทางที่ผิดวัตถุประสงค์

โดยได้กำหนดรายละเอียดเป็นหลักเกณฑ์ต่าง ๆ เช่น หลักเกณฑ์การจัดเก็บข้อมูลส่วนบุคคล (Data localisation rule) หรือหลักเกณฑ์ในการกำหนดให้มีการเปิดเผยนโยบายในการเก็บรักษาและการนำข้อมูลส่วนบุคคลไปใช้ (Privacy Notices) หรือหลักเกณฑ์การได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนการจัดเก็บหรือการประมวลผลข้อมูล[25]

ข้อกังวลของภาคประชาชนในการบังคับใช้กฎหมาย[26]

ข้อกังวลเกี่ยวกับสิทธิและเสรีภาพขั้นพื้นฐานของประชาชนมีลักษณะเดียวกันกับปัญหาที่เกิดขึ้นในสหภาพยุโรป กล่าวคือ ความไม่ชัดเจนในทางปฏิบัติ โดยเฉพาะอย่างยิ่ง ในเรื่องของการต้องเก็บรักษาข้อมูลส่วนบุคคลและข้อมูลสำคัญของผู้ประกอบการที่ประกอบกิจการในดินแดนของสาธารณรัฐประชาชนจีน ไว้ในดินแดนของสาธารณรัฐประชาชนจีนเท่านั้น และหากต้องการส่งข้อมูลเหล่านั้นไปนอกดินแดนของสาธารณรัฐประชาชนจีน ผู้ให้บริการนั้นจะต้องดำเนินการตามมาตรการที่หน่วยงานโครงข่ายสารสนเทศและหน่วยงานภายใต้การกำกับดูแลของสภาแห่งรัฐกำหนด เพื่อประเมินความปลอดภัย เว้นแต่จะได้กำหนดเป็นอย่างอื่นตามกฎหมาย ซึ่งปัญหาในเรื่องนี้ผู้ประกอบการต่างชาติมีข้อกังวลว่า ข้อมูลส่วนบุคคลเกี่ยวกับพนักงานของบริษัทที่มีการจัดเก็บอยู่แล้ว (ในทางปกติธุรกิจ) จะอยู่ในความหมายดังกล่าวหรือไม่ ซึ่งจะมีผลให้ไม่สามารถถ่ายโอนข้อมูลดังกล่าวไปยังบริษัทแม่ที่อยู่ต่างประเทศได้[27]

ปัญหาความไม่ชัดเจนในเรื่องนิยามของคำว่า “ความมั่นคงของชาติ” (ที่กำหนดให้ผู้ให้บริการจะต้องให้ความร่วมมือ กรณีเป็นภัยต่อความมั่นคงของชาติ) โดยกฎหมายดังกล่าวได้ก่อให้เกิดภาระหน้าที่ต่อผู้ประกอบการบางประการ กล่าวคือ ในมาตรา 28 กำหนดให้ ผู้ให้บริการเครือข่ายพึงจัดให้มีการสนับสนุนและช่วยเหลือทางเทคนิคแก่หน่วยงานที่เกี่ยวข้องกับ ความ

---

[24]Hogan Lovells, “China passes controversial Cyber Security Law,” [Online], Available: https://www.hoganlovells.com/en/publications/china-passes-controversial-cyber-security-law [2016]. Retrieved Apr 19, 2017.

[25]*Ibid*

[26]Hogan Lovells, “IP aspects of China's new controversial Cyber Security Law,” [Online], p. 1-2, Available: http://f.datasrvr.com/fr1/016/41094/HKGLIB01-1707823-v1-IP_alert_-_IP_aspects_ of_Chinas_new_controversial_Cyber_security_law_-_December_2016.pdf [2016]. Retrieved Apr 19, 2017.

[27]Supra note 25

ปลอดภัยสาธารณะและความมั่นคงของรัฐในการรักษาไว้ซึ่งความมั่นคงของชาติและการสืบสวนการก่ออาชญากรรม โดยกฎหมายฉบับนี้ไม่ได้มีการกล่าวถึงหรือจำกัดความคำว่า “ความมั่นคงของชาติ” และ “อาชญากรรม” ไว้ในขอบเขตของกฎหมายฉบับนี้ ซึ่งเงื่อนไขในเรื่อง “ความมั่นคงของชาติ” และ “อาชญากรรม” ถือเป็นจุดเริ่มต้นที่ควรจะต้องมีความชัดเจน เนื่องจากจะเกิดภาระผูกพันให้ผู้ประกอบการด้านโครงข่ายอินเทอร์เน็ตหรือที่เกี่ยวข้องมีหน้าที่ตามกฎหมายต่อไป

อนึ่ง ประเทศจีนเห็นว่ากฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ถือเป็นส่วนหนึ่งที่ใช้ในการรักษาอธิปไตยของประเทศ เพื่อไม่อาจให้มีการรุกล้ำได้เช่นเดียวกันกับเขตแดนอธิปไตยทางกายภาพ (ทางบก ทางน้ำ ทางอากาศ)[28] ซึ่งแนวคิดพื้นฐานดังกล่าวจึงสะท้อนออกมาในการบังคับใช้ที่เข้มงวดและเคร่งครัด มีลักษณะที่ให้อำนาจรัฐอย่างเบ็ดเสร็จเด็ดขาดในภัยคุกคามที่เห็นว่าเป็นภัยร้ายแรงของประเทศ ดังความที่ปรากฏในมาตรา 1 แห่งพระราชบัญญัติว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์แห่งสาธารณรัฐประชาชนจีน

“...กฎหมายนี้ตราขึ้นเพื่อประโยชน์แห่งการรักษาไว้ซึ่งความมั่นคงปลอดภัยเครือข่าย ปกป้องอธิปไตยของโลกเทคโนโลยีสารสนเทศ ความมั่นคงแห่งชาติ และประโยชน์สาธารณะ ปกป้องสิทธิทางกฎหมายและประโยชน์ของพลเมือง สร้างความร่วมมือกับองค์กรอื่น และเสริมสร้างการพัฒนาที่สร้างสรรค์ของเทคโนโลยีสารสนเทศในส่วนของเศรษฐกิจและสังคม...”[29]

ดังนั้น จึงอาจกล่าวได้ว่าการกำหนดเนื้อหาบทบัญญัติที่ไม่ชัดเจนและให้อำนาจหน่วยงานของรัฐในการตีความว่าเป็นภัยต่อความมั่นคงของประเทศหรือไม่ ในกฎหมายว่าด้วยความมั่นคงปลอดภัยทางไซเบอร์ จึงมิใช่เรื่องบังเอิญหรือความผิดพลาดของฝ่ายนิติบัญญัติแต่อย่างใด หากแต่เป็นความจงใจและจำเป็นต้องมีเพื่อรักษาความสงบเรียบร้อยและความมั่นคงของรัฐ

2.1.3 กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา

ประเทศสหรัฐอเมริกาใช้ระบบการปกครองแบบสหพันธ์สาธารณรัฐ จึงมีกฎหมายทั้งในระดับมลรัฐและระดับสหพันธรัฐ โดยจะนำเสนอกฎหมายในระดับสหพันธรัฐอันเป็นกฎหมายที่มีผลผูกพันและครอบคลุมประเทศสหรัฐอเมริกาทั้งหมด ซึ่งกฎหมายหลักในเรื่องความมั่นคงปลอดภัยไซเบอร์คือ “รัฐบัญญัติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2015” (the Cybersecurity Act of 2015) ที่ออกมาบังคับใช้ในยุคสมัยของประธานาธิบดี บารัค โอบามา (Barack Obama) ซึ่งเป็นการตรากฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับล่าสุด และมีผลเป็นการเปลี่ยนแปลงวิธีการในการจัดการปัญหาความมั่นคงทางไซเบอร์ของประเทศอย่างมีนัยสำคัญ กล่าวคือ กฎหมายดังกล่าว

---

[28] Supra note 21, Retrieved Jan 15, 2017.

[29] People's Republic of China Cybersecurity Law

Article 1: This law is formulated so as to ensure network security, to preserve cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization.

มุ่งป้องกันโลกไซเบอร์ของประเทศให้มีความมั่นคงปลอดภัยด้วยความร่วมมือจากทุกภาคส่วนอย่างแท้จริง หรือกล่าวอีกนัยหนึ่งได้ว่าลำพังเพียงหน่วยงานของรัฐไม่เพียงพอที่จะสอดส่องดูแลโลกไซเบอร์ให้มีความปลอดภัยได้ จึงจำเป็นที่จะต้องมอบหมายหน้าที่บางประการให้กับภาคเอกชนในการทำหน้าที่สอดส่องดูแลการกระทำความผิดและการคุกคามบนโลกไซเบอร์ ดังนั้น กฎหมายฉบับนี้จึงเป็นผลิตผลจากการประนีประนอมหลายครั้งระหว่างหน่วยงานภาครัฐและหน่วยงานภาคเอกชนที่อยู่ในขอบข่ายการบริหารความเสี่ยงในเรื่องความมั่นคงปลอดภัยไซเบอร์ และยุทธวิธีในการสร้างความมั่นคงด้านไซเบอร์ตามที่ปรากฏในกฎหมายฉบับนี้ จึงมีผลในการเปลี่ยนแปลงวิถีการดำเนินธุรกิจในโลกไซเบอร์ของภาคเอกชนอย่างมีนัยสำคัญ

การจัดทำรัฐบัญญัติความมั่นคงปลอดภัยไซเบอร์ของประเทศสหรัฐอเมริกา “The Cybersecurity Act 2015” เป็นการนำบางส่วนของรัฐบัญญัติที่มีความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศจำนวน 3 ฉบับมารวมกันเพื่อให้สามารถบังคับใช้ได้ง่ายและบูรณาการซึ่งกันและกัน กล่าวคือ **รัฐบัญญัติฉบับที่หนึ่ง** รัฐบัญญัติว่าด้วยการแบ่งปันข้อมูลเกี่ยวกับความปลอดภัยทางไซเบอร์ (The Cybersecurity Information Sharing ACT 2015 หรือ CISA) **รัฐบัญญัติฉบับที่สอง** รัฐบัญญัติว่าด้วยการเพิ่มประสิทธิภาพระบบรักษาความปลอดภัยไซเบอร์ของรัฐบาลกลาง (the Federal Cybersecurity Enhancement Act of 2015) **รัฐบัญญัติฉบับที่สาม** รัฐบัญญัติว่าด้วยการประเมินหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ของรัฐบาลกลาง (the Federal Cybersecurity Workforce Assessment Act of 2015) จึงอาจกล่าวได้ว่าในประเทศสหรัฐอเมริกาได้มีการตรากฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มาแล้วหลายฉบับ และแต่ละฉบับก็ยังมีผลใช้บังคับอยู่ในปัจจุบัน หากแต่รัฐบัญญัติความมั่นคงปลอดภัยไซเบอร์ฉบับที่กล่าวถึงนี้ คือ “the Cybersecurity Act 2015” (อันเป็นฉบับล่าสุดและมีชื่อทางกฎหมายตรงที่สุด) มีเจตนาในการบังคับใช้กฎหมายทั้งสามฉบับข้างต้นอย่างบูรณาการร่วมกัน กล่าวคือ กำหนดให้หน่วยงานของรัฐ (ทั้งรัฐบาลกลางและรัฐบาลมลรัฐ) และบริษัทเอกชนต่าง ๆ สามารถแบ่งปันข้อมูลเกี่ยวกับความมั่นคงไซเบอร์ระหว่างกันได้ในระยะเวลาอันรวดเร็ว เพื่อให้หน่วยงานของรัฐบาลกลางที่มีอำนาจและหน้าที่เกี่ยวข้องสามารถป้องกันและโต้ตอบกับภัยคุกคามทางไซเบอร์ได้ อีกทั้งผู้ประกอบการเอกชนรายอื่น ๆ จะได้สามารถเตรียมพร้อมรับมือกับภัยคุกคามที่เกิดขึ้นได้อย่างทันต่อเวลา ยิ่งไปกว่านั้น การแบ่งปันข้อมูลระหว่างกันยังเป็นการสร้างวัฒนธรรมการเรียนรู้ร่วมกันในโลกไซเบอร์ และสามารถนำข้อมูลเหล่านั้นมาใช้งานได้ด้วยวิธีการต่าง ๆ อาทิ การป้องกันอาชญากรรมทางคอมพิวเตอร์ การรวบรวมพยานหลักฐานจากการคุกคามทางไซเบอร์ เป็นต้น

ตัวอย่างหน่วยงานสำคัญทางด้านความมั่นคงปลอดภัยทางไซเบอร์

หน่วยงานที่รับผิดชอบโดยตรงกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศสหรัฐอเมริกาโดยตรง คือ **กระทรวงความมั่นคงภายในประเทศ (Department of Homeland Security หรือ DHS)** ซึ่งเป็นหน่วยงานระดับสหพันธรัฐ จัดตั้งขึ้นเพื่อตอบสนองต่อการโจมตี 11 กันยายน 2001 ซึ่งมีหน้าที่รับผิดชอบด้านความมั่นคงสาธารณะภายในประเทศ โดยมีภารกิจเกี่ยวข้องโดยตรงกับการต่อต้านการก่อการร้าย การรักษาความปลอดภัยชายแดน การดูแลการ

อพยพและคนเข้าเมือง การรักษาความปลอดภัยในโลกไซเบอร์ และการป้องกันและบริหารจัดการภัยพิบัติ กระทรวงความมั่นคงภายในประเทศเป็นหน่วยงานที่ใหญ่เป็นอันดับสามของประเทศสหรัฐอเมริกา (รองจากกระทรวงกลาโหม (the Departments of Defense) และกระทรวงกิจการทหารผ่านศึก (the Departments of Veterans Affairs) ซึ่งในปีงบประมาณ 2017 ได้รับการจัดสรรงบประมาณสูงถึง 40.6 $ พันล้านเหรียญสหรัฐฯ และมีพนักงานมากกว่า 240,000 ราย การทำงานของกระทรวงความมั่นคงภายในประเทศ (DHS) แตกต่างจากกระทรวงกลาโหม กล่าวคือ กระทรวงกลาโหมจะปฏิบัติการทางทหารในต่างประเทศเป็นหลัก ขณะที่กระทรวงความมั่นคงภายในประเทศทำงานในรูปแบบของพลเรือนเพื่อปกป้องความมั่นคงภายในของประเทศสหรัฐอเมริกาจากการคุกคามที่เกิดขึ้นภายในและที่เกิดจากภายนอกประเทศ

ภารกิจของกระทรวงความมั่นคงภายในประเทศกับการคุ้มครองความมั่นคงปลอดภัยทางไซเบอร์นั้น จะทำงานร่วมกับกระทรวงกลาโหม (the Department of Defense) และสำนักงานข่าวกรองแห่งชาติ (the Office of the Director of National Intelligence) ในการพัฒนากรอบการแบ่งปันข้อมูลภัยคุกคามไซเบอร์ ซึ่งกรอบการแบ่งปันข้อมูลนี้ จะมีการศึกษาและทดลองก่อนจะนำมาใช้งานจริงเพื่อหาจุดสมดุลระหว่างความมั่นคงของชาติกับกิจการพาณิชย์อิเล็กทรอนิกส์

ยิ่งไปกว่านั้น ภายใต้กระทรวงความมั่นคงภายในประเทศยังมีหน่วยงานศูนย์ความปลอดภัยทางไซเบอร์แห่งชาติ (NCSC) เป็นอีกหน่วยงานหนึ่งที่สำคัญ จัดตั้งขึ้นในเดือนมีนาคม 2008 ตามข้อกำหนดของประธานาธิบดีว่าด้วยความมั่นคงภายในประเทศ (the National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54 / HSPD -23)) และขึ้นตรงต่อเลขาธิการกระทรวงความมั่นคงภายในประเทศ (DHS) โดยมีหน้าที่ปกป้องเครือข่ายการสื่อสารของรัฐบาลสหรัฐฯ จากการคุกคามทางไซเบอร์ทั้งในและนอกประเทศ ตรวจสอบเก็บรวบรวมและแบ่งปันข้อมูลเกี่ยวกับระบบต่าง ๆ ให้กับหน่วยงานด้านความมั่นคงของประเทศ อาทิ กระทรวงกลาโหม หน่วยงานสืบสวนกลาง (FBI) เป็นต้น

ตัวอย่างมาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามทางไซเบอร์

มาตรการสำคัญที่นำมาใช้ในการต่อสู้กับภัยคุกคามไซเบอร์ของกฎหมายฉบับนี้ประกอบด้วยมาตรการสำคัญ 2 ประการ ดังนี้

มาตรการที่หนึ่ง การแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามไซเบอร์

หมวดที่ 1 ของกฎหมายดังกล่าว เป็นหมวดว่าด้วยการแบ่งปันข้อมูลเกี่ยวกับความปลอดภัยทางไซเบอร์กำหนดมาตรการในการแบ่งปันข้อมูลตามที่ปรากฏในกฎหมายฉบับนี้เป็นมาตรการสมัครใจของผู้ประกอบการ กล่าวคือ ผู้ประกอบการจะต้องเข้าร่วมโครงการกับทางภาครัฐในการแบ่งปันข้อมูล (อย่างเต็มใจ) ให้กับหน่วยงานภาครัฐและจะต้องมีหน้าที่ในการจัดส่งข้อมูลไซเบอร์ให้กับหน่วยงานของรัฐ กรณีที่มีภัยคุกคามที่เป็นไปตามตัวชี้วัดภัยคุกคามทางไซเบอร์ที่กระทรวงความมั่นคงภายในประเทศกำหนด และกระทรวงความมั่นคงภายในประเทศจะเป็นผู้กลั่นกรองและประเมินข้อมูลภัยอันตรายที่เกิดขึ้น และจะกระจาย (ส่งต่อ) ข้อมูลเหล่านั้นให้กับ

หน่วยงานของรัฐและหน่วยงานของเอกชน เพื่อให้หน่วยงานเหล่านั้นเตรียมการรับมือกับภัยคุกคามที่กำลังจะเกิดขึ้น ดังนั้น การรู้ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ล่วงหน้า ก่อนที่ภัยคุกคามจะเกิดขึ้นกับระบบไซเบอร์ของตนจึงเปรียบเสมือนกับการสร้างเกราะคุ้มกันสำหรับหน่วยงานเหล่านั้นจากการรุกรานทางไซเบอร์ อย่างไรก็ตาม เนื่องด้วยการเข้าร่วมโครงการแบ่งปันข้อมูลเป็นโครงการอาศัยความสมัครใจ ดังนั้น ผู้ประกอบการรายใดที่ไม่ประสงค์จะเข้าร่วมโครงการหรือมิได้ต้องการแบ่งปันข้อมูลภัยคุกคามไซเบอร์ก็ไม่มีบทบัญญัติสำหรับการลงโทษแต่อย่างใด

อนึ่ง กุญแจสำคัญของโครงการแบ่งปันข้อมูลสำหรับต่อสู้กับภัยคุกคามไซเบอร์คือการได้รับการแจ้งข้อมูลอย่างรวดเร็ว และมีการประมวลผลได้อย่างแม่นยำ ดังนั้น กระทรวงความมั่นคงภายในประเทศจึงได้จัดทำฐานข้อมูลการแบ่งปันข้อมูลที่เรียกว่าระบบ “Automated Indicator Sharing” อันเป็นฐานข้อมูลที่มีวัตถุประสงค์เพื่อสร้างกระบวนการและขั้นตอนในการรวบรวมและแจกจ่ายข้อมูลระหว่างหน่วยงานภาครัฐและภาคเอกชน ซึ่งการทำงานเบื้องต้นของระบบดังกล่าวจะตัดชื่อหรือสิ่งหนึ่งสิ่งใดที่สามารถระบุตัวบุคคลได้ออกไป ซึ่งยังรวมถึงการตัดข้อมูลที่มีเจ้าของซึ่งการเผยแพร่ข้อมูลออกไปนั้นอาจจะทำให้เจ้าของข้อมูลเสียหายได้ ดังนั้น ผู้ประกอบการที่ได้รับการแบ่งปันข้อมูลจากกระทรวงความมั่นคงภายในประเทศจะไม่สามารถเข้าถึงหรือรู้ถึงข้อมูลดั้งเดิมเริ่มแรกที่หน่วยงานหรือบริษัทต่าง ๆ ส่งเข้ามายังฐานข้อมูลของกระทรวงความมั่นคงภายในประเทศได้เลย ยิ่งไปกว่านั้น ข้อมูลที่ปรากฏในฐานข้อมูลของกระทรวงความมั่นคงภายในประเทศจะต้องเป็นข้อมูลล่าสุดแบบตามเวลาจริง (Real time) เนื่องจากการโจมตีทางไซเบอร์สามารถทำได้อย่างรวดเร็ว ดังนั้น การรู้ถึงภัยคุกคามและการเตรียมการรับมือจึงต้องดำเนินการไปอย่างรวดเร็วเช่นเดียวกัน จึงอาจกล่าวได้ว่าฐานข้อมูลที่ดีจะทำให้การดำเนินการตามโครงการแบ่งปันข้อมูลเป็นไปอย่างมีประสิทธิภาพและช่วยให้บริษัทเอกชนสามารถตรวจตราและตรวจสอบระบบเครือข่ายและข้อมูลของตนเองได้ดีขึ้น อีกทั้งยังเป็นข้อมูลล่าสุดที่เป็นประโยชน์ในการเตือนภัยให้แก่หน่วยงานรัฐและบริษัทเอกชนทราบว่ามีความผิดปกติเกิดขึ้นในลักษณะใดบ้าง ซึ่งอาจถือได้ว่าเป็นวิธีการที่ดีที่สุดในการป้องกันภัยคุกคามที่จะเกิดขึ้น ตลอดจนเป็นการสร้างการเรียนรู้และวัฒนธรรมในการป้องกันร่วมกันของภัยคุกคามทางไซเบอร์

มาตรการที่สอง การจัดทำรายงานของหน่วยงานของรัฐ

หมวดที่ 4 ของกฎหมายดังกล่าว อันเป็นบททั่วไปที่กำหนดให้หน่วยงานในระดับสหพันธรัฐจัดทำรายงานความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดให้หัวหน้าหน่วยงานของรัฐบาลกลางทุกหน่วยงานมีหน้าที่ระบุสถานะโดยรวมของหน่วยงานของตนสำหรับการดำเนินการด้านความปลอดภัยในโลกไซเบอร์และต้องรายงานต่อรัฐสภาว่าภายในหน่วยงานมีบุคลากรที่ทำงานในด้านนี้กี่คนและเหมาะสมหรือไม่ ตลอดจนมีแผนพัฒนาบุคลากร การทดสอบระบบความปลอดภัยไซเบอร์ และแผนรับมือต่อภัยคุกคามอย่างไร โดยวัตถุประสงค์เบื้องต้นในการจัดทำรายงานคือการทบทวนเครื่องมือต่าง ๆ และความพร้อมของบุคลากรที่จะรับมือกับภัยคุกคามที่อาจเกิดขึ้น

ตัวอย่างมาตรการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐานของประชาชน

ในประเด็นเรื่องข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัว ก็มีบทบัญญัติในการป้องกันการกระทำการแบ่งปันข้อมูลส่วนบุคคล หรือข้อมูลอื่นใดที่สามารถระบุถึงตัวตนได้ แต่ไม่เกี่ยวข้องกับการรักษาความปลอดภัยในโลกไซเบอร์ โดยกฎหมายดังกล่าวกำหนดให้จะต้องมีการลบออกไปก่อนที่จะมีการแบ่งปันข้อมูลและต้องแจ้งให้ผู้รับข้อมูลใช้ข้อมูลที่ได้รับเท่าที่อนุญาตเท่านั้น[30]

ข้อกังวลของภาคประชาชนในการบังคับใช้กฎหมาย

ข้อกังวลเกี่ยวกับการปรับใช้กฎหมายที่มีผลต่อสิทธิและเสรีภาพขั้นพื้นฐานนั้น เป็นกรณีเมื่อผู้ประกอบการถูกโจมตีหรือคุกคามทางไซเบอร์แล้ว ผู้ประกอบการก็ยังมีความลังเลว่าควรจะแบ่งปันข้อมูลให้กับหน่วยงานของรัฐหรือไม่ ส่วนหนึ่งเนื่องจากกลัวที่จะเสียชื่อเสียง และอีกส่วนหนึ่งคือการไม่แน่ใจว่าจะถูกฟ้องร้องดำเนินคดีหรือไม่ (แม้จะมีกฎหมายกำหนดว่าไม่ต้องรับผิดก็ตาม) เนื่องจากยังไม่มีแนวทางการปฏิบัติที่ผ่านมาทั้งในหน่วยงานของรัฐและองค์กรศาล ตลอดจนยังไม่มีการศึกษาเรื่องดังกล่าวนี้อย่างจริงจัง ดังนั้น การปรับใช้บทบัญญัติที่ยกเว้นความรับผิดจึงยังเป็นปัญหาในทางปฏิบัติ ซึ่งผลที่ตามมาก็คือการไม่แบ่งปันข้อมูล จึงทำให้ความสำคัญของกฎหมายลดลงและอาจจะมีผลต่อระบบกฎหมายว่าด้วยการป้องกันภัยคุกคามไซเบอร์ทั้งระบบได้

อนึ่ง ความยินยอมพร้อมใจในการแบ่งปันข้อมูลของผู้ประกอบการนั้น ผู้ประกอบการจะต้องเข้าใจวัตถุประสงค์และกระบวนการในการทำงานของแต่ละหน่วยงานตามที่ปรากฏในกฎหมายฉบับนี้เป็นอย่างดี มิเช่นนั้นแล้วผู้ประกอบการย่อมไม่ต้องการที่จะแบ่งปันข้อมูลที่เกิดขึ้นด้วยหลายเหตุผลทั้งในเรื่องความรับผิดตามกฎหมายก็ดี ความลับทางการค้าก็ดี หรือความเชื่อมั่นของลูกค้าก็ดี ดังนั้น รัฐจะต้องผลักดันให้คณะกรรมการของบริษัทจะต้องมีความรู้และเข้าใจในกฎหมายฉบับนี้อย่างจริงจัง

2.2 กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยและข้อกังวลของภาคประชาชน

เมื่อได้ทราบถึงประเด็นสำคัญในด้านต่าง ๆ ทั้งในเรื่องของวัตถุประสงค์ในการบังคับใช้กฎหมาย หน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรการที่นำมาใช้ในการต่อสู้กับภัยคุกคามไซเบอร์ มาตรการคุ้มครองสิทธิและเสรีภาพขั้นพื้นฐาน และปัญหาและข้อกังวลในการบังคับใช้กฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในต่างประเทศแล้ว ส่วนต่อไปจะนำเสนอให้ทราบถึงกลไกทางด้านกฎหมายในประเทศไทยเกี่ยวกับความมั่นคงทางไซเบอร์ โดยจะอธิบายถึงสถานการณ์ก่อนที่จะมีการจัดทำ “ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคง

---

[30] SEC. 105: sharing of cyber threat indicators and defensive measures with the federal government.

(E) protect the confidentiality of cyber threat indicators containing personal information or information that identifies specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

ปลอดภัยทางไซเบอร์ พ.ศ. ....” และข้อกังวลของภาคประชาชนต่อ “ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....” ตามลำดับ ดังนี้

สถานการณ์ก่อนที่จะมีการจัดทำ “ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....”

ปัจจุบันประเทศไทยอยู่ระหว่างการจัดทำ “(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....” ซึ่งก่อนที่จะมีการจัดทำ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ฉบับนี้นั้นมิได้หมายความว่าประเทศไทยปลอดภัยจากการคุกคามทางไซเบอร์ แต่ได้มีการปรับใช้กฎหมายบางฉบับเพื่อแก้ไขสถานการณ์และปัญหาที่เกิดขึ้นเฉพาะหน้า ได้แก่ 1. พระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 โดยมีวัตถุประสงค์เพื่อกำหนดมาตรฐานความปลอดภัยของธุรกรรมทางอิเล็กทรอนิกส์ทั้งจากภาครัฐและภาคเอกชนเพื่อส่งเสริมให้การทำธุรกรรมอิเล็กทรอนิกส์มีความน่าเชื่อถือ และ 2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ตราขึ้นด้วยเหตุผลที่ระบบคอมพิวเตอร์ได้เข้ามามีบทบาทสำคัญในการใช้ชีวิตของมนุษย์ จึงควรมีมาตรการเพื่อป้องกันและปราบปรามการกระทำของบุคคลที่จะทำให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานได้ หรือเข้าถึง แก้ไขหรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยไม่ชอบ หรือใช้ระบบคอมพิวเตอร์เผยแพร่ข้อมูลอันเป็นเท็จ ลามกอนาจารที่จะก่อให้เกิดความเสียหายต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมถึงความสงบสุขและศีลธรรมอันดีของประชาชน[31]

อย่างไรก็ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นกฎหมายอาญาที่นำมาปรับใช้กับความผิดเกี่ยวกับคอมพิวเตอร์ซึ่งรวมถึงระบบเทคโนโลยีสารสนเทศด้วย ซึ่งขอบเขตการบังคับใช้ของกฎหมายดังกล่าวมุ่งลงโทษผู้กระทำความผิดเป็นสำคัญ ดังนั้น การนำมาปรับใช้โดยมีวัตถุประสงค์เพื่อป้องกันการคุกคามทางไซเบอร์อาจจะไม่ได้ผลที่มีประสิทธิภาพมากนัก เนื่องจากการรักษาความมั่นคงปลอดภัยทางไซเบอร์นั้น หน่วยงานของรัฐจำเป็นจะต้องมีเครื่องมือทางกฎหมายที่สามารถนำมาใช้ป้องกันและแก้ไขปัญหาการคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์เป็นสำคัญ มิใช่มีวัตถุประสงค์ในการลงโทษผู้กระทำความผิด[32]

หน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในประเทศไทยประกอบด้วย

1. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม[33] โดยมีอำนาจหน้าที่เกี่ยวกับการวางแผน ส่งเสริม พัฒนา และดำเนินกิจการเกี่ยวกับดิจิทัลเพื่อเศรษฐกิจและสังคม และกำกับดูแลกฎหมาย

---

[31]หมายเหตุท้ายพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

[32]ทศพล ทรรศนกุลพันธ์ และคณะ, (24 กุมภาพันธ์ 2560) *โครงการเสวนาทางวิชาการเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ : ความเป็นมา หลักการ และข้อควรพิจารณา*. คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์ลำปาง

[33]ข้อมูลเพิ่มเติมสืบค้นได้จาก กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, “รู้จักกระทรวง”, [ออนไลน์], เข้าถึงได้จาก: http://www.mdes.go.th/ [ม.ป.ป.] สืบค้น 27 มีนาคม 2560.

ด้านดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารในความรับผิดชอบ รวมทั้งกำกับดูแล สนับสนุน และประสานงานด้านความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร

2. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)[34] มีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้กับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้งโดยมีภาระหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

3. ศูนย์ไซเบอร์กองทัพบก (Army Cyber Center)[35] มีหน้าที่สำคัญหลัก 3 ประการ คือ การปฏิบัติการไซเบอร์ เพื่อเฝ้าระวัง แจ้งเตือน ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามด้านไซเบอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างความรู้ ความเข้าใจ สร้างความตระหนัก ติดตาม กำกับดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย รวมถึงการเฝ้าระวัง แจ้งเตือนภัยคุกคาม การติดตาม สืบค้น และตรวจสอบช่องโหว่ของระบบ และการสนับสนุนการปฏิบัติการข่าวสารบนไซเบอร์ เพื่อสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้อง โดยทำหน้าที่เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ ที่ส่งผลกระทบต่อสถาบัน และความมั่งคงของชาติ

4. กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี[36] มีอำนาจหน้าที่ในการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีอันเป็นอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อยป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ เช่น การกระทำผิดที่มุ่งต่อระบบคอมพิวเตอร์เป็นเป้าหมาย การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด การนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์สู่ระบบคอมพิวเตอร์ที่เป็นความผิด และปฏิบัติการโต้ตอบในเชิงรุกโดยฉับพลันทางอินเทอร์เน็ต

---

[34]ข้อมูลเพิ่มเติมสืบค้นได้จาก ThaiCert, “เกี่ยวกับไทยเซิร์ต,” [ออนไลน์], เข้าถึงได้จาก: https://www.thaicert.or.th/about.html [ม.ป.ป.], สืบค้น 27 มีนาคม 2560.

[35]ข้อมูลเพิ่มเติมสืบค้นได้จาก ศูนย์ไซเบอร์กองทัพบก, “ประวัติศูนย์ไซเบอร์กองทัพบก,” [ออนไลน์], เข้าถึงได้จาก: http://cyber.rta.mi.th/about.php [ม.ป.ป.] สืบค้น 27 มีนาคม 2560.

[36]ข้อมูลเพิ่มเติมสืบค้นได้จาก กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, “เกี่ยวกับหน่วยงาน,” [ออนไลน์], เข้าถึงได้จาก: http://www.tcsd.in.th/ [ม.ป.ป.] สืบค้น 27 มีนาคม 2560.

เห็นได้ว่าหน่วยงานที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ต่างก็มีความหลากหลายและมีอำนาจหน้าที่ตามส่วนที่เกี่ยวข้องของแต่ละหน่วยงานเอง เช่น ด้านการทหาร ด้านอาญา และด้านเศรษฐกิจ

กฎหมายที่มีการกล่าวถึงความมั่นคงปลอดภัยทางไซเบอร์

ก่อนที่จะมีการจัดทำร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... นั้น ประเทศไทยมีกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์อยู่บ้าง หากแต่เป็นการปรับใช้โดยอนุโลม กล่าวคือพระราชบัญญัติว่าด้วยธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2544 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 เป็นมาตรการในเชิงป้องกันที่มีวัตถุประสงค์ให้การทำธุรกรรมอิเล็กทรอนิกส์มีความน่าเชื่อถือและมีมาตรฐานในการรักษาความปลอดภัย อนึ่ง แม้จะมีการกำหนดมาตรการต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์เอาไว้ แต่ก็เป็นมาตรการที่ใช้เฉพาะกรณีของการทำธุรกรรมทางอิเล็กทรอนิกส์เท่านั้น อาทิ มาตรการที่ให้ผู้ทำธุรกรรมอิเล็กทรอนิกส์ดำเนินการตามข้อกำหนดและมาตรฐานที่กำหนดไว้ เป็นต้น ดังนั้น จึงอาจกล่าวได้ว่ายังไม่ครอบคลุมเพียงพอสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นบทบัญญัติที่กำหนดโทษทางอาญา ซึ่งหลักการทั่วไปของกฎหมายอาญาก็คือบุคคลจะต้องรับผิดต่อเมื่อได้กระทำการในสิ่งที่กำหนดให้เป็นความผิด ดังนั้น ตราบใดที่ “ไม่มีความผิด” ผู้กระทำจึงจะไม่ได้รับโทษใด ๆ หรืออาจกล่าวอีกนัยหนึ่งได้ว่า เป็นมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ปลายเหตุเท่านั้น แต่การป้องกันภัยคุกคามทางไซเบอร์นั้น จำเป็นที่จะต้องมีการบูรณาการกันทุกภาคส่วนเพื่อป้องกันภยันตรายที่อาจจะเกิดขึ้น

ภัยคุกคามทางไซเบอร์บางประเภทมีระดับความอันตรายที่กระทบกับความมั่นคงของรัฐและสวัสดิภาพของประชาชน อาทิ กรณีที่มีการคุกคามระบบการผลิตและแจกจ่ายกระแสไฟฟ้า การโจมตีระบบการเงินและการธนาคารของประเทศ เป็นต้น ซึ่งการป้องกันภัยคุกคามที่อาจจะเกิดขึ้นนั้น จำเป็นที่จะต้องมีเครื่องมือทางกฎหมายที่เหมาะสมกับสถานการณ์ เพื่อให้อำนาจกับหน่วยงานที่เกี่ยวข้องในการทำงาน ด้วยเหตุนี้ประเทศไทยจึงจัดทำ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ขึ้น เพื่อจะนำมาใช้ในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของประเทศโดยเฉพาะ

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....[37] ถูกจัดให้เป็นหนึ่งใน “ชุดกฎหมายเศรษฐกิจดิจิทัล” ตามกรอบนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม

[37]สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, “ร่างกฎหมายเศรษฐกิจดิจิทัล (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....,” [ออนไลน์], เข้าถึงได้จาก: https://ictlawcenter.etda.or.th/ [ม.ป.ป.] สืบค้น 10 พฤษภาคม 2560.

หรือ Digital Economy ที่ต้องมีการพัฒนาและส่งเสริมพร้อมบูรณาการงาน 5 เสาสำคัญ โดยงานเสาที่ 2 “การพัฒนา Soft Infrastructure” ในส่วนของกฎหมายนั้น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ได้จัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคมหรือเรียกสั้น ๆ ว่า “ชุดกฎหมายเศรษฐกิจดิจิทัล” (Digital Economy) โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เสนอคณะรัฐมนตรีและคณะรัฐมนตรีได้พิจารณาอนุมัติเห็นชอบในหลักการร่างกฎหมายเมื่อวันที่ 16 ธันวาคม 2557 และวันที่ 6 มกราคม 2558[38] และต่อมาในวันที่ 5 เมษายน พ.ศ. 2559 คณะรัฐมนตรีได้เห็นชอบให้กำหนดยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมขึ้นมา

ข้อกังวลของภาคประชาชนต่อ “ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. ....

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... ประกอบไปด้วยบทบัญญัติทั้งสิ้น 43 มาตรา โดยแบ่งออกเป็น 6 หมวด กล่าวคือ

หมวด 1 การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด 2 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด 3 สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด 4 การปฏิบัติการและการรับมือภัยคุกคามทางไซเบอร์

หมวด 5 พนักงานเจ้าหน้าที่

หมวด 6 บทเฉพาะกาล

วัตถุประสงค์ในการตราพระราชบัญญัติดังกล่าว เพื่อปกป้องให้การใช้เทคโนโลยีสารสนเทศจากภัยคุกคามไซเบอร์ประเภทต่าง ๆ โดยการปกป้องเช่นว่านั้นต้องมีความรวดเร็ว และการประสานงานที่ดี และมีการดูแลรักษาอย่างต่อเนื่องอย่างมีประสิทธิภาพและเกิดผลสัมฤทธิ์

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... ได้จัดตั้งหน่วยงานสำคัญขึ้นมา 2 หน่วยงาน กล่าวคือคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีรายละเอียดดังนี้

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา 5 แห่งร่างพระราชบัญญัติฯ ได้กำหนดให้มี “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” มีอำนาจหน้าที่ ในการกำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ และจัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่สอดคล้องกับนโยบาย ยุทธศาสตร์ และแผนระดับชาติว่าด้วยการ

[38]สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, “ร่างกฎหมายเศรษฐกิจดิจิทัล,” [ออนไลน์], เข้าถึงได้จาก: https://ictlawcenter.etda.or.th/de_laws [ม.ป.ป.] สืบค้น 10 พฤษภาคม 2560.

พัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งบทบาทและหน้าที่ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะอยู่ในระดับการจัดทำนโยบายและรับผิดชอบในภาพรวมของประเทศเป็นหลัก ดังนั้น บทบาทของคณะกรรมการดังกล่าวจะมีความสำคัญอย่างยิ่งสำหรับการจัดทำแนวทางเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในอนาคต

สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา 14 แห่งร่างพระราชบัญญัติฯ ได้กำหนดให้จัดตั้ง “สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” ขึ้น เป็นหน่วยงานของรัฐมีฐานะเป็นนิติบุคคล ซึ่งไม่เป็นส่วนราชการและรัฐวิสาหกิจ ทำหน้าที่เป็นฝ่ายธุรการให้กับคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และในขณะเดียวกันยังมีหน้าที่สำคัญหลายประการในการรักษาความมั่นคงทางไซเบอร์ อาทิ ประสานความร่วมมือทางปฏิบัติในการดำเนินการกับหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เพื่อยับยั้งปัญหาภัยคุกคามไซเบอร์ และเพื่อได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศทั้งภายในและภายนอกประเทศ ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

อนึ่ง จากการสัมมนาที่จัดขึ้นโดย “ไอลอว์” (iLaw) และที่จัดขึ้นที่คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ศูนย์ลำปาง ในงานเสวนาวิชาการ เรื่อง โครงการเสวนาทางวิชาการเรื่อง ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์: ความเป็นมา หลักการ และข้อควรพิจารณา ตลอดจนตามประเด็นข้อเรียกร้องของภาคประชาชนตามที่ปรากฏในสื่อต่าง ๆ นั้น อาจจำแนกข้อกังวลของภาคประชาชนได้สองประการ ดังนี้

ข้อกังวลที่หนึ่ง ข้อกังวลเกี่ยวกับเรื่องของถ้อยคำและบทนิยามศัพท์ในกฎหมายที่ไม่ชัดเจนแน่นอน

ข้อกังวลในเรื่องของถ้อยคำและบทนิยามศัพท์ในกฎหมายนั้น กฎหมายบัญญัติโดยใช้ถ้อยคำที่ค่อนข้างกว้างและครอบคลุม ซึ่งอาจจะก่อให้เกิดปัญหาในการใช้และตีความกฎหมายได้ อาทิ ความหมายของ “ความมั่นคงปลอดภัยไซเบอร์” ตามที่ปรากฏในมาตรา 3 แห่งร่างพระราชบัญญัติฯ นี้ ได้ให้นิยามของคำว่า *“ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ”*

ดังนั้น ความมั่นคงปลอดภัยไซเบอร์ตามความหมายของร่างพระราชบัญญัติดังกล่าวนี้ อาจจะหมายถึงการกระทำทุกประการที่กระทำไปเพื่อปกป้องและรักษาไว้ซึ่งการให้บริการหรือการใช้เทคโนโลยีสารสนเทศที่เกี่ยวข้องกับความมั่นคงของชาติ ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ให้รอดพ้นจากภัยคุกคามไซเบอร์

อีกตัวอย่างหนึ่งคือ “การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” ตามที่ปรากฏในบทบัญญัติมาตรา 5 แห่งร่างพระราชบัญญัติฯ ได้กำหนดว่า

“...การรักษาความมั่นคงไซเบอร์แห่งชาติต้องดำเนินการ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งเห็นชอบโดยคณะรัฐมนตรี

การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยจึงต้องครอบคลุมในเรื่องดังต่อไปนี้

(1) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

(2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

(3) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

(4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์

(5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์

(6) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์

(7) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

(8) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

เห็นได้ว่า ถ้อยคำตามที่ปรากฏข้างต้น ไม่มีความชัดเจนแน่นอน ซึ่งส่งผลให้ภาคประชาชนบางส่วนเกิดข้อกังวลได้ เช่น คำว่า “ภัยคุกคามทางไซเบอร์” นั้น มิได้ระบุให้ชัดเจนว่าเป็นภัยคุกคามในเชิงเทคนิคที่มีต่อตัวระบบ หรือรวมไปถึงการเผยแพร่เนื้อหาที่เจ้าหน้าที่เห็นว่ากระทบต่อความมั่นคงด้วย[39] เป็นต้น

[39]โครงการอินเตอร์เน็ตเพื่อกฎหมายประชาชน (iLAW), “ความน่ากังวลบางประการต่อร่าง พ.ร.บ. ความมั่นคงไซเบอร์ฯ,” [ออนไลน์], เข้าถึงได้จาก: https://ilaw.or.th/node/3404 [2558]. สืบค้น 29 กันยายน 2559.

ข้อกังวลที่สอง ข้อกังวลเรื่องความสมดุลระหว่างการใช้อำนาจรัฐกับสิทธิและเสรีภาพของประชาชน

ข้อกังวลเรื่องความสมดุลระหว่างการใช้อำนาจรัฐกับสิทธิและเสรีภาพของประชาชน โดยบทบัญญัติบางมาตราในร่างพระราชบัญญัติฉบับนี้มีลักษณะที่น่ากังวล ดังความคิดเห็นของ คุณสฤณี อาชวานันทกุล ที่ให้ความเห็นว่า[40]

“เพราะให้อำนาจเจ้าหน้าที่ตรวจสอบการสื่อสารของประชาชนโดยทุกช่องทางและไม่มีกระบวนการตรวจสอบใด ๆ เลย คล้ายกับการให้อำนาจเจ้าหน้าที่ทหารอย่างเต็มที่เวลาที่ประกาศใช้กฎอัยการศึก...” และ “เป็นการมอบอำนาจให้กับหน่วยงานความมั่นคงอย่างมหาศาลในทางที่ขาดกลไกตรวจสอบถ่วงดุลต่าง ๆ”

ยิ่งไปกว่านั้น กฎหมายดังกล่าวนี้ ได้กำหนดให้อำนาจพนักงานเจ้าหน้าที่ในการเข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศเพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังความที่ปรากฏในบทบัญญัติมาตรา 35 วรรคหนึ่ง (3) ของร่างพระราชบัญญัติฯ

“...(3) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์โทรเลข โทรศัพท์โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใดเพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์...”

ยิ่งไปกว่านั้น ร่างพระราชบัญญัติฯ ฉบับนี้ได้ให้อำนาจและหน้าที่ขององค์กรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในการดำเนินการหลายประการ ซึ่งอาจจะกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐานได้ อาทิ อำนาจในการสั่งการและบังคับบัญชาหน่วยงานของรัฐในเรื่องความมั่นคงปลอดภัยทางไซเบอร์[41] อำนาจของพนักงานเจ้าหน้าที่ในการทำหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใด ๆ มาให้ถ้อยคำหรือส่งคำชี้แจงเป็นหนังสือ และมีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช. และสามารถเข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์[42] เป็นต้น

จึงอาจกล่าวได้ว่า บทบัญญัติของกฎหมายดังกล่าวอาจกระทบต่อสิทธิเสรีภาพของประชาชนที่ได้รับการบัญญัติรับรองเอาไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 หลายประการ เช่น สิทธิในความเป็นอยู่ส่วนตัวตามที่กำหนดรับรองไว้ในมาตรา 32 เสรีภาพในการติดต่อสื่อสารของบุคคลที่กำหนดไว้ในมาตรา 36 เป็นต้น กรณีนี้จึงอาจก่อให้เกิดปัญหาในอนาคตได้

---

[40] สฤณี อาชวานันทกุล, ““เศรษฐกิจดิจิทัล” เพื่อใคร? อันตรายของชุดกฎหมายไซเบอร์,” [ออนไลน์], เข้าถึงได้จาก: http://thaipublica.org/2015/01/dangers-new-cyber-laws/ [2558] สืบค้น 29 กันยายน 2559.

[41] มาตรา 28 แห่ง (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

[42] มาตรา 35 แห่ง (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ว่าบทบัญญัติของกฎหมายอาจไม่สอดคล้องกับสิทธิและเสรีภาพของประชาชนที่รัฐธรรมนูญได้บัญญัติรับรองไว้

อนึ่ง กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกฎหมายที่มีลักษณะเป็นมาตรการตั้งรับในเชิงรุก ซึ่งเห็นได้จากหลักการและบทบัญญัติต่าง ๆ ตามที่ปรากฏในกฎหมาย อาทิ การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ การวิจัยและพัฒนาเพื่อความมั่นคงไซเบอร์ เป็นต้น ซึ่งมาตรการเหล่านี้ไม่ปรากฏอยู่ในพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่อย่างใด ดังนั้นประเทศไทยจึงมีความจำเป็นอย่างยิ่งในการจัดทำร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. .... และควรจะมีการปรับใช้กฎหมายดังกล่าวโดยเร็ว

2.3 ตารางเปรียบเทียบกฎหมายว่าด้วยความมั่นคงทางไซเบอร์

การพิจารณาเชิงเปรียบเทียบกับประเทศต่าง ๆ ที่ศึกษาเบื้องต้น เพื่อจะได้เห็นถึงความเหมือนและความแตกต่าง ข้อเด่นและข้อด้อยของพระราชบัญญัติด้านความมั่นคงทางไซเบอร์ของประเทศต่าง ๆ ทั้งนี้ เพื่อจะได้สามารถพิจารณาถึงการจัดการความมั่นคงไซเบอร์ตามที่กำหนดใน (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์แห่งชาติ พ.ศ. .... ว่า มีประเด็นใดที่ควรจะแก้ไขเพิ่มเติมได้ ดังนี้

ตารางเปรียบเทียบกฎหมายว่าด้วยความมั่นคงทางไซเบอร์

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	**สหรัฐอเมริกา**	**ประเทศจีน**	**ประเทศไทย**
ชื่อกฎหมาย	กฎรัฐสภาและคณะกรรมการยุโรปฯ ว่าด้วยมาตรการทั่วไประดับสูงสำหรับความปลอดภัยเครือข่ายและระบบข้อมูลข่าวสารแห่งสหภาพ	Cybersecurity Information Sharing Act of 2015	กฎหมายรักษาความมั่นคงไซเบอร์แห่งสาธารณรัฐประชาชนจีน	(ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงไซเบอร์แห่งชาติ พ.ศ. ....

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	**สหรัฐอเมริกา**	**ประเทศจีน**	**ประเทศไทย**
เจตนารมณ์	เพื่อตอบสนองนโยบายในการสร้างความเชื่อมั่นสำหรับการสื่อสารให้มีความปลอดภัยมากที่สุดโดย 1) การสร้างความร่วมมือระหว่างประเทศสมาชิก 2) การสร้างความพร้อมในการรับมือกับภัยคุกคามไซเบอร์สำหรับประเทศสมาชิก 3) การสร้างวัฒนธรรมในเชิงป้องกันและการใช้งานที่ปลอดภัยจากภัยคุกคามไซเบอร์	เพื่ออำนวยความสะดวกในการสื่อสารและการแบ่งปันข้อมูลระหว่างองค์กรเอกชนกับองค์กรภาครัฐเพื่อต่อสู้กับภัยคุกคามและความรุนแรงในโลกไซเบอร์	เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยเครือข่ายปกป้องอธิปไตยของโลกเทคโนโลยีสารสนเทศความมั่นคงแห่งชาติ และประโยชน์สาธารณะปกป้องสิทธิทางกฎหมายและประโยชน์ของพลเมือง สร้างความร่วมมือกับองค์กรอื่น และเสริมสร้างการพัฒนาที่สร้างสรรค์ของเทคโนโลยีสารสนเทศในส่วนของเศรษฐกิจและสังคม	เพื่อปกป้องและป้องกันการประยุกต์ใช้เทคโนโลยีสารสนเทศ จากภัยคุกคามไซเบอร์ประเภทต่าง ๆ
องค์กรที่รับผิดชอบ	1) หน่วยงานทางด้านความมั่นคงปลอดภัยทางโครงข่ายและ	กระทรวงความมั่นคงภายในประเทศ (Department of	the State Council Internet Information	คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	**สหรัฐอเมริกา**	**ประเทศจีน**	**ประเทศไทย**
องค์กรที่รับผิดชอบ (ต่อ)	สารสนเทศแห่งสหภาพยุโรป (The European Union Agency for Network Information Security หรือ ENISA) 2) หน่วยงานตอบสนองเหตุการณ์ด้านความปลอดภัยคอมพิวเตอร์ (computer security incident response teams (CSIRT)) หรือ (computer emergency response team (CERT))	Homeland Security หรือ DHS)	Office (สำนักงานสารสนเทศทางอินเทอร์เน็ตของสภาแห่งรัฐ) (国务院新闻办公室)[43]	(กปช.)
เครื่องมือหลักในการบังคับใช้กฎหมาย	- กำหนดให้มีการรวบรวมรายชื่อของผู้ประกอบการเอกชนในภาค	- กำหนดสิ่งบ่งชี้การเกิดภัยคุกคามไซเบอร์ -ให้มีการประสานงาน	- ผู้ให้บริการโครงข่ายต้องมีระบบการจัดการความปลอดภัยภายในบริษัท	- คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีอำนาจตาม

[43]Hauke Johannes Gierow, "Cyber Security in China: New Political Leadership Focuses on Boosting National Security," p.1, [Online], Avaiable: http://www.merics.org/ [n.d.] Retrieved Jan 15, 2017.

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	สหรัฐอเมริกา	ประเทศจีน	ประเทศไทย
เครื่องมือหลักในการบังคับใช้กฎหมาย (ต่อ)	ส่วนต่างๆ ที่เป็นส่วนสำคัญต่อระบบเศรษฐกิจ - กำหนดขั้นตอนการรับมือกับภัยคุกคามโดยยกระดับตามความร้ายแรงของภัยคุกคาม - การส่งเสริมความร่วมมือและการแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิก - จัดตั้งกลุ่มความร่วมมือทางยุทธศาสตร์เพื่ออำนวยความสะดวกในการแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ดีที่สุดระหว่างประเทศสมาชิกสหภาพยุโรป - จัดตั้งหน่วยงานตอบสนองเหตุการณ์ด้านความปลอดภัย	ป้องกัน วิเคราะห์และบรรเทาวิเคราะห์ภัยคุกคามไซเบอร์โดยให้มีการสังเกตการณ์ และกำหนดมาตรการป้องกันต่าง ๆ - การแบ่งปันข้อมูลระหว่างหน่วยงานต่าง ๆ	- หน้าที่ในการบำรุงรักษาระบบรักษาความปลอดภัย - หน้าที่ในการขอการรับรองจากรัฐบาล (Government certification) ก่อนที่จะมีการขายหรือผลิตสินค้าหรือบริการในโลกไซเบอร์ในตลาดสาธารณรัฐประชาชนจีน - กำหนดให้ผู้ให้บริการอินเทอร์เน็ตจะต้องตรวจสอบตัวตนที่แท้จริงของบุคคลก่อนที่จะให้บริการอินเทอร์เน็ต - ให้อำนาจ State Council หรือหน่วยงานของรัฐที่เกี่ยวข้องมีอำนาจในการสั่ง	กฎหมายในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ การเข้าถึงข้อมูลและอำนาจในการกำกับดูแลองค์กรต่างๆ เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นในระบบสารสนเทศ - เรียกให้หน่วยงานของรัฐหรือบุคคลใดๆ มาให้ถ้อยคำหรือส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด - เรียกให้หน่วยงานของรัฐหรือบุคคลใดๆ มาให้ถ้อยคำหรือส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด - เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	สหรัฐอเมริกา	ประเทศจีน	ประเทศไทย
เครื่องมือหลักในการบังคับใช้กฎหมาย (ต่อ)	คอมพิวเตอร์แห่งชาติ (National CSIRT) เพื่อเป็นจุดติดต่อระหว่างประเทศต่างๆ		หรือจำกัดการเข้าถึงอินเทอร์เน็ตได้หากเป็นเรื่อง “ความมั่นคงของชาติ” (national security) หรือเพื่อรักษา “ความสงบเรียบร้อยทางสังคม” (Social order) - กำหนดความรับผิดชอบของผู้เข้าเว็บไซต์ -การปกป้องการใช้งานของผู้เยาว์เพื่อคุ้มครองผู้เยาว์ในโลกไซเบอร์ - ความรับผิดตามกฎหมายกรณีไม่ปฏิบัติตามกฎหมายโดยจะถูกขึ้นบัญชีดำและอาจต้องได้รับโทษทางปกครองและค่าปรับ	โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	สหรัฐอเมริกา	ประเทศจีน	ประเทศไทย
เครื่องมือหลักในการบังคับใช้กฎหมาย (ต่อ)			- หน้าที่ในการรวบรวมและเก็บรักษาข้อมูลส่วนบุคคลของผู้ใช้บริการ	
มาตรการคุ้มครองสิทธิและเสรีภาพของประชาชน	- กำหนดให้การดำเนินการตามกฎฯ นี้จะต้องเคารพสิทธิขั้นพื้นฐานและตามหลักการตามที่ได้รับการรับรองจากกฎบัตรสิทธิพื้นฐานของสหภาพยุโรป	- บรรดาข้อมูลใด ๆ ที่เป็นข้อมูลส่วนบุคคลที่รัฐได้รับมาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์หรือต่อต้านภัยคุกคามไซเบอร์ หากปรากฏว่าข้อมูลดังกล่าวนั้นไม่มีความเกี่ยวข้องหรือจะบ่งชี้ได้ว่าเป็นภัยคุกคามไซเบอร์ รัฐต้องดำเนินการลบข้อมูลเช่นว่านั้น	- มีการบัญญัติเรื่องหลักเกณฑ์การจัดเก็บข้อมูลส่วนบุคคล - กำหนดให้มีการเปิดเผยนโยบายในการเก็บรักษาและการนำข้อมูลส่วนบุคคลไปใช้ - ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อนการจัดเก็บหรือการประมวลผลข้อมูล	- ไม่ได้กล่าวถึงชัดแจ้งในกฎหมายแต่อาจจะใช้การคุ้มครองจากกฎหมายอื่น ๆ ได้
ข้อกังวล	- บทบัญญัติของกฎหมายมีลักษณะทั่วไปและไม่ชัดเจนในหลายประเด็นจึงยากแก่การปฏิบัติ - ข้อกังวลว่าจะ	- เมื่อผู้ประกอบการถูกโจมตีหรือคุกคามทางไซเบอร์แล้วผู้ประกอบการก็ยังมีความลังเล	- ความไม่ชัดเจนในทางปฏิบัติ - ความไม่ชัดเจนในเรื่องผู้ที่มีหน้าที่ตามกฎหมาย	- นิยามศัพท์ไม่ชัดเจนมีความหมายที่กว้างและเปิดโอกาสให้เจ้าหน้าที่รัฐใช้ดุลพินิจได้อย่าง

ประเด็นเปรียบเทียบ	ประเทศ/กลุ่มประเทศ			
	สหภาพยุโรป	สหรัฐอเมริกา	ประเทศจีน	ประเทศไทย
ข้อกังวล (ต่อ)	กำหนดให้ภาคส่วนใดมีความสำคัญกับระบบเศรษฐกิจ - ข้อกังวลในเรื่องการสั่งซื้อวัสดุอุปกรณ์ตลอดจนระบบต่าง ๆ จากพื้นที่นอกสหภาพยุโรปจะเป็นจุดอ่อนที่ถูกคุกคามทางไซเบอร์ได้ - มาตรฐานความพร้อมสำหรับรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละประเทศแตกต่างกัน	ว่าควรจะแบ่งปันข้อมูลให้กับหน่วยงานของรัฐหรือไม่ เนื่องจากกลัวที่จะเสียชื่อเสียง และไม่แน่ใจว่าจะถูกฟ้องร้องดำเนินคดีหรือไม่	- ความไม่ชัดเจนในเรื่องนิยามของคำว่า “ความมั่นคงของชาติ” (ที่กำหนดให้ผู้ให้บริการจะต้องให้ความร่วมมือ กรณีเป็นภัยต่อความมั่นคงของชาติ)	กว้างขวาง - ปัญหาความทับซ้อนกันระหว่างความมั่นคงแห่งชาติและความมั่นคงปลอดภัยไซเบอร์ - ปัญหาเกี่ยวกับการคุ้มครองสิทธิและเสรีภาพของประชาชน

จากการเปรียบเทียบกฎหมายว่าด้วยการรักษาความมั่นคงไซเบอร์ของทั้งสหภาพยุโรป สาธารณรัฐประชาชนจีน และประเทศสหรัฐอเมริกา และประเทศไทย พบว่ามีเจตนารมณ์หรือวัตถุประสงค์ที่คล้ายคลึงกัน กล่าวคือการรักษาหรือปกป้องระบบเทคโนโลยีสารสนเทศของประเทศเพื่อสร้างความเชื่อมั่นในการใช้งาน แต่ความแตกต่างประการสำคัญของแต่ละประเทศคือเครื่องมือทางกฎหมายที่ปรากฏในกฎหมายแต่ละฉบับที่อาจจะมีความแตกต่างกันตามแต่บริบทและความจำเป็นของแต่ละประเทศ โดยกฎหมายของประเทศสหรัฐอเมริกา ของสหภาพยุโรป และของประเทศจีนกำหนดถึงหน้าที่ของผู้ให้บริการอย่างชัดเจน ว่าจะต้องดำเนินการอย่างไรและมีลำดับขั้นตอนอย่างไรในกรณีที่เกิดภัยคุกคามทางไซเบอร์ ขณะที่กฎหมายของประเทศไทยไม่ได้มีความชัดเจนในเรื่องดังกล่าวซึ่งควรจะปรับปรุงหรือแก้ไขเพิ่มเติมต่อไป

ประเด็นด้านมาตรการคุ้มครองสิทธิและเสรีภาพของประชาชน กฎหมายของประเทศสหรัฐอเมริกา ของสหภาพยุโรป และของประเทศจีน ก็ได้มีการบัญญัติชัดเจนเช่นเดียวกันถึงมาตรการคุ้มครองสิทธิขั้นพื้นฐานของประชาชน โดยเฉพาะอย่างยิ่ง ในเรื่องของข้อมูลส่วนบุคคล กฎหมายของประเทศสหรัฐอเมริกากำหนดให้ทำการลบทิ้งทันที หากพิสูจน์ทราบในภายหลังว่าข้อมูลส่วนบุคคลนั้นไม่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือกฎหมายของประเทศจีนก็กำหนดในเรื่องหลักเกณฑ์ในการจัดเก็บและการนำข้อมูลส่วนบุคคลไปประมวลผลเช่นเดียวกัน แต่กฎหมายของประเทศไทยไม่ได้ปรากฏมาตรการคุ้มครองสิทธิและเสรีภาพของประชาชนแต่อย่างใด ดังนั้นในทางปฏิบัติจึงอาจจะต้องพิจารณากฎหมายอื่นประกอบเพื่อนำมาคุ้มครองสิทธิขั้นพื้นฐานของประชาชน

ประเด็นเรื่องข้อกังวลจากการบังคับใช้กฎหมายตามที่ปรากฏในแต่ละประเทศ พบว่าโดยส่วนใหญ่จะคล้ายคลึงกัน กล่าวคือมีความกังวลเกี่ยวกับความไม่ชัดเจนของกฎหมาย ตลอดจนหน้าที่ที่จะต้องปฏิบัติตามกฎหมาย

3. บทสรุปและข้อเสนอแนะ

จากการวิเคราะห์เปรียบเทียบถึงประเด็นต่าง ๆ ทั้งในส่วนของกฎหมายว่าด้วยการรักษาความมั่นคงทางไซเบอร์ของต่างประเทศและของประเทศไทย รวมไปถึงหน่วยงานที่เกี่ยวข้อง และข้อกังวลในประการต่าง ๆ จากประชาชนหรือผู้ที่ต้องอยู่ภายใต้บังคับของกฎหมายแล้ว เห็นควรสร้างแนวทางในการจัดการกับปัญหาในประการต่าง ๆ ที่เกิดขึ้น ดังนี้

1. ควรเพิ่มแนวคิดในเรื่องการสร้างความสมดุลของกฎหมายความมั่นคงปลอดภัยกับสิทธิและเสรีภาพของประชาชน โดยรัฐควรสร้างสมดุลทางกฎหมายระหว่างการใช้อำนาจทางด้านความมั่นคงปลอดภัยทางไซเบอร์ของรัฐกับการคุ้มครองสิทธิและเสรีภาพของประชาชนในโลกไซเบอร์ใหม่ โดยการให้สิทธิแก่ภาคประชาชนในการโต้แย้งการใช้อำนาจรัฐบางเรื่อง หรือการกำหนดให้ภาคประชาชนมีสัดส่วนในคณะกรรมการ กปช. หรือการกำหนดค่าชดเชยตามกฎหมายให้แก่ผู้ที่ได้รับความเดือดร้อนเสียหายจากการกระทำของรัฐในกรณีที่มีการดำเนินการของรัฐที่เกินกว่าเหตุเกิดขึ้นเป็นต้น

2. สร้างบทบัญญัติที่มีความชัดเจน หรือสร้างกลไกการตีความหรือการบังคับใช้กฎหมายที่ภาคประชาชนให้ความเชื่อถือ เช่น สร้างคู่มือการใช้อำนาจของเจ้าหน้าที่รัฐ เพื่อให้เจ้าหน้าที่รัฐและผู้ที่ได้รับผลกระทบจากการบังคับใช้กฎหมายสามารถเข้าใจในทำนองเดียวกันได้ว่าเจ้าหน้าที่รัฐสามารถดำเนินการภายใต้ขอบเขตและเงื่อนไขใด และผู้ที่ได้รับผลกระทบมีสิทธิที่จะทำอย่างไรได้บ้าง โดยในคู่มือดังกล่าวอาจจะมีการกล่าวถึงสถานการณ์ตัวอย่าง หรือใช้วิธีการเขียนที่ประชาชนทั่วไปสามารถเข้าใจได้โดยง่าย หรือมีการสร้างกลไกการตีความหรือการบังคับใช้กฎหมายที่ภาคประชาชนให้ความเชื่อถือ ซึ่งหากองค์กรที่มีภารกิจหน้าที่ในการคุ้มครองสิทธิขั้นพื้นฐานของประชาชนมีความเข้มแข็ง หรือประเทศไทยมีหลักการทางกฎหมายที่รับประกันสิทธิขั้นพื้นฐานของ

ประชาชนอย่างมีประสิทธิภาพแล้ว การใช้อำนาจในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ก็จะมีขอบเขตและควบคุมได้ ทำให้ภาคประชาชนมีความมั่นใจมากยิ่งขึ้นว่าตนจะได้รับความคุ้มครองอย่างเป็นธรรมและรวดเร็ว

3. รัฐควรสร้างวัฒนธรรมการมีส่วนร่วมในการต่อสู้กับภัยคุกคามไซเบอร์ให้กับประชาชนในรูปแบบของความร่วมมือในการสอดส่องดูแลกันและกัน และส่งเสริมให้ประชาชนรู้จักวิธีการใช้ชีวิตอย่างปลอดภัยในโลกไซเบอร์ โดยเฉพาะในเรื่องของการแบ่งปันข้อมูล (Framework for information sharing) ควรจะกำหนดกรอบโดยระบุประเภทของข้อมูลที่ผู้ประกอบการภาคเอกชนหรือหน่วยงานของรัฐควรจะต้องนำมาเผยแพร่ร่วมกัน เพื่อเรียนรู้ และเตรียมรับมือกับภัยคุกคามทางด้านความมั่นคงทางไซเบอร์ร่วมกัน

4. รัฐควรสร้างพันธมิตรนานาชาติและยกระดับมาตรฐานความปลอดภัยไซเบอร์ให้ได้มาตรฐานระดับโลก เพราะระบบความมั่นคงปลอดภัยทางไซเบอร์นั้น มิใช่เกี่ยวกับความมั่นคงปลอดภัยในระบบหรือโครงข่ายที่เกี่ยวกับคอมพิวเตอร์หรือระบบโทรคมนาคมเท่านั้น แต่ยังรวมถึงระบบการทำงานคอมพิวเตอร์หรือโครงข่ายการทำงานที่นำไปใช้กับระบบอื่น ๆ เช่น ระบบพลังงาน ระบบสาธารณสุข ระบบการขนส่งคมนาคม ระบบไฟฟ้า ระบบการติดต่อระหว่างหน่วยงานของรัฐหรือระบบธนาคาร ด้วย นอกจากนี้ ความมั่นคงปลอดภัยทางไซเบอร์ดังกล่าวยังเป็นปัจจัยสำคัญในการสร้างความเชื่อมั่นในการใช้งานระบบเศรษฐกิจดิจิทัลแก่ผู้ที่ลงทุนและเป็นผู้ประกอบการในระบบเศรษฐกิจดิจิทัลซึ่งมิใช่เป็นเพียงคนไทยหรือคนที่อาศัยอยู่ในประเทศไทยเท่านั้น แต่ยังรวมถึงผู้ประกอบการที่อยู่ในต่างประเทศด้วย กล่าวคือ เศรษฐกิจดิจิทัลไม่มีข้อจำกัดทางด้านพรมแดนหรือเขตแดนทางภูมิศาสตร์ ดังนั้น การเตรียมการในทุกหน่วยงานทั้งภาครัฐและภาคเอกชนเพื่อรองรับปัญหาและจำกัดความเสียหายจากภัยคุกคามไซเบอร์ให้น้อยที่สุดในกรณีที่มีภัยคุกคามทางระบบที่เกี่ยวข้องจึงเป็นสิ่งจำเป็นอย่างยิ่ง

สุดท้ายผลจากการศึกษาจะเห็นได้ว่า ความมั่นคงของรัฐกับสิทธิเสรีภาพของประชาชนจากภัยคุกคามทางไซเบอร์เป็นเรื่องที่มีความสำคัญเท่าเทียมกัน ด้วยเหตุนี้จึงต้องสร้างและพัฒนากฎหมายเพื่อป้องกันภัยคุกคามทางไซเบอร์และคำนึงถึงสิทธิเสรีภาพของประชาชนไปพร้อม ๆ กัน รวมทั้งต้องเตรียมพร้อมให้ทันกับความก้าวหน้าของเทคโนโลยีในด้านต่าง ๆ ที่เกิดขึ้นอย่างรวดเร็วด้วย