ด่วนที่สุด

ที่ สผ ๐๐๑๗.๑๑/๔๓๓

คณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
สภาผู้แทนราษฎร
ถนนสามเสน เขตดุสิต กรุงเทพฯ ๑๐๓๐๐

๓ กันยายน ๒๕๖๔

เรื่อง รายงานการศึกษาของคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สภาผู้แทนราษฎร

กราบเรียน ประธานสภาผู้แทนราษฎร

สิ่งที่ส่งมาด้วย รายงานการศึกษาเรื่อง ความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ ชุด

ตามที่ที่ประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๒๑ (สมัยสามัญประจำปี ครั้งที่หนึ่ง) วันพุธที่ ๑๑ กันยายน ๒๕๖๒ ที่ประชุมสภาผู้แทนราษฎร ได้ลงมติตั้งคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สภาผู้แทนราษฎร เพื่อให้มีหน้าที่และอำนาจตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๐ ในการกระทำกิจการ การสอบหาข้อเท็จจริง หรือศึกษาเรื่องใด ๆ ที่เกี่ยวกับการส่งเสริมและการพัฒนาด้านการสื่อสาร โทรคมนาคม และเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคมนั้น ซึ่งกรรมาธิการคณะนี้ ประกอบด้วย

๑. นางสาวกัลยา รุ่งวิจิตรชัย	ประธานคณะกรรมาธิการ
๒. นายสยาม หัตถสงเคราะห์	รองประธานคณะกรรมาธิการ คนที่หนึ่ง
๓. พันเอก เศรษฐพงค์ มะลิสุวรรณ	รองประธานคณะกรรมาธิการ คนที่สอง
๔. นายนิคม บุญวิเศษ	รองประธานคณะกรรมาธิการ คนที่สาม
๕. นายปกรณ์วุฒิ อุดมพิพัฒน์สกุล	รองประธานคณะกรรมาธิการ คนที่สี่
๖. นายดล เหตระกูล	รองประธานคณะกรรมาธิการ คนที่ห้า
๗. นายสรอรรถ กลิ่นประทุม	ประธานที่ปรึกษาคณะกรรมาธิการ
๘. นายสราวุธ อ่อนละมัย	ที่ปรึกษาคณะกรรมาธิการ
๙. นายชาญวิทย์ วิภูศิริ	ที่ปรึกษาคณะกรรมาธิการ
๑๐. นายนพ ชีวานันท์	ที่ปรึกษาคณะกรรมาธิการ
๑๑. นายกฤษฎา ตันเทอดทิตย์	ที่ปรึกษาคณะกรรมาธิการ
๑๒. นายภาควัต ศรีสุรพล	ที่ปรึกษาคณะกรรมาธิการ
๑๓. นางสาวภาดาท์ วรกานนท์	โฆษกคณะกรรมาธิการ
๑๔. นายสมเกียรติ ถนอมสินธุ์	โฆษกคณะกรรมาธิการ
๑๕. นายเสมอกัน เที่ยงธรรม	เลขานุการคณะกรรมาธิการ

/ในคราว...

ในคราวประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๙ (สมัยสามัญประจำปีครั้งที่สอง) วันพฤหัสบดีที่ ๒๘ พฤศจิกายน ๒๕๖๒ ที่ประชุมได้ลงมติตั้งนายดล เหตระกูล เป็นกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม แทนนายชัยวุฒิ ธนาคมานุสรณ์ ซึ่งได้ขอลาออกจากการเป็นกรรมาธิการสามัญ เมื่อวันที่ ๒๑ พฤศจิกายน ๒๕๖๒

บัดนี้ คณะกรรมาธิการได้ดำเนินการพิจารณาศึกษา เรื่อง ความมั่นคงปลอดภัยไซเบอร์ เสร็จเรียบร้อยแล้ว จึงกราบเรียนมาเพื่อโปรดนำเสนอที่ประชุมสภาผู้แทนราษฎร เพื่อพิจารณารายงานและข้อสังเกตของคณะกรรมาธิการต่อไป

ขอแสดงความนับถืออย่างยิ่ง

(นางสาวกัลยา รุ่งวิจิตรชัย)
ประธานคณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักกรรมาธิการ ๑
กลุ่มงานคณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
โทรศัพท์ ๐ ๒๒๔๒ ๕๙๐๐ ต่อ ๖๒๑๑
ไปรษณีย์อิเล็กทรอนิกส์ : telecom@parliament.go.th

รายงาน
เรื่อง ความมั่นคงปลอดภัยไซเบอร์

ของคณะกรรมาธิการการสื่อสารโทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
สภาผู้แทนราษฎร

สำนักกรรมาธิการ ๑
สำนักงานเลขาธิการสภาผู้แทนราษฎร

รายงาน
เรื่อง ความมั่นคงปลอดภัยไซเบอร์

ของคณะกรรมาธิการการสื่อสารโทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
สภาผู้แทนราษฎร

สำนักกรรมาธิการ ๑
สำนักงานเลขาธิการสภาผู้แทนราษฎร

ด่วนที่สุด

สำเนา

ที่ สผ ๐๐๑๗.๑๑/๔๓๓

คณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
สภาผู้แทนราษฎร
ถนนสามเสน เขตดุสิต กรุงเทพฯ ๑๐๓๐๐

๓ กันยายน ๒๕๖๔

เรื่อง รายงานการศึกษาของคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สภาผู้แทนราษฎร

กราบเรียน ประธานสภาผู้แทนราษฎร

สิ่งที่ส่งมาด้วย รายงานการศึกษาเรื่อง ความมั่นคงปลอดภัยไซเบอร์ จำนวน ๑ ชุด

ตามที่ที่ประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๒๑ (สมัยสามัญประจำปี ครั้งที่หนึ่ง) วันพุธที่ ๑๑ กันยายน ๒๕๖๒ ที่ประชุมสภาผู้แทนราษฎร ได้ลงมติตั้งคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สภาผู้แทนราษฎร เพื่อให้มีหน้าที่และอำนาจตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๐ ในการกระทำกิจการ การสอบหาข้อเท็จจริง หรือศึกษาเรื่องใด ๆ ที่เกี่ยวกับการส่งเสริมและการพัฒนาด้านการสื่อสาร โทรคมนาคม และเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคมนั้น ซึ่งกรรมาธิการคณะนี้ ประกอบด้วย

๑. นางสาวกัลยา รุ่งวิจิตรชัย	ประธานคณะกรรมาธิการ
๒. นายสยาม หัตถสงเคราะห์	รองประธานคณะกรรมาธิการ คนที่หนึ่ง
๓. พันเอก เศรษฐพงค์ มะลิสุวรรณ	รองประธานคณะกรรมาธิการ คนที่สอง
๔. นายนิคม บุญวิเศษ	รองประธานคณะกรรมาธิการ คนที่สาม
๕. นายปกรณ์วุฒิ อุดมพิพัฒน์สกุล	รองประธานคณะกรรมาธิการ คนที่สี่
๖. นายดล เหตระกูล	รองประธานคณะกรรมาธิการ คนที่ห้า
๗. นายสรอรรถ กลิ่นประทุม	ประธานที่ปรึกษาคณะกรรมาธิการ
๘. นายสราวุธ อ่อนละมัย	ที่ปรึกษาคณะกรรมาธิการ
๙. นายชาญวิทย์ วิภูศิริ	ที่ปรึกษาคณะกรรมาธิการ
๑๐. นายนพ ชีวานันท์	ที่ปรึกษาคณะกรรมาธิการ
๑๑. นายกฤษฎา ตันเทอดทิตย์	ที่ปรึกษาคณะกรรมาธิการ
๑๒. นายภาควัต ศรีสุรพล	ที่ปรึกษาคณะกรรมาธิการ
๑๓. นางสาวภาดาท์ วรกานนท์	โฆษกคณะกรรมาธิการ
๑๔. นายสมเกียรติ ถนอมสินธุ์	โฆษกคณะกรรมาธิการ
๑๕. นายเสมอกัน เที่ยงธรรม	เลขานุการคณะกรรมาธิการ

/ในคราว...

ในคราวประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๙ (สมัยสามัญประจำปีครั้งที่สอง) วันพฤหัสบดีที่ ๒๘ พฤศจิกายน ๒๕๖๒ ที่ประชุมได้ลงมติตั้งนายดล เหตระกูล เป็นกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม แทนนายชัยวุฒิ ธนาคมานุสรณ์ ซึ่งได้ขอลาออกจากการเป็นกรรมาธิการสามัญ เมื่อวันที่ ๒๑ พฤศจิกายน ๒๕๖๒

บัดนี้ คณะกรรมาธิการได้ดำเนินการพิจารณาศึกษา เรื่อง ความมั่นคงปลอดภัยไซเบอร์ เสร็จเรียบร้อยแล้ว จึงกราบเรียนมาเพื่อโปรดนำเสนอที่ประชุมสภาผู้แทนราษฎร เพื่อพิจารณารายงานและข้อสังเกตของคณะกรรมาธิการต่อไป

ขอแสดงความนับถืออย่างยิ่ง

ลงชื่อ กัลยา รุ่งวิจิตรชัย

(นางสาวกัลยา รุ่งวิจิตรชัย)
ประธานคณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักกรรมาธิการ ๑
กลุ่มงานคณะกรรมาธิการการสื่อสาร โทรคมนาคม
และดิจิทัลเพื่อเศรษฐกิจและสังคม
โทรศัพท์ ๐ ๒๒๔๒ ๕๙๐๐ ต่อ ๖๒๑๑
ไปรษณีย์อิเล็กทรอนิกส์ : telecom@parliament.go.th

สำเนาถูกต้อง

(นางสาวปรียาภรณ์ แก้วโยน)
ผู้อำนวยการสำนักกรรมาธิการ ๑

นายกฤช ฤทธา/ร่าง
นางสาวนัยนา แสนวิชา/พิมพ์
นายพิศณุ พลพืชน์/ตรวจ

นัยนา D : กมธ.ชุดที่ ๒๕/รายงานผลการศึกษาของ กมธ.

ตรวจทาน
ครั้งที่ ๑ นายพิศณุ พลพืชน์
ครั้งที่ ๒ ว่าที่ร้อยตรี เอกศักดิ์ โชติมัย

รายนามคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม

นางสาวกัลยา รุ่งวิจิตรชัย
ประธานคณะกรรมาธิการ

นายสยาม หัตถสงเคราะห์
รองประธานคณะกรรมาธิการ คนที่หนึ่ง

พันเอก เศรษฐพงศ์ มะลิสุวรรณ
รองประธานคณะกรรมาธิการ คนที่สอง

นายนิคม บุญวิเศษ
รองประธานคณะกรรมาธิการ คนที่สาม

นายปกรณ์วุฒิ อุดมพิพัฒน์สกุล
รองประธานคณะกรรมาธิการ คนที่สี่

นายดล เหตระกูล
รองประธานคณะกรรมาธิการ คนที่ห้า

นายสรอรรถ กลิ่นประทุม
ประธานที่ปรึกษาคณะกรรมาธิการ

นายสราวุธ อ่อนละมัย
ที่ปรึกษาคณะกรรมาธิการ

นายชาญวิทย์ วิภูศิริ
ที่ปรึกษาคณะกรรมาธิการ

นายนพ ชีวานันท์
ที่ปรึกษาคณะกรรมาธิการ

นายกฤษฎา ตันเทอดทิตย์
ที่ปรึกษาคณะกรรมาธิการ

นายภาควัต ศรีสุรพล
ที่ปรึกษาคณะกรรมาธิการ

นางสาวภาดาท์ วรกานนท์
โฆษกคณะกรรมาธิการ

นายสมเกียรติ ถนอมสินธุ์
โฆษกคณะกรรมาธิการ

นายเสมอกัน เที่ยงธรรม
เลขานุการคณะกรรมาธิการ

รายนามที่ปรึกษา ผู้ชำนาญการ นักวิชาการ และเลขานุการประจำคณะกรรมาธิการ (ปัจจุบัน)

๑. นายศักดิ์ สมบุญโต	ที่ปรึกษาประจำคณะกรรมาธิการ
๒. นางสาวอารีรัตน์ เลาพหล	ที่ปรึกษาประจำคณะกรรมาธิการ
๓. นายสิทธา สุวิรัชวิทยกิจ	ผู้ชำนาญการประจำคณะกรรมาธิการ
๔. นางสาวอัจจิมา ศิริอ่อน	นักวิชาการประจำคณะกรรมาธิการ
๕. นายธาดา โอฬาริก	เลขานุการประจำคณะกรรมาธิการ
๖. นายธีรชาติ ก่อตระกูล	เลขานุการประจำคณะกรรมาธิการ
๗. นายศิลป์วิชญ์ น้อยสมมิตร	เลขานุการประจำคณะกรรมาธิการ
๘. นางสุดนภา เจริญเวชชการ	เลขานุการประจำคณะกรรมาธิการ
๙. นายธนบดี มณีสว่างวงศ์	เลขานุการประจำคณะกรรมาธิการ
๑๐. นายพันธสร กฤษฎาธิวุฒิ	เลขานุการประจำคณะกรรมาธิการ
๑๑. นายอัฏฐพร ดำรงกุล	เลขานุการประจำคณะกรรมาธิการ
๑๒. นายฐาคณิษฐ์ พรทองประเสริฐ	เลขานุการประจำคณะกรรมาธิการ
๑๓. นายพิรุณ ไพรีพ่ายฤทธิ์	เลขานุการประจำคณะกรรมาธิการ
๑๔. นายพิศฐ์ศักดิ์ เครือไชย	เลขานุการประจำคณะกรรมาธิการ
๑๕. นายยอดยิ่ง ชุมแสง ณ อยุธยา	เลขานุการประจำคณะกรรมาธิการ
๑๖. นายกิตตินันท์ พจน์ประสาท	เลขานุการประจำคณะกรรมาธิการ
๑๗. นายธีระพจน์ ผดุงธรรม	เลขานุการประจำคณะกรรมาธิการ
๑๘. นายชัยยะวัฒน์ พึงจิตติสานติ์	เลขานุการประจำคณะกรรมาธิการ
๑๙. นายอภิวงษ์ วนะไชยเกียรติ	เลขานุการประจำคณะกรรมาธิการ
๒๐. นายปกรณ์ เกยานนท์	เลขานุการประจำคณะกรรมาธิการ
๒๑. นางสาวกมลชนก วรรณวิจิตร	เลขานุการประจำคณะกรรมาธิการ
๒๒. นางสาวสุดารัตน์ พิทักษ์พรพัลลภ	เลขานุการประจำคณะกรรมาธิการ
๒๓. นายนาคร วรกานนท์	เลขานุการประจำคณะกรรมาธิการ
๒๔. นายณัฐวุธ จุลกะเศียน	เลขานุการประจำคณะกรรมาธิการ
๒๕. นางสาวรินนภา คุณะวัฒน์สถิต	เลขานุการประจำคณะกรรมาธิการ
๒๖. นายธนกฤต แก้วนุ้ย	เลขานุการประจำคณะกรรมาธิการ
๒๗. นายวีรชน วังกาวี	เลขานุการประจำคณะกรรมาธิการ
๒๘. นางสาวชนัญชิดา ศิริโภคพัฒน์	เลขานุการประจำคณะกรรมาธิการ
๒๙. นางสาวธนัชพร พงษ์โภคา	เลขานุการประจำคณะกรรมาธิการ

รายนามที่ปรึกษา ผู้ชำนาญการ นักวิชาการ และเลขานุการประจำคณะกรรมาธิการ (ในอดีต)

๑. นายปกรณ์เกียรติ ไพรวัลย์	นักวิชาการประจำคณะกรรมาธิการ
๒. นางทิพวรรณ ซำซูดิน	นักวิชาการประจำคณะกรรมาธิการ
๓. นายนิปัจกร กรรณสูต	นักวิชาการประจำคณะกรรมาธิการ
๔. นายวุฒิรักษ์ เดชะพงษ์พันธ์	นักวิชาการประจำคณะกรรมาธิการ
๕. นายศิลปชัย บุญราย	เลขานุการประจำคณะกรรมาธิการ
๖. นายวรฐ สุนทรนนท์	เลขานุการประจำคณะกรรมาธิการ
๗. นายธนกฤต สายเครื่อง	เลขานุการประจำคณะกรรมาธิการ
๘. นายกิตติโชค จิตต์สดศรี	เลขานุการประจำคณะกรรมาธิการ
๙. นายณัฐพงษ์ มงคลนาวิน	เลขานุการประจำคณะกรรมาธิการ
๑๐. นายปกรณ์ พรรณเชษฐ์	เลขานุการประจำคณะกรรมาธิการ
๑๑. นายธนพันธ์ วงษ์ชินศรี	เลขานุการประจำคณะกรรมาธิการ
๑๒. นายธรรม์ธีร์ สุกโชติรัตน์	เลขานุการประจำคณะกรรมาธิการ
๑๓. นางสาวภริณ ธนบุญญากิตติ์	เลขานุการประจำคณะกรรมาธิการ
๑๔. นายชิษณุพงศ์ ปานอำพันธ์	เลขานุการประจำคณะกรรมาธิการ
๑๕. ผู้ช่วยศาสตราจารย์อภิญญา กลิ่นประทุม	เลขานุการประจำคณะกรรมาธิการ
๑๖. นายสหทัศน์ สถาพรวรศักดิ์	เลขานุการประจำคณะกรรมาธิการ
๑๗. นายสุรวุติ อิทธิโรจนกุล	เลขานุการประจำคณะกรรมาธิการ
๑๘. นายชัยยศ จิรบวรกุล	เลขานุการประจำคณะกรรมาธิการ
๑๙. นายสุประวีณ์ อนรรฆพันธ์	เลขานุการประจำคณะกรรมาธิการ
๒๐. นายธวัชชัย กุลาตี	เลขานุการประจำคณะกรรมาธิการ
๒๑. นายเจษฎา วิริยะสุนทรพันธ์	เลขานุการประจำคณะกรรมาธิการ
๒๒. นายประยุทธ์ ศุภวราพงษ์	เลขานุการประจำคณะกรรมาธิการ
๒๓. นางสาวจันทร์เพ็ญ ใจกล้า	เลขานุการประจำคณะกรรมาธิการ
๒๔. นายทิพย์ธนวัฒน์ พงษ์วัฒนา	เลขานุการประจำคณะกรรมาธิการ
๒๕. นายศิริวัฒน์ วงศ์จารุกร	เลขานุการประจำคณะกรรมาธิการ
๒๖. นายนิรุฬ วรกานนท์	เลขานุการประจำคณะกรรมาธิการ

รายนามที่ปรึกษาประจำคณะกรรมาธิการ (ไม่มีค่าตอบแทน)

รายนามที่ปรึกษาประจำคณะกรรมาธิการ (ปัจจุบัน)

๑. นางทรงพร โกมลสุรเดช
๒. นายเฉลิมชัย วิรุณสาร
๓. นายยอด ชินสุภัคกุล
๔. ร้อยโท เจษฎา ศิวรักษ์
๕. นายกัญจนาภา ประสิทธิลาโภ
๖. นายไพศาล อิทธิธรรม
๗. พลโท ปรัญชา เฉลิมวัฒน์
๘. นายอภิจิต เจริญเวชชการ
๙. นายชัยทัต แซ่ตั้ง
๑๐. นายปริญญา จารวิจิต
๑๒. นายศิริชัย สุขสันติชัย
๑๓. นายสรร ก่อนันทวัฒน์
๑๔. นายเจษฎา วิริยะสุนทรพันธ์

รายนามที่ปรึกษาประจำคณะกรรมาธิการ (อดีต)

๑. นายจำรัส บุตรดี
๒. นายไพรัช บุญประกอบวงศ์
๓. นายสุรวุต อิทธิโรจนกุล
๔. นายวิศัลย์ วนะศักดิ์ศรีสกุล
๕. นายธัชกร แต้ศิริเวช
๖. นายธนกร ภัทรบุญสิริ
๗. นายภัทร ภมรมนตรี

รายนามคณะอนุกรรมาธิการติดตามและตรวจสอบการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

พันเอก เศรษฐพงศ์ มะลิสุวรรณ
ประธานคณะอนุกรรมาธิการ

นายสมเกียรติ ถนอมสินธุ์
รองประธานคณะอนุกรรมาธิการ คนที่หนึ่ง

นางสาวภาดาท์ วรกานนท์
รองประธานคณะอนุกรรมาธิการ คนที่สอง

นายชัยชนะ มิตรพันธ์
อนุกรรมาธิการ

นายปรัชญา อนัตเมฆ
อนุกรรมาธิการ

นายธเนศ กิตตินเรศวร
อนุกรรมาธิการ

นางสาวภัคธภา ฉัตรโกเมศ
อนุกรรมาธิการ

นางสาวนวพร สอดศรี
อนุกรรมาธิการ

นายรัฐภูมิ โตคงทรัพย์
อนุกรรมาธิการ

นายนพดล เทียมนรา
เลขานุการ
คณะอนุกรรมาธิการ

รายนามที่ปรึกษาประจำคณะอนุกรรมาธิการ

๑. ผู้ช่วยศาสตราจารย์จิรศิลป์ จยาวรรณ
๒. ร้อยโท เจษฎา ศิวรักษ์
๓. นายสุทธิศักดิ์ ตันตะโยธิน
๔. นายกิตตินันท์ พจน์ประสาท
๕. นายจักรกฤษณ์ อุไรรัตน์
๖. นางสุวรรณา หรรษาจารุพันธ์
๗. นายเชาวน์วัศ วณิชพันธุ์
๘. นายชติพจน์ ศรีเมือง
๙. นางสมจิตต์ ธีระชุติกุล
๑๐. นายรัชกฤต ภูชัชวณิชกุล
๑๑. นายชัยทัต แซ่ตั้ง
๑๒. นายเศกสิทธิ์ เสงี่ยมศักดิ์
๑๓. นายศิลป์วิชญ์ น้อยสมมิตร
๑๔. นายศิลปชัย บุญราย
๑๕. นายแสงเทียน เชิดชิด
๑๖. นายแสงชัย ธีรกุลวาณิช
๑๗. พันเอก ผู้ช่วยศาสตราจารย์ทวิวัชร วีระแกล้ว
๑๘. รองศาสตราจารย์อุดมเกียรติ นนทแก้ว
๑๙. ผู้ช่วยศาสตราจารย์นริศ หนูหอม
๒๐. นายปริญญา หอมอเนก
๒๑. นายเลิศรัตน์ รตะนานุกูล
๒๒. นายวุฒิรักษ์ เดชะพงษ์พันธุ์
๒๓. นายพงศธร สายสุจริต
๒๔. นายชัชวาล กาญจนะหุต
๒๕. นางสุดนภา เจริญเวชชการ

รายงานการศึกษา
ของคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม
สภาผู้แทนราษฎร

ตามที่ที่ประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๒๑ (สมัยสามัญประจำปีครั้งที่หนึ่ง) วันพุธที่ ๑๑ กันยายน ๒๕๖๒ ที่ประชุมสภาผู้แทนราษฎร ได้ลงมติตั้งคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สภาผู้แทนราษฎร เพื่อให้มีหน้าที่และอำนาจตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๐ ในการกระทำกิจการการสอบหาข้อเท็จจริง หรือศึกษาเรื่องใด ๆ ที่เกี่ยวกับการส่งเสริมและการพัฒนาด้านการสื่อสาร โทรคมนาคม และเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม กรรมาธิการคณะนี้ ประกอบด้วย

๑. นางสาวกัลยา รุ่งวิจิตรชัย	ประธานคณะกรรมาธิการ
๒. นายสยาม หัตถสงเคราะห์	รองประธานคณะกรรมาธิการ คนที่หนึ่ง
๓. พันเอก เศรษฐพงค์ มะลิสุวรรณ	รองประธานคณะกรรมาธิการ คนที่สอง
๔. นายนิคม บุญวิเศษ	รองประธานคณะกรรมาธิการ คนที่สาม
๕. นายปกรณ์วุฒิ อุดมพิพัฒน์สกุล	รองประธานคณะกรรมาธิการ คนที่สี่
๖. นายดล เหตระกูล	รองประธานคณะกรรมาธิการ คนที่ห้า
๗. นายสรอรรถ กลิ่นประทุม	ประธานที่ปรึกษาคณะกรรมาธิการ
๘. นายสราวุธ อ่อนละมัย	ที่ปรึกษาคณะกรรมาธิการ
๙. นายชาญวิทย์ วิภูศิริ	ที่ปรึกษาคณะกรรมาธิการ
๑๐. นายนพ ชีวานันท์	ที่ปรึกษาคณะกรรมาธิการ
๑๑. นายกฤษฎา ตันเทอดทิตย์	ที่ปรึกษาคณะกรรมาธิการ
๑๒. นายภาควัต ศรีสุรพล	ที่ปรึกษาคณะกรรมาธิการ
๑๓. นางสาวภาดาท์ วรกานนท์	โฆษกคณะกรรมาธิการ
๑๔. นายสมเกียรติ ถนอมสินธุ์	โฆษกคณะกรรมาธิการ
๑๕. นายเสมอกัน เที่ยงธรรม	เลขานุการคณะกรรมาธิการ

อนึ่ง เมื่อวันพฤหัสบดีที่ ๒๑ พฤศจิกายน ๒๕๖๒ นายชัยวุฒิ ธนาคมานุสรณ์ ได้ลาออกจากตำแหน่งกรรมาธิการ และในคราวการประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๙ (สมัยสามัญประจำปีครั้งที่สอง) วันพฤหัสบดีที่ ๒๘ พฤศจิกายน ๒๕๖๒ ที่ประชุมเห็นชอบให้ตั้งนายดล เหตระกูล เป็นกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม แทนตำแหน่งที่ว่าง

บัดนี้ คณะกรรมาธิการได้ดำเนินการพิจารณาศึกษาเรื่อง ความมั่นคงปลอดภัยไซเบอร์เสร็จเรียบร้อยแล้ว จึงขอรายงานผลการพิจารณาศึกษาเรื่องดังกล่าวต่อสภาผู้แทนราษฎร ตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๐

๑. การดำเนินงาน

๑.๑ คณะกรรมาธิการได้มีมติแต่งตั้ง นายพิศณุ พลพืชน์ ผู้บังคับบัญชากลุ่มงานคณะกรรมาธิการ การสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักกรรมาธิการ ๑ สำนักงานเลขาธิการสภาผู้แทนราษฎรทำหน้าที่เป็นผู้ช่วยเลขานุการประจำคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม ตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๓ วรรคสี่

๑.๒ คณะกรรมาธิการได้มีมติตั้งคณะอนุกรรมาธิการขึ้นคณะหนึ่ง เพื่อทำหน้าที่ติดตามและตรวจสอบการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ หรือกิจการอื่นที่คณะกรรมาธิการมอบหมาย ทั้งนี้ ตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๖ ซึ่งคณะอนุกรรมาธิการคณะนี้ ประกอบด้วย

๑. พันเอก เศรษฐพงค์ มะลิสุวรรณ	ประธานคณะอนุกรรมาธิการ
๒. นายสมเกียรติ ถนอมสินธุ์	รองประธานคณะอนุกรรมาธิการ คนที่หนึ่ง
๓. นางสาวภาดาท์ วรกานนท์	รองประธานคณะอนุกรรมาธิการ คนที่หนึ่ง
๔. นายชัยชนะ มิตรพันธ์	อนุกรรมาธิการ
๕. นายปรัชญา อนันตเมฆ	อนุกรรมาธิการ
๖. นายธเนศ กิตติธเนศวร	อนุกรรมาธิการ
๗. นางสาวภัคธภา ฉัตรโกเมศ	อนุกรรมาธิการ
๘. นางสาวนวพร สอดศรี	อนุกรรมาธิการ
๙. นายรัฐภูมิ โตคงทรัพย์	อนุกรรมาธิการ
๑๐. นายนพดล เทียมนรา	อนุกรรมาธิการและเลขานุการ

อนึ่ง เมื่อวันที่ นางสาวชลิดา อภิบาลภูธร ได้ลาออกตำแหน่งอนุกรรมาธิการและในคราวการประชุมคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม ครั้งที่ ๓๑ เมื่อวันพฤหัสบดีที่ ๙ กรกฎาคม ๒๕๖๓ ที่ประชุมเห็นชอบให้ตั้งนางสาวนวพร สอดศรี เป็นอนุกรรมาธิการติดตามและตรวจสอบการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ ในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม แทนตำแหน่งที่ว่าง

๒. วิธีการพิจารณาศึกษา

๒.๑ คณะกรรมาธิการได้จัดให้มีการประชุม จำนวน ๓ ครั้ง

๒.๒ คณะกรรมาธิการได้ดำเนินการโดยเชิญหน่วยงานมาให้ข้อมูลข้อเท็จจริงและประกอบการพิจารณา ดังนี้

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๑. นายภุชพงค์ โนดไธสง	รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
๒. นายปฐมพงษ์ ขาวจันทร์	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๓. นางสุนทรีย์ ส่งเสริม	นักวิชาการคอมพิวเตอร์ชำนาญการ
๔. นายภัทรพงษ์ ลือชัย	นิติกรชำนาญการ
๕. นางกนิษฐกา พานิชชอบ	นิติกรปฏิบัติการ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นายปริญญา หอมเอนก	กรรมการผู้ทรงคุณวุฒิด้านรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงานส่งเสริมเศรษฐกิจดิจิทัล

รองศาสตราจารย์ธีรณี อจลากุล	ผู้อำนวยการสถาบันส่งเสริมการวิเคราะห์และบริหารข้อมูลขนาดใหญ่ภาครัฐ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

นายชัยชนะ มิตรพันธ์	รองผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

๓. ผลการพิจารณาศึกษา

คณะกรรมาธิการขอรายงานผลการพิจารณาศึกษาเรื่อง ความมั่นคงปลอดภัยไซเบอร์ โดยคณะกรรมาธิการได้มอบหมายให้คณะอนุกรรมาธิการติดตามและตรวจสอบการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ ดำเนินการพิจารณาศึกษากรณีดังกล่าว ซึ่งคณะกรรมาธิการได้พิจารณารายงานของคณะอนุกรรมาธิการด้วยความละเอียดรอบคอบแล้ว และได้มีมติให้ความเห็นชอบกับรายงานดังกล่าว โดยถือเป็นรายงานการศึกษาของคณะกรรมาธิการ

จากการพิจารณาศึกษาเรื่องดังกล่าวข้างต้น คณะกรรมาธิการจึงขอเสนอรายงานการพิจารณาศึกษาของคณะกรรมาธิการ โดยมีรายละเอียดตามรายงานท้ายนี้ เพื่อให้สภาผู้แทนราษฎรได้พิจารณา หากสภาผู้แทนราษฎรให้ความเห็นชอบด้วยกับผลการพิจารณาศึกษาของคณะกรรมาธิการ ขอให้โปรดแจ้งไปยังคณะรัฐมนตรีเพื่อพิจารณาและดำเนินการตามแต่จะเห็นสมควรต่อไป ทั้งนี้ เพื่อประโยชน์ของประเทศชาติและประชาชนสืบไป

บทสรุปผู้บริหาร

ในปัจจุบัน การบริการของกิจการโทรคมนาคมและเทคโนโลยีสารสนเทศบนโลกไซเบอร์ ได้กลายเป็นหนึ่งในปัจจัยที่สำคัญของการประกอบกิจการทั้งภาครัฐ และภาคเอกชน ตลอดจนการดำเนินชีวิตประจำวันของภาคประชาชนในยุคเศรษฐกิจดิจิทัล ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์กำลังเพิ่มสูงขึ้น ทั้งในด้านปริมาณและผลกระทบจึงเป็นประเด็นที่สำคัญอย่างยิ่งสำหรับการให้บริการที่มีเสถียรภาพ ต่อเนื่อง มีความมั่นคงและปลอดภัยต่อผู้ใช้บริการและผู้ให้บริการ

กรอบนโยบายและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ อ้างอิงได้ ๒ แนวทางหลัก คือ NIST CSF ของสหรัฐอเมริกา ซึ่งมีลักษณะเป็นข้อเสนอนำให้นำไปปฏิบัติตามความสมัครใจ และ NIS Directive ของสหภาพยุโรป ซึ่งมีลักษณะเป็นกฎหมายบังคับที่มีบทลงโทษชัดเจน ส่วนรายละเอียดสำหรับการกำหนดนโยบาย สามารถอ้างอิงได้จากมาตรฐานต่าง ๆ เช่น มาตรฐาน ISO/IEC 27001 : 2013 (Information Security Management Systems: ISMS) ว่าด้วยข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และสถาปัตยกรรม ITU-T X. 805 สำหรับกรอบการดำเนินงานด้านความมั่นคงปลอดภัยบนเครือข่ายการสื่อสาร กรอบแนวทางการกำกับดูแลทั้งแบบ NIST CSF และ NIS Directive ได้มีการนำมาใช้เป็นแนวทางการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ อาทิ ประเทศมาเลเซีย สหราชอาณาจักร และเอสโตเนีย เป็นต้น

สำหรับสถานการณ์กำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย มีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตั้งแต่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๒ ปัจจุบันได้ผ่านขั้นตอนการจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. (National Cyber Security Committee หรือ NCSC) ซึ่งมีหน้าที่กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และอยู่ในระหว่างการดำเนินการจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. มีหน้าที่กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและแนวทางปฏิบัติ ตลอดจนประสานงานเมื่อเผชิญเหตุภัยคุกคามไซเบอร์ ซึ่งมีด้วยกัน ๘ ด้าน ได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่น ๆ ตามที่ กกม. กำหนดเพิ่มเติม การรับมือภัยคุกคามทางไซเบอร์ จะแบ่งเกณฑ์พิจารณาเป็น ๓ ระดับ ได้แก่ ระดับไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤติ อย่างไรก็ดี ยังมีรายละเอียดที่ยังต้องเร่งดำเนินการเพื่อทำให้เกิดความชัดเจนสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในทางปฏิบัติตามที่ได้บัญญัติไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ดังนั้น ข้อเสนอแนะแนวทางการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สำหรับระยะเวลา ๓ ปี (พ.ศ.๒๕๖๓ – ๒๕๖๕) ที่สอดคล้องกับบริบทของประเทศไทย จึงแบ่งออกเป็นการสร้างการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง

๗ ด้านจากภาครัฐซึ่งเปรียบเสมือนไข่แดง และการสนับสนุนการสร้างระบบนิเวศน์ที่เหมาะสมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงภาคเอกชน ผู้ใช้งาน และผู้มีส่วนเกี่ยวข้องต่าง ๆ เรียกว่า Public Private Partnerships หรือ PPP ซึ่งเปรียบเสมือนไข่ขาว ตามระยะเวลาที่เหมาะสม ดังนี้

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๓

๑) ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

ควรติดตามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee หรือ NCSC) ในการเร่งผลักดันให้เกิดการจัดตั้งคณะทำงานในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ได้แก่

- คณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กกม.)
- คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
- การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและผู้รับผิดชอบแต่ละหน่วยงานที่เกี่ยวข้อง ให้ครบองค์ประกอบสำหรับการดำเนินงานกำกับดูแล
- การจัดทำแผนงบประมาณที่จำเป็นและสอดคล้องสำหรับการดำเนินการที่เกี่ยวข้องกับแผนพัฒนาและการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ให้ทันสำหรับการพิจารณางบประมาณปี พ.ศ. ๒๕๖๔
- การกำหนดนิยาม ขอบเขต และองค์กรต่าง ๆ ที่เข้าข่ายอยู่ในการกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน
- การกำหนดหน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๘ ด้านให้ครบสมบูรณ์
- การกำหนดลักษณะข้อมูลสำคัญสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์
- การกำหนดแผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับเทคโนโลยีการสื่อสาร 5G และกิจการระบบพิสูจน์และยืนยันตัวตน ระยะ ๓ ปี และ ๕ ปี

หมายเหตุ: การจัดตั้ง กกม. และ กบส. ตลอดจนการแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ที่ได้แล้วเสร็จในเดือนตุลาคม ๒๕๖๔ ที่ถือได้ว่าเป็นความก้าวหน้าที่สำคัญ แต่ยังมีความล่าช้าจากแผนการดำเนินการ ทำให้อาจต้องปรับระยะเวลาของแผนที่นำเสนอตามความเหมาะสม ดังนั้น คณะกรรมาธิการควรเร่งรัดติดตามให้แผนการจัดทำงบประมาณในขั้นตอนนี้เสร็จสมบูรณ์โดยเร็วที่สุดเท่าที่จะเป็นไปได้ อาทิ จัดทำร่างกรอบโครงสร้างและอัตรากำลัง จัดทำร่างแผนปฏิบัติการระยะ ๓ ปี (พ.ศ. ๒๕๖๓ – ๒๕๖๕) จัดทำกรอบวงเงินงบประมาณปี ๒๕๖๔ – ๒๕๖๕ ในการขอทุนประเดิม จัดทำร่างคำขอจัดกลุ่มองค์การมหาชนของ สกมช. จัดทำร่างข้อบังคับ กบส. ว่าด้วยการบริหารงานบุคคล และจัดทำร่างข้อบังคับ กบส. ว่าด้วยการบริหารงานการเงิน บัญชี งบประมาณ และทรัพย์สิน และภารกิจที่สำคัญอีกด้านคือ

การจัดทำกฎหมายลำดับรอง ซึ่งอยู่ระหว่างดำเนินขั้นตอนการดำเนินการภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒) ด้านการกำกับดูแลความมั่งคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานกำกับดูแลโครงข่ายสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่ได้ถูกกำหนดจากคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ควรเร่งดำเนินการ

- การประเมินสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน ซึ่งอาจมีความพร้อมของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่เท่ากัน โดยอาจใช้ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์จากต่างประเทศที่ได้มาตรฐาน

- การจัดทำแผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานระยะ ๓ ปี และ ระยะ ๕ ปี ตลอดจนกำหนดให้มีการดำเนินการตรวจสอบ ทั้งนี้ ควรมีการผลักดันให้แผนนำทางของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน แล้วเสร็จทันตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่เลื่อนการบังคับใช้ไปจนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๔ ตามความพร้อมของหน่วยงาน

๓) ด้านการพัฒนาสร้างระบบนิเวศน์ไซเบอร์ (Ecosystem) ของประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติควรมีการเริ่มดำเนินการที่เกี่ยวข้องกับการสร้างระบบนิเวศน์ไซเบอร์สำหรับประเทศ คู่ขนานกับกิจการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ควรมีบทบาทเป็นผู้อำนวยความสะดวก (Facilitator) หรือ ผู้ฝึกสอน (Coaching) คอยส่งเสริมและสนับสนุนให้องค์กรเอกชนสามารถเกิดความมั่นคงปลอดภัยไซเบอร์ภายในองค์กรได้ด้วยตัวเอง เน้นสนับสนุนการพัฒนาด้านบุคลากรรองรับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรทั้งภาครัฐ และภาคเอกชนที่จะเกิดขึ้น ได้แก่

- การจัดตั้งศูนย์พัฒนาและปฏิบัติการด้านความมั่นคงไซเบอร์ และการจัดศูนย์สอบวัดระดับความชำนาญด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้มาตรฐานสากล

- นโยบายอื่น ๆ ตลอดจนการประสานงานระหว่างหน่วยงานรัฐอื่น ๆ ที่เกี่ยวข้องในการสนับสนุนการผลิตบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๔

๑) ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

ติดตามคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ต่อเนื่องจากการดำเนินการก่อนหน้าให้เกิดความสมบูรณ์ ได้แก่

- นิยาม ขอบเขต และ หน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศและองค์กรต่าง ๆ ที่เข้าข่ายอยู่ในการกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน

- ลักษณะข้อมูลสำคัญสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

- กำหนดกรอบ หรือนโยบายสำหรับสนับสนุนการประสานความร่วมมือกับหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่กำหนดไว้แล้วทั้งในภาวะปกติ และภาวะฉุกเฉิน

- ตรวจประเมิน แผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี และ ๕ ปี ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- จัดตั้งกองทุนเพื่อการพัฒนายกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกองทุนเพื่อการสนับสนุนการสร้างระบบนิเวศน์ไซเบอร์ โดยมีการกำกับดูแลจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒) ด้านการกำกับดูแลความมั่งคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานกำกับดูแลโครงข่ายสร้างพื้นฐานสำคัญทั้ง ๗ ด้านควรเร่งดำเนินการ

- สรุปการประเมินสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน

- จัดตั้งส่วนงานที่มีหน้าที่ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะสำหรับหน่วยงานกำกับดูแล แยกออกจากส่วนงานเทคโนโลยีสารสนเทศขององค์กร

- เสนอแผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี และ ระยะ ๕ ปี ของแต่ละหน่วยงานที่รองรับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓) ด้านการพัฒนาสร้างระบบนิเวศน์ไซเบอร์ (Ecosystem) ของประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ/หรือองค์กรกำกับดูแลอื่น ๆ ที่มีส่วนเกี่ยวข้อง ควรมีการร่วมกันดำเนินการต่าง ๆ ที่สนับสนุนการสร้างระบบนิเวศน์ไซเบอร์สำหรับประเทศอย่างต่อเนื่องจากแผนปี พ.ศ. ๒๕๖๓ ได้แก่

- สนับสนุนนโยบายต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาด้านบุคลากรรองรับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้จัดทำในปี พ.ศ. ๒๕๖๓ อย่างต่อเนื่อง

- กำหนดกรอบมาตรฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการแบ่งปัน

- ออกมาตรการสนับสนุนทางภาษี สำหรับองค์กรที่มีการดำเนินการได้มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับต่าง ๆ

- กำหนดนโยบายสนับสนุนการส่งเสริมให้ประเทศเป็นศูนย์กลางการรักษาความมั่นคงปลอดภัยไซเบอร์ชั้นนำของภูมิภาค (Cybersecurity Hub)

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๕

๑) ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

ดำเนินการตรวจประเมินผลการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามแผนยกระดับที่ได้ดำเนินการไปในปี ๒๕๖๔ และติดตามการดำเนินการของกองทุนเพื่อการพัฒนายกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกองทุนเพื่อการสนับสนุนการสร้างระบบนิเวศน์ไซเบอร์

๒) ด้านการกำกับดูแลความมั่งคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ดำเนินการต่อเนื่องจากแผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๓ และปี พ.ศ. ๒๕๖๔ เพื่อการปรับปรุงและพัฒนาแผนยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓) ด้านการพัฒนาสร้างระบบนิเวศน์ไซเบอร์ (Ecosystem) ของประเทศ

สนับสนุนการพัฒนาระบบนิเวศน์ไซเบอร์ให้ครอบคลุมด้านต่าง ๆ โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ/หรือองค์กรกำกับดูแลอื่น ๆ ที่เกี่ยวข้อง เป็นแกนหลักในการผลักดันให้ทุกภาคส่วนมีความเข้มแข็งทางความมั่นคงปลอดภัยไซเบอร์ มุ่งให้ประเทศเป็นศูนย์กลางการรักษาความมั่นคงปลอดภัยไซเบอร์ชั้นนำของภูมิภาค (Cybersecurity Hub) สร้างเป็นสังคมที่มีภูมิคุ้มกันต่อการต้านเหตุภัยไซเบอร์แบบยั่งยืน ดังนี้

- ด้านฐานข้อมูลความมั่นคงปลอดภัยไซเบอร์ ควรมีนโนบายสร้างแรงจูงใจในการสนับสนุนองค์กรภาคเอกชนให้มีการจัดตั้งดูแลด้านความมั่นคงปลอดภัยไซเบอร์ตามระดับขีดความสามารถขององค์กรที่เหมาะสม และนโยบายสนับสนุนกลไกการสร้างความน่าเชื่อถือ และความเชื่อใจในการแบ่งปันข้อมูลสำหรับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ในอนาคต

- ด้านการสร้างความตระหนักรู้ โดยมีนโยบายการส่งเสริมให้เกิดกิจกรรมความมั่นคงปลอดภัยไซเบอร์กับการดำเนินชีวิตของภาคประชาชนโดยทั่วไป ให้มีความเข้าใจที่ถูกต้องในการใช้งานบนโลกออนไลน์อย่างถูกวิธีและด้วยความมั่นใจ ลดความเสี่ยงและสามารถปกป้องตนเองจากภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ

- ด้านการวิจัยและพัฒนา อาจเป็นการสนับสนุนการจัดการรวมกลุ่มของภาคการวิจัยและภาคอุตสาหกรรม เพื่อเพิ่มโอกาสการพบปะ แลกเปลี่ยนความคิด และความต้องการให้มีทิศทางเดียวกัน เกิดประโยชน์จริงในทางปฏิบัติ มีการจัดตั้งกองทุนสนับสนุนการวิจัยที่เกี่ยวข้อง สร้างการประสานงานในกลุ่มองค์กรภาคการศึกษา ไม่ให้เกิดงานวิจัยซ้ำซ้อน สร้างแรงจูงใจให้มีงานวิจัยตามสาขาที่ตรงต่อความต้องการของอุตสาหกรรม เพื่อการพัฒนาเครื่องมือในการช่วย ปกป้อง ตรวจจับ และปรับตัว ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทันทุกสถานการณ์

สารบัญ

สารบัญ

สารบัญภาพ

หน้า

สารบัญตาราง

หน้า

บทที่ ๑
บทนำ

๑.๑ ความเป็นมา

ในปัจจุบัน การบริการของกิจการโทรคมนาคมและเทคโนโลยีสารสนเทศได้เป็นรากฐานของการประกอบกิจการทั้งภาครัฐ ภาคเอกชน และภาคประชาชน จนเป็นหนึ่งในปัจจัยที่สำคัญของการดำเนินชีวิตประจำวันในยุคเศรษฐกิจดิจิทัล จึงควรคำนึงถึงการให้บริการที่มีเสถียรภาพและต่อเนื่องตลอดเวลา เพื่อให้เกิดความมั่นคงและปลอดภัยต่อผู้ใช้บริการและผู้ให้บริการนอกเหนือไปจากการกำกับดูแลกิจการให้มีความเท่าเทียมและทั่วถึง[๑] [๒]

ในปัจจุบัน ความมั่นคงและปลอดภัยไซเบอร์อาจไม่ได้เป็นเพียงการกำกับดูแลระบบเครือข่ายเพียงอย่างเดียว เมื่อเทคโนโลยีสารสนเทศและการให้บริการด้านข้อมูลได้กลายเป็นส่วนของการให้บริการในกิจกรรมแต่ละภาคส่วนในการดำเนินการที่สำคัญของประเทศด้านต่าง ๆ ซึ่งก่อให้เกิดประเด็นใหม่ที่มีความท้ายทาย เช่นการรั่วไหลและบิดเบือนของข้อมูล ภัยคุกคามไซเบอร์ที่มีต่อโครงสร้างพื้นฐานสำคัญของประเทศ อาทิ โครงข่ายไฟฟ้าอัจฉริยะ (Smart Grid) โครงข่ายอินเทอร์เน็ตของสรรพสิ่ง (IoT) ตลอดจนโครงข่ายเทคโนโลยีคลาวด์ (Cloud Networks) เป็นต้น แนวทางการจัดการกับมาตรฐานการสร้างความปลอดภัยไซเบอร์จึงไม่เพียงแต่การคำนึงถึงความมั่นคงปลอดภัยบนระบบเครือข่าย แต่ควรให้ความสำคัญครอบคลุมถึงปัญหาด้านข้อมูลที่อยู่บนเครือข่าย เช่น การรักษาความลับ ความถูกต้อง และความพร้อมในการเข้าถึงข้อมูลด้วย

จากรายงานเรื่อง “The Global Risks Report 2018, 13th Edition” โดย World Economic Forum (World Economic Forum, 2018) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์กำลังเพิ่มสูงขึ้น ทั้งในด้านปริมาณและผลกระทบในช่วงห้าปีที่ผ่านมา จำนวนภัยคุกคามไซเบอร์ได้เกิดขึ้นกับภาคธุรกิจเพิ่มขึ้นเป็นเกือบสองเท่า และถือเป็นความเสี่ยงที่มีแนวโน้มจะเกิดขึ้นได้มากที่สุดเป็นอันดับ ๓ และอาจก่อให้เกิดผลกระทบมากที่สุดเป็นอันดับ ๖

ในช่วงหลายปีที่ผ่านมา กลุ่มอาชญากรไซเบอร์ได้พัฒนาความรู้ ความสามารถและเครื่องมือที่จำเป็นในการจัดการกับโครงสร้างพื้นฐานสำคัญของประเทศและระบบที่เกี่ยวข้อง จนทำให้เกิดการหยุดชะงักของการให้บริการเป็นบริเวณกว้าง และอาจส่งผลให้เกิดการหยุดชะงักของภาคเศรษฐกิจและสังคม จนอาจกลายเป็นปัญหาระดับโลกได้ เช่น การทำให้ระบบการจ่ายไฟฟ้าของประเทศยูเครนเป็นอัมพาต ส่งผลกระทบต่อผู้ใช้ไฟฟ้ากว่า ๒๒๕,๐๐๐ ครัวเรือน[๓]

---

[๑] แผนแม่บทกิจการโทรคมนาคม ฉบับที่ ๑ (พ.ศ. ๒๕๕๕ - ๒๕๕๙), ราชกิจจานุเบกษา, ๒๕๕๕.

[๒] แผนแม่บทกิจการโทรคมนาคม ฉบับที่ ๒ (พ.ศ. ๒๕๖๒ - ๒๕๖๖), ราชกิจจานุเบกษา, ๒๕๖๑.

[๓] Reuters, (2016).

ความเสียหายทางการเงินอันเกิดจากอาชญากรรมไซเบอร์ไม่เพียงแต่ส่งผลต่อภาคเศรษฐกิจและสังคมโดยตรง แต่การตกเป็นเป้าหมายของอาชญากรรมไซเบอร์ส่งผลให้เกิดการสูญเสียความเชื่อมั่นจากผู้ใช้บริการ คุณค่าและความน่าเชื่อถือขององค์กรย่อมลดลงไปอย่างหลีกเลี่ยงไม่ได้ เป็นผลกระทบต่อภาคธุรกิจในทางอ้อมและภาคเศรษฐกิจโดยรวมที่มิควรละเลยความสำคัญเช่นเดียวกัน มีการคาดการณ์ว่า ความเสียหายทางการเงินอันเกิดจากอาชญากรรมไซเบอร์เพิ่มขึ้นเป็นเท่าตัวจากปี ค.ศ. ๒๐๑๕ ที่ ๓ แสนล้านเหรียญสหรัฐ ไปเป็นประมาณ ๖ แสนล้านเหรียญสหรัฐในปี ค.ศ. ๒๐๒๑[๔]

นอกเหนือไปจากนี้ ประเด็นสมรภูมิแห่งสงครามการค้าในยุคดิจิทัลที่เกิดขึ้นไม่เพียงระดับภายในประเทศ แต่รวมไปถึงระดับระหว่างประเทศ ซึ่งเกี่ยวข้องกับการเปิดเผยข้อมูลส่วนบุคคลของผู้บริโภคแต่ละประเทศ ตลอดจนการหลบเลี่ยงภาษีและกฎหมายอื่น ๆ ของธุรกิจดิจิทัลข้ามชาติทำให้เกิดการทบทวน และผ่านกฎหมายเพื่อปกป้องอธิปไตยทางอินเทอร์เน็ตของบางประเทศให้อำนาจในการตัดขาดระบบอินเทอร์เน็ตของชาติออกจากโลกภายนอก ป้องกันภัยคุกคามทางไซเบอร์ และทำให้อินเทอร์เน็ตภายในประเทศสามารถดำเนินการต่อไปได้[๕]

สำหรับประเทศไทย ในระดับนานาชาติ มีรายงานปัญหาด้านอาชญากรรมไซเบอร์ของกลุ่มอาชญากรข้ามชาติ ซึ่งใช้เซิร์ฟเวอร์ที่ตั้งอยู่ในเขตของมหาวิทยาลัยธรรมศาสตร์ เพื่อเป็นฐานปฏิบัติการโจมตีระบบโครงสร้างพื้นฐานใน ๑๗ ประเทศทั่วโลก ภายใต้ชื่อปฏิบัติการ GhostSecret [๖] และจากการสำรวจในระดับองค์กรจากผู้เข้าร่วมสำรวจที่มีอำนาจการตัดสินใจระดับสูง (Senior Decision Makers) ๒๖๑ คน แนวโน้มของอาชญากรรมไซเบอร์ในประเทศไทยเพิ่มขึ้นสูงอย่างมีนัยสำคัญ ตั้งแต่ พ.ศ. ๒๕๕๔ และมีองค์กรเพียงร้อยละ ๒๖ ของการสำรวจ เท่านั้น ที่มีการวางแผนรับมืออย่างเต็มรูปแบบ ซึ่งต่ำกว่าค่าเฉลี่ยของโลกที่ร้อยละ ๓๗ ของการสำรวจ (PWC, 2016) ส่วนในระดับผู้บริโภค เหตุอาชญากรรมทางคอมพิวเตอร์ในประเทศไทย มักเป็นการอาศัยช่องโหว่ในการปลอมแปลงเป็นผู้เสียหาย และหลอกลวงเอาทรัพย์สินจากบุคคลใกล้ชิดบนสังคมออนไลน์ การปลอมแปลงเอกสารส่วนตัว เช่น บัตรประชาชน เพื่อเข้าสู่ระบบการธนาคารอินเทอร์เน็ต (Internet Banking) และโอนเงินออก ตลอดจนการเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต (Hacking) และปลอมแปลงเอกสารของผู้ประกอบการในขณะตกลงทำธุรกรรมซื้อขาย ทำให้เกิดความเสียหายทางธุรกิจ อาชญากรรมไซเบอร์หลากหลายรูปแบบที่เกิดขึ้นเหล่านี้ ภาครัฐจำเป็นต้องสร้างความรู้ความเข้าใจให้กับประชาชนและผู้ประกอบการที่เกี่ยวข้องในการใช้อินเทอร์เน็ต

---

[๔] Cybersecurity Ventures, (2017), Cybercrime Report.

[๕] อธิป อัศวานันท์, “อธิปไตยทางอินเทอร์เน็ต การโต้กลับของจักรวรรดิ”, กรุงเทพธุรกิจ, ๒๕๖๓.

[๖] แฮ็กเกอร์เกาหลีเหนือเจาะเซิร์ฟเวอร์ธรรมศาสตร์เป็นฐานโจรกรรมข้อมูลการเงินทั่วโลก, ไทยโพสต์, ๒๕๖๑.

อย่างระมัดระวัง และมีมาตรการที่เหมาะสมสำหรับผู้ให้บริการ เพื่อป้องกันเหตุอาชญากรรมอย่างมีประสิทธิภาพ[๗]

ดังที่กล่าวมาเบื้องต้นทั้งหมดนั้น ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญระดับโลกเกี่ยวข้องกับอาชญากรรมข้ามชาติหรือได้รับการสนับสนุนจากรัฐบาล มีแรงจูงใจที่หลากหลาย ทั้งเพื่อผลประโยชน์ทางการเงิน ข้อมูลความลับทางการค้า ข้อมูลส่วนบุคคล ไปจนถึงเพื่ออุดมการณ์บางอย่าง จนเกิดผลกระทบต่อโครงสร้างพื้นฐานสำคัญของประเทศ ทั้งในรูปการปฏิเสธการเข้าใช้บริการ ผลกระทบด้านความมั่นคง ผลกระทบทางการเงิน การฟ้องร้องในชั้นศาล การเสียชื่อเสียง การสูญเสียความสามารถในการแข่งขัน และการสูญเสียความมั่นใจของลูกค้า เป็นต้น

๑.๑.๑ คำนิยามที่เกี่ยวข้อง

เนื่องจากคำนิยามที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่ใช้กันปัจจุบันมีความหมายได้หลากหลาย ไม่ชัดเจน ซ้ำซ้อน และอาจเปลี่ยนแปลงตามการนำไปใช้งานของแต่ละองค์กร ในเอกสารชุดนี้ จึงขออ้างอิงคำนิยามจากมาตรฐาน ISO/IEC 27032 : 2012 ซึ่งแสดงเป็นความสัมพันธ์ไว้ตามรูปที่ ๑ ดังนี้

- โลกไซเบอร์ (Cyberspace) หมายถึง สิ่งแวดล้อมที่ซับซ้อนอันเกิดจากการปฏิสัมพันธ์ระหว่างมนุษย์ ซอฟต์แวร์ และบริการต่าง ๆ บนอินเทอร์เน็ต ด้วยการใช้เทคโนโลยีผ่านอุปกรณ์และเครือข่ายที่เชื่อมโยงถึงกัน โดยไม่ปรากฏรูปในทางกายภาพความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) หมายถึง การปกป้องรักษาความเป็นความลับ ความถูกต้อง และความพร้อมในการเข้าถึงของข้อมูลภายในโลกไซเบอร์

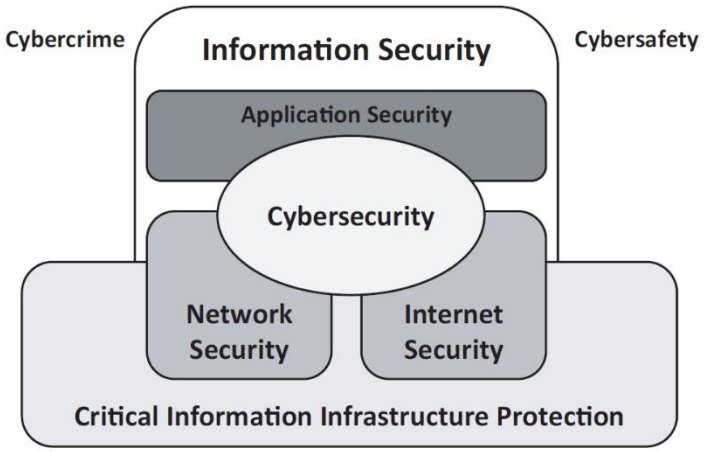
- ความมั่นคงปลอดภัยของข้อมูล (Information Security) หมายถึง การปกป้องรักษาความเป็นความลับ ความถูกต้อง และความพร้อมในการเข้าถึงของข้อมูลโดยทั่วไปทั้งที่อยู่และไม่อยู่ในโลกไซเบอร์ เพื่อตอบสนองต่อความต้องการของผู้ใช้บริการข้อมูลนั้น

- ความมั่นคงปลอดภัยของแอปพลิเคชัน (Application Security) หมายถึง กระบวนการที่ถูกนำไปปฏิบัติเพื่อควบคุมและวัดผลแอปพลิเคชันในองค์กร อันเป็นส่วนหนึ่งของการบริหารจัดการความเสี่ยงของการใช้แอปพลิเคชันนั้น มาตรการดังกล่าวอาจถูกนำไปใช้กับตัวแอปพลิเคชัน ข้อมูลที่เกี่ยวข้องและส่วนอื่น ๆ ไม่ว่าจะเป็นเทคโนโลยี กระบวนการ และผู้เกี่ยวข้องทั้งหมดในวงจรชีวิตของแอปพลิเคชัน

- ความมั่นคงปลอดภัยของเครือข่าย (Network Security) หมายถึง การออกแบบการลงมือทำ และการปฏิบัติงานบนเครือข่าย เพื่อจุดประสงค์ในการรักษาความมั่นคงปลอดภัยของข้อมูลบนเครือข่ายภายในองค์กร ระหว่างองค์กร และระหว่างองค์กรกับผู้ใช้บริการ

---

[๗] แฉกลลวง! เตือน “ผู้ใช้” พึงระวัง ตกเป็นเหยื่อ อาชญากรตุ๋นโลกไซเบอร์, ไทยรัฐออนไลน์, ๒๕๕๙.



รูปที่ ๑ : ความสัมพันธ์ระหว่างความมั่นคงปลอดภัยในด้านต่าง ๆ (ISO/IEC, 2012)

- ความมั่งคงปลอดภัยของอินเทอร์เน็ต (Internet Security) หมายถึง การปกป้องบริการที่เกี่ยวข้องกับอินเทอร์เน็ต รวมไปถึงระบบและเครือข่ายสื่อสารสารสนเทศ ซึ่งถือเป็นส่วนขยายจากการรักษาความมั่นคงปลอดภัยของเครือข่าย ภายในองค์กรและภายในบ้าน เพื่อให้สามารถรักษาความมั่นคงปลอดภัยโดยรวมได้อย่างสมบูรณ์ โดยหมายรวมถึง การรักษาความพร้อมในการเข้าถึงและความน่าเชื่อถือของบริการบนอินเทอร์เน็ตอีกด้วย

- การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure Protection) หมายถึง การปกป้องระบบที่ทำหน้าที่ให้บริการสารสนเทศหรือเป็นส่วนหนึ่งของการปฏิบัติงานของผู้ให้บริการโครงสร้างพื้นฐานสำคัญ เช่น พลังงาน การสื่อสารโทรคมนาคม และการประปา เพื่อให้ระบบและเครือข่ายที่เกี่ยวข้องสามารถดำเนินงานได้อย่างราบรื่น แม้จะมีความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล ความมั่นคงปลอดภัยของเครือข่ายและความมั่นคงปลอดภัยไซเบอร์โดยรวมก็ตาม

ตามความสัมพันธ์การนิยามความมั่นคงปลอดภัยในด้านต่าง ๆ ในรูปที่ ๑ จะเห็นได้ว่าความมั่นคงปลอดภัยในแต่ละด้าน มีความหมายครอบคลุมจุดประสงค์และมุ่งเน้นปกป้องในจุดที่แตกต่างกัน และมีการทับซ้อนกัน เช่น ความมั่นคงปลอดภัยของข้อมูลมุ่งเน้นการปกป้องข้อมูลทั้งที่อยู่และไม่อยู่ในโลกไซเบอร์ ได้แก่ ข้อมูลในกระดาษ ส่วนความมั่นคงปลอดภัยของเครือข่ายมุ่งเน้นการปกป้องเครือข่าย ซึ่งส่วนประกอบของเครือข่ายก็มีทั้งส่วนที่อยู่และไม่อยู่ในโลกไซเบอร์

โดยทั่วไป คำว่า Cybersecurity และ Information Security มีการใช้อย่างแพร่หลาย และมักใช้แทนกันในบางบริบทแบบกว้าง ๆ โดยไม่มีข้อกำหนดหรือนิยามที่ชัดเจน ส่วน Network and Information Security มักถูกนำมาใช้เมื่อมีการกล่าวถึงนโยบายในรายละเอียดหรือมาตรการกำกับดูแลในกรณีที่ต้องการเน้นด้านความมั่นคงปลอดภัยบนเครือข่ายและข้อมูล

อย่างไรก็ดี การบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลที่เน้นรากฐานที่สำคัญด้านความมั่นคงปลอดภัยของเครือข่ายเพียงอย่างเดียว ไม่เพียงพออีกต่อไปในปัจจุบัน

จำเป็นต้องอาศัยกลไกที่เกี่ยวข้องอย่างรอบด้าน ความมั่นคงปลอดภัยไซเบอร์ จึงเป็นการอ้างอิงที่เกี่ยวข้องกับความมั่นคงปลอดภัยในโลกไซเบอร์ในภาพรวม ส่วนความมั่นคงปลอดภัยของเครือข่ายจะเป็นการอ้างอิงที่เกี่ยวข้องกับเครือข่ายโดยเฉพาะ

๑.๒ วัตถุประสงค์

๑.๒.๑ สร้างความเข้าใจและการตระหนักถึงความสำคัญของความมั่นคงปลอดภัยไซเบอร์ในภาพรวม

๑.๒.๒ สรุปทบทวนกรณีศึกษาแนวทางการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

๑.๒.๓ สรุปสถานะปัจจุบันด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

๑.๒.๔ เสนอกรอบแนวทางการพัฒนาและการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

๑.๓ วิธีการพิจารณา/วิธีการดำเนินงาน

เอกสารรายงานผลการศึกษาฉบับนี้ อาศัยการค้นคว้า รวบรวม และวิเคราะห์ โดยอ้างอิงข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ จากแหล่งข้อมูลต่าง ๆ ได้แก่ เอกสารรายงานฉบับสมบูรณ์การศึกษามาตรการสร้างความปลอดภัยบนเครือข่าย ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) บทสัมภาษณ์ผู้เชี่ยวชาญ ตลอดจนการสืบค้นข้อมูลจากฐานข้อมูลและฐานข้อมูลงานวิจัยออนไลน์

ทั้งนี้ เอกสารรายงานฉบับสมบูรณ์การศึกษามาตรการสร้างความปลอดภัยบนเครือข่ายของ กสทช. ได้ถูกใช้เป็นแหล่งข้อมูลอ้างอิงหลัก เนื่องจากได้มีการขยายความอ้างอิงองค์ความรู้พื้นฐาน รวมถึงมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การยกกรณีศึกษาในประเทศต่าง ๆ ข้อมูลแนวโน้มที่เกี่ยวข้อง บทสัมภาษณ์จากผู้เกี่ยวข้องจากหลากหลายภาคส่วน และการวิเคราะห์สถานะของประเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยบนเครือข่ายในการศึกษาดังกล่าว ซึ่งเป็นข้อมูลที่ค่อนข้างมีรายละเอียดครอบคลุม และตรงประเด็นสำหรับการขยายบริบทสำหรับการศึกษาความมั่นคงปลอดภัยไซเบอร์นี้

๑.๔ กรอบแนวทางในการศึกษา

ในการศึกษาฉบับนี้ เป็นการศึกษาข้อมูลพื้นฐาน สถานะปัจจุบันด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ร่วมกับข้อมูลอ้างอิงจากแหล่งต่าง ๆ นำไปสู่การวิเคราะห์ช่องว่างเพื่อการเสนอแนะแนวทางการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในระยะเวลาดำเนินการต่าง ๆ สร้างความตระหนักจากทุกภาคส่วนที่เกี่ยวข้อง เพื่อให้เข้าใจภาพรวมและเกิดความร่วมมือในการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ให้เป็นไปได้แบบยั่งยืนและยืดหยุ่นต่ออาชญากรรมไซเบอร์ที่เปลี่ยนแปลงได้อย่างรวดเร็ว

บทที่ ๒
การทบทวนวรรณกรรม

๒.๑ มาตรการที่เกี่ยวข้อง

๒.๑.๑ Directive on Security of Network and Information Systems หรือ NIS Directive เป็นกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ฉบับแรกของสหภาพยุโรป ถูกสร้างขึ้นเพื่อความปลอดภัยบนเครือข่ายและระบบข้อมูล โดยใช้มาตรฐานระดับสูงอย่างเท่าเทียมกันและเป็นไปในทิศทางเดียวกันทั่วทั้งประเทศสมาชิกสหภาพยุโรป ด้วยหลักปฏิบัติสามประการ คือ

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

๒. การเพิ่มความร่วมมือระหว่างประเทศสมาชิกทั้งในด้านนโยบายด้วยการแต่งตั้งกลุ่มความร่วมมือ (Cooperation Group) และเครือข่ายความร่วมมือระหว่างองค์กร CSIRT ระดับประเทศ (CSIRTs Network) โดยกลุ่มความร่วมมือ มีประธานสภาแห่งสหภาพยุโรปเป็นผู้นำ และมีผู้แทนจากประเทศสมาชิก ผู้แทนจากคณะกรรมาธิการยุโรปเป็นเลขาธิการ และองค์กรความปลอดภัยบนเครือข่ายและระบบข้อมูลของสหภาพยุโรป (European Union Agency for Network and Information Security หรือ ENISA) จัดตั้งขึ้นเพื่อสนับสนุนและประสานงานด้านความร่วมมือในระดับยุทธศาสตร์ และแลกเปลี่ยนข้อมูลกันระหว่างประเทศสมาชิก สร้างความเชื่อใจและความมั่นใจในการทำงานร่วมกัน ขับเคลื่อนการดำเนินงานต่าง ๆ ภายใต้ NIS Directive และมีหน้าที่รายงานผลการดำเนินงานต่อคณะกรรมาธิการยุโรปทุกหนึ่งปีครึ่งเพื่อประเมินผลของ NIS Directive ส่วนเครือข่ายความร่วมมือระหว่างองค์กร CSIRT ระดับประเทศ ประกอบด้วยผู้แทนจาก CSIRT ของประเทศสมาชิก และ CERT-c EU (Computer Emergency Response Team for the EU Institutions, Agencies and Bodies) ของสหภาพยุโรป สนับสนุนให้การปฏิบัติงานเป็นไปได้อย่างรวดเร็วและมีประสิทธิภาพเมื่อต้องทำงานร่วมกัน มีการรายงานผลการดำเนินงานในส่วนที่เกี่ยวข้องกับประสบการณ์ที่ได้รับจากการทำงานร่วมกัน บทสรุป และคำแนะนำต่อคณะกรรมาธิการยุโรปทุก ๑๘ เดือน เป็นส่วนหนึ่งในการประเมินผลของ NIS Directive อีกด้วย

๓. การกำหนดข้อบังคับด้านการบริหารจัดการความเสี่ยงและการรายงานผลกรณีที่เกิดเหตุ สำหรับผู้ให้บริการในกิจการที่มีความสำคัญ (Operators of Essential Services

หรือ OESs) สำหรับการดำรงอยู่ของกิจกรรมทางเศรษฐกิจและสังคมของประเทศ และผู้ให้บริการในกิจการดิจิทัล (Digital Service Providers หรือ DSPs) แต่ไม่รวมวิสาหกิจขนาดกลางและขนาดย่อมตามกฎหมาย Commission Recommendation 2003/362/EC โดยผู้ให้บริการในกิจการที่มีความสำคัญมีหน้าที่ใช้มาตรการด้านความปลอดภัยที่เหมาะสมและรายงานผลต่อองค์กรที่เกี่ยวข้องในกรณีที่มีเหตุภัยคุกคามขั้นรุนแรง ซึ่งพิจารณาระดับความรุนแรงจาก จำนวนผู้ใช้บริการที่ได้รับผลกระทบ ระยะเวลาที่เกิดเหตุ และพื้นที่ที่ได้รับผลกระทบ ส่วนผู้ให้บริการในกิจการดิจิทัลมีหน้าที่ใช้มาตรการด้านความปลอดภัยที่เหมาะสม มีลักษณะเดียวกันกับผู้ให้บริการในกิจการที่มีความสำคัญ และรายงานเหตุภัยคุกคามที่ส่งผลกระทบขั้นรุนแรงต่อองค์กรที่เกี่ยวข้อง หรือ CSIRT โดยพิจารณาความรุนแรงจากจำนวนผู้ใช้บริการที่ได้รับผลกระทบ ระยะเวลาที่เกิดเหตุ พื้นที่ที่ได้รับผลกระทบ ลักษณะการหยุดชะงักของบริการ และผลกระทบที่มีต่อภาคเศรษฐกิจและสังคม ซึ่งจะมีการกำหนดให้รายงานผลต่อองค์กรที่เกี่ยวข้อง หรือ CSIRT เมื่อมีเหตุให้ไม่สามารถให้บริการได้มากกว่า ๕ ล้านคนต่อชั่วโมง มีผู้ได้รับผลกระทบจากบริการที่หยุดชะงักมากกว่า ๑๐๐,๐๐๐ คน สร้างความเสียหายต่อความมั่นคงปลอดภัยของชีวิตและทรัพย์สินสาธารณะ หรือสร้างความเสียหายมากกว่า ๑ ล้านยูโร

๒.๑.๒ NIST Cybersecurity Framework (NIST CSF)

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology หรือ NIST) ถูกพัฒนาขึ้นเพื่อลดความเสี่ยงที่มีต่อโครงสร้างพื้นฐานสำคัญของประเทศ ๑๖ กลุ่ม ได้แก่ ภาคเคมีภัณฑ์ ภาคอุตสาหกรรมโทรคมนาคมสื่อสาร ภาคอุตสาหกรรมการผลิตที่สำคัญ เขื่อนการป้องกันฐานอุตสาหกรรม บริการช่วยเหลือในภาวะฉุกเฉิน พลังงาน บริการทางด้านการเงิน อุตสาหกรรมอาหารและการเกษตร การอำนวยความสะดวกภาครัฐ บริการดูแลสุขภาพและการสาธารณสุข เทคโนโลยีสารสนเทศ อุตสาหกรรมเกี่ยวกับนิวเคลียร์ ระบบขนส่ง ระบบน้ำและกำจัดน้ำเสีย อย่างไรก็ดี NIST CSF ไม่ใช่แนวทางและวิธีการกำกับดูแล แต่เป็นการรวบรวมมาตรฐาน แนวทาง ข้อเสนอแนะ และข้อควรปฏิบัติ เพื่อพัฒนาโปรแกรมด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กรที่มีเนื้อหาครอบคลุมประเด็นสำคัญด้านความมั่นคงปลอดภัยไซเบอร์อย่างครบถ้วนและมีความยืดหยุ่น สามารถนำไปปรับใช้ได้กับองค์กรทุกประเภทตามความต้องการ ความพร้อมและความเสี่ยง ทำให้ได้รับการยอมรับทั้งในสหรัฐอเมริกา ทั่วโลก รวมถึงประเทศไทย

รายละเอียดโครงสร้างกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์จะขออ้างอิงตามการอธิบายร่วมกับสถาปัตยกรรมด้านความมั่นคงปลอดภัยในหัวข้อ ๒.๒.๒

๒.๑.๓ COBIT 5

COBIT 5 เป็นกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการไอทีในระดับองค์กรซึ่งถูกกำหนดโดยหน่วยงานที่ไม่หวังผลกำไร Information Systems Audit and Control Association (ISACA) ช่วยให้องค์กรสามารถสร้างคุณค่าที่เกิดประโยชน์สูงสุดจาก

เทคโนโลยีสารสนเทศ (Information Technology หรือ IT) โดยการรักษาความสมดุลระหว่างประโยชน์ที่จะได้รับกับระดับความเสี่ยง และการใช้ทรัพยากรให้เกิดประโยชน์สูงสุดต่อองค์กร

กรอบการดำเนินงานของ COBIT 5 มีลักษณะเป็น Process Reference Model สามารถระบุความแตกต่างระหว่างกระบวนการกำกับดูแล (Governance Process) ที่มีแนวคิดตามมาตรฐาน ISO/IEC 38500 และกระบวนการบริหารจัดการ (Management Process) ซึ่งผู้บริหารจะวางแผน สร้าง ดำเนินการ และเฝ้าติดตามกิจกรรมต่าง ๆ เพื่อให้องค์กรสามารถกำหนดกรอบการดำเนินงานสำหรับการกำกับดูแลและการบริหารจัดการที่มีประสิทธิผล และบรรลุวัตถุประสงค์ขององค์กร โดยทำให้การใช้สารสนเทศและการลงทุนด้านเทคโนโลยีเกิดประโยชน์สูงสุด

๒.๑.๔ มาตรฐานเทคนิคที่เกี่ยวข้องกับ ITU

สหภาพโทรคมนาคมระหว่างประเทศ กลุ่มงานมาตรฐานโทรคมนาคม (International Telecommunication Union – Telecommunication Standardization หรือ ITU-T) ได้พัฒนามาตรฐานด้านความมั่นคงปลอดภัยเพื่อจัดการกับปัญหาด้านความมั่นคงปลอดภัยบนโลกไซเบอร์และปกป้องทุกภาคส่วนที่เกี่ยวข้อง ทั้งในการให้บริการ สนับสนุน และใช้งานเทคโนโลยีสารสนเทศ มีมาตรฐานทางเทคนิคที่สำคัญ คือ ITU-T X. 200 ที่สอดคล้องตามมาตรฐาน OSI (Open System Interconnection) เพื่อการสื่อสารแบบครบวงจร โดยได้กำหนดถึงมาตรฐานการบริหารความมั่นคงปลอดภัยในกิจกรรมต่าง ๆ เช่น การควบคุมและการป้องกันการเข้าสู่โครงข่าย และการใช้ทรัพยากรในโครงข่ายโทรคมนาคม การเฝ้าระวังและการรายงาน การกำหนดนโยบายด้านการตรวจสอบและการบริหารข้อมูลสารสนเทศที่เกี่ยวข้อง การบริหารจัดการความเสี่ยง ตลอดจนการบริหารจัดการทรัพยากร

นอกจากนี้ ITU-T ยังกำหนดและพัฒนามาตรฐานทางเทคนิคที่เกี่ยวข้องกับความมั่นคงปลอดภัย สำหรับกิจกรรมที่เกี่ยวข้องในการบริการสำคัญหลายชนิด รวมไปถึงมาตรฐานทางเทคนิคสำหรับแอปพลิเคชันใหม่ ๆ เช่น

- ITU-T X. 500 เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการพิสูจน์ตัวตนของผู้ขอเข้าใช้งาน ซึ่งได้รับการพัฒนาร่วมกับ ISO/IEC เป็นมาตรฐาน ISO/IEC/ITU X. 509 ในการสร้างระบบ PKI (Public Key Infrastructure)
- ITU-T X. 1120 - 1139 เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการให้บริการโทรคมนาคมเคลื่อนที่
- ITU-T X. 1180 - 1199 เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการให้บริการ IPTV
- ITU-T X. 1360 - 1369 เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการให้บริการ IoT
- ITU-T X. 1370 – 1389 เป็นมาตรฐานด้านความมั่นคงปลอดภัยในการให้บริการระบบขนส่งอัจฉริยะ (Intelligent Transport System)
- ITU-T X. 1400 - 1429 เป็นมาตรฐานด้านความมั่นคงปลอดภัยสำหรับเทคโนโลยีบล็อกเชน (Blockchain) ภายใต้ชื่อ Distributed Ledger Technology (DLT)

สำหรับภาพรวมและสถาปัตยกรรมด้านความมั่นคงปลอดภัย ได้ถูกกำหนดไว้ในมาตรฐาน ITU-T X. 800 – X. 849 บนโครงสร้าง OSI ซึ่งเป็นแนวความคิดเกี่ยวกับความมั่นคงปลอดภัย ภัยคุกคาม ช่องโหว่ และมาตรการป้องกันในปัจจุบัน โดยมีรายละเอียดมาตรฐาน ITU-T X. 800 และ ISO 7498 - 2 ที่สอดคล้องกัน

๒.๑.๕ ISO/IEC 27001 : 2013

มาตรฐาน ISO/IEC 27001 : 2013 (Information Security Management Systems : ISMS) เป็นมาตรฐานสากลว่าด้วยข้อกำหนดระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เป็นมาตรฐานสำหรับการปฏิบัติงานภายในองค์กร ให้ความสำคัญกับการพัฒนาด้านบุคลากรและกระบวนการตามแนวคิด People Process Technology หรือ PPT ประกอบด้วย นโยบาย วิธีปฏิบัติ ข้อแนะนำดำเนินการ ตลอดจนทรัพยากรและกิจกรรมที่เกี่ยวข้อง เพื่อปกป้องทรัพย์สินสารสนเทศ เป็นแนวทางที่เป็นระบบ สำหรับการจัดทำ นำไปใช้ ดำเนินการ ติดตามผล ทบทวน ดำรงรักษา และปรับปรุงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจ โดยอยู่บนพื้นฐานการประเมินความเสี่ยงและระดับการยอมรับความเสี่ยงขององค์กร ที่จะลด บรรเทา และจัดการความเสี่ยงอย่างได้ผล

การนำระบบบริหารจัดการความมั่งคงปลอดภัยสารสนเทศ มาใช้ดำเนินการได้อย่างสัมฤทธิ์ผล จะช่วยให้องค์กรมั่นใจว่าทรัพย์สินสารสนเทศได้รับการปกป้องต่อเนื่องอย่างเพียงพอ มีกรอบการดำเนินงานอย่างเป็นรูปธรรม ปรับปรุงสภาพแวดล้อมการควบคุมอย่างต่อเนื่อง และบรรลุผลสัมฤทธิ์ในการปฏิบัติตามกฎหมายและกฎระเบียบต่าง ๆ

องค์กรที่จะยื่นตรวจประเมินรับรองมาตรฐาน ต้องดำเนินการจัดทำและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามข้อกำหนดมาตรฐาน ISO/IEC 27001 : 2013 อ้างอิงตาม Clause 4 ถึง Clause 10 ให้ครบถ้วน อย่างไรก็ดี มาตรฐาน ISO/IEC 27001 : 2013 ไม่ได้ระบุคำแนะนำสำหรับแนวทางการจัดทำและดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเอาไว้ ดังนั้น องค์กรสามารถเลือกใช้แนวทางใดก็ได้เพื่อการดำเนินการและปรับปรุง ISMS อย่างต่อเนื่อง ซึ่งสามารถประยุกต์แนวคิดกรอบการดำเนินงานและการปรับปรุงต่อเนื่องที่เรียกว่า PDCA Approach หรือ ISMS Continual Improvement Approach ผนวกกับข้อกำหนดของมาตรฐาน ISO/IEC 27001 : 2013

๒.๒ สถาปัตยกรรมด้านความมั่นคงปลอดภัย

๒.๒.๑ ITU – T.X 800 Series

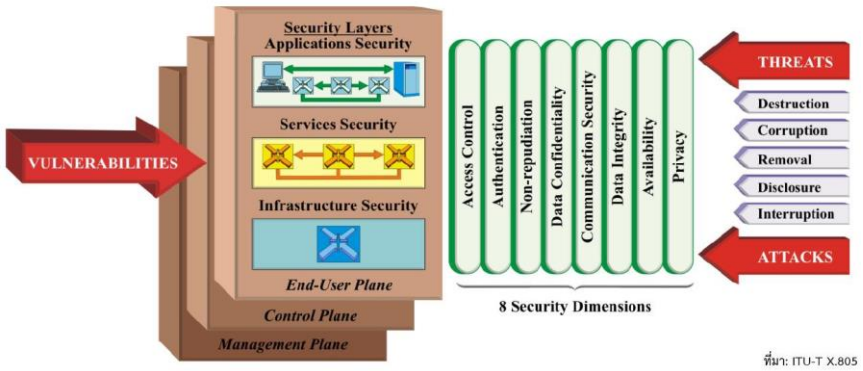
มาตรฐาน ITU-T X. 800 ได้ถูกกำหนดขึ้นเพื่อใช้เป็นกรอบการดำเนินงานด้านความมั่นคงปลอดภัยบนเครือข่ายการสื่อสาร ประกอบด้วยโครงสร้างที่ถูกออกแบบมาเพื่อรองรับบริการด้านความมั่นคงปลอดภัยบนเครือข่ายและกลไกที่เกี่ยวข้องที่ได้รับการยอดรับในระดับสากล เป็นมาตรฐานแรก โดยบริการด้านความมั่นคงปลอดภัยขั้นพื้นฐานนี้ได้แก่ กระบวนการเพื่อพิสูจน์

ตัวตน (Authentication) การปกป้องเครือข่ายเพื่อมิให้เข้าถึงทรัพยากรหรือนำทรัพยากรไปใช้โดยมิได้รับอนุญาต (Access Control) การป้องกันมิให้เกิดการบิดเบือนหลักฐานหลังเกิดเหตุ (Non-repudiation) ลักษณะของข้อมูลที่มิได้เปิดเผยเป็นการทั่วไปและรับรู้ได้เฉพาะเมื่อได้รับอนุญาต (Confidentiality) และลักษณะของข้อมูลที่ไม่สามารถเปลี่ยนแปลงได้โดยมิได้รับอนุญาต (Data Integrity)

ต่อมาได้มีการพัฒนาต่อยอดจากมาตรฐาน ITU-T X. 800 กำหนดเป็นมาตรฐานที่เกี่ยวข้องกับสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบที่ให้บริการสื่อสารครบวงจร หรือ ITU-T X. 805 ขึ้น ดังแสดงในรูปที่ ๒ โดยได้ขยายขอบเขตรายละเอียดสร้างกรอบการดำเนินงานที่มีส่วนประกอบหลัก คือ ชั้น (Layer) ส่วน (Plane) และมิติ (Dimension) ทำให้สามารถนำไปปรับใช้กับการรักษาความมั่นคงปลอดภัยกับโครงข่ายหลากหลายประเภทแบบครบวงจรในทุกมิติตามภัยคุกคามแต่ละชนิดได้อย่างมีประสิทธิภาพ

โดยมิติด้านความมั่นคงปลอดภัย (Security Dimensions) เป็นแนวทางการรับมือกับปัญหาด้านความมั่นคงปลอดภัยแต่ละประเภทต่อยอดจากบริการด้านความมั่นคงปลอดภัยขั้นพื้นฐานของมาตรฐาน ITU-T X. 800 โดยมีการเพิ่มมิติด้านความมั่นคงปลอดภัยอีกสามด้าน คือ ความมั่นคงปลอดภัยด้านการสื่อสาร (Communication Security) ความพร้อมในการใช้งาน (Availability) และความเป็นส่วนตัว (Privacy) เพื่อให้สามารถนำไปปรับใช้ได้ทั้งในโครงข่าย แอปพลิเคชัน และผู้ใช้บริการรายย่อย อย่างยืดหยุ่น

ทุกมิติด้านความมั่นคงปลอดภัยจะถูกนำไปปรับใช้ให้เข้ากับอุปกรณ์และสิ่งที่เกี่ยวข้องตามลำดับชั้น (Layer) โดยแบ่งตามประเภทกิจกรรมภายในโครงข่ายออกเป็นสามชั้น คือ ชั้นโครงข่ายพื้นฐานหลัก (Infrastructure Layer) ชั้นบริการ (Services Layer) และชั้นแอปพลิเคชันบนเครือข่ายที่ใช้งาน (Application Layer)



รูปที่ ๒ : สถาปัตยกรรมด้านความมั่นคงปลอดภัยตามมาตรฐาน ITU-T X.805 (ITU, 2004)

สถาปัตยกรรมด้านความมั่นคงปลอดภัยยังถูกแบ่งเป็นส่วน (Plane) ที่เกี่ยวข้องกับการบริหารจัดการเครือข่าย (Management Plane) การควบคุมเครือข่ายหรือสัญญาณควบคุม (Control Plane) และผู้ใช้บริการปลายทาง (End-user Plane) แยกกิจกรรมแต่ละส่วนออกจากกันอย่างชัดเจน

สถาปัตยกรรมตามมาตรฐาน ITU-T X.805 สามารถใช้เป็นแนวทางในการกำหนดนโยบายด้านความมั่นคงปลอดภัยของเครือข่าย รวมถึงเป็นแนวทางในการรับมือกับเหตุภัยคุกคามและแผนการฟื้นคืนสู่สภาวะปกติได้ และยังสามารถนำไปปรับใช้เพื่อประเมินระดับความมั่นคงปลอดภัยของเครือข่ายภายในองค์กร เป็นโครงสร้างพื้นฐานในการปรับปรุง และเปลี่ยนแปลงเครือข่ายให้เหมาะสมกับสภาวะภัยคุกคามที่เปลี่ยนไปแบบพลวัตได้

๒.๒.๒ NIST Cybersecurity Framework

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยโครงสร้าง ๓ ส่วน คือ

๑. โครงสร้างหลัก (Core) เป็นกิจกรรม และผลลัพธ์ต่าง ๆ ทางความมั่นคงปลอดภัยไซเบอร์ที่ต้องการ เพื่อให้องค์กรสามารถบริหารจัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ร่วมกับกระบวนการจัดการความเสี่ยงในด้านอื่นที่มีอยู่ภายในองค์กรอย่างมีประสิทธิภาพ โครงสร้างหลักประกอบไปด้วย ๕ องค์ประกอบคือ ฟังก์ชัน (Functions) หมวดหมู่ (Categories) หมวดหมู่ย่อย (Subcategories) และข้อมูลอ้างอิง (Informative References) ดังแสดงในรูปที่ ๓

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

รูปที่ ๓ : ตัวอย่างการจำแนกฟังก์ชัน หมวดหมู่ หมวดหมู่ย่อย และมาตรฐานอ้างอิง ของ NIST CSF (NIST, 2019)

- ฟังก์ชัน เป็นการจัดกลุ่มกิจกรรมพื้นฐานออกเป็น ๕ กิจกรรม ได้แก่ กำหนดป้องกัน ตรวจจับ รับมือ และคืนสภาพ ตามรายละเอียดในตารางที่ ๑ เพื่อให้สามารถตัดสินใจด้านการบริหารจัดการความเสี่ยง แก้ปัญหาภัยคุกคาม และพัฒนาการเรียนรู้จากกิจกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ขององค์กรที่ผ่านมา ช่วยแสดงให้เห็นถึงประโยชน์ที่ได้รับจากการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การวางแผนและซ้อมเตรียมการรับมือเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำให้การตอบสนองและการคืนสู่สภาวะปกติเกิดได้อย่างทันท่วงที เป็นผลให้ลดผลกระทบต่อการให้บริการแก่ผู้ใช้

ตารางที่ ๑ : ฟังก์ชันหลักของ NIST Cybersecurity Framework

ฟังก์ชัน	ความหมาย	หมวดหมู่
กำหนด (Identify)	ศึกษาและทำความเข้าใจ วิธีการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ทรัพย์สิน ข้อมูล และขีดความสามารถขององค์กร	การจัดการทรัพย์สิน สภาพแวดล้อมทางธุรกิจ การดำเนินงานภาครัฐ การประเมินความเสี่ยง กลยุทธ์การจัดการความเสี่ยง
ป้องกัน (Protect)	ควบคุมและดำเนินงาน ตามมาตรการป้องกันที่เหมาะสม เพื่อป้องกันหรือจำกัดระดับของภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์	การควบคุมการเข้าถึง การรับรู้และการฝึกอบรม ความปลอดภัยของข้อมูล กระบวนการป้องกันข้อมูล การดูแลรักษาเทคโนโลยีที่ใช้ในการป้องกัน
ตรวจจับ (Detect)	การเฝ้าระวัง หรือมีการตรวจสอบติดตามอย่างต่อเนื่องเพื่อการเตือนภัยกับเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันที และสามารถควบคุมสถานการณ์ได้	ความผิดปกติและเหตุการณ์ต่าง ๆ การสังเกตการณ์อย่างต่อเนื่อง และกระบวนการตรวจสอบ
รับมือ (Respond)	กิจกรรมการรับมือกับเหตุการณ์ต่าง ๆ ที่เกิดขึ้น	การวางแผนรับมือ การสื่อการ การวิเคราะห์ การลดความเสี่ยง และปรับปรุงแก้ไข
คืนสภาพ (Recover)	แผนความต่อเนื่องทางธุรกิจเพื่อรองรับการดำเนินงานต่อเนื่อง แผนการกู้คืนขีดความสามารถภายหลังจากการโดนคุกคามทางไซเบอร์	การวางแผนฟื้นฟู การปรับปรุง การสื่อสาร

- หมวดหมู่ เป็นกลุ่มของผลลัพธ์ที่ต้องการตามแต่กิจกรรมที่ระบุไว้ในฟังก์ชัน ได้แก่ การบริหารจัดการสินทรัพย์ (Asset Management) การบริหารจัดการข้อมูลแสดงตัวตนและการควบคุมการเข้าถึง (Identity Management and Access Control) และกระบวนการตรวจจับ (Detection Processes)

- หมวดหมู่ย่อย เป็นการแบ่งหมวดหมู่ย่อยลงไปถึงผลลัพธ์ทางการบริหารจัดการหรือผลลัพธ์ทางด้านเทคนิคที่ต้องการ มีความละเอียดเพียงพอที่จะช่วยให้เกิดความสำเร็จ

ในแต่ละหมวดหมู่ได้ เช่น ข้อมูลที่เกี่ยวกับระบบภายนอกได้รับการจัดเก็บแล้ว หรือ การแจ้งเตือนจากระบบตรวจจับได้รับการสืบสวนแล้ว

- ข้อมูลอ้างอิง เป็นมาตรฐาน แนวทาง หรือข้อปฏิบัติที่สามารถนำมาใช้เป็นแนวทางดำเนินการเพื่อให้บรรลุผลลัพธ์ที่ต้องการในแต่ละหมวดหมู่ย่อยได้

๒. ระดับการบริหารจัดการ (Implementation Tiers) เป็นการสร้างความเข้าใจถึงระดับความเข้มข้นของมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ภายในองค์กร ตามความเสี่ยงที่ยอมรับได้ ตามความสำคัญของพันธกิจองค์กร และงบประมาณ โดยกำหนดระดับขั้นจากระดับย่อย (ระดับ ๑) ไปถึง ระดับปรับตัว (ระดับ ๔) ตามรายละเอียดในตารางที่ ๒ โดยพิจารณากำหนดระดับความเข้มข้นจากสามปัจจัย คือ กระบวนการบริหารจัดการความเสี่ยง (Risk Management Process) การผนวกกระบวนการบริหารจัดการความเสี่ยงด้านไซเบอร์และด้านอื่นเข้าด้วยกัน (Integrated Risk Management Program) และการมีส่วนร่วมกับองค์กรภายนอก (External Participation)

ตารางที่ ๒ : ระดับการบริหารจัดการของ NIST Cybersecurity Framework

ระดับ	ลักษณะ	รายละเอียด
ระดับ ๑	ระดับย่อย (Partial)	การบริหารจัดการความเสี่ยงเป็นแบบเฉพาะกิจ ด้วยข้อจำกัดในการรับรู้ความเสี่ยง และยังไม่มีความร่วมมือกับภาคส่วนอื่น
ระดับ ๒	รับทราบความเสี่ยง (Risk Informed)	มีขั้นตอนและแนวทางจัดการความเสี่ยง แต่ยังไม่ได้นำไปใช้ครอบคลุมทั่วทั้งองค์กร องค์กรมีความเข้าใจการประสานงานและความร่วมมือ แต่ยังขาดความสามารถในการปฏิบัติ
ระดับ ๓	ทำซ้ำ (Repeatable)	มีการใช้นโยบายการปฏิบัติสำหรับกระบวนการและแนวทางจัดการความเสี่ยงในองค์กร พร้อมกับเริ่มมีความร่วมมือกับองค์กรภายนอกแล้วในบางส่วน
ระดับ ๔	ปรับตัว (Adaptive)	กระบวนการและแนวทางจัดการความเสี่ยง เป็นพื้นฐานมาจากบทเรียนที่ได้รับ และจากการปลูกฝังทางวัฒนธรรม พร้อมกับมีการร่วมมือกันในเชิงรุก

๓. โปรไฟล์ (Profiles) เป็นการรวบรวมข้อมูลด้านความต้องการ วัตถุประสงค์ขององค์กร ความเสี่ยงที่รับได้ และทรัพยากรที่มี เพื่อเทียบกับผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องการ สำหรับการพิจารณาหาช่องว่างที่ยังขาดอยู่และการพัฒนาแนวทางเพื่อปรับปรุงองค์กรสู่ผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องการ (Target Profile) ดังแสดงเป็นตัวอย่างตามรูปที่ ๔

Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

รูปที่ ๔ : การเปรียบเทียบโปรไฟล์ในปัจจุบันกับเป้าหมายที่ต้องการ (NIST, 2019)

๒.๓ สถานะปัจจุบันของประเทศไทย

ในปัจจุบันพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้ประกาศลงในราชกิจจานุเบกษา มีผลบังคับใช้ตั้งแต่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๒ โดยได้ผ่านขั้นตอนการจัดตั้ง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. (National Cyber Security Committee หรือ NCSC) ซึ่งมีหน้าที่กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และอยู่ในระหว่างการดำเนินการจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. มีหน้าที่กำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและแนวทางปฏิบัติ ตลอดจนประสานงานเมื่อเผชิญเหตุภัยคุกคามไซเบอร์ ซึ่งมีด้วยกัน ๘ ด้าน ได้แก่ ความมั่นคงของรัฐ บริการภาครัฐที่สำคัญ การเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การขนส่งและโลจิสติกส์ พลังงานและสาธารณูปโภค สาธารณสุข และด้านอื่น ๆ ตามที่ กกม. กำหนดเพิ่มเติม การรับมือภัยคุกคามทางไซเบอร์ จะแบ่งเกณฑ์พิจารณาเป็น ๓ ระดับ ได้แก่

ระดับไม่ร้ายแรง หมายถึงมีความเสี่ยงอย่างมีนัยยะสำคัญจนถึงทำให้โครงสร้างพื้นฐานและบริการของภาครัฐด้อยประสิทธิภาพ

ระดับร้ายแรง หมายถึงภัยคุกคามที่โจมตียังระบบคอมพิวเตอร์อันทำให้โครงสร้างสารสนเทศได้รับความเสียหายจนไม่อาจใช้การได้ ซึ่งกระทบทั้งทั้งบริการของรัฐ ความมั่นคง ไปจนถึงการกระทบความสัมพันธ์ระหว่างประเทศ

ระดับวิกฤติ หมายถึงภัยคุกคามที่ส่งผลต่อโครงสร้างสำคัญเป็นวงกว้าง ทำให้ล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ หรือเป็นภัยคุกคามที่กระทบต่อความสงบเรียบร้อยของประชาชนหรือความมั่นคงของรัฐหรือทำให้ประเทศตกอยู่ในภาวะคับขัน

อย่างไรก็ตาม มีองค์กรที่ดำเนินการเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญของประเทศอยู่ในปัจจุบันบ้างแล้ว ตลอดจนยังมีกฎหมายที่เกี่ยวข้อง

กับความมั่นคงปลอดภัยไซเบอร์อยู่หลายฉบับจากหลากหลายหน่วยงานภาครัฐ อีกทั้งคำศัพท์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ยังไม่ได้มีการให้คำนิยามไว้อย่างชัดเจน ทำให้การบังคับใช้กฎหมายอาจเกิดปัญหาจากความทับซ้อนของอำนาจหน้าที่ของหน่วยงานที่เกี่ยวข้อง อาทิ กสทช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ ฯลฯ จึงขอกล่าวถึงรายละเอียดพอสังเขป ดังนี้

ในส่วนของ กสทช. ได้มีการกำหนดการกำกับดูแลด้านความมั่นคงปลอดภัยของโครงข่ายเชิงกายภาพ (Physical Security) ของโครงข่ายโทรคมนาคมไว้อย่างชัดเจน ตามพระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. ๒๕๔๔ แต่ก็ยังไม่ปรากฏหน้าที่ความรับผิดชอบชัดเจนเกี่ยวกับการกำกับดูแลความมั่นคงปลอดภัยของโครงข่ายโดยรวม หรือแม้กระทั่งในเชิงกายภาพสำหรับโครงข่ายในการประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ ในเนื้อหาหมวด ๔ ของพระราชบัญญัติการประกอบกิจการกระจายเสียงและกิจการโทรทัศน์ พ.ศ. ๒๕๕๑ แต่อาจอาศัยการอนุมานตีความให้ครอบคลุมได้ อย่างไรก็ดี ได้มีการเพิ่มเนื้อหาบางส่วนในการกำกับดูแลด้านความมั่นคงปลอดภัยโดยรวมของเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยของเครือข่ายเข้าในพระราชบัญญัติองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการ วิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม หรือพระราชบัญญัติ กสทช. (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ เพื่อให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ถูกจัดตั้งตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม (ฉบับที่ ๑๗) พ.ศ. ๒๕๕๙ ในมาตรา ๕ โดยมีการโอนบรรดาอำนาจหน้าที่เกี่ยวกับการปฏิบัติของสำนักงานรัฐมนตรีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร มาเป็นอำนาจหน้าที่ของสำนักงานรัฐมนตรี กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งมิได้กำหนดอำนาจหน้าที่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และความมั่นคงปลอดภัยบนเครือข่ายไว้อย่างชัดเจน

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ได้กำหนดวิธีการแบบปลอดภัยของธุรกรรมอิเล็กทรอนิกส์ไว้สามระดับ คือ (๑) ระดับเคร่งครัด (๒) ระดับกลาง และ (๓) ระดับพื้นฐาน โดยกำหนดให้การทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคง หรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน ใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด และการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กร ที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) ใช้วิธีการแบบปลอดภัยในระดับกลาง ซึ่งได้มีการจัดทำรายละเอียดวิธีการดำเนินการไว้ในประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์ประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย

พ.ศ. ๒๕๕๕ เพื่อใช้ประเมินระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับประเภทธุรกรรมทางอิเล็กทรอนิกส์ อีกทั้งยังมีการกำหนดนิยามที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ไว้อย่างชัดเจน

นอกจากนี้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้มีการออกประกาศเพื่อดำเนินการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เป็นประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙

คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ ถูกจัดตั้งตามพระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐ ซึ่งมีหน้าที่กำหนดแผนระดับชาติ ให้ กสทช. และคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดำเนินงานให้สอดคล้องไปในทิศทางเดียวกัน และแบ่งหน้าที่อย่างมีประสิทธิภาพ

ทั้งนี้ การพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ได้ถูกกำหนดไว้ในร่างยุทธศาสตร์ชาติตามพระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ.๒๕๖๐ ในยุทธศาสตร์ชาติด้านการสร้างความสามารถในการแข่งขัน เป็นหนึ่งในอุตสาหกรรมและบริการแห่งอนาคต ภายใต้หัวข้ออุตสาหกรรมความมั่นคงของประเทศ กำหนดการสร้างอุตสาหกรรมที่ส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ เพื่อลดผลกระทบจากภัยคุกคามไซเบอร์ต่อเศรษฐกิจและสังคม และปกป้องอธิปไตยทางไซเบอร์ เพื่อรักษาผลประโยชน์ของชาติจากการทำธุรกิจดิจิทัล ส่งผลให้แผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมที่กำหนดโดยคณะกรรมการดิจิทัลฯ มีความสอดคล้องและเป็นไปในทิศทางเดียวกัน

๒.๔ กรณีศึกษาในต่างประเทศ

๒.๔.๑ ประเทศมาเลเซีย

๒.๔.๑.๑ สถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ประเทศมาเลเซียเป็นประเทศที่มีความก้าวหน้าในการบุกเบิก และพัฒนาเทคโนโลยี จนเป็นศูนย์กลางระบบสารสนเทศของระดับภูมิภาค โดยได้มีการแปลการพัฒนาทั่วไปที่เกี่ยวกับไซเบอร์ไปสู่กลยุทธ์อย่างเป็นทางการ มาเลเซียได้เริ่มโปรแกรม Multimedia Super Corridor ในปี ค.ศ. ๑๙๙๖ เพื่อเร่งการเปลี่ยนแปลงไปสู่สภาวะทันสมัยโดยใช้กรอบการทำงานบนพื้นฐานความรู้ ซึ่งถูกกำหนดอยู่ในวิสัยทัศน์ของกลยุทธ์ระยะยาว ค.ศ. ๒๐๒๐

ภัยคุกคามและการหลอกลวงออนไลน์เป็นความท้าทายและดึงดูดภาคธุรกิจหรือประเทศเป็นผลให้การลงทุนลดลง สูญเสียเสถียรภาพทางเศรษฐกิจและการเมือง

ในปัจจุบัน การใช้อุปกรณ์ดิจิทัลที่มากขึ้นทำให้อาชญากรรมไซเบอร์มีโอกาสเกิดขึ้นมากกว่าอาชญากรรมแบบอื่น ๆ โดยอาชญากรรมการค้าก็ได้เปลี่ยนรูปแบบมาเป็นแบบออนไลน์มากขึ้น ในทางปฏิบัติทุกคนใช้คอมพิวเตอร์และอินเทอร์เน็ตสามารถประกอบอาชญากรรมไซเบอร์ได้

ดังนั้น เพื่อตอบสนองต่อความท้าทายของภัยคุกคามยุคใหม่ มาเลเซียได้จัดตั้งหน่วยงานที่มีเป้าหมายเพื่อพัฒนาความชำนาญด้านไซเบอร์ วิธีการตอบสนองและการจัดการความเสี่ยง การแก้ไขกฎหมายที่เกี่ยวข้อง และออกโปรแกรมกระตุ้นความตระหนักรู้ และการร่วมมือระหว่างประเทศ มีการฝึกอบรมผู้เชี่ยวชาญ และคนทั่วไปอย่างต่อเนื่อง เป็นผลทำให้มาเลเซียสามารถอยู่ในตำแหน่งที่เป็นเป้าหมายในการลงทุน และร่วมมือกันด้านความปลอดภัยไซเบอร์

๒.๔.๑.๒ หน่วยงานที่เกี่ยวข้อง

๑) ความปลอดภัยไซเบอร์มาเลเซีย

ความปลอดภัยไซเบอร์มาเลเซียมีหน้าที่ขยายขอบเขตครอบคลุมโดยการเพิ่มบทบาทของการดำเนินงานตามนโยบายความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์ประสานงานทางเทคนิคและศูนย์วิจัยความเสี่ยงภัยไซเบอร์ โดยจะเฝ้าระวังด้าน e-security มีโครงสร้างการรายงานในการบริหารด้านความปลอดภัยไซเบอร์ของมาเลเซียคือ การทำงานของความปลอดภัยไซเบอร์แห่งชาติต้องรายงานต่อหน่วยงานความปลอดภัยไซเบอร์แห่งชาติ (NACSA) ในขณะที่งานอุตสาหกรรมวิจัยและพัฒนารายงานต่อกระทรวงวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม (MOSTI)

ในทางปฏิบัติ ความปลอดภัยไซเบอร์มาเลเซียมีหน้าที่ความรับผิดชอบในการประสานงานความริเริ่มความปลอดภัยไซเบอร์ของทุกองค์กรและหน่วยงาน มีกลไกในการแบ่งปันข้อมูลและความรู้ ให้โปรแกรมการเพิ่มความตระหนักรู้ ฝึกอบรมและพัฒนาขีดความสามารถของความเชี่ยวชาญ กำหนดและสื่อสารข้อบังคับที่ได้จาก CNII เพื่อให้ดำเนินการตามนโยบายความปลอดภัยไซเบอร์แห่งชาติ ตลอดจนเฝ้าระวังความสอดคล้องต่อนโยบายความปลอดภัยไซเบอร์และมาตรฐานผู้ให้บริการ CNII และให้การประเมินความเสี่ยงความปลอดภัยไซเบอร์สำหรับผู้ให้บริการ CNII

มาเลเซียได้พัฒนาและสร้างมาตรฐานกรอบการทำงานสำหรับองค์กร Information Security Certification Body (ISCB) เป็นแผนกหนึ่งในความปลอดภัยไซเบอร์มาเลเซียที่จัดการให้ใบรับรองความปลอดภัยของข้อมูล ซึ่งใช้มาตรฐานและแนวทางของนานาชาติ

๒) หน่วยงานความปลอดภัยไซเบอร์แห่งชาติ

มาเลเซียได้จัดตั้งหน่วยงานความปลอดภัยไซเบอร์แห่งชาติ (NACSA) ขึ้นในปี ค.ศ. ๒๐๑๗ ทำงานภายใต้การควบคุมของสภาความมั่นคงแห่งชาติ โดยกำหนดให้เป็นหน่วยงานผู้นำแห่งชาติด้วยความปลอดภัยไซเบอร์ มีวัตถุประสงค์เพื่อสร้างความปลอดภัยและเพิ่มความแข็งแกร่งในการปรับตัวของมาเลเซียต่อการเผชิญหน้าต่อภัยคุมคามและการโจมตีทางไซเบอร์โดยการรวบรวมประสานงานผู้เชี่ยวชาญและทรัพยากรดีที่สุดของชาติ รวมถึงการพัฒนา

และดำเนินการระดับชาติตามนโยบายและกลยุทธ์ความปลอดภัยไซเบอร์เพื่อปกป้องโครงสร้างข้อมูลของชาติ (CNII) และสนับสนุนเครือข่ายระดับภูมิภาคและสากลเพื่อแบ่งปันความสนใจในความปลอดภัยไซเบอร์

๓) NC4

NC4 ตั้งขึ้นเพื่อเป็นศูนย์กลางจัดการภัยคุกคามและวิกฤตไซเบอร์ระดับชาติตามนโยบาย ความปลอดภัยไซเบอร์และคำสั่งเลขที่ ๒๔ เป้าหมายเพื่อประกันการร่วมมือและทำงานร่วมกันระหว่างหน่วยงาน CNII เพื่อเสริมการจัดการแบบบูรณาการของความปลอดภัยไซเบอร์ของประเทศ และได้ถูกจัดสรรหน้าที่แตกต่างตามช่วงเวลาสงบและวิกฤต โดยในช่วงเวลาสงบมีหน้าที่เฝ้าระวังสถานการณ์ความปลอดภัยไซเบอร์แห่งชาติ เฝ้าระวังระดับภัยไซเบอร์ระดับชาติ วิเคราะห์ภัยคุกคาม และให้ข้อมูลเกี่ยวกับระดับภัยคุกคามแก่รัฐ แจ้งระดับภัยคุกคามแก่คณะกรรมการจัดการวิกฤตไซเบอร์แห่งชาติ (NCCMC) และ เฝ้าระวังความสอดคล้องและเสริมกระบวนการจัดการวิกฤตไซเบอร์แห่งชาติ (NCCMP) ตลอดจนวัดระดับความพร้อมของความปลอดภัยไซเบอร์แห่งชาติ ออกคำเตือน แนวทางและคำปรึกษาแก่หน่วยงานหรือองค์กร CNII ขณะที่ในช่วงเวลาวิกฤต มีหน้าที่ประสานงานและจัดการวิกฤตไซเบอร์ระดับชาติ รายงานต่อรัฐบาลถึงสถานการณ์ล่าสุดจนกระทั่งระดับคุกคามอยู่ที่ ๑ ตลอดจนให้ความช่วยเหลือจากผู้เชี่ยวชาญกรณีที่มีคำร้อง และเป็นที่ปรึกษาทางเทคนิคให้กับกลุ่มทางานและคณะกรรมการจัดการวิกฤตไซเบอร์แห่งชาติ

๒.๔.๑.๓ ข้อกฎหมายที่เกี่ยวข้อง (Laws and Regulations)

มาเลเซียได้ถูกจัดอยู่อันดับต้น ๆ ของโลกในการเตรียมความพร้อมด้านความปลอดภัยไซเบอร์ และมีคะแนนโดดเด่นด้านการสร้างสมรรถนะ เป็นประเทศที่มีความมุ่งมั่นสูงในความปลอดภัยไซเบอร์จากทุกมุมมอง มีกรอบการทำงานที่รองรับพื้นฐานสำคัญที่เกี่ยวกับความทันสมัยของกฎหมาย โดยมีรายละเอียด ดังนี้

- พระราชบัญญัติอาชญากรรมคอมพิวเตอร์ ซึ่งอธิบายวิธีการจัดการ Virus, Worm, Trojan
- พระราชบัญญัติสื่อและการสื่อสารปี ค.ศ. ๑๙๙๘ เพื่อประกันเครือข่ายและความปลอดภัยของข้อมูล ความน่าเชื่อถือ และความถูกต้องในมาเลเซีย
- พระราชบัญญัติลายเซ็นดิจิทัล ค.ศ. ๑๙๙๗ เพื่ออธิบายข้อกาหนดในการยอมรับเทคโนโลยีการเซ็นสัญญาดิจิทัล
- พระราชบัญญัติ Copyright ปี ค.ศ. ๑๙๙๗ อธิบายมาตรการป้องกันเทคโนโลยี
- พระราชบัญญัติธุรกิจอิเล็กทรอนิกส์ ค.ศ. ๒๐๐๖ ต้องมีการเซ็นชื่ออิเล็กทรอนิกส์ และความน่าเชื่อและความถูกต้อง

- พระราชบัญญัติกลยุทธ์การค้า ค.ศ. ๒๐๑๐ อธิบายกลยุทธ์ทางไซเบอร์ รวมถึงเทคโนโลยีไซเบอร์

- ประมวลกฎหมายอาญาอาชญากรรมคอมพิวเตอร์และอินเทอร์เน็ต

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ค.ศ. ๒๐๑๐ ควบคุมกระบวนการธุรกรรมในโฆษณาทางการค้า

- พระราชบัญญัติต่อต้านข่าวปลอม ค.ศ. ๒๐๑๘ เพื่อจัดการกับการสร้าง นำเสนอ เผยแพร่ของข่าวปลอมหรือกิจกรรมที่เกี่ยวข้อง เช่น การเงินที่ผิดกฎหมาย

อย่างไรก็ดี แนวโน้มที่เพิ่มขึ้นของภัยคุกคาม และการโจมตีทางไซเบอร์ทำให้กฎหมายและข้อบังคับต่าง ๆ ที่มีอยู่อาจจะไม่ครอบคลุมต่อภัยใหม่ ๆ ที่เพิ่มขึ้นเหล่านี้ ทางรัฐบาลมาเลเซียโดยรองนายกรัฐมนตรีจึงประกาศพระราชบัญญัติความปลอดภัยไซเบอร์ฉบับใหม่เพื่อกำลังเตรียมและผ่านเข้าสู่รัฐสภาเพื่อจัดการปัญหาและความท้าทายเหล่านี้ อย่างไรก็ตาม พระราชบัญญัติใหม่นี้ยังไม่ได้บังคับใช้อย่างเป็นทางการในปัจจุบัน

๒.๔.๑.๔ แนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ด้านความมั่นคงปลอดภัยไซเบอร์

มาเลเซียเป็นประเทศแรก ๆ ของเอเชียแปซิฟิกที่มีนโยบายความมั่นคงปลอดภัยไซเบอร์ กระทรวงวิทยาศาสตร์ เทคโนโลยีและนวัตกรรมได้ทำการศึกษาเพื่อประเมินสถานการณ์และการปฏิบัติการของความปลอดภัยทางข้อมูลในปัจจุบัน นโยบายความปลอดภัยด้านไซเบอร์และทำแผนการดำเนินงาน สำหรับการริเริ่มการคุ้มครองโครงสร้างพื้นฐานของข้อมูลที่สำคัญเริ่มออกใช้ในปี ค.ศ. ๒๐๐๘ วิสัยทัศน์ของนโยบายคือ “โครงสร้างพื้นฐานด้วยข้อมูลแห่งชาติที่สำคัญของประชาชนมาเลเซียต้องมีความปลอดภัย ยืดหยุ่น และพึ่งตนเองได้ และด้วยการใส่วัฒนธรรมของความปลอดภัย จะสนับสนุนเสถียรภาพ ความเป็นอยู่ที่ขึ้นและสร้างความมั่งคั่งให้กับประเทศ”

เนื่องจากความวิกฤตและการพึ่งพากันของแต่ภาคส่วน นโยบายจึงมีเป้าหมายเพื่อจัดการความเชื่อมโยงเหล่านี้ในรูปแบบของความมั่นคงปลอดภัยไซเบอร์ การจัดตั้งโปรแกรมและกรอบงานเพื่อประกันการควบคุม ความปลอดภัยที่เหมาะสม ซึ่งมีนโยบายหลักทั้งหมด ๘ ด้าน ได้แก่

- การปกครองที่มีประสิทธิภาพ

มีการประสานงานส่วนกลางของการริเริ่มความปลอดภัยไซเบอร์แห่งชาติ สนับสนุนการร่วมมือที่มีประสิทธิภาพระหว่างภาครัฐและเอกชน และจัดตั้งและกระตุ้นการแลกเปลี่ยนแบ่งปันข้อมูลอย่างเป็นทางการ

- กรอบการทำงานของกฎหมายและข้อบังคับ

ทบทวนและส่งเสริมกฎหมายไซเบอร์ที่ระบุประเด็นธรรมชาติที่ไม่หยุดนิ่งของภัยไซเบอร์ และจัดตั้งโปรแกรมสร้างขีดความสามารถก้าวหน้าเพื่อหน่วยงานบังคับใช้กฎหมาย เพื่อประกันการส่งเสริมและสอดคล้องระหว่างกฎหมายท้องถิ่นและกฎหมายนานาชาติ

- กรอบการทำงานเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์

พัฒนากรอบการทำงานที่สำหรับเฉพาะควบคุมข้อกำหนดด้านความปลอดภัยไซเบอร์และเป็นพื้นฐานสำหรับส่วน CNII ตลอดจนดำเนินการตามโปรแกรมประเมิน/รับรองผลิตภัณฑ์และระบบความปลอดภัยไซเบอร์

- การสร้างวัฒนธรรมของความสามารถและความปลอดภัย

ทำมาตรฐานและประสานในโปรแกรมความตระหนักและการศึกษาด้านความปลอดภัยไซเบอร์ข้ามส่วนต่าง ๆ ของ CNII ตลอดจนจัดตั้งกลไกที่มีประสิทธิภาพสำหรับกระจายความรู้ด้านความปลอดภัยไซเบอร์ เพื่อพัฒนา สนับสนุนและรักษาวัฒนธรรมความปลอดภัยแห่งชาติ

- การพัฒนาและวิจัยเพื่อความยืดหยุ่น

สร้างความร่วมมือและจัดลำดับความสำคัญสำหรับงานวิจัยและพัฒนาขยายและสร้างความแข็งแกร่งของชุมชนงานวิจัยความมั่นคงปลอดภัยไซเบอร์ สนับสนุนและพัฒนาทรัพย์สินทางปัญญา และบำรุงการเติบโตของอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์

- การบังคับและสอดคล้อง

พัฒนากรอบการประเมินความเสี่ยงด้านความปลอดภัยไซเบอร์ ทำให้ระบบความปลอดภัยเป็นมาตราฐานเดียวกัน รวมถึงเพิ่มความแข็งแกร่งในการเฝ้าระวังและบังคับใช้มาตรฐาน

- ความพร้อมรับมือสถานการณ์ฉุกเฉินความปลอดภัยไซเบอร์

เพิ่มความแข็งแกร่งทีม CERT และพัฒนากลไกรายงานเหตุการณ์ความปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ตลอดจนกระตุ้นทุกภาคส่วนของ CNII ให้ประเมินจุดอ่อนตามช่วงเวลา เพื่อเฝ้าระวังเหตุการณ์ไซเบอร์ รวมถึงพัฒนากรอบการบริหารงานมาตรฐานธุรกิจอย่างต่อเนื่อง และให้คำปรึกษาด้านจุดอ่อนและเตือนภัยทันเวลา

- ความร่วมมือระหว่างชาติ

กระตุ้นการเข้าร่วมของหน่วยงานความปลอดภัยไซเบอร์นานาชาติ และสนับสนุนการเข้าร่วมความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง เช่น เป็นเจ้าภาพสัมมนานานาชาติประจำปี

โดยสรุป การดำเนินงานช่วงแรกจะเป็นเรื่องโครงสร้างพื้นฐานที่เป็นจุดอ่อน การเพิ่มความตระหนักรู้ และรูปแบบกลไกความปลอดภัยส่วนกลาง จากนั้นการดำเนินงานในระยะยาวจะเน้นการสนับสนุน สร้าง เพิ่มขีดความสามารถและความชำนาญของระบบกระบวนการและมาตรฐาน

มาเลเซียเป็นเจ้าภาพ Workshop ด้านความปลอดภัยของข้อมูลและเครือข่ายและรักษาความปลอดภัยไซเบอร์แห่งชาติ จากหลาย ๆ ภาคปฏิบัติจนกลายเป็นศูนย์กลางในที่สุด

๒.๔.๒ ประเทศสหราชอาณาจักร

๒.๔.๒.๑ สถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

ปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยีทำให้อุตสาหกรรมการสื่อสารเปลี่ยนแปลงรวดเร็ว การร่วมมือกันของหลายฝ่ายทำให้ยากต่อการจัดการควบคุม เนื่องจากการเข้าถึงเทคโนโลยีที่ง่ายและสูงขึ้น เกิดเป็นแนวโน้มของการโจมตีและภัยคุกคามที่มากขึ้นอย่างที่ไม่เคยมีมาก่อน

ด้วยการตระหนักถึงความสำคัญของการให้บริการการสื่อสารและความปลอดภัย จากการเปลี่ยนแปลงของสภาพแวดล้อมทางตลาด จึงได้มีการปรับปรุงข้อบังคับทางการสื่อสารประมาณปี ค.ศ. ๒๐๑๐ – ๒๐๑๑ เพื่อให้บริการและเสริมให้เครือข่ายของการสื่อสารมีความปลอดภัยและน่าเชื่อถือตลอดเวลา

อย่างไรก็ดี ความสนใจอย่างสูงต่อความปลอดภัยไซเบอร์ไม่ได้จำกัดอยู่แค่กิจการโทรคมนาคม เพราะเป็นเพียงส่วนหนึ่งของกิจกรรมในการดำรงชีวิต การร่วมมือกันระหว่างชาติในเรื่องความปลอดภัยและความยืดหยุ่นเริ่มแข็งแกร่งและซับซ้อนขึ้น การไหลของข้อมูลที่มากขึ้นทำให้ความปลอดภัยส่งผลกระทบต่อระบบและบริการที่ใช้ในชีวิตประจำวัน ดังนั้นวิธีการจัดการความปลอดภัยไซเบอร์จึงเป็นสิ่งจำเป็นต่อการดำรงชีวิตประจำวันในปัจจุบัน

๒.๔.๒.๒ หน่วยงานที่เกี่ยวข้อง (Stakeholders)

สหราชอาณาจักร มีหน่วยงานชื่อ กรมความปลอดภัยของไซเบอร์และรัฐบาล (CGSD) มีหน้าที่ในการจัดลำดับความสำคัญในเรื่องความปลอดภัยไซเบอร์ การประสานงานความปลอดภัยไซเบอร์แห่งชาติและ ความรับผิดชอบต่อบุคคล นโยบายข้อมูลระหว่างรัฐและนานาชาติโดยมีวัตถุประสงค์ ดังนี้

- ให้กลยุทธ์ความปลอดภัยไซเบอร์แห่งชาติ (NSCC) ค.ศ. ๒๐๑๖ – ๒๐๒๑
- จัดทำโปรแกรมความปลอดภัยไซเบอร์ ๕ ปี (NCSP) ค.ศ. ๒๐๑๖ – ๒๐๒๑
- สนับสนุนการจัดตั้งศูนย์ความปลอดภัยไซเบอร์แห่งชาติ (NCSC)
- ตั้งนโยบายความปลอดภัยของรัฐอย่างต่อเนื่อง
- ดำเนินการทบทวนและค้นหาความปลอดภัยของรัฐ

จะเห็นได้ว่าสหราชอาณาจักร มีการพิจารณาภัยไซเบอร์ว่าเป็นสิ่งสำคัญอันดับต้น ๆ ของประเทศ โดยมีการจัดตั้งกลยุทธ์ระดับสูง และวางกรอบกฎหมาย และข้อบังคับซึ่งมีแหล่งที่มาหรือมีความสอดคล้องกับของสหภาพยุโรป โดยมีการแก้ไขพระราชบัญญัติการสื่อสาร ค.ศ. ๒๐๐๓ เพื่อสะท้อนการเปลี่ยนแปลงที่เกิดขึ้นกับการสื่อสารโทรคมนาคม

และมีการจัดตั้งหน่วยงาน The Office of Communication (Ofcom) เพื่อดำเนินงานตามข้อกำหนดในพระราชบัญญัติโดยมีพื้นฐานจาก Section 105 A – D ของพระราชบัญญัติการสื่อสาร

แม้ว่าจะไม่มีการคาบเกี่ยวของข้อบังคับสำหรับความปลอดภัยไซเบอร์ในสหราชอาณาจักร แต่มีบางส่วนที่การทำงานได้รับผลกระทบจากประเด็นดังกล่าว และยังอยู่ในเส้นทางที่ต้องจัดการกับภัยไซเบอร์ที่เปลี่ยนแปลงตลอดเวลา Ofcom จึงกำหนดให้ผู้ให้บริการมีความตระหนักรู้ในระดับหนึ่ง มีการปรับปรุงเหตุการณ์ให้ทันสมัยเสมอ ทำตามมาตรฐานความปลอดภัย และมีการกำหนดให้ขอใบรับรองมาตรฐานต่าง ๆ ในกรณีที่เป็นไปได้

๒.๔.๒.๓ ข้อกฎหมายที่เกี่ยวข้อง (Laws and Regulations)

ทิศทางการออกกฎหมายของอังกฤษได้แนวทางจากคำสั่ง สหภาพยุโรป จากวันที่ ๒๕ พฤษภาคม ค.ศ. ๒๐๑๘ ที่ข้อบังคับการคุ้มครองข้อมูลทั่วไป ๒๐๑๖/๖๗๐ (GDPR) ได้เริ่มมีผลบังคับใช้ ซึ่งมีผลสำคัญต่อความปลอดภัยไซเบอร์เพราะเป็นกุญแจหลักของคำสั่งที่ต้องคุ้มครองข้อมูลส่วนบุคคล

อีกหนึ่งคำสั่งที่สำคัญโดยสหภาพยุโรป ปี ค.ศ. ๒๐๑๖ คือ คำสั่งความปลอดภัยเครือข่ายและข้อมูล ๒๐๑๖/๑๑๔๘ ซึ่งทำให้อังกฤษออกข้อบังคับระบบเครือข่ายและข้อมูล ๒๐๑๘ (NIS Regulations) เพื่อขับเคลื่อนการปรับปรุงการคุ้มครองของระบบเครือข่ายและข้อมูลที่เป็นส่วนสำคัญในการให้บริการของอังกฤษ โดยข้อบังคับจะกำหนดใน ๔ ภาคส่วน คือ พลังงาน การขนส่ง สาธารณสุข และประปา

โครงสร้างพื้นฐานดิจิทัล ตลาดออนไลน์ เครื่องมือค้นหา และผู้ให้บริการ Cloud Computing ต้องกำหนดมาตรการตามที่ NIS ระบุไว้เพื่อความปลอดภัยของข้อมูลและเครือข่าย สิ่งที่คล้ายกันระหว่างข้อบังคับ NIS และ GDPR คือการมุ่งเน้นในด้านความปลอดภัยและการรายงานเหตุการณ์ตามข้อกำหนดและบทลงโทษ

การตัดสินใจออกจากสหภาพยุโรป ของอังกฤษปี ค.ศ. ๒๐๑๖ ไม่ได้มีผลกระทบอย่างมีนัยสำคัญใด ๆ ต่อกฎหมายแต่จะมีความท้าทายใหม่จากการออกนี้ เนื่องจากความซับซ้อนและธรรมชาติของเหตุการณ์ รวมถึงพันธมิตรระหว่างชาติที่ยังมีอยู่ทำให้คาดหวังว่าสหราชอาณาจักรจะเป็นสมาชิกใกล้ชิดในชุมชนความปลอดภัยไซเบอร์ต่อไป

๒.๔.๒.๔ แนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

การสร้างกลยุทธ์เพื่อความปลอดภัยไซเบอร์มีรูปแบบมาจากสหภาพยุโรป สหราชอาณาจักรให้ความสำคัญกับการจัดการความปลอดภัยไซเบอร์เป็นอันดับต้นของประเทศ กลยุทธ์ความปลอดภัยไซเบอร์ตั้งขึ้นครั้งแรกปี ค.ศ. ๒๐๐๙ และอีกครั้งในปี ค.ศ. ๒๐๑๑ โดยวัตถุประสงค์หลักเพื่อเพิ่มการร่วมงานและแบ่งปันความรับผิดชอบภายในประเทศ และพันธมิตรโดยส่วนใหญ่เน้นไปที่เอกชน

กลยุทธ์ความปลอดภัยไซเบอร์ล่าสุดปี ค.ศ. ๒๐๑๖ มีวิสัยทัศน์ คือ เพื่อบรรลุ “ความปลอดภัยและการปรับตัวต่อภัยคุกคามไซเบอร์ ความเจริญรุ่งเรืองและความลับ

ในโลกไซเบอร์ของสหราชอาณาจักร” มีการเน้นในเรื่องความร่วมมือระหว่างรัฐและเอกชน และมีการสร้างกลยุทธ์ใหม่ชื่อ “การคุ้มครองไซเบอร์แบบแอคทีฟ” มีเป้าหมายเพื่อป้องกันและลดผลกระทบจากการโจมตีไซเบอร์ในสหราชอาณาจักร โดยทำเครื่องข่ายให้แข็งแรงผ่านวิธีการป้องกันอัตโนมัติ ทั้งนี้ กลยุทธ์มี ๓ วัตถุประสงค์ ดังนี้

ป้องกัน ป้องกันภัยคุกคามและโต้ตอบเหตุการณ์อย่างมีประสิทธิภาพ

สกัด ตรวจพบ เข้าใจ สืบสวนและทำลายการปฏิบัติมุ่งร้าย

พัฒนา ผ่านทางการพัฒนาและวิจัยทางวิทยาศาสตร์

ความคิดในการตอบสนองด้วย “อะไรที่มีความสามารถเป็นสิ่งที่เหมาะสมสุด” นั่นคือความเป็นไปได้ของความสามารถในการตอบกลับจะปรากฏในกลยุทธ์ แล้วยังมีการมุ่งเน้นไปในการวิจัยและพัฒนารวมถึงการสร้างนวัตกรรม งบประมาณสำหรับกลยุทธ์นี้อยู่ที่ ๑.๙ พันล้านปอนด์ เพื่อให้บรรลุผลลัพธ์ที่ต้องการ รัฐบาลมีการใช้มาตรการและการปฏิบัติงานจำเพาะเจาะจงโดยการจัดตั้งศูนย์ความปลอดภัยไซเบอร์แห่งชาติ (NCSC) เพื่อให้ความรู้ ความชำนาญและภาวะผู้นำต่อเรื่องความปลอดภัยไซเบอร์ในการจัดการจุดอ่อน

NCSC ยังทำหน้าที่ออกคำเตือนและให้คำปรึกษาสำหรับประเด็นความปลอดภัยไซเบอร์ที่ตรวจพบในอังกฤษ ได้รับความร่วมมือจากหลายฝ่ายของภาครัฐเพื่อกำหนดทิศทางกลยุทธ์สำหรับความปลอดภัยไซเบอร์ของอังกฤษ และได้เสนอแนวทางความปลอดภัยไซเบอร์สำหรับองค์กรที่ต้องการคุ้มครองตัวเองจากภัยไซเบอร์ในปี ค.ศ. ๒๐๑๒ เป็นแนวทางประเทศต่อบริษัทใหญ่ที่ตระหนักถึงความปลอดภัยไซเบอร์อยู่แล้ว ซึ่งมี ๑๐ ขั้นตอนดังนี้

- การเคร่งครัดในการจัดการความเสี่ยง
- การตั้งค่าความปลอดภัย
- ความปลอดภัยเครือข่าย
- การจัดการลำดับความสำคัญของผู้ใช้บริการ
- การให้ความรู้และตระหนักรู้ของผู้ใช้บริการ
- การจัดการเหตุการณ์
- การป้องกันมัลแวร์
- การเฝ้าระวัง
- การควบคุมสื่อที่ถอนเข้าออกได้
- การทำงานที่บ้านและเคลื่อนที่

นอกเหนือไปจาก ๑๐ ขั้นตอนดังกล่าว NSCS ได้ตั้งความจำเป็นของไซเบอร์ขึ้น เพื่อให้คำแนะนำที่เจาะจงกว่านี้ถึงวิธีการเลือกการควบคุมความปลอดภัยให้เหมาะสม ซึ่งมีรายการดังนี้

- ใช้ Firewall ในการเชื่อมต่ออินเทอร์เน็ตให้ปลอดภัย
- เลือกการตั้งค่าที่ปลอดภัยที่สุดสาหรับอุปกรณ์และซอฟต์แวร์

- ควบคุมคนที่มีการเข้าถึงข้อมูลและบริการ
- ป้องกันตัวเองจากไวรัสและมัลแวร์ต่าง ๆ
- ปรับปรุงอุปกรณ์และซอฟต์แวร์เสมอ

นอกจากนี้ ความจำเป็นไซเบอร์ยังให้ทางเลือกในการได้รับการรับรอง ไม่ว่าจะเป็นผ่านกระบวนการประเมินหรือได้รับการรับรองจากความจำเป็นไซเบอร์เอง และนอกจากเรื่องความปลอดภัยไซเบอร์แล้วยังมีการออกกฎหมายและระเบียบต่าง ๆ ที่สร้างขึ้นเพื่อคุ้มครองความปลอดภัยของข้อมูล

๒.๔.๓ ประเทศเอสโตเนีย

๒.๔.๓.๑ สถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันเอสโตเนียเป็นหนึ่งในประเทศสหภาพยุโรปที่มีความก้าวหน้าด้านความปลอดภัยไซเบอร์ โดยมีการพัฒนาระบบการจัดการด้านไซเบอร์อย่างเด่นชัดในช่วงเวลากว่าสิบปีที่ผ่านมา เอสโตเนียรับเป็นเจ้าภาพงานความเป็นเลิศของศูนย์ประสานงานป้องกันภัยด้านไซเบอร์ของกลุ่มประเทศองค์การสนธิสัญญาแอตแลนติกเหนือ (NATO) และดำรงตำแหน่งเป็นผู้อำนวยการองค์กรด้วย โดยในปัจจุบันมีหลายประเทศเข้าร่วมกับศูนย์ประสานงานฯ รวมไปถึงการยอมรับของชาติมหาอำนาจของโลก เช่น เยอรมัน สหรัฐอเมริกา อังกฤษ และฝรั่งเศส มีพันธกิจของศูนย์ประสานงานฯ คือ “เพื่อเสริมความสามารถ ความร่วมมือ การแบ่งปันข้อมูลระหว่างประเทศสมาชิก NATO และพันธมิตรในการป้องกันไซเบอร์โดยการให้การศึกษา วิจัยและพัฒนา เรียนรู้จากบทเรียนและการปรึกษาหารือ แลกเปลี่ยนความรู้ และประสบการณ์” โดยมีวิสัยทัศน์คือ “เป็นแหล่งรวมผู้เชี่ยวชาญด้านการป้องกันไซเบอร์ด้วยการรวบรวมสั่งสม สร้าง และกระจายความรู้ ความเข้าใจเกี่ยวกับเรื่องนี้ภายในประเทศสมาชิก NATO โดยประเทศสมาชิก NATO และพันธมิตร” (NATO Cooperative Cyber Defence Centre of Excellence, 2018 : CCDCOE) โดยจะจัดงานสัมมนา Cyber Conflict (Cycon) ซึ่งเป็นการสัมมนาฝึกอบรมที่สำคัญด้านความปลอดภัยไซเบอร์ในเอสโตเนียขึ้นทุกปี โดยจะมีการจัด Crossed Swords เป็นที่ทดสอบการเจาะระบบ และ Locked Shields เป็นการทดลองการป้องกันไซเบอร์จากผู้เข้าร่วม และรวบรวมโดยเอสโตเนีย

CCDCOE จะเชิญกลุ่มผู้เชี่ยวชาญจากนานาชาติ เพื่อเตรียมคู่มือชื่อ “Tallinn” ระหว่างปี ค.ศ. ๒๐๐๙ - ๒๐๑๒ สรุปผลจากการศึกษาและวิเคราะห์ว่าการประยุกต์ใช้กฎหมายระหว่างชาติเกี่ยวกับความขัดแย้งทางไซเบอร์ และสงครามไซเบอร์ ซึ่งเป็นจุดเริ่มต้นในความพยายามครั้งแรกที่วิเคราะห์เพื่อนำไปสู่ความกระจ่างในประเด็นกฎหมายที่เกี่ยวข้องที่ซับซ้อน จุดเน้นของการจัดทำคู่มือคือการกำหนดกิจกรรมไซเบอร์ที่ทำความเสียหายซึ่งจัดอยู่ในกลุ่ม “การโจมตีติดอาวุธ” โดยทั่วไปประเทศต่าง ๆ จะอนุญาตให้โต้ตอบ ก็เป็นไปเพื่อการป้องกันตัวเอง ต่อมามีการปรับปรุงเป็น “Tallinn 2.0” ในปี ค.ศ. ๒๐๑๗ จะเน้นการปฏิบัติการไซเบอร์ทุกชนิด ไม่เพียงแต่ที่สร้างความขัดแย้งที่ถูกกำหนดไว้ในฉบับแรกเท่านั้น

นอกจากการบริหารใน CCDCOE แล้ว เอสโตเนียยังเป็นผู้จัดการศูนย์ MalwareBytes เป็นบริษัทที่มีชื่อทางความปลอดภัยทางอินเทอร์เน็ตที่มีความสามารถพิเศษด้านการป้องกันอุปกรณ์อิเล็กทรอนิกส์ และ Symantec ที่ให้บริการความปลอดภัยไซเบอร์โดยมีผลิตภัณฑ์และการแก้ปัญหาความปลอดภัยเพื่อปกป้องค์กรและบุคคลจากมัลแวร์ ภัยคุกคามและประเด็นไซเบอร์อื่น ๆ ที่เกี่ยวข้อง เรียกว่า Guardtime ซึ่งเป็นซอฟต์แวร์ทางด้านความปลอดภัยที่มีชื่อเสียง มีที่ตั้งอยู่ในเอสโตเนียที่จัดการเรื่องการปกป้องข้อมูล Cryptography และเป็นบริษัทพัฒนาระบบลายมือชื่อดิจิทัลที่ใช้เทคโนโลยี Blockchain โดยเป็นหนึ่งในผู้ใช้บริการที่ใหญ่ที่สุดของเทคโนโลยี Blockchain ในปัจจุบัน

เอสโตเนียได้มีการพัฒนาเทคโนโลยีดิจิทัลมาเป็นเวลาหลายปีแล้ว ในช่วงกลางทศวรรษที่ ๒๐๑๐ เอสโตเนียเริ่มวางแผน และอภิปรายการริเริ่มทางไซเบอร์หลัก ๆ สองอย่างคือ การจัดตั้ง NATO CCDCOE และทีมหน่วยงานการป้องกันไซเบอร์ของเอสโตเนีย โดยปัจจุบัน ทีมป้องกันภัยไซเบอร์ของเอสโตเนียมีการประสานงานโดยเจ้าหน้าที่ของ Republic of Estonia Information System Authority (RIA) ซึ่งเป็นผู้รับผิดชอบในการควบคุมไซเบอร์สเปซทั้งหมดในประเทศ หน่วยงานนี้จะมีการใช้ทีมป้องกันในการเพิ่มขีดความสามารถเมื่อมีความจำเป็นต้องได้รับการช่วยเหลือ

หน่วยงานป้องกันภัยทางไซเบอร์นับเป็นการสร้างโมเดลนวัตกรรมที่จะมีอาสาสมัครจากทั่วประเทศ โดยจุดเน้นของหน่วยงานคือ เพิ่มความแข็งแกร่งในความเชี่ยวชาญในการป้องกันไซเบอร์ของสมาชิก เพื่อเตรียมการ และสนับสนุนการเพิ่มขีดความสามารถตามที่กำหนดในทางปฏิบัติหมายถึงการป้องกันโครงสร้างพื้นฐานสำคัญของภาครัฐเอสโตเนียและระบบโทรคมนาคมของภาคเอกชนให้รอดพ้นจากการถูกโจมตีทางไซเบอร์ นอกจากนี้ยังมีการสร้างความตระหนักและให้แนวปฏิบัติที่เป็นเลิศ ในการทดลองทำ และฝึกอบรม นับเป็นส่วนหนึ่งของกิจกรรมที่เพิ่มการแลกเปลี่ยนข้อมูล และร่วมมือกันของผู้เชี่ยวชาญด้านความปลอดภัยของข้อมูลทั้งจากภาครัฐ และเอกชนผ่านทางเครือข่ายผู้เชี่ยวชาญ เป็นตัวช่วยเพิ่มขีดความสามารถให้กับผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

ในปี ค.ศ. ๒๐๐๗ เอสโตเนียเผชิญกับการโจมตีไซเบอร์อย่างกว้างขวางจากความขัดแย้งทางการเมืองระหว่างเอสโตเนียและรัสเซีย การโจมตีมีเป้าหมายไปที่โครงสร้างพื้นฐานทางดิจิทัลทำให้ ๕๘ เว็บไซต์ล่มซึ่งส่งผลกระทบต่อรัฐบาล การเงิน และสื่อ ซึ่งเป็นภัยคุกคามทางไซเบอร์ครั้งแรกในระดับประเทศ

การเรียนรู้จากประสบการณ์ทำให้เอสโตเนียตัดสินใจเสริมสร้างความสามารถในการป้องกัน และจัดการความมั่นคงปลอดภัยไซเบอร์ได้ด้วยตนเอง โดยปัจจุบันประเทศได้มีการใช้เทคโนโลยี Blockchain มาใช้อย่างกว้างขวางเพื่อทำให้เกิดความมั่นใจว่าข้อมูลมีความถูกต้องอยู่เสมอ และลดความเสี่ยงต่อผลเสียหายจากการโจมตีทางไซเบอร์ การร่วมมือระหว่าง

ภาครัฐและเอกชนเป็นไปอย่างอัตโนมัติ ความตระหนักรู้ของผู้ใช้บริการในเอสโตเนียถือว่าเป็นลำดับต้น ๆ ของโลก

เอสโตเนียถือเป็นหนึ่งในประเทศที่มีการพัฒนาแล้วในเรื่องของโครงสร้างพื้นฐานดิจิทัล e-government การระบุตัวตนทางดิจิทัล และการดำเนินธุรกิจแบบดิจิทัล การพัฒนาเทคโนโลยี (รวมถึงภัยคุกคามไซเบอร์) พร้อมกับสภาวะความปลอดภัยในระดับที่นานาชาติยอมรับเป็นที่ดึงดูดความต้องการและขีดความสามารถในการป้องกันภัยไซเบอร์ ดังนั้นประเทศจึงได้มีการจัดตั้งกฎพื้นฐานความปลอดภัยสำหรับรัฐและระบบกลางเพื่อเฝ้าระวัง รายงานและแก้ไขเหตุการณ์ไซเบอร์ วัตถุประสงค์คือตรวจสอบความสามารถของระบบและการใช้ประโยชน์จากช่องโหว่ของเครือข่าย และระบบจากบริการและผู้ให้บริการพื้นฐานที่สำคัญ

๒.๔.๓.๒ หน่วยงานที่เกี่ยวข้อง (Stakeholders)

๑) เจ้าหน้าที่ระบบสารสนเทศเอสโตเนีย – RIA

พระราชบัญญัติความปลอดภัยไซเบอร์เอสโตเนีย อธิบายบทบาทหน้าที่งานและรายละเอียดที่เกี่ยวกับการปฏิบัติงานของ RIA โดยเจ้าหน้าที่ RIA ทำหน้าที่ควบคุมการบริหารจัดการและจะต้องดำเนินการให้สอดคล้องกับข้อกำหนดของพระราชบัญญัติฯ และกฎหมายที่เกี่ยวข้องทั้งหมด โดยผู้ให้บริการดิจิทัลต้องอยู่ภายใต้ การควบคุมของเจ้าหน้าที่ RIA อย่างไรก็ตามจะมีหนึ่งหน่วยงานที่เกี่ยวกับการประสานงานทางทหารกับนานาชาติที่อยู่ภายใต้การดูแลของกระทรวงกลาโหม การบังคับใช้กฎหมายอาจจะใช้กับมาตรการควบคุมดูแลรัฐแบบพิเศษเพื่อให้การควบคุมดูแลภาครัฐเป็นไปตามพระราชบัญญัติฯ

๒) การควบคุมดูแลภาครัฐ

ตามที่ระบุในพระราชบัญญัติฯ RIA มีทางเลือกในการขัดขวางมากมายขึ้นอยู่กับระดับภัยคุกคามของเหตุการณ์ไซเบอร์ โดยอาจจะจำกัดการเข้าถึงระบบเพื่อจัดการหรือกำจัดภัยคุกคามทันที โดยมีเงื่อนไขบางอย่างที่ต้องสอดคล้องเพื่อให้ RIA ควบคุมดูแลภาครัฐโดยเป็นไปตามกรณี[๕] ดังต่อไปนี้

- เหตุการณ์ไซเบอร์ที่ละเมิด หรือทำความเสียหายให้กับอีกระบบ
- ผู้ดูแลระบบไม่สามารถจัดการกับภัยคุกคามที่มีต้นกำเนิดจากเหตุการณ์ไซเบอร์
- ไม่สามารถจัดการกับเหตุการณ์ไซเบอร์ ด้วยมาตรการทั่วไป
- มีบุคคลที่ไม่ได้เป็นเหตุให้เกิดความเสียหายโดยการจัดการกับเหตุการณ์ไซเบอร์

[๕] Riigikogu, (2018) Estonian Cybersecurity Act, paragraph 16.

ทั้งนี้ RIA อาจพิจารณาจำกัดการเข้าถึงระบบ และถ้ามีการปฏิบัติงานที่ส่งผลกระทบต่อบริการภายใต้ พ.ร.บ. ภาวะฉุกเฉิน จะต้องมีการแจ้งเตือนโดยเร็ว และ RIA ควรบันทึกมาตรการที่ดำเนินการ

๓) การควบคุมการบริหาร

หน่วยงาน RIA มีหน้าที่ให้สิทธิ และจำกัดสิทธิในการเข้าถึงระบบตามเงื่อนไข [๙](Estonian Cybersecurity Act, paragraph ๑๗) ดังต่อไปนี้

- เหตุการณ์ไซเบอร์ที่ละเมิดหรือสร้างความเสียหายให้กับระบบอื่น
- ผู้ดูแลระบบไม่สามารถจัดการกับเหตุการณ์ไซเบอร์ได้
- ไม่สามารถจัดการกับเหตุการณ์ไซเบอร์ด้วยมาตรการทั่วไป
- มีบุคคลที่ไม่ได้เป็นเหตุให้เกิดความเสียหายโดยการจัดการกับเหตุการณ์ไซเบอร์

การดำเนินการควบคุมการบริหารจะคล้ายกับมาตรการควบคุมดูแลภาครัฐ ที่กำหนดโดย RIA ต้องแจ้งเตือนให้เร็วที่สุด และบันทึกมาตรการที่ใช้

๒.๒.๓.๓ ข้อกฎหมายที่เกี่ยวข้อง (Laws and Regulations)

๑) General Data Protection Regulation (GDPR)

เอสโตเนียมีปัญหาในการดำเนินการ GDPR เพราะมี “พระราชบัญญัติคุ้มครองข้อมูลส่วนตัว” ตั้งแต่ปี ค.ศ. ๒๐๑๖ โดยครอบคลุมทุกมุมมองของการปกป้องข้อมูลส่วนบุคคล แต่พระราชบัญญัติดังกล่าวเกิดขึ้นก่อนที่กลุ่มประเทศสหภาพยุโรปออก GDPR จึงต้องมีการดำเนินการแก้ไขในข้อกฎหมายเดิมที่ไม่สอดคล้องกับ GDPR รัฐบาลจึงได้นำเสนอร่างกฎหมายคุ้มครองข้อมูลส่วนตัวฉบับใหม่ต่อสภา

รัฐสภาได้ยอมรับร่างกฎหมายการดำเนินการคุ้มครองข้อมูลส่วนตัว โดยร่างกฎหมายนี้ได้เปลี่ยน ๑๓๐ ประเด็นทางกฎหมายเดิมของเอสโตเนียเพื่อให้สอดคล้องกับ GDPR โดยปัจจุบันยังอยู่ระหว่างการพิจารณาของรัฐสภา แต่อย่างไรก็ตาม ยังมีข้อบังคับเดิมในคุ้มครองข้อมูลส่วนบุคคลที่ใช้อยู่ ดังนั้นการดำเนินการให้สอดคล้องตาม GDPR จะไม่ส่งผลกระทบอย่างมีนัยสำคัญมากนัก

๒) พระราชบัญญัติความปลอดภัยไซเบอร์เอสโตเนีย (คำสั่ง NIS)

คำสั่งที่สำคัญอันหนึ่งโดยสหภาพยุโรปปี ค.ศ. ๒๑๐๖ คือคำสั่งด้านความปลอดภัยของข้อมูล และเครือข่าย ๒๑๐๖/๑๑๔๘ โดยจะต้องดำเนินการให้เสร็จสิ้นภายใน ๑๐ พฤษภาคม ค.ศ. ๒๐๑๘ โดยเอสโตเนียเป็นประเทศในไม่กี่ประเทศที่ได้มีการปฏิบัติตามคำสั่ง

---

[๙]Ibid., paragraph 17.

ได้ก่อนกำหนด โดยประกาศพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ (Estonian Cybersecurity Act) สำเร็จในวันที่ ๙ พฤษภาคม ค.ศ. ๒๐๑๘ [๑๐]

พระราชบัญญัติฯ ของเอสโตเนียเป็นหนึ่งในการพัฒนาที่ก้าวหน้าที่สุดในด้านความปลอดภัยไซเบอร์ที่มีเกี่ยวกับกฎหมายของยุโรป วัตถุประสงค์หลักคือกำหนดให้ “ข้อกำหนดสำหรับการบำรุงรักษาระบบเครือข่าย และข้อมูลที่จำเป็นต่อการทำงานของภาคสังคม และภาครัฐ และการกำหนดอำนาจทางเครือข่าย และระบบสารสนเทศ รวมทั้งการกำหนดความรับผิดชอบ และให้คำแนะนำในการป้องกัน และแก้ไขเหตุการณ์ไซเบอร์”[๑๑]

ส่วนหลักของพระราชบัญญัติฉบับนี้มาจากคำสั่ง NIS คือ ข้อบังคับในการดำเนินการมาตรการความปลอดภัย และแจ้งเตือนเหตุการณ์ไซเบอร์ โดยจะเกี่ยวข้องกับผู้ปฏิบัติงานบริการ และเครือข่ายดิจิทัลที่สำคัญในเอสโตเนีย นอกจากนี้พระราชบัญญัติดังกล่าวยังได้กำหนดหน้าที่ของ State Information System Authority (RIA) โดยพระราชบัญญัติสามารถแบ่งออกเป็น ๔ บทที่สำคัญ โดยในบทแรกจะเป็นเพียงการนิยามความรับผิดชอบ และการดำเนินการโดยส่วนสำคัญจะถูกกำหนดไว้ในบท ๒ คือข้อผูกมัดเพื่อประกันความมั่นคงปลอดภัยไซเบอร์ บท ๓ การประกันความมั่นคงปลอดภัยไซเบอร์ และบท ๔ การควบคุมดูแลการทางรัฐและบริหาร

พระราชบัญญัติได้กำหนดหลักการเพื่อประกันความมั่นคงปลอดภัยไซเบอร์ไว้ดังต่อไปนี้ [๑๒]

- หลักการส่วนบุคคล – เพื่อประกันว่าระบบความปลอดภัยที่จะต้องมีสำหรับผู้ให้บริการ

- หลักการคุ้มครองความถูกต้อง – ผู้ให้บริการต้องแน่ใจในความเสี่ยงที่ปรากฏในระบบและใช้มาตรการจัดการที่เหมาะสม

- หลักการลดผลกระทบ – ในกรณีที่เกิดเหตุการณ์ ผู้ให้บริการต้องใช้มาตรการจัดการที่หลีกเลี่ยงการเพิ่มขึ้นของเหตุการณ์หรือแพร่กระจายไปยังระบบอื่น และต้องแจ้งต่อผู้ควบคุมดูแลตามพระราชบัญญัติฯ

- หลักการการร่วมมือ – ในการแก้ปัญหาไซเบอร์ควรมีการร่วมมือกันจากหลายฝ่าย และต้องพิจารณาการเชื่อมโยงกันระหว่างระบบและบริการที่พึ่งพากัน

๓) มาตรการความปลอดภัยที่กำหนดโดยพระราชบัญญัติ

พระราชบัญญัติฯ กำหนดให้ผู้ให้บริการใช้มาตรการความปลอดภัยต่อข้อมูล และองค์กรเพื่อป้องกัน และแก้ไขเหตุการณ์ไซเบอร์ ทั้งนี้เพื่อป้องกันบรรเทาผลกระทบต่อความปลอดภัย และบริการของระบบ เพื่อให้สอดคล้องกับข้อกำหนด ดังนั้นผู้ให้บริการต้อง

---

[๑๐] Ibid.

[๑๑] Ibid., paragraph 1.

[๑๒] Ibid., paragraph 6

เตรียมการประเมินความเสี่ยงของระบบ โดยจะต้องสามารถจัดการความเสี่ยงที่เหตุการณ์ไซเบอร์จะส่งผลกระทบต่อระบบความปลอดภัยและความต่อเนื่องในการให้บริการ โดยจะต้องหาความเสี่ยงที่เกิดขึ้นและผลที่ตามมาของเหตุการณ์ไซเบอร์ ยิ่งไปกว่านั้นจะต้องเน้นมาตรการที่องค์การจะใช้ในการแก้ปัญหา การประเมินความเสี่ยงควบคู่กับข้อกำหนดทางความปลอดภัย และรายละเอียดของมาตรการที่ใช้กับความปลอดภัย โดยจะต้องเขียนไว้ในเอกสาร หรือส่งมอบให้กับ RIA ตามเวลาที่กำหนด นอกจากนี้ ผู้ให้บริการ และเครือข่ายต้องใช้ทุกมาตรการที่สามารถลดผลกระทบและการแพร่กระจายของเหตุการณ์ไซเบอร์ ถึงแม้ว่าจะมีการจำกัดการเข้าถึงระบบหรือเครือข่ายก็ตาม

สิ่งสำคัญสำหรับมาตรการความปลอดภัยไซเบอร์ตามพระราชบัญญัติที่ต้องมี คือ ระบบเฝ้าระวัง และกลไกการตรวจพบ ซึ่งจะแจ้งการปฏิบัติการ หรือซอฟต์แวร์ที่อาจจะมีผลกับระบบความปลอดภัย ทุกข้อมูลจะต้องพร้อมมีตลอดกระบวนการเฝ้าระวัง และควรจะส่งมอบให้กับ RIA

นอกจากการจัดทำเอกสารในเรื่องประเมินความเสี่ยงแล้ว ผู้ให้บริการต้องเตรียมเอกสารสำหรับการตรวจความเพียงพอ และสอดคล้องของมาตรการที่ใช้ รวมทั้งต้องรักษาเอกสารไว้ไม่น้อยกว่า ๓ ปี โดยข้อกำหนดของการเตรียมการประเมินความเสี่ยง และรายละเอียดของมาตรการที่ใช้ จะถูกกำหนดโดยรัฐมนตรีที่รับผิดชอบเรื่องนี้ ผู้ให้บริการจะต้องรับผิดชอบต่อหน่วยงานภายนอกที่ทำงานร่วมกัน ซึ่งคล้ายกับประเทศ อื่น ๆ โดยเป็นผู้บริหารระบบ เจ้าของระบบหรืออื่น ๆ เพื่อประกันว่าจะใช้มาตรการความปลอดภัยตลอดห่วงโซ่การดำเนินงาน

๔) ข้อผูกมัดการแจ้งเหตุการณ์ไซเบอร์

จากคำสั่ง NIS ทุกประเทศจะต้องมีกลไกในการแจ้งเตือน เพื่อให้สามารถรับมือกับสถานการณ์ได้ทันท่วงที ในประเทศเอสโตเนีย พระราชบัญญัติกำหนดให้ผู้ให้บริการแจ้งเตือนเหตุการณ์ไซเบอร์ทันทีที่ทราบ หรือภายใน ๒๔ ชั่วโมง แม้ว่าจะไม่ได้เป็นข้อกำหนดที่ต้องแจ้ง RIA ถึงผลกระทบและขนาดผลกระทบทุกอย่าง ซึ่งผู้ให้บริการต้องรายงานทุกกรณีที่มีเหตุการณ์ที่มีผลกระทบสำคัญต่อความปลอดภัยของระบบ หรือความต่อเนื่องในการให้บริการที่เกิดขึ้น

- เมื่อผลกระทบทำความเสียหายอย่างน้อยตามที่ประเมินความเสี่ยงไว้
- ไม่สามารถให้บริการได้อย่างต่อเนื่อง หลังจากระยะเวลาตามที่กำหนด หรือตาม SLA
- ถ้าส่งผลต่อการรบกวนการให้บริการต่อหน่วยงานอื่น
- การแก้ไขความต่อเนื่องของการให้บริการต้องใช้มาตรการพิเศษที่บรรยายไว้ในการประเมินความเสี่ยง
- ความเสียหายอย่างมีนัยสำคัญต่อผู้ให้บริการ หรือผู้ใช้บริการ
- เมื่อมีอย่างน้อย ๑ บริการของสมาชิกสหภาพยุโรปถูกรบกวน

ทั้งนี้ การแจ้งต่อ RIA ต้องมีรายงานที่มีข้อมูลเกี่ยวกับสาเหตุของเหตุการณ์ เวลาที่ใช้แก้ปัญหา มาตรการที่ใช้ และผลกระทบที่เกิด

นอกจากแจ้งต่อ RIA แล้ว ต้องแจ้งต่อหน่วยงานอื่นที่ได้รับผลกระทบโดยเร็ว ถ้าไม่ได้แจ้งตรงต่อหน่วยงาน ก็ควรต้องมีการประกาศต่อสาธารณะ ในกรณีที่ไม่สามารถทำตามข้อกำหนด ทาง RIA อาจจะแจ้ง ผู้ให้บริการสำหรับการเตือนนี้ รูปแบบ และวิธีการของรายงานเป็นไปตามที่รัฐมนตรีที่เกี่ยวข้องกำหนด

จากวัตถุประสงค์ และโครงสร้างของ NIS ผู้ให้บริการดิจิทัลจะต้องมีความรับผิดชอบเพิ่มในส่วนของการรายงานเหตุการณ์ไซเบอร์ และมาตรการความปลอดภัยที่ใช้

๕) การประกันความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัติฯ กำหนดว่าทุกการร่วมมือเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ การป้องกัน และแก้ปัญหาเหตุการณ์ไซเบอร์ที่อยู่ภายใต้กรอบพระราชบัญญัติเป็นหน้าที่ของ RIA โดย RIA จะตรวจดูโดเมนของ IP address ในเอสโตเนียโดยใช้รหัสประเทศ และวิเคราะห์ความเสี่ยงต่อระบบความปลอดภัย และผลกระทบต่อรัฐ สังคม และระบบความปลอดภัย

ตามพระราชบัญญัติ RIA มีหน้าที่แจ้งเตือนประชาชน และขั้นตอนในการหลีกเลี่ยงการเกิด หรือลดผลกระทบเหตุการณ์ไซเบอร์ การแจ้งเตือนจะรวมถึงมาตรการป้องกัน และวิธีการตอบสนองในการแก้ไขเหตุการณ์ไซเบอร์ที่เกิดขึ้นแล้ว

คณะกรรมการ RIA ทำงานร่วม และแบ่งปันข้อมูลกับองค์กรของรัฐที่รับผิดชอบความปลอดภัยด้านเครือข่ายและข้อมูล รวมถึง ENISA (เจ้าหน้าที่สหภาพยุโรปที่รับผิดชอบเรื่องนี้) โดยคาดว่าจะมีการสื่อสารเพื่อป้องกันและแก้ไขเหตุการณ์ไซเบอร์ตามข้อตกลงระหว่างประเทศหรือกฎหมายสหภาพยุโรป สิทธิในการแจ้งเตือนนี้ไม่ควรเป็นผลร้ายต่อความปลอดภัยของประเทศ หรือนำไปสู่อาชญากรรม และ RIA ควรพิจารณาผลกระทบทางธุรกิจของผู้ให้บริการเพื่อให้เป็นความลับทางธุรกิจ

พระราชบัญญัติยังกำหนดให้ RIA รักษาฐานข้อมูลเหตุการณ์ไซเบอร์ที่ลงทะเบียนไว้ เพื่อเก็บรักษาข้อมูลและใช้ในการวิเคราะห์เพื่อหาทางแก้ไขเหตุการณ์ ฐานข้อมูลนี้ยังเป็นตัวสนับสนุนข้อผูกมัดของ RIA กับการปฏิบัติการควบคุมดูแลอื่น ๆ ตราบใดที่ไม่ขัดต่อกฎหมาย ฐานข้อมูลนี้จะต้องไม่เปิดเผยต่อสาธารณะ โดยจะต้องมีการจำกัดการเข้าถึงของทะเบียนข้อมูลเพื่อใช้เป็นการภายในเท่านั้น รายละเอียดเกี่ยวกับฐานข้อมูลควรจัดตั้งโดยรัฐมนตรีที่เกี่ยวข้องเป็นผู้กำหนด

๖) กฎหมายอื่น

นอกจากพระราชบัญญัติความปลอดภัยไซเบอร์และคุ้มครองข้อมูลส่วนตัวแล้ว มีกฎหมายอีกบางส่วนที่มีผลต่อข้อบังคับความมั่นคงปลอดภัยไซเบอร์ เช่น พระราชบัญญัติฉุกเฉินที่กำหนดกฎหมายพื้นฐานในการจัดการวิกฤตต่าง ๆ รวมถึงการเตรียมตัวสำหรับภาวะฉุกเฉินและการแก้ไขปัญหารวมถึงการประกันความต่อเนื่องในการปฏิบัติการ

พระราชบัญญัติข้อมูลสาธารณะกำหนดให้ใช้ฐานข้อมูลของรัฐและการปกครองส่วนท้องถิ่น ยิ่งไปกว่านั้นหัวข้อส่วนใหญ่ที่ศึกษาในพระราชบัญญัติการสื่อสารอิเล็กทรอนิกส์จะเป็นการอธิบายข้อกำหนดการให้บริการสื่อสารเพื่อประกันความปลอดภัยและถูกต้องของเครือข่ายและบริการสื่อสารข้อมูล

๒.๔.๓.๔ แนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

๑) ความเป็นมาของกลยุทธ์

เอสโตเนียยึดหลักการความปลอดภัยเป็นเรื่องของทุกคน และไม่สามารถจัดการด้วยคนใดคนหนึ่งอย่างอิสระ ทำให้มีโครงสร้างข้ามกันในองค์กรเพื่อให้การร่วมมือเป็นไปได้ด้วยดี โดยในปี ค.ศ. ๒๐๐๙ เอสโตเนียได้มีการตั้งสภาความปลอดภัยไซเบอร์ภายใต้คณะกรรมการความปลอดภัยของรัฐบาล โดยมีบทบาทในการอำนวยความสะดวกในการร่วมมือทุกระดับระหว่างหน่วยงาน และเจ้าหน้าที่ที่รับผิดชอบความมั่นคงปลอดภัยไซเบอร์ และเพื่อประกันว่าการดำเนินงานเป็นไปตามวัตถุประสงค์ของรัฐสภา นำโดยรัฐมนตรีว่าการกระทรวงเศรษฐกิจและการสื่อสาร

พระราชบัญญัติความปลอดภัยไซเบอร์ กำหนดรายละเอียดหน้าที่ของ RIA ในการควบคุมดูแลและบังคับสิ่งที่เกี่ยวกับความปลอดภัยไซเบอร์ของประเทศ โดย RIA จัดตั้งโดยเจ้าหน้าที่ระบบสารสนเทศของประเทศในเดือนเมษายน ค.ศ. ๒๐๑๑ โดยปฏิบัติงานภายใต้รัฐมนตรีว่าการกระทรวงเศรษฐกิจและการสื่อสาร ค่าใช้จ่ายรวมอยู่ในงบประมาณของรัฐ ผู้อำนวยการที่ถูกแต่งตั้งโดยรัฐมนตรีได้นำเสนอแนวทางการดำเนินงานต่อเลขาธิการกระทรวงฯ ดังนี้

- RIA จะประสานงานการพัฒนาและบริหารระบบสารสนเทศเพื่อให้ระบบสารสนเทศปฏิบัติงานระหว่างหน่วยงานได้ จัดกิจกรรมเกี่ยวกับความปลอดภัยข้อมูลและจัดการเหตุการณ์ความปลอดภัยในเครือข่ายคอมพิวเตอร์

- RIA เป็นผู้นำการพัฒนาระบบสารสนเทศแห่งชาติเพื่อให้มีความปลอดภัย มีการพัฒนาความปลอดภัยของ E-State (ระบบการทางานของรัฐแบบดิจิทัล) RIA ยังจัดการ และคุ้มครองเครือข่ายอินเทอร์เน็ตของรัฐ โดยมีเป้าหมายเพื่อให้การระบุตัวตนทางดิจิทัลสามารถใช้ในทั่วโลกได้ มีการพัฒนาความปลอดภัยของเอกสาร และชั้นการแลกเปลี่ยนข้อมูล นอกจากนี้ RIA รับผิดชอบดูแลการทำงาน และคุ้มครองเครือข่ายบรอดแบนด์ของรัฐ งานบางอย่างของ RIA ได้รับงบประมาณ จากสหภาพยุโรปเพื่อพัฒนาสังคมข้อมูลข่าวสาร จัดลำดับวิธีการประยุกต์ การนำเสนอโครงการที่ได้รับความเห็นชอบ และปรึกษาการให้งบประมาณต่าง ๆ การเพิ่มความตระหนักรู้เกี่ยวกับสังคมข้อมูลข่าวสาร และอื่น ๆ ที่เกี่ยวกับความปลอดภัยไซเบอร์

นอกเหนือจากความรับผิดชอบที่กล่าวมาแล้วข้างต้น RIA มีภาระหน้าที่ดูแลความปลอดภัยไซเบอร์ของเอสโตเนีย ซึ่งจะต้องพัฒนากลยุทธ์ และนโยบายความปลอดภัยไซเบอร์ เฝ้าระวังเครือข่าย และแก้ปัญหาเหตุการณ์ไซเบอร์ โดยกรอบงานมี ดังนี้

CERT-EE รับผิดชอบการจัดการเหตุการณ์ความปลอดภัยของเครือข่ายในประเทศ

CIIP คุ้มครองระบบสารสนเทศของโครงสร้างพื้นฐานสำคัญอย่างยิ่งยวด เพื่อให้การทำงานเป็นไปอย่างราบรื่น และมีประสิทธิภาพตามพระราชบัญญัติความปลอดภัยไซเบอร์

ISKE ระบบรักษาความปลอดภัยสารสนเทศ ๓ ระดับ ที่พัฒนามาตรฐานภาครัฐและช่วยกระบวนการรักษาความปลอดภัยในระบบสารสนเทศ

การบริหารจัดการวิกฤต จัดตั้งการป้องกัน และประสานงานในการจัดการเหตุฉุกเฉิน และวิกฤตที่เกิดจากเหตุการณ์ไซเบอร์

การควบคุมดูแล ดูแลตามพระราชบัญญัติตรวจสอบมาตรการรักษาความปลอดภัย ขององค์กรของระบบสารสนเทศ ได้แก่ เจ้าหน้าที่การปกครองท้องถิ่นและรัฐ ผู้ให้บริการที่จำเป็นและสำคัญ ผู้ให้บริการดิจิทัล ผู้ให้บริการที่เชื่อถือได้ และองค์กรอื่น ๆ ที่มีรายชื่อในกฎหมาย

แม้ว่าจะไม่มีพันธมิตรภาครัฐ และเอกชนอย่างเป็นทางการ แต่ RIA มีความสัมพันธ์แนบแน่นกับหน่วยงานเอกชน โมเดลการร่วมมืออยู่บนพื้นฐานของความซื่อสัตย์และศรัทธา การแบ่งปันโดยมีเป้าหมายเพื่อความปลอดภัยของโครงสร้างพื้นฐานสำคัญอย่างยิ่งยวด แทนที่จะผลักดันความรับผิดชอบออกไปให้หน่วยงานอื่น ๆ ทำให้ไม่มีบทบาทในแบบแผนความปลอดภัยไซเบอร์ในภาคธุรกิจ หรืออุตสาหกรรม เพราะมีผู้ชำนาญทางสารสนเทศ ที่เป็นสมาชิกทีมการป้องกันไซเบอร์แห่งชาติที่มีตำแหน่งในโครงสร้างที่สำคัญของชาติ

๒) กลยุทธ์ความปลอดภัย

เอสโตเนียเป็นประเทศแรกที่พัฒนากลยุทธ์ความปลอดภัยไซเบอร์ในปี ค.ศ. ๒๐๐๘ - ๒๐๑๓ กลยุทธ์มีการปรับปรุงเมื่อปี ค.ศ. ๒๐๑๔ ให้ครอบคลุมช่วงระยะเวลาปี ค.ศ. ๒๐๑๔ - ๒๐๑๗ กลยุทธ์มีเอกสารหลักสำหรับการวางแผน และปฏิบัติงานความปลอดภัยไซเบอร์ และยังกำหนดความปลอดภัยไซเบอร์ข้ามฟังก์ชันไว้ด้วย เพราะจะต้องให้เกิดการประสานกันในหลายส่วนของความปลอดภัยแสดงในรูปที่ ๕ ตาม Sectoral Methodology[๑๓] ดังต่อไปนี้

กลยุทธ์ปี ค.ศ. ๒๐๑๔ - ๒๐๑๗ มีวัตถุประสงค์ดังนี้

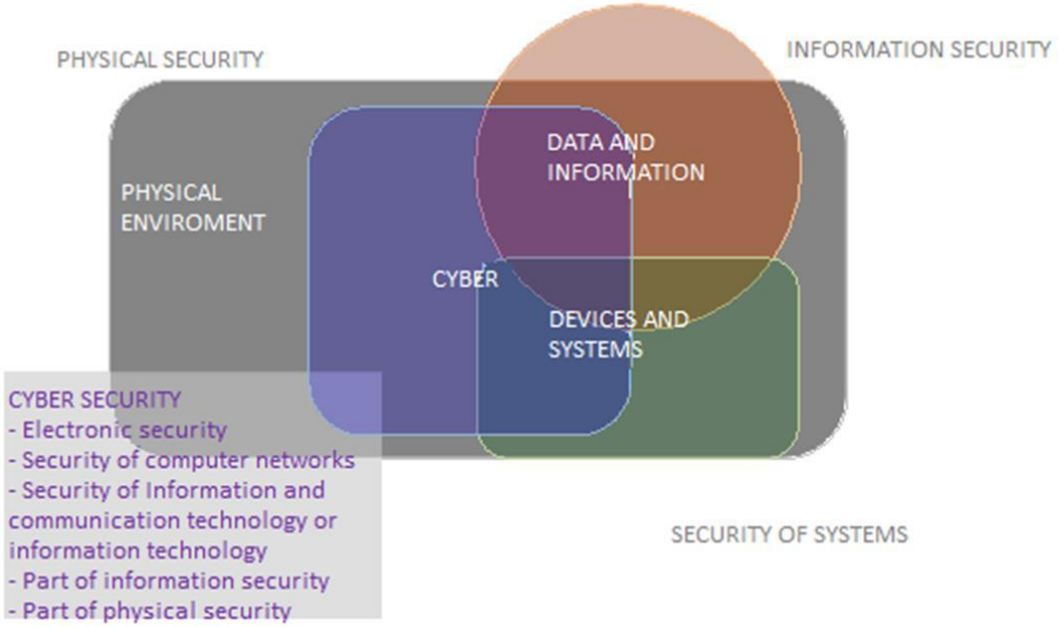
- ดำเนินงานตามมาตรการความปลอดภัยของระบบ
- รักษา และปรับปรุงตำแหน่งของประเทศให้อยู่ในระดับสูงทั้งด้านสมรรถนะ และการสร้างความตระหนักรู้ในความปลอดภัยไซเบอร์

---

[๑๓] Estonia Ministry of Economic Affairs and Communications. (2014), Estonia Cyber Security Strategy 2014 -2017.

- ความปลอดภัยในการใช้ระบบสารสนเทศต้องมีการสนับสนุนทางกฎหมายอย่างเหมาะสม

- รักษาตำแหน่งของประเทศในการเป็นผู้นำด้านความปลอดภัยไซเบอร์



รูปที่ ๕ : ภาคส่วนต่าง ๆ ของความมั่นคงปลอดภัยไซเบอร์ ของเอสโตเนีย

กลยุทธ์กำหนดและเรียงลำดับความสำคัญตามวัตถุประสงค์ของประเทศในระยะยาว และมีการจัดทรัพยากรและความรับผิดชอบอย่างเหมาะสม เพื่อให้มั่นใจว่าไม่มีความขัดแย้งเกิดขึ้นระหว่างนโยบาย และกลยุทธ์ รวมถึงทิศทางของประเทศ กลยุทธ์จึงควรวิเคราะห์สิ่งสำคัญที่ต้องพัฒนาก่อน รวมถึงการประเมินภัยคุกคามและมาตรการจัดการ โดยมีวิสัยทัศน์ของกลยุทธ์คือ เพื่อให้เอสโตเนียมีความปลอดภัย และสนับสนุนการทำงานแบบเปิดและสร้างความปลอดภัยของสังคม

เป้าหมายของกลยุทธ์มีรายละเอียด [๑๔] ดังนี้

- เพื่อประกันการคุ้มครองของระบบสารสนเทศภายใต้การให้บริการที่สำคัญ

- เพื่อเสริมการโต้ตอบต่ออาชญากรรมไซเบอร์

- เพื่อการพัฒนาความสามารถด้านการป้องกันไซเบอร์แห่งชาติ

- เพื่อจัดการภัยคุกคามด้านความปลอดภัยไซเบอร์ที่วิวัฒนาการขึ้นมา

- เพื่อพัฒนากิจกรรมข้ามสายงาน

---

[๑๔] Ibid.

กลยุทธ์ดำเนินการภายใต้กระทรวงเศรษฐกิจ และการสื่อสาร ซึ่งจะมีการรายงานในการดำเนินการตามมาตรการเป็นประจำทุกปี กระทรวงจะต้องประเมินรายงานว่ามีประสิทธิผลเพียงใดในแต่ละปี

นอกจากเป้าหมายแล้ว ยังมีความท้าทายในกลยุทธ์ และกระบวนการที่ต้องจัดการ เช่น การเปลี่ยนแปลงความคิด คุณค่า และลำดับความสำคัญในการแข่งขันกับหน่วยงานอื่น และควรจะมีระบบติดตามผลการดำเนินงานเพื่อปรับปรุงกลยุทธ์ให้ก้าวหน้าต่อไป เพราะประสิทธิผล และความสำเร็จของกลยุทธ์ขึ้นอยู่กับหลายปัจจัย

กลยุทธ์ในการปรึกษาสาธารณะหลัง ๒๐๑๘ (๒๐๑๙ - ๒๐๒๒) ที่จะนำมาใช้ในอนาคตอันใกล้ มีวิธีการบางอย่างเปลี่ยนไป เช่น กลยุทธ์ความปลอดภัยไซเบอร์จะเป็นส่วนหนึ่งของระบบสารสนเทศ/กลยุทธ์การพัฒนาสังคมสารสนเทศมีเป้าหมายในการจัดการสภาพแวดล้อมของข้อมูลทั้งหมดเพื่อสร้าง e-infrastructure กับชาติ กลยุทธ์ใหม่จะเน้นสังคมดิจิทัลยั่งยืนมากขึ้น วิธีเพิ่มการปรับตัวเทคโนโลยี วิธีสร้างความแข็งแกร่งนานาชาติ การกระตุ้นวิจัยและพัฒนา รวมทั้งเพิ่มการตระหนักรู้ และความเชี่ยวชาญในสังคม

นอกจากนี้ RIA ยังทำประเมินความปลอดภัยไซเบอร์ประจำปี เพื่อประเมินเหตุการณ์สำคัญทางความปลอดภัยไซเบอร์ที่เกิดขึ้นปีก่อน รวมถึงจำนวนเหตุการณ์ที่เกิด กิจกรรมมุ่งร้าย เป็นต้น และยังวิเคราะห์การพัฒนาของภัยคุกคามตามประเด็นเกี่ยวกับ GDPR อีกด้วย

๓) Three - level IT Baseline Security System ISKE

ปี ค.ศ. ๒๐๑๔ เอสโตเนียประกาศใช้มาตรฐานความปลอดภัยของข้อมูลที่พัฒนาจากภาครัฐที่มีชื่อว่า Three - level IT Baseline Security System - ISKE โดยมีพื้นฐานจากมาตรฐานของเยอรมัน (IT - Grunshutz) และปรับแก้ตามสถานการณ์ให้สอดคล้องกับเอสโตเนีย [๑๕] ดังนี้

- วางแผนฐานข้อมูล
- วางแผนระบบสารสนเทศ หรือทรัพย์สินเกี่ยวกับสารสนเทศ
- ระบุความเชื่อมโยงระหว่างฐานข้อมูล ระบบสารสนเทศ และทรัพย์สินเกี่ยวกับสารสนเทศ
- ระบุข้อกำหนดระดับชั้นของฐานข้อมูล
- ระบุข้อกำหนดระดับชั้นของระบบสารสนเทศ และทรัพย์สินเกี่ยวกับสารสนเทศ
- ระบุโครงสร้างทั่วไปที่สอดคล้องกับระบบสารสนเทศ และทรัพย์สินเกี่ยวกับสารสนเทศ

---

[๑๕] Information System Authority, 2018.

- ระบุข้อกำหนดของมาตรการความปลอดภัยสำหรับระบบสารสนเทศและทรัพย์สินเกี่ยวกับสารสนเทศ

ISKE มีมาตรการมากกว่า ๑,๐๐๐ มาตรการที่ใช้กับทรัพย์สินเกี่ยวกับสารสนเทศ ข้อบังคับรวมถึงกระบวนการทวนสอบมาตรฐาน หลังจากจัดลำดับชั้นของข้อมูล มาตรการที่เหมาะสมก็จะถูกใช้เพื่อความปลอดภัยตามที่อธิบายในคู่มือของ ISKE องค์กรต้องมีการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ เพื่อให้ระบบการจัดการความปลอดภัยดำเนินไปอย่างเหมาะสม โดยมีการตรวจสอบทุก ๆ ๒ ปี

๔) การวิเคราะห์ความเสี่ยง

RIA จะคอยกระตุ้นเตือนให้องค์กรต่าง ๆ ป้องกันบริการที่จำเป็นของตนเอง เพื่อรักษาระบบการทำงาน และข้อมูลที่จำเป็น เช่น การวิเคราะห์ความเสี่ยง โดยการกำหนดให้การประเมินความเสี่ยงควรครอบคลุมหัวข้อ ดังไปนี้

- รายละเอียดของวิธีการ และแหล่งอ้างอิงเพิ่มเติมในเอกสาร
- รายการกิจกรรม และภาวะวิกฤตที่ต้องควบคุมดูแล
- รายการทรัพยากรของระบบ
- รายการภัยคุกคาม
- รายการจุดอ่อนที่มีความเสี่ยง
- การประเมินความน่าจะเป็นของภัยคุกคาม ที่จะเกิดโดยการพิจารณาจุดอ่อนความเสี่ยงที่ทำรายการไว้ล่วงหน้า และมาตรการจัดการ
- การประเมินผลที่ตามมา หรือความร้ายแรงของผลที่เกิดจากเหตุการณ์ไซเบอร์
- รายการความเสี่ยง และสภาวะวิกฤต
- รายละเอียดมาตรการบรรเทาความเสี่ยง

ผู้ให้บริการต้องนำเสนอวิธีการ ทรัพยากร และกิจกรรมที่ใช้ประกันความปลอดภัยของระบบ และตอบสนองต่อเหตุการณ์ไซเบอร์ มาตรการต้องครอบคลุมการสำรองข้อมูล ซอฟต์แวร์ที่ใช้ การแก้ปัญหา การเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) การตรวจพบและควบคุมภัยคุกคามความปลอดภัย รวมทั้งวิธีการกู้ระบบให้ทำงานอย่างปลอดภัยและต่อเนื่อง

บทที่ ๓
การวิเคราะหาช่องว่าง (Gap Analysis)

๓.๑ สภาพการณ์การกำกับดูแลด้านเทคโนโลยีความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันของประเทศไทย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่มีผลบังคับใช้ตั้งแต่ ๒๘ พฤษภาคม พ.ศ. ๒๕๖๒ ทำให้เกิดความชัดเจนของการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ตามแผนยุทธศาสตร์ชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม อาศัยแผนของคณะกรรมการดิจิทัลฯ ในระยะเริ่มต้น โดยได้จัดตั้ง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. ณ วันที่ ๑๑ ธันวาคม พ.ศ. ๒๕๖๒ เป็นที่เรียบร้อยแล้ว ซึ่งมีหน้าที่กำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ถือได้ว่าเป็นจุดเริ่มต้นที่ดีในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

อย่างไรก็ดี ยังมีความจำเป็นต้องเร่งดำเนินการในรายละเอียดเพื่อความต่อเนื่องเชิงปฏิบัติการด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ตามที่ได้บัญญัติไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้แก่

- การจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. ซึ่งจะเป็นคณะปฏิบัติงาน เป็นผู้กำหนดแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ และกรอบครอบคลุมโครงสร้างพื้นฐานสำคัญทั้ง ๗ ด้าน ซึ่งถือเป็นเครื่องจักรกลที่สำคัญในการขับเคลื่อนนโยบายต่าง ๆ ให้สำเร็จได้ โดยตามบทเฉพาะกาลของพระราชบัญญัติได้กำหนดให้มีการจัดตั้งให้แล้วเสร็จภายใน ๙๐ วันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรียบร้อยแล้ว

- การจัดตั้งคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ กบส. ให้แล้วเสร็จภายใน ๙๐ วันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรียบร้อยแล้ว

- การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้แล้วเสร็จภายใน ๑ ปีนับแต่วันที่พระราชบัญญัติใช้บังคับ

- การแต่งตั้งเลขาธิการคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้แล้วเสร็จภายใน ๙๐ วันนับแต่วันที่จัดตั้งสำนักงาน

โดยการจัดตั้งคณะกรรมการตามขั้นตอนดังกล่าว เป็นขั้นตอนที่สำคัญและจำเป็นอย่างยิ่งที่ต้องดำเนินการให้แล้วเสร็จโดยเร็ว เนื่องจากเป็นขั้นตอนที่ทำให้คณะทำงานการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สมบูรณ์ และเริ่มกระบวนการหรือโครงการต่าง ๆ สำหรับแผนพัฒนาการกำกับดูแลในทางปฏิบัติได้ ความล่าช้าในการจัดตั้งคณะกรรมการฯ อาจส่งผลให้กระบวนการอื่น ๆ ในแผนพัฒนาการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ล่าช้าตามไปด้วย

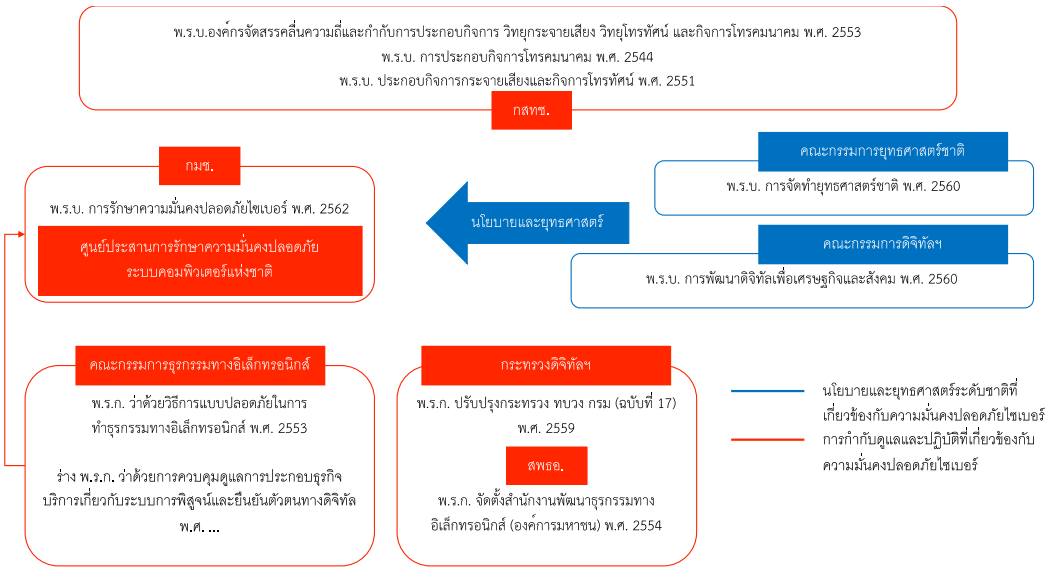
ในส่วนของกรอบครอบคลุมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทั้ง ๗ ด้าน ยังต้องการความชัดเจนในการกำหนดนิยามครอบคลุมความสำคัญและแนวทางการปฏิบัติของกิจการในแต่ละด้าน เนื่องจากโครงสร้างพื้นฐานแต่ละด้านมีลักษณะการดำเนินงาน และส่งผลกระทบต่อผู้ใช้งานที่แตกต่างกัน ในระยะเริ่มต้น มีความจำเป็นต้องดำเนินการประเมินสถานะปัจจุบันของระดับของความมั่นคงปลอดภัยไซเบอร์ของกิจการที่เกี่ยวข้องกับโครงสร้างพื้นฐานแต่ละด้าน เทียบกับมาตรฐานความมั่นคงปลอดภัยไซเบอร์ เพื่อการกำหนดทิศทางในแผนการพัฒนาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญแต่ละด้านในระยะต่าง ๆ

นอกจากนี้ การกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ไม่ควรเป็นการกำหนดมาตรฐานเพื่อประเมินหน่วยงาน หรือกิจการต่าง ๆ ที่เกี่ยวข้องเพียงอย่างเดียว ควรมีการดำเนินการสร้างความชัดเจนในการสนับสนุนเกี่ยวกับแนวทางการพัฒนาระบบนิเวศน์ด้านความมั่นคงปลอดภัยไซเบอร์ ให้มีความเข้มแข็ง ช่วยให้เกิดความร่วมมือในการป้องกันด้านความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานทุกภาคส่วน รวมถึงกิจการเอกชนในระดับต่าง ๆ ที่เกี่ยวข้อง ได้แก่ การเพิ่มความแข็งแกร่งในความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ การเตรียมการและการเพิ่มขีดความสามารถในการป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ การแบ่งปันข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

อย่างไรก็ดี เมื่อพิจารณาข้อมูลกฎหมายที่กำหนดอำนาจหน้าที่ให้หน่วยงานทำหน้าที่กำกับดูแลในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ยังมีหน่วยงานที่รับผิดชอบดูแลความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานแต่ละด้านอยู่แล้ว จึงอาจทำให้เกิดประเด็นความสอดคล้องในการดำเนินการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในภาพรวม พอสรุปรายละเอียดได้ดังนี้

การกำหนดอำนาจหน้าที่อย่างชัดเจนในเรื่องความปลอดภัยโครงข่ายต่อหน่วยงานกำกับดูแล ในระดับพระราชบัญญัติของ ๓ หน่วยงาน ได้แก่ กสทช. กระทรวงดิจิทัลฯ และคณะกรรมการดิจิทัลฯ ไม่ได้มีการกำหนดไว้ มีเพียงคณะกรรมการดิจิทัลฯ ที่ใช้อ้างอิงตามในหัวข้อเป้าหมายการดำเนินการเท่านั้น โดยมีหน้าที่กำหนดแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งมีการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์เป็นหนึ่งในแผนยุทธศาสตร์ชาติ

เมื่อมีการจัดตั้ง กมช. เพื่อรับผิดชอบในเรื่องความมั่นคงปลอดภัยไซเบอร์ โดยมีหน่วยงานที่มีหน้าที่เกี่ยวข้องกับการกำกับดูแลความมั่นคงปลอดภัยโดยตรงในแต่ละด้านอยู่แล้ว จึงมีความจำเป็นต้องแบ่งแยกการกำกับดูแลให้ชัดเจนกับหน่วยงานกำกับดูแลอื่น ๆ เช่น ความมั่นคงปลอดภัยโครงข่าย ความมั่นคงปลอดภัยของระบบสารสนเทศ ความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ความมั่นคงปลอดภัยของโครงข่ายที่สำคัญ ความมั่นคงปลอดภัยของการเชื่อมโยงอินเทอร์เน็ต และควรมีการเพิ่มเติมอำนาจหน้าที่ในการกำกับดูแลเหล่านี้ รวมทั้งการเชื่อมโยง การกำกับดูแลกับหน่วยงานอื่น ๆ ด้วย ทั้งนี้ การเชื่อมโยงของหน่วยงานและกฎหมายที่กล่าวมาข้างต้นแสดงอยู่ในรูปที่ ๖



รูปที่ ๖ : ความเชื่อมโยงหน่วยงานและกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

อย่างไรก็ตาม หน่วยงานกำกับดูแลโดยตรงในแต่ละด้านของโครงข่ายสำคัญ อาจยังไม่ได้มีการจัดตั้งหน่วยงานภายในเพื่อรองรับภารกิจนี้ไว้ ดังนั้น อาจจะเกิดปัญหาในทางปฏิบัติเมื่อพระราชบัญญัติมีผลบังคับใช้ อีกทั้งหน่วยงานกำกับดูแลยังขาดประสบการณ์ในการดูแลความมั่นคงโครงข่าย เนื่องจากไม่เคยมีการดำเนินการเรื่องนี้มาก่อน ซึ่งอาจทำให้ขาดความเชื่อถือและมีการตั้งข้อสงสัยสำหรับการออกกฎเกณฑ์ ข้อบังคับต่าง ๆ เป็นการเฉพาะ ที่เกิดขึ้นในภาคปฏิบัติจากผู้ประกอบการภายใต้การกำกับดูแล ที่ได้มีการดำเนินการอย่างเป็นระบบเป็นเวลานานแล้วพอสมควร โดยไม่ได้รอการเข้ามาสั่งการกำกับดูแลจากหน่วยงานกำกับดูแล

มีข้อสังเกตว่า การออกประกาศของสำนักงานฯ ที่อ้างตามพระราชกำหนดว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ มีความชัดเจนในเรื่องการกำกับดูแลความมั่นคงไซเบอร์มากที่สุด อย่างไรก็ตาม สำนักงานธุรกรรมอิเล็กทรอนิกส์ มีอำนาจหน้าที่ในระดับพระราชกำหนดที่ให้แต่เพียงการส่งเสริม การเรียนรู้ ไม่ได้เป็นอำนาจกำกับดูแลโดยตรง ทั้งนี้พระราชกำหนดฉบับนี้ออกโดยอาศัยฐานอำนาจของพระราชบัญญัติธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ที่ไม่มีความชัดเจนในเรื่องหน้าที่รับผิดชอบของความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยโครงข่าย

นอกจากนี้ คำนิยามที่เกี่ยวข้องในด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในกฎหมายและบทบัญญัติต่าง ๆ มีความไม่ชัดเจนและไม่สอดคล้องในหลายกรณี เช่น ความมั่นคงปลอดภัยโครงข่าย ความมั่นคงปลอดภัยของระบบสารสนเทศ ความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ความมั่นคงปลอดภัยของโครงข่ายที่สำคัญ ความมั่นคงปลอดภัยของการเชื่อมโยงอินเทอร์เน็ตมีความจำเป็นต้องเรียบเรียงให้เป็นไปในทิศทางเดียวกัน

๓.๒ ประเด็นท้าทายในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

ในปัจจุบัน จำนวนผู้ใช้บริการทางข้อมูลสารสนเทศต่าง ๆ ผ่านระบบเครือข่ายโทรศัพท์ที่ทวีจำนวนขึ้นอย่างรวดเร็ว ระบบการบริหารจัดการเครือข่ายที่ถูกพัฒนาเป็นระบบเปิดมากยิ่งขึ้น เพื่อรองรับการเข้าถึงระบบได้จากทั่วทุกมุมโลก ประกอบกับความซับซ้อนของเทคโนโลยีและโครงสร้างของเครือข่ายที่เพิ่มสูงขึ้น ทำให้การรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นความท้าทายอย่างยิ่งของผู้ประกอบการ

จากการศึกษารวบรวมข้อมูลและบทสัมภาษณ์ตัวแทนที่เกี่ยวข้องกับการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย ผู้ประกอบการขนาดใหญ่มีความพร้อมในระดับหนึ่ง ในขณะที่ผู้ประกอบการขนาดกลางและเล็กอื่น ๆ ยังมีความแตกต่างในด้านความพร้อมขององค์กรอยู่ อย่างไรก็ดี จำนวนเหตุภัยคุกคามไซเบอร์บนเครือข่าย ตลอดจนความพยายามทำให้เกิดการหยุดชะงักของบริการ หรือ Distributed Denial of Service (DDoS) มีแนวโน้มจะเพิ่มสูงขึ้น ภาครัฐจึงควรมีบทบาทในการสนับสนุน เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์โดยรวมในทุกระดับ โดยเฉพาะในผู้ประกอบการขนาดกลางและเล็ก ในการรองรับและบรรเทาความท้าทายในการป้องกันและรับมือกับปัญหาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง ประเด็นความท้าทายต่าง ๆ ที่สำคัญสามารถสรุปได้ดังนี้

๓.๒.๑ ขาดความเชื่อใจในการประสานความร่วมมือ

การแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ จำเป็นต้องอาศัยความร่วมมือระหว่างผู้ที่เกี่ยวข้องอย่างกว้างขวาง เนื่องจากการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นกระบวนการที่ซับซ้อน ไม่มีมาตรฐานในการจัดการที่ชัดเจน แตกต่างกันไปในแต่ละองค์กร เกี่ยวข้องกับหลายภาคส่วน สามารถเปลี่ยนแปลงได้อย่างรวดเร็ว และต้องใช้งบประมาณค่อนข้างสูงโดยมิได้สร้างรายได้โดยตรง แต่เนื่องจากการประสานความร่วมมือจากทุกภาคส่วนในด้านนี้เป็นความท้าทายอย่างสูง เนื่องจากมีข้อมูลองค์กรที่โดยปกติเป็นคู่แข่งทางการค้าซึ่งเป็นความลับและมีความอ่อนไหวสูง ตลอดจนข้อมูลเหล่านี้มีต้นทุนการดำเนินงาน ดังนั้นความร่วมมือจากภาคเอกชนจึงมักเป็นการให้ความร่วมมือตามหน้าที่

๓.๒.๒ ขาดข้อมูลในการวิเคราะห์

ในปัจจุบัน ประเทศไทยยังไม่มีการเก็บข้อมูลสถิติที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ทำให้การศึกษาลักษณะและปริมาณของเหตุภัยคุกคาม (Threat Landscape) เพื่อทำการวิเคราะห์สภาพปัญหาในด้านนี้เป็นไปได้ยาก อีกทั้งยังไม่เคยมีการประสานความร่วมมือเพื่อแลกเปลี่ยนข้อมูลดังกล่าวระหว่างผู้ประกอบการกับสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. แต่อย่างใด และยังไม่มีการกำหนดข้อปฏิบัติที่ชัดเจนเกี่ยวกับกระบวนการแจ้งเหตุภัยคุกคามไซเบอร์ (Incident Reporting) โดยภาครัฐทำให้ผู้ประกอบการมีเพียงข้อมูลภายในองค์กร ไม่มีกระบวนการแจ้งเตือนหรือแนะนำแนวทางการแก้ไขซึ่งกันและกัน เมื่อตรวจพบหรือเกิดเหตุความเสี่ยงที่เกี่ยวข้อง นอกจากนี้ ข้อมูลสถิติ

ที่เกี่ยวข้องกับภัยคุกคามที่เกิดขึ้นทั่วโลก (Threat Intelligence) สำหรับการเตรียมตัวและป้องกันปัญหาได้อย่างทันท่วงที ก็มีราคาสูง จำเป็นต้องได้รับการสนับสนุนจากภาครัฐหรือการร่วมมือกันของภาคเอกชน

๓.๒.๓ ขาดบุคลากร

ปัญหาการขาดแคลนบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในทุกแขนง ถือเป็นปัญหาและความท้าทายระดับโลก เนื่องจากมีบุคลากรที่มีความสามารถในระดับสูงจำนวนน้อยมาก และมีค่าใช้จ่ายที่สูงมากสำหรับการมีบุคลากรระดับนี้ในทุกองค์กร การแบ่งปันบุคลากรด้วยการสนับสนุนจากภาครัฐหรือความร่วมมือกันของภาคเอกชนอาจเป็นแนวทางที่คุ้มค่ากว่า

๓.๒.๔ ขาดแนวทางการสื่อสารที่เหมาะสมเมื่อเกิดเหตุภัยคุกคาม

แม้ผู้ประกอบการขนาดใหญ่จะมีความสามารถในการจัดการกับปัญหาได้ในระดับหนึ่ง แต่การแจ้งเหตุสู่ภาครัฐ ระหว่างองค์กร และสาธารณะนั้น ยังไม่มีกระบวนการที่ชัดเจน โดยเฉพาะเมื่อเหตุภัยคุกคามเกี่ยวข้องกับความมั่นคงของประเทศ เช่น แนวทางการสื่อสารกับผู้ใช้บริการสาธารณะ ควรแจ้งข้อมูลมากน้อยเพียงใด เพื่อสร้างความมั่นใจและการเสนอแนวทางการจัดการที่เหมาะสม แนวทางการสื่อสารกับหน่วยงานภาครัฐ ควรแจ้งข้อมูลอะไร อย่างไร ต่อหน่วยงานใด แนวทางการสื่อสารระหว่างองค์กร ควรแจ้งข้อมูลหรือไม่ อย่างไร เพื่อป้องกันการขยายตัวของเหตุภัยคุกคาม

๓.๒.๕ ขาดความตระหนักรู้และขาดกฎหมายที่ชัดเจน

การโจมตีการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการอาศัยจุดอ่อน ความไม่รู้หรือความประมาท ที่เป็นที่นิยมมากของแฮ็กเกอร์ เรียกว่า วิศวกรรมสังคม หรือ Social Engineering ซึ่งมักปรากฏในรูปเป็นการส่งอีเมลพร้อมไฟล์แนบ หรือการหลอกให้เข้าถึงเว็บไซต์ที่มีมัลแวร์แฝงตัวอยู่ การให้ความรู้แก่ผู้ใช้บริการทุกภาคส่วนจึงถือเป็นความจำเป็น เพื่อยกระดับความตระหนักรู้ของผู้ใช้

ในด้านกฎหมาย แม้ในปัจจุบันจะมีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมีการตั้งหน่วยงานรับผิดชอบด้านนี้โดยตรง ยังพบว่ามีกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อยู่หลายฉบับ เกี่ยวข้องกับหลากหลายหน่วยงานภาครัฐ ทำให้การบังคับใช้กฎหมายอาจเกิดปัญหาจากความทับซ้อนของอำนาจหน้าที่ของหน่วยงานที่เกี่ยวข้อง ตลอดจนยังไม่มีการออกกฎหมายรองรับถึงอำนาจในการกำกับดูแลของแต่ละหน่วยงาน ก็ทำให้เป็นการยากที่จะทำให้หน่วยงานสามารถดำเนินการได้อย่างมีประสิทธิภาพ

๓.๓ แนวโน้มด้านเทคโนโลยีที่น่าสนใจ

- มัลแวร์ กำลังได้รับการพัฒนาให้ซับซ้อนและสร้างผลกระทบที่รุนแรงขึ้น โดยเป้าหมายอาจไม่ได้อยู่ที่เงินค่าไถ่เพียงอย่างเดียว แต่อาจอยู่ที่การทำลายระบบ และขโมยข้อมูลสำคัญบนเครือข่ายโดยอาศัยค่าไถ่เป็นเครื่องมือเท่านั้น เช่น มัลแวร์ WannaCry Angler Nyetya เป็นต้น

- ผู้บุกรุก (Attackers) จำนวนมากสามารถหลบเลี่ยง หรือซ่อนตัวจากการตรวจจับของระบบ ด้วยการที่ใช้เทคโนโลยีที่ดูเหมือนเป็นปกติ เช่น การใช้คลาวด์ และการใช้เทคนิคการเข้ารหัส ซึ่งปกติถูกนำมาใช้เพื่อความปลอดภัยในการรับส่งข้อมูลบนเครือข่าย จนทำให้ผู้ปกป้องไม่สามารถแยกทราฟฟิคที่ดีออกจากทราฟฟิคที่ไม่ดีได้ ผู้ดูแลความปลอดภัยจำเป็นต้องปรับตัวต่อการเปลี่ยนแปลงจากระบบเครือข่ายที่เคยควบคุมได้อย่างเบ็ดเสร็จ ไปสู่คลาวด์และ IoT ซึ่งเป็นระบบที่กว้างขึ้น ตลอดจน การจัดสรรความรับผิดชอบระหว่างผู้เกี่ยวข้องที่ไม่ชัดเจน

- มาตรฐานเทคโนโลยี 5G ได้มาพร้อมกับเทคโนโลยีการแบ่งเครือข่ายย่อย (Network Slicing) ทำให้มีความสามารถในการรับส่งข้อมูลที่รวดเร็วขึ้น การตอบสนองที่ฉับไวขึ้น (Low Latency) ความจุในการรับส่งข้อมูลที่เพิ่มขึ้น และต้นทุนต่อเมกะบิตที่ถูกลง ทำให้กระตุ้นการเติบโตของปริมาณการรับส่งข้อมูลบนเครือข่ายให้สูงยิ่งขึ้น อย่างไรก็ดี มาตรการด้านความปลอดภัยเพื่อแบ่งแยกเครือข่ายย่อยออกจากกันเป็นสิ่งจำเป็น เพื่อปกป้องข้อมูลในแต่ละเครือข่ายย่อย และป้องกันไม่ให้ส่วนประกอบเสมือนในแต่ละเครือข่ายย่อยสื่อสารกันได้

- ลักษณะของเครือข่าย 5G ยังมีลักษณะโครงสร้างแบบกระจายศูนย์ เพื่อให้บริการได้อย่างยืดหยุ่น ณ ที่ใดก็ได้บนเครือข่าย 5G ซึ่งหมายถึงการให้บริการทั้งหมดไม่จำเป็นต้องอยู่ภายใต้การดูแลของผู้ให้บริการเครือข่าย แม้ว่าโครงสร้างแบบนี้จะมีประโยชน์มาก แต่ก็เปิดโอกาสให้เหล่าแฮ็กเกอร์สามารถเข้าถึงเครือข่ายได้ง่ายขึ้นจากแทบทุกจุด ดังนั้น ผู้ให้บริการเครือข่ายต้องเตรียมตัวรับมือกับความท้าทายด้านความปลอดภัยที่สูงขึ้นและไม่เคยมีมาก่อนอีกด้วย

- เมื่อเครือข่าย 5G ถูกนำมาใช้ จะทำให้เกิดการเพิ่มขึ้นของจำนวนอุปกรณ์ IoT อย่างก้าวกระโดด โดยมีการคาดการณ์ไว้ว่าจะมีจำนวนอุปกรณ์ IoT มากถึง ๕๐ พันล้านอุปกรณ์ทั่วโลกภายใน ค.ศ. ๒๐๒๐ ซึ่งอาจกลายเป็นจุดอ่อนที่สำคัญต่อเป้าหมายการก่อเหตุไปที่อุปกรณ์ IoT เหล่านี้ เนื่องจากอุปกรณ์มักมีการเปิดใช้งานตลอดเวลา มีการเปิดเผยข้อมูลด้านความปลอดภัยเป็นสาธารณะ อาจไม่มีการเข้ารหัสข้อมูลรหัสผ่าน ไม่สามารถพิสูจน์ตัวตนของผู้ที่พยายามเปลี่ยนการตั้งค่าต่าง ๆ ของอุปกรณ์ และอาจไม่ได้รับการดูแลอย่างสม่ำเสมอ ซึ่งปัจจุบัน ยังไม่มีการแสดงความรับผิดชอบเรื่องความปลอดภัยของอุปกรณ์ IoT อย่างชัดเจน

- การเชื่อมต่อของอุปกรณ์ IoT ผ่านอินเทอร์เน็ตจำนวนมากเพื่อเชื่อมพลังการประมวลผลที่เรียกว่า Botnet อาจถูกนำมาใช้ประโยชน์ในทางที่เป็นโทษได้ (Bad Bots) จำนวน Botnet ที่กำลังเพิ่มสูงขึ้นอย่างรวดเร็วอาจก่อให้เกิดภัยคุกคามขนาดใหญ่ที่ทำให้เครือข่ายหยุดชะงักเป็นเวลานาน ตลอดจนมีการเปลี่ยนแปลงเป้าหมายของ Botnet จากการเจาะระบบโครงสร้างพื้นฐาน ไปสู่การเจาะระบบในระดับแอปพลิเคชัน ที่มีความหลากหลายและยากแก่การป้องกัน นอกจากนี้ ยังมีแนวโน้ม

การพัฒนา Botnet ไปสู่เครือข่ายแบบ รังผึ้งติดเชื้อ หรือ Hivenet ที่สามารถสื่อสารกันได้ ทำงานประสานกันผ่านการแชร์ข้อมูล ใช้ข้อมูลของฝูงในการปฏิบัติการโดยไม่จำเป็นต้องรอคำสั่งของจ่าฝูง สามารถฝึกสอนซึ่งกันและกันได้ เมื่อเครือข่ายใหญ่ขึ้นก็สามารถจู่โจมได้มากขึ้นในเวลาเดียวกัน ซึ่งหากได้รับการพัฒนาอย่างเต็มรูปแบบ อาจก่อให้เกิดความเสียหายเพิ่มทวีคูณหลายเท่าตัว

- เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence หรือ AI) และ Machine Learning (ML) ได้ถูกนำมาใช้ในเทคโนโลยีออโตเมชัน (Automation) สำหรับการต่อสู้กับภัยคุกคามไซเบอร์ในปัจจุบัน อย่างไรก็ดี อาจยังจำเป็นต้องมีการพัฒนาเทคโนโลยีเหล่านี้ให้มีความแม่นยำ สามารถแยกแยะความ “ปกติ” และความ “ไม่ปกติ” บนเครือข่ายที่ดูแลอยู่ให้มีความแม่นยำมากขึ้น ขณะเดียวกัน มัลแวร์ที่ใช้เทคโนโลยีออโตเมชันในการโจมตีเครือข่ายก็ได้ถูกพัฒนาขึ้น โดยมีการดำเนินการอัตโนมัติแทบทุกขั้นตอน เพิ่มอัตราความสำเร็จของเหล่าอาชญากรไซเบอร์ให้สูงยิ่งขึ้นไปอีก ถือเป็นความท้ายทายของในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างยิ่ง

บทที่ ๔
ผลการศึกษา

๔.๑ การดำเนินการทางกฎหมายที่เกี่ยวข้อง

การออกประกาศพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้มีผลบังคับใช้ ถือได้ว่าเป็นจุดเริ่มต้นที่ดีในการดำเนินการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทำให้ประเทศไทยเป็นหนึ่งในเพียงไม่กี่ประเทศในโลกที่มีกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล แม้ว่าจะยังต้องมีการปรับปรุงตัวบทกฎหมายให้เกิดการยอมรับจากผู้มีส่วนได้เสียที่สำคัญต่าง ๆ จากหลากหลายภาคส่วนในระดับหนึ่ง และให้มีความทันสมัยกับสถานการณ์ หรือเหตุการณ์ด้านความมั่นคงทางไซเบอร์ที่เปลี่ยนแปลงได้อย่างรวดเร็วตลอดเวลา

อย่างไรก็ดี หากพิจารณาการดำเนินการสำหรับการกำกับดูแลในภาคปฏิบัติ ในปัจจุบันได้แล้วเสร็จในกระบวนการแต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งยังมีขั้นตอนที่สำคัญที่จำเป็นต้องเร่งดำเนินการให้แล้วเสร็จอีกค่อนข้างมาก เพื่อผลักดันให้เกิดการกำกับดูแลได้อย่างเป็นรูปธรรม ได้แก่ การดำเนินการจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ กบส. ตลอดจนการจัดตั้งสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์ การดำเนินการที่ล่าช้าอาจเป็นผลทำให้ไม่มีผู้รับผิดชอบดำเนินการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจนได้ ดังนั้น การตั้งคณะกรรมการสรรหา เพื่อดำเนินการจัดตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงเป็นขั้นตอนสำคัญที่ควรเร่งดำเนินการโดยเร็ว

แม้ว่า พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ มุ่งเน้นการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญ ๘ ด้าน แต่ขอบเขตครอบคลุมของพระราชบัญญัติฉบับนี้ ยังเป็นประเด็นที่ต้องการความชัดเจนในรายละเอียด โดยการกำหนดจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งต้องอาศัยการทำความเข้าใจถึงที่มา ความจำเป็น และลักษณะเฉพาะที่แตกต่างกันที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานที่สำคัญทั้ง ๗ ด้านที่ถูกกำหนดไว้ใน พระราชบัญญัติ จึงอาจจำเป็นต้องใช้ระยะเวลาในการกำหนดรายละเอียดให้ชัดเจน

ทั้งนี้ ยังไม่มีรายละเอียดที่เกี่ยวข้องกับการจัดการทรัพยากรต่าง ๆ เพื่อรองรับการดำเนินการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ได้แก่ งบประมาณสำหรับรองรับการดำเนินการ อัตรากำลังบุคลากรระดับปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ตลอดจนระเบียบรองรับการดำเนินการต่าง ๆ ซึ่งปัญหารายละเอียดที่ไม่ชัดเจนดังกล่าว เป็นปัญหาในลักษณะที่เป็นเงื่อนไขของกันและกัน อาทิ การไม่มีหน่วยงาน ทำให้ไม่สามารถตั้งอัตรากำลังบุคลากรได้ ตั้งงบประมาณไม่ได้ ไม่มีระเบียบรองรับ เป็นต้น

๔.๒ การดำเนินการระหว่างหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

จำนวนเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เพิ่มขึ้นอย่างรวดเร็ว และโอกาสที่จะเกิดเหตุภัยความมั่นคงปลอดภัยไซเบอร์ที่สูงขึ้นอย่างไม่เคยมีมาก่อน รวมถึงการพัฒนาความซับซ้อนของเหตุภัยความมั่นคงปลอดภัยไซเบอร์ที่สูงขึ้นอยู่ตลอดเวลา ทำให้เกิดเป็นความปกติในรูปแบบใหม่ (New Normal) ที่มีผลต่อการกำกับ และดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวคิดในการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่เกี่ยวข้อง จึงไม่ควรเป็นแนวคิดเชิงป้องกันภัยความมั่นคงปลอดภัยไซเบอร์อีกต่อไป แต่ควรมีแนวทางเตรียมความพร้อมในการดำเนินการจัดการกับภัยความมั่นคงปลอดภัยไซเบอร์ได้อย่างเหมาะสม และทันท่วงทีเมื่อมีเหตุการณ์ที่เกี่ยวข้องกับภัยความมั่นคงปลอดภัยไซเบอร์

ด้วยแนวคิดดังกล่าว จึงเป็นที่มาของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีกรอบการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในเชิงบังคับขึ้น โดยมีการให้ความสำคัญต่อการเตรียมความพร้อมสำหรับการรับมือภัยความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิด หรือไม่เกิดขึ้นก็ได้ กล่าวคือ ถึงแม้ว่าไม่มีเหตุการณ์ที่เกี่ยวข้องกับภัยความมั่นคงปลอดภัยไซเบอร์เกิดขึ้น แต่ยังมีความจำเป็นที่หน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๘ ด้านที่ระบุไว้ใน พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์จะต้องมีการเตรียมพร้อมรับมืออยู่เสมอ โดยมีการกำหนดบทลงโทษหากไม่มีการเตรียมความพร้อม ทำให้หน่วยงานที่กำกับดูแลต้องตระหนัก คอยติดตามตรวจสอบ และเตรียมความพร้อมสำหรับสถานการณ์ที่อาจเกี่ยวข้องกับการเกิดภัยไซเบอร์ตลอดเวลา เพื่อลดความเสี่ยง และผลกระทบต่อผู้ที่ใช้บริการ ตลอดจนสร้างความเชื่อมั่นในเสถียรภาพการดำเนินงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศทุก ๆ ด้าน

อย่างไรก็ดี การกำหนดหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่แล้วเสร็จเรียบร้อยเนื่องจากยังอยู่ในขั้นตอนการสรรหาและแต่งตั้งคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ แม้ว่าในโครงสร้างพื้นฐานสำคัญทางสารสนเทศบางส่วนมีหน่วยงานกำกับดูแลอยู่แล้ว จึงเป็นประเด็นที่จำเป็นต้องได้รับการผลักดันให้เกิดเป็นรูปธรรมโดยเร็ว

การกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน ควรเป็นลักษณะผู้อำนวยความสะดวก (Facilitator) หรือ ผู้ฝึกสอน (Coaching) ที่สร้างความร่วมมือและคอยให้การสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้สามารถกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในแต่ละด้านที่รับผิดชอบได้อย่างมีประสิทธิภาพ เนื่องจากหน่วยงานที่กำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีอยู่เดิม มีความรู้ ความเข้าใจ และรายละเอียดลักษณะงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่รับผิดชอบอยู่แล้ว โดยอาจมีการกำหนดกรอบ

การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ตาม NIST CSF ให้ทุกหน่วยงานที่เกี่ยวข้องมีทิศทางการกำกับดูแลในแนวทางเดียวกัน

อย่างไรก็ตาม ยังไม่ปรากฏว่า หน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละด้านมีการกำหนดหน่วยงานเพื่อทำหน้าที่ดำเนินการ และรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์โดยตรง อาจทำให้เกิดความไม่ชัดเจนในการกำกับดูแล เช่น หน่วยงานไม่ทราบสถานะปัจจุบันของการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของตน ทำให้ไม่มีแผนพัฒนายกระดับความมั่นคงปลอดภัยไซเบอร์ที่ชัดเจน อีกทั้งยังมีประเด็น การขาดแคลนบุคลากรที่มีความชำนาญด้านความมั่นคงปลอดภัยไซเบอร์ในระดับปฏิบัติการ เพื่อรองรับการดำเนินการของหน่วยงานที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์โดยตรง ที่จำเป็นต้องได้รับการสนับสนุน

๔.๓ การดำเนินการระหว่างหน่วยงานเอกชนที่เกี่ยวข้อง

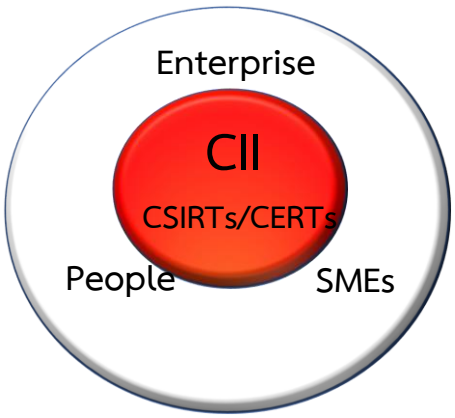
จากข้อมูลประเด็นความท้าทายในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ และแนวโน้มที่น่าสนใจในหัวข้อที่ ๓.๒ และ ๓.๓ ทำให้เห็นภาพความท้าทายในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในระดับที่เกี่ยวข้องกับหน่วยงานเอกชนได้ เนื่องจากหน่วยงานเอกชนในแต่ละอุตสาหกรรมอาจมีความต้องการการกำกับดูแลภัยด้านความมั่นคงปลอดภัยไซเบอร์ทั้งที่เหมือนกัน และแตกต่างกันในรายละเอียดแต่ละอุตสาหกรรม ดังนั้น แนวทางที่เป็นไปได้จึงควรเป็นการสนับสนุนการพัฒนาระบบนิเวศน์ (Ecosystem) ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานเอกชนในแต่ละอุตสาหกรรมที่เกี่ยวข้อง เพื่อให้หน่วยงานเอกชนมีความพร้อมรองรับ และสามารถจัดการกับภัยไซเบอร์ที่อาจเกิดขึ้นด้วยตนเองในระดับหนึ่ง ซึ่งมีกรอบการพัฒนาดังนี้

- สนับสนุนสร้างกลไกให้หน่วยงานเอกชนเห็นความสำคัญของการมีหน่วยงานรับผิดด้านความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน และมีความสามารถสร้างความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับหน่วยงานได้ด้วยตนเอง
- สนับสนุนสร้างกลไกให้หน่วยงานเอกชนในอุตสาหกรรมเดียวกัน หรือเกี่ยวข้องกันให้มีความเชื่อใจในการให้ความร่วมมือ แบ่งปันข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- มีกลไกการส่งเสริมให้เกิดกิจกรรมความมั่นคงปลอดภัยไซเบอร์กับการดำเนินชีวิตและการดำเนินงานทางธุรกิจ
- มีกลไกสนับสนุนการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการรับรองมาตรฐานสากล เพื่อรองรับการดำเนินการในระดับปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์
- มีกลไกสร้างความร่วมมือจากหน่วยงานเอกชนในการสร้างอธิปไตยไซเบอร์ของประเทศในระยะยาว เช่น มีแพลตฟอร์มไซเบอร์แห่งชาติที่ได้รับการยอมรับจากหน่วยงานทั้งภาครัฐและเอกชน หรือ การสร้างสังคมอุดมความรู้และการตระหนักถึงความมั่นคงปลอดภัยไซเบอร์ในระดับการดำเนินชีวิตของประชาชนทั่วไป

บทที่ ๕
ข้อสังเกตหรือข้อเสนอแนะที่สอดคล้องกับบริบทของประเทศไทย

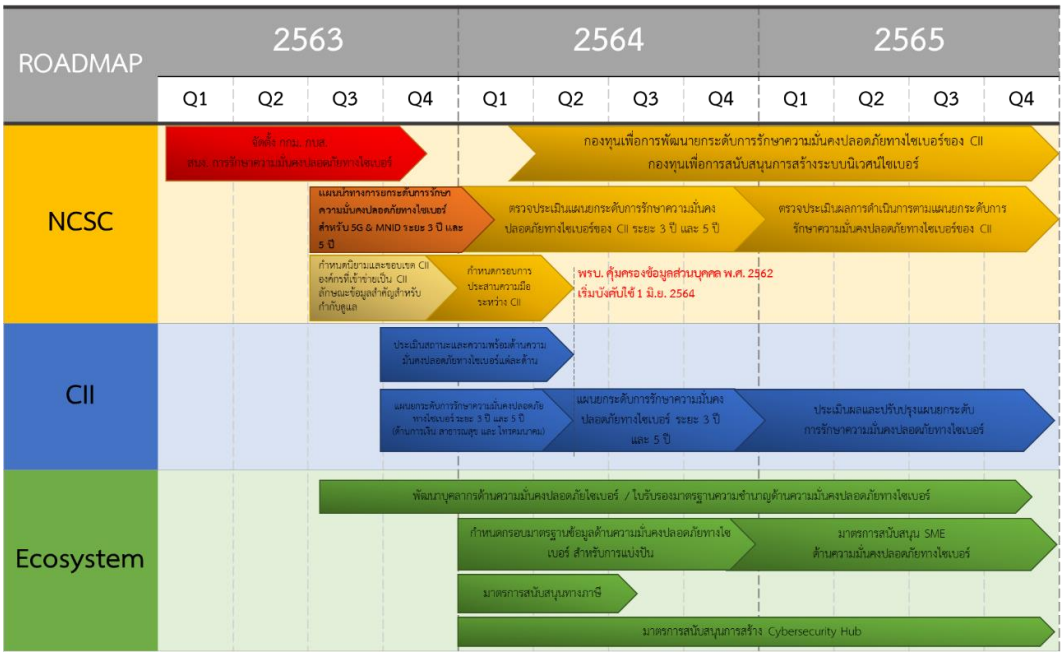
จากข้อมูลบทวิเคราะห์ช่องว่าง และสถานะการดำเนินการทางกฎหมาย ความสัมพันธ์ของการกำกับดูแลระหว่างโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ และการดูแลความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาคเอกชนที่เกี่ยวข้อง สามารถสรุปเป็นแนวทางการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ตามบริบทของประเทศไทย แบ่งออกเป็นการสร้างการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ภาครัฐ และการสนับสนุนการสร้างระบบนิเวศน์ที่เหมาะสมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ครอบคลุมถึงภาคเอกชน ผู้ใช้งาน และผู้มีส่วนเกี่ยวข้องต่าง ๆ ตามระยะเวลาที่เหมาะสม

ในระยะต้นจำเป็นต้องเน้นเร่งการสร้างการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน ตามที่ได้กำหนดไว้ใน พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้เกิดขึ้น ซึ่งเป็นรากฐานและส่วนสำคัญเปรียบเสมือนไข่แดงในการพัฒนาการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ดังรูปที่ ๗ ส่วนไข่ขาวเปรียบเสมือนระบบนิเวศน์ทางไซเบอร์ของประเทศ โดยความร่วมมือระหว่างภาครัฐกับภาคเอกชน ผู้ใช้งาน และผู้มีส่วนเกี่ยวข้องต่าง ๆ ในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ให้เข้มแข็ง เรียกว่า Public Private Partnerships หรือ PPP ซึ่งสามารถพัฒนาขึ้นได้ภายหลังจากการมีกรอบทิศทางการพัฒนาความมั่งปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เข็มแข็งแล้ว



รูปที่ ๗ : แบบจำลองแนวทางการพัฒนาการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

จากแบบจำลองแนวทางการพัฒนาการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ที่เสนอไปแล้ว สามารถสรุปแบบข้อเสนอแนวทางการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์สำหรับระยะเวลา ๓ ปี (พ.ศ. ๒๕๖๓ – ๒๕๖๕) ได้ดังรูปที่ ๘



รูปที่ ๘ : แนวทางการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕)

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๓

๑. ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

ปัจจุบัน ควรติดตามคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee หรือ NCSC) ในการเร่งผลักดันให้เกิดการจัดตั้งคณะทำงานในการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ได้แก่

- คณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ (กกม.)
- คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)
- การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และเลขาธิการคณะกรรมการการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำหรับการดำเนินงานของสำนักงาน
- การจัดทำแผนงบประมาณที่จำเป็นและสอดคล้องสำหรับการดำเนินการที่เกี่ยวข้องกับแผนพัฒนาและการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ให้ทันสำหรับการพิจารณางบประมาณปี พ.ศ. ๒๕๖๔

หมายเหตุ: ตามที่บทเฉพาะกาลของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดไว้ให้มี กกม. และ กบส. ภายใน ๙๐ วันนับแต่มีคณะ กมช. (๑๑ ธันวาคม พ.ศ. ๒๕๖๒) ซึ่งทำให้ใกล้ครบกำหนดเวลาเมื่อมีรายงานฉบับนี้ ตลอดจนกำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายใน ๑ ปีนับแต่มี พระราชบัญญัติ (๒๘ พฤษภาคม พ.ศ. ๒๕๖๒) และเลขาธิการภายใน ๙๐ วันนับแต่มีสำนักงาน อย่างไรก็ดี การจัดตั้ง กกม. และ กบส. ตลอดจนการแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ที่ได้แล้วเสร็จในเดือนตุลาคม ๒๕๖๔ ที่ถือได้ว่าเป็นความก้าวหน้าที่สำคัญ แต่ยังมีความล่าช้าจากแผนการดำเนินการในรูปที่ ๘ ทำให้อาจต้องปรับระยะเวลาของแผนที่นำเสนอตามความเหมาะสม ดังนั้น คณะกรรมาธิการควรเร่งรัดติดตามให้แผนการจัดทำงบประมาณในขั้นตอนนี้เสร็จสมบูรณ์โดยเร็วที่สุดเท่าที่จะเป็นไปได้ อาทิ จัดทำร่างกรอบโครงสร้างและอัตรากำลัง จัดทำร่างแผนปฏิบัติการระยะ ๓ ปี (พ.ศ. ๒๕๖๓ - ๒๕๖๕) จัดทำกรอบวงเงินงบประมาณปี ๒๔๖๔ - ๒๕๖๕ ในการขอทุนประเดิม จัดทำร่างคำขอจัดกลุ่มองค์การมหาชนของ สกมช. จัดทำร่างข้อบังคับ กบส. ว่าด้วยการบริหารงานบุคคล และจัดทำร่างข้อบังคับ กบส. ว่าด้วยการบริหารงานการเงิน บัญชี งบประมาณ และทรัพย์สิน และภารกิจที่สำคัญอีกด้านคือ การจัดทำกฎหมายลำดับรอง ซึ่งอยู่ระหว่างดำเนินขั้นตอนการดำเนินการภายใต้ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ไตรมาสที่ ๓ – ไตรมาสที่ ๔ ควรติดตามคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในการเร่งดำเนินการให้เกิด

- การกำหนดนิยาม ขอบเขต และองค์กรต่าง ๆ ที่เข้าข่ายอยู่ในการกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน
- การกำหนดหน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๘ ด้านให้ครบสมบูรณ์
- การกำหนดลักษณะข้อมูลสำคัญสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์
- การกำหนดแผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับเทคโนโลยีการสื่อสาร 5G และกิจการระบบพิสูจน์และยืนยันตัวตน ระยะ ๓ ปี และ ๕ ปี

หมายเหตุ: เนื่องจากมีการดำเนินงานของโครงสร้างพื้นฐานสำคัญทางโทรคมนาคมที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ไปแล้ว เช่น การประมูลคลื่นความถี่สำหรับเทคโนโลยีการสื่อสาร 5G โดย กสทช. การลงนามในบันทึกความร่วมมือการศึกษาและพัฒนาระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลโดยใช้ฐานข้อมูลจากหมายเลขโทรศัพท์เคลื่อนที่ และแนวทางจัดตั้งบริษัท Mobile National ID (MNID) ร่วมกันของผู้ประกอบการโทรศัพท์เคลื่อนที่ ๕ ราย จึงมีความจำเป็นที่ต้องเร่งกระบวนการดังกล่าวจากแผนติดตามปกติ เพื่อรองรับการดำเนินการ

ด้านความมั่นคงปลอดภัยไซเบอร์กับกิจการที่เกี่ยวข้องกับเทคโนโลยีการสื่อสาร 5G และระบบพิสูจน์และยืนยันตัวตนที่จะเกิดขึ้นในอนาคต

๒. ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ไตรมาสที่ ๔ หน่วยงานกำกับดูแลโครงข่ายสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่ได้ถูกกำหนดจากคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ควรเร่งดำเนินการ

- การประเมินสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน ซึ่งอาจมีความพร้อมของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่เท่ากัน โดยอาจใช้ผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์จากต่างประเทศที่ได้มาตรฐาน

- การจัดทำแผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานระยะ ๓ ปี และ ระยะ ๕ ปี ตลอดจนกำหนดให้มีการดำเนินการตรวจสอบ เช่น การดำเนินการทดสอบเจาะระบบ (Penetration Test) เพื่อวางแผนและปรับปรุงองค์กรอย่างต่อเนื่อง ทั้งนี้ เนื่องจากการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์มีความสัมพันธ์กับการคุ้มครองข้อมูลส่วนบุคคล จึงควรผลักดันให้แผนนำทางของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน แล้วเสร็จทันตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ที่เลื่อนการบังคับใช้ไปจนถึงวันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๖๔ อย่างไรก็ดี หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้านอาจมีความพร้อมในการดำเนินงานไม่เท่ากัน จึงควรแบ่งการจัดทำแผนนำทางตามกลุ่มหน่วยงานที่มีความพร้อมและสามารถดำเนินการให้แล้วเสร็จทันตามกำหนด และกลุ่มหน่วยงานที่ต้องดำเนินการให้แล้วเสร็จภายหลังกำหนดเป็นระยะต่าง ๆ

๓. ด้านการพัฒนาสร้างระบบนิเวศไซเบอร์ (Ecosystem) ของประเทศ

ไตรมาสที่ ๓ – ไตรมาสที่ ๔ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติควรมีการเริ่มดำเนินการที่เกี่ยวข้องกับการสร้างระบบนิเวศน์ไซเบอร์สำหรับประเทศเป็นการดำเนินการคู่ขนานกับกิจการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ตามแสดงในรูปที่ ๘ ให้ครอบคลุมถึงภาคเอกชน ทั้งองค์กรขนาดใหญ่ที่ไม่ได้ถูกจัดเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศสำคัญ และองค์กรขนาดกลางและขนาดเล็ก (SME) หน่วยงานกำกับดูแลควรมีบทบาทเป็นผู้อำนวยความสะดวก (Facilitator) หรือ ผู้ฝึกสอน (Coaching) คอยส่งเสริมและสนับสนุนให้องค์กรเอกชนสามารถเกิดความมั่นคงปลอดภัยไซเบอร์ภายในองค์กรได้ด้วยตัวเอง โดยไม่คำนึงถึงผลประโยชน์จากบทบาทดังกล่าว อันจะเป็นการเพิ่มต้นทุนโดยไม่จำเป็นขององค์กรเอกชน โดยในระยะนี้ ควรเร่งเน้นสนับสนุนการพัฒนาด้านบุคลากรรองรับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับความต้องการบุคลากรสำหรับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรทั้งภาครัฐ และภาคเอกชนที่จะเกิดขึ้น ได้แก่

- การจัดตั้งศูนย์พัฒนาและปฏิบัติการด้านความมั่นคงไซเบอร์ สามารถให้คำแนะนำการฝึกอบรมบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

- การจัดศูนย์สอบวัดระดับความชำนาญด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้มาตรฐานสากล

- นโยบายอื่น ๆ ตลอดจนการประสานงานระหว่างหน่วยงานรัฐอื่น ๆ ที่เกี่ยวข้องในการสนับสนุนการผลิตบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๔

๑. ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

ไตรมาสที่ ๑ ติดตามคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ต่อเนื่องจากการดำเนินการก่อนหน้าให้เกิดความสมบูรณ์ ได้แก่

- นิยาม ขอบเขต และ หน่วยงานกำกับดูแลความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศและองค์กรต่าง ๆ ที่เข้าข่ายอยู่ในการกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน

- ลักษณะข้อมูลสำคัญสำหรับการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์

- กำหนดกรอบ หรือนโยบายสำหรับสนับสนุนการประสานความร่วมมือกับหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่กำหนดไว้แล้วทั้งในภาวะปกติ และภาวะฉุกเฉิน เพื่อเพิ่มความเชื่อมั่น และเชื่อใจซึ่งกันและกัน ทำให้การกำกับดูแลความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ ได้แก่

- การกำหนดกลไก หลักการ และกฎเกณฑ์สำหรับการแบ่งปันข้อมูลที่เหมาะสมตามแนวทางการรักษาข้อมูลที่เป็นความลับ

- การเชื่อมต่อข้อมูลระหว่างหน่วยงาน

- การกำหนดเจ้าหน้าที่ที่เกี่ยวข้องในกระบวนการดำเนินการ

- การสร้างแรงจูงใจและการมีส่วนร่วม เช่น การจัดประชุมสัมมนาผู้ที่เกี่ยวข้องเพื่อแบ่งปันข้อมูล ประสบการณ์ สำหรับการปรับปรุงพัฒนาการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์

- การตรวจประเมิน แผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี และ ๕ ปี ของกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีความพร้อมในการดำเนินการร่วมกับการเริ่มบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ได้แก่ ด้านการเงินการธนาคาร ด้านสาธารณสุข และด้านเทคโนโลยีสารสนเทศและโทรคมนาคม โดยเฉพาะอย่างยิ่ง กลุ่มที่เกี่ยวกับเทคโนโลยีการสื่อสาร 5G และกิจการระบบพิสูจน์และยืนยันตัวตนที่ควรได้เริ่มดำเนินการตามแผนในปี ๒๕๖๓ ไปแล้ว

ไตรมาสที่ ๒ – ไตรมาสที่ ๔ ติดตามคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ในการเร่งดำเนินการดังต่อไปนี้

- การตรวจประเมิน แผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านอื่น ๆ ระยะ ๓ ปี และ ๕ ปี

- การจัดตั้งกองทุนเพื่อการพัฒนายกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกองทุนเพื่อการสนับสนุนการสร้างระบบนิเวศน์ไซเบอร์ โดยมีการกำกับดูแลจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. ด้านการกำกับดูแลความมั่งคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ไตรมาสที่ ๑ – ไตรมาสที่ ๒ หน่วยงานกำกับดูแลโครงข่ายสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่ได้ถูกกำหนดจากคณะกรรมการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ ควรเร่งดำเนินการ

- สรุปการประเมินสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้ง ๗ ด้าน

- หน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการเงินการธนาคาร ด้านสาธารณสุข และด้านเทคโนโลยีสารสนเทศและโทรคมนาคมเสนอแผนยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี และ ๕ ปี ที่รองรับการบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

ไตรมาสที่ ๒ – ไตรมาสที่ ๔ ติดตามหน่วยงานกำกับดูแลโครงข่ายสร้างพื้นฐานสำคัญทั้ง ๗ ด้านที่ได้รับการประเมินสภานะความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ในการดำเนินการ

- จัดตั้งส่วนงานที่มีหน้าที่ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะสำหรับหน่วยงานกำกับดูแล แยกออกจากส่วนงานเทคโนโลยีสารสนเทศขององค์กร

- แผนนำทาง (Roadmap) สำหรับการยกระดับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ระยะ ๓ ปี และ ระยะ ๕ ปี ของแต่ละหน่วยงาน

หมายเหตุ : กรอบและขอบเขตการพัฒนาความมั่นคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตลอดจนกำหนดรายละเอียดปัจจัย ตัวชี้วัด และกลไกสำหรับการรายงานเหตุภัยคุกคามทางไซเบอร์ที่สำคัญตามระดับความร้ายแรง สามารถอ้างอิงได้จากกรอบการดำเนินการ NIST CSF โดยมีรายละเอียดการดำเนินการตามมาตรฐาน ISO 27103 : 2018 ส่วนมาตรฐานการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ สามารถอ้างอิงได้ตามมาตรฐาน ISO 27001 : 2013 และมาตรฐานด้านการบริหารจัดการข้อมูลส่วนบุคคล ISO 27701 : 2019

๓. ด้านการพัฒนาสร้างระบบนิเวศน์ไซเบอร์ (Ecosystem) ของประเทศ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ/หรือองค์กรกำกับดูแลอื่น ๆ ที่มีส่วนเกี่ยวข้อง ควรมีการร่วมกันดำเนินการต่าง ๆ ที่สนับสนุนการสร้างระบบนิเวศน์ไซเบอร์สำหรับประเทศอย่างต่อเนื่องจากแผนปี พ.ศ. ๒๕๖๓ ได้แก่

- สนับสนุนนโยบายต่าง ๆ ที่เกี่ยวข้องกับการพัฒนาด้านบุคลากรรองรับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้จัดทำในปี พ.ศ. ๒๕๖๓ อย่างต่อเนื่อง

- กำหนดกรอบมาตรฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์สำหรับการแบ่งปัน

- ออกมาตรการสนับสนุนทางภาษี สำหรับองค์กรที่มีการดำเนินการได้มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับต่าง ๆ

- กำหนดนโยบายสนับสนุนการส่งเสริมให้ประเทศเป็นศูนย์กลางการรักษาความมั่นคงปลอดภัยไซเบอร์ชั้นนำของภูมิภาค (Cybersecurity Hub)

แผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๕

๑. ด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์จากหน่วยงานกลาง

เป็นการดำเนินการตรวจประเมินผลการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามแผนยกระดับที่ได้ดำเนินการไปในปี ๒๕๖๔ และติดตามการดำเนินการของกองทุนเพื่อการพัฒนายกระดับการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกองทุนเพื่อการสนับสนุนการสร้างระบบนิเวศน์ไซเบอร์

๒. ด้านการกำกับดูแลความมั่งคงปลอดภัยไซเบอร์สำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เป็นการดำเนินการต่อเนื่องจากแผนการดำเนินการติดตามและประเมินผลปี พ.ศ. ๒๕๖๓ และปี พ.ศ. ๒๕๖๔ เพื่อการปรับปรุงและพัฒนาแผนยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. ด้านการพัฒนาสร้างระบบนิเวศน์ไซเบอร์ (Ecosystem) ของประเทศ

เป็นการสนับสนุนการพัฒนาระบบนิเวศน์ไซเบอร์ให้ครอบคลุมด้านต่าง ๆ โดยมีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ/หรือองค์กรกำกับดูแลอื่น ๆ ที่มีส่วนเกี่ยวข้องเป็นแกนหลักในการผลักดันให้ผู้มีส่วนเกี่ยวข้องทุกภาคส่วนมีความเข้มแข็งทางความมั่นคงปลอดภัยไซเบอร์ มุ่งให้ประเทศเป็นศูนย์กลางการรักษาความมั่นคงปลอดภัยไซเบอร์ชั้นนำของภูมิภาค (Cybersecurity Hub) สร้างเป็นสังคมที่มีภูมิคุ้มกันต่อการต้านเหตุภัยไซเบอร์แบบยั่งยืน ดังนี้

- ด้านฐานข้อมูลความมั่นคงปลอดภัยไซเบอร์ ควรมีนโนบายสร้างแรงจูงใจในการสนับสนุนองค์กรภาคเอกชนให้มีการจัดตั้งดูแลด้านความมั่นคงปลอดภัยไซเบอร์ตามระดับขีดความสามารถขององค์กรที่เหมาะสม เพื่อทำให้เกิดฐานข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นประโยชน์ และนโยบายสนับสนุนกลไกการสร้างความน่าเชื่อถือ และความเชื่อใจในการแบ่งปันข้อมูลสำหรับการพัฒนาความมั่นคงปลอดภัยไซเบอร์ในอนาคต

- ด้านการสร้างความตระหนักรู้ โดยมีนโยบายการส่งเสริมให้เกิดกิจกรรมความมั่นคงปลอดภัยไซเบอร์กับการดำเนินชีวิตของภาคประชาชนโดยทั่วไป การทำให้ผู้ใช้บริการโครงสร้าง

พื้นฐานสำคัญทางสารสนเทศมีความเข้าใจที่ถูกต้องในการใช้งานบนโลกออนไลน์อย่างถูกวิธีและด้วยความมั่นใจ ลดความเสี่ยงและสามารถปกป้องตนเองจากภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ โดยเป็นการกำหนดกลุ่มเป้าหมาย และดำเนินการพัฒนาแนวทางการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์กับภาคประชาชนที่เป็นกลุ่มเป้าหมาย

- ด้านการวิจัยและพัฒนา อาจเป็นการสนับสนุนการจัดการรวมกลุ่มของภาคการวิจัยและภาคอุตสาหกรรม เพื่อเพิ่มโอกาสการพบปะ แลกเปลี่ยนความคิด และความต้องการให้มีทิศทางเดียวกัน เกิดประโยชน์จริงในทางปฏิบัติ มีการจัดตั้งกองทุนสนับสนุนการวิจัยที่เกี่ยวข้อง สร้างการประสานงานในกลุ่มองค์กรภาคการศึกษา ไม่ให้เกิดงานวิจัยซ้ำซ้อน สร้างแรงจูงใจให้มีงานวิจัยตามสาขาที่ตรงต่อความต้องการของอุตสาหกรรม เพื่อการพัฒนาเครื่องมือในการช่วย ปกป้อง ตรวจจับ และปรับตัว ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทันทุกสถานการณ์

คณะกรรมาธิการขอเสนอรายงานผลการพิจารณาศึกษา เรื่อง ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งข้อสังเกตหรือเสนอแนะของคณะกรรมาธิการมาเพื่อโปรดพิจารณาและนำเสนอต่อที่ประชุมสภาผู้แทนราษฎรพิจารณาต่อไป

(นายเสมอกัน เที่ยงธรรม)
เลขานุการคณะกรรมาธิการ

บรรณานุกรม

สื่ออิเล็กทรอนิกส์

Cybersecurity Ventures, (2017), 2017 *Cybercrime Report.*

Riigikogu. (2018), Estonia Cybersecurity Act, 23 May 2018 เข้าถึงได้จาก https://www.riigiteataja.ee/en/eli/523052018003/consolide.

ENISA. (2012), *National Cyber Security Strategies : Setting the course for national efforts to strenthen security in cyberspace,* เข้าถึงได้จาก https://www.enisa.europa.eu/publications/cyber-security-strategies-paper.

ENISA. (2015), *Definition of Cybersecurity : Gaps and overlaps in standardization,* เข้าถึงได้จาก https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

ENISA. (2016), *NCSS Good Practice Guide : Designing and Implementing National Cyber Security Strategies,* เข้าถึงได้จาก https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Estonia Ministry of Economic Affairs and Communications, (2014), *Estonia Cyber Security Strategy 2014 – 2017*, เข้าถึงได้จาก https://www.mkm.ee/en/objectives-activities/information-society/cyber-security.

European Commission, (2018), *Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity MEMO/28/3651.* เข้าถึงได้จาก Press Release Database: http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm.

European Commission. (2018), *What does the NIS Directive means for the EU citizens?* เข้าถึงได้จาก Digital Single Market: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=81974.

European Parliament, Council of the European Union, (2016), *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,* เข้าถึงได้จาก EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L1148.

บรรณานุกรม

Information System Authority, (2018), เข้าถึงได้จาก https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html.

Information System Authority. (2018), เข้าถึงได้จาก https://www.ria.ee/sites/default/files/content-editors/RIA/ria-structure-2018.pdf.

International Centre for Defence and Security, (2018), เข้าถึงได้จาก https://icds.ee/.

ISO/IEC, (2012), *ISO/IEC/27043 : 2012 Information technology - Security techniques - Guidelines for cybersecurity.*

ITU. (2004), *ITU-T X.805: Security Architecture for Systems Providing End-to-end Communications.*

NIST. (2019), *Cybersecurity Framework*, เข้าถึงได้จาก National Institute of Standards and Technology: https://www.nist.gov/cyberframework.

PWC. (2016), *Economic Crime in Thailand.*

Reuters. (26 February 2016), *U.S. government concludes cyber attack caused Ukraine power outage,* เข้าถึงได้จาก Reuters: https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K.

Technical Regulatory Authority. (2016), *TJA Annual Report 2016.* Estonia.

Technical Regulatory Authority. (2018), เข้าถึงได้จาก https://www.tja.ee/en/fields-services/communications-services.

The Estonian Investment Agency. (2018), เข้าถึงได้จาก https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/.

The Office of Communications. (2017), *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003,* เข้าถึงได้จาก https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf.

บรรณานุกรม

The Office of Communications. (2017), *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003,* เข้าถึงได้จาก https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf.

The Office of Communications. (2018), *The Office of Communications Annual Report & Accounts for the period 1 April 2017 to 31 March2018,* เข้าถึงได้จาก https://www.ofcom.org.uk/__data/assets/pdf_file/0021/115185/annual-report-1718-interactive.pdf.

World Economic Forum. (2018), *The Global Risks Report 2018, 13th Edition.*

อธิป อัศวานันท์. “อธิปไตยทางอินเทอร์เน็ต การโต้กลับของจักรวรรดิ”, กรุงเทพธุรกิจ, ๗ มกราคม ๒๕๖๓. เข้าถึงได้ https://joo.gl/j1grQH

ไทยโพสต์. (๑ พฤษภาคม ๒๕๖๑), *แฮ็กเกอร์เกาหลีเหนือเจาะเซิร์ฟเวอร์ธรรมศาสตร์เป็นฐานโจรกรรมข้อมูลการเงินทั่วโลก,* เข้าถึงได้จาก ไทยโพสต์: https://www.thaipost.net/main/detail/8222

ไทยรัฐออนไลน์. (๒๓ สิงหาคม ๒๕๕๙), *แฉกลลวง! เตือน “ผู้ใช้” พึงระวัง ตกเป็นเหยื่อ อาชญากรตุ๋นโลกไซเบอร์,* เข้าถึงได้จาก ไทยรัฐ: https://www.thairath.co.th/content/697968.

รายงานทางวิชาการ

สำนักงาน กสทช. (๒๕๖๒), *รายงานโครงการจ้างที่ปรึกษาเพื่อศึกษามาตรการสร้างความปลอดภัยบนเครือข่าย (Network Security).*

ราชกิจจานุเบกษา

ราชกิจจานุเบกษา. (๒๕๕๕). *แผนแม่บทกิจการโทรคมนาคม ฉบับที่ ๑ (พ.ศ. ๒๕๕๕ - ๒๕๕๙).*

ราชกิจจานุเบกษา. (๒๕๖๑). *แผนแม่บทกิจการโทรคมนาคม ฉบับที่ ๒ (พ.ศ. ๒๕๖๒ - ๒๕๖๖).*

ราชกิจจานุเบกษา. (๒๕๖๒). *พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒.*

ภาคผนวก

ภาคผนวก ก
คำสั่งแต่งตั้ง

ด่วนที่สุด

ที่ สผ ๐๐๑๔/ว ๒๔๕

สำนักงานเลขาธิการสภาผู้แทนราษฎร
ถนนประดิพัทธ์ พญาไท กทม. ๑๐๔๐๐

๑๖ กันยายน ๒๕๖๒

เรื่อง ตั้งคณะกรรมาธิการสามัญประจำสภา

เรียน

ด้วยในคราวประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๑ ครั้งที่ ๒๑ (สมัยสามัญประจำปีครั้งที่หนึ่ง) วันพุธที่ ๑๑ กันยายน ๒๕๖๒ ที่ประชุมได้ลงมติตั้งคณะกรรมาธิการสามัญประจำสภาตามข้อบังคับการประชุมสภาผู้แทนราษฎร พ.ศ. ๒๕๖๒ ข้อ ๙๐ และท่านได้รับเลือกตั้งเป็นกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม กรรมาธิการคณะนี้ประกอบด้วย

๑. นายกฤษฎา ตันเทอดทิตย์	๒. นางสาวกัลยา รุ่งวิจิตรชัย
๓. นายชัยวุฒิ ธนาคมานุสรณ์	๔. นายชาญวิทย์ วิภูศิริ
๕. นายนพ ชีวานันท์	๖. นายนิคม บุญวิเศษ
๗. นายปกรณ์วุฒิ อุดมพิพัฒน์สกุล	๘. นายภาควัต ศรีสุรพล
๙. นางสาวภาดาห์ วรกานนท์	๑๐. พันเอก เศรษฐพงค์ มะลิสุวรรณ
๑๑. นายสมเกียรติ ถนอมสินธุ์	๑๒. นายสยาม หัตถสงเคราะห์
๑๓. นายสรอรรถ กลิ่นประทุม	๑๔. นายสราวุธ อ่อนละมัย
๑๕. นายเสมอกัน เที่ยงธรรม	

อนึ่ง คณะกรรมาธิการจะได้มีการประชุมครั้งแรก ในวันพฤหัสบดีที่ ๑๒ กันยายน ๒๕๖๒ เวลา ๑๑.๐๐ นาฬิกา ณ ห้องประชุม ๔๐๘ ชั้น ๔ อาคารรัฐสภา เกียกกาย

จึงขอเชิญท่านไปประชุมตามกำหนดวัน เวลา และสถานที่ดังกล่าวข้างต้น

ขอแสดงความนับถือ

(นายสรศักดิ์ เพียรเวช)
เลขาธิการสภาผู้แทนราษฎร

สำนักการประชุม
โทร. ๐ ๒๒๔๔ ๒๕๒๙
โทรสาร ๐ ๒๒๔๔ ๒๕๓๘

ประกาศสภาผู้แทนราษฎร
เรื่อง ตั้งกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม
แทนตำแหน่งที่ว่าง

ตามที่ได้มีประกาศสภาผู้แทนราษฎร ลงวันที่ ๑๒ กันยายน ๒๕๖๒ ตั้งนายชัยวุฒิ ธนาคมานุสรณ์ เป็นกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม นั้น

เนื่องจาก นายชัยวุฒิ ธนาคมานุสรณ์ ได้พ้นจากกรรมาธิการในคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม เพราะลาออก และในคราวประชุมสภาผู้แทนราษฎร ชุดที่ ๒๕ ปีที่ ๓ ครั้งที่ ๙ (สมัยสามัญประจำปีครั้งที่สอง) วันพฤหัสบดีที่ ๒๘ พฤศจิกายน ๒๕๖๒ ที่ประชุมเห็นชอบให้ตั้ง นายดล เหตระกูล เป็นกรรมาธิการแทน

จึงประกาศให้ทราบทั่วกัน

ประกาศ ณ วันที่ ๔ ธันวาคม พุทธศักราช ๒๕๖๒

(นายชวน หลีกภัย)
ประธานสภาผู้แทนราษฎร

ภาคผนวก ข

ภาพกิจกรรม

ภาพการดำเนินงานของคณะกรรมาธิการการสื่อสาร โทรคมนาคม และดิจิทัลเพื่อเศรษฐกิจและสังคม และคณะอนุกรรมาธิการการติดตามและตรวจสอบการพัฒนาโครงสร้างพื้นฐานทางดิจิทัลและความมั่นคงปลอดภัยไซเบอร์

ภาพการประชุม

ภาพการเดินทางไปศึกษาดูงานและจัดสัมมนา

ภาคผนวก ค

รายนามเจ้าหน้าที่ประจำคณะกรรมาธิการผู้จัดทำ

รายนามผู้จัดทำ

๑. ร้อยโท เจษฎา ศิวรักษ์	ที่ปรึกษาประจำคณะอนุกรรมาธิการ
๒. ผู้ช่วยศาสตราจารย์จิรศิลป์ จยาวรรณ	ที่ปรึกษาประจำคณะอนุกรรมาธิการ
๓. ผู้ช่วยศาสตราจารย์ยุทธพงษ์ จิรรักษ์โสภากุล	คณะทำงาน
๔. นายพิศณุ พลพืชน์	ผู้บังคับบัญชากลุ่มงานฯ
๕. นายกฤช ฤทธา	นิติกรชำนาญการ
๖. ว่าที่ร้อยตรี เอกศักดิ์ โชติมัย	วิทยากรชำนาญการ
๗. นางสาวนัยนา แสนวิชา	เจ้าพนักงานธุรการชำนาญงาน
๘. นางสาวทิพย์วิมล แก่นจันทร์	เจ้าพนักงานธุรการปฏิบัติงาน

สำนักการพิมพ์ สำนักงานเลขาธิการสภาผู้แทนราษฎร