National Cybersecurity Strategy

ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

พันเอก ดร. เศรษฐพงค์ มะลิสุวรรณ
กสทช.

คำนำ

การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว ทั้งในแง่ความถี่และความรุนแรง ซึ่งจะส่งผลต่อการลุกลามของอาชญากรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุค Industry 4.0

มีแนวโน้มที่ชัดเจนว่า อาชญากรรมไซเบอร์กำลังเพิ่มขึ้นอย่างต่อเนื่องในอีก 5 ปีข้างหน้า ในขณะที่มีจำนวนแฮกเกอร์ที่เพิ่มมากขึ้นเป็นจำนวนมาก ซึ่งคาดว่าจะต้องมีการสูญเสียทางเศรษฐกิจทั่วโลกมูลค่ามากกว่า 6 ล้านล้านเหรียญสหรัฐฯ ภายในปี 2021 โดยเพิ่มขึ้นจาก 3 ล้านล้านเหรียญสหรัฐฯ ในปี 2015 ซึ่งสาเหตุที่ทำให้เกิดอาชญากรรมไซเบอร์เพิ่มขึ้นที่เด่นชัดที่สุดคือ เกิดจากการขยายตัวของเป้าโจมตีทั่วโลกของแฮกเกอร์ เช่น การแพร่หลายของอุปกรณ์ IoT และเครื่องจักรอัตโนมัติ ที่แพร่หลายทั่วโลก

การสร้างความมั่นคงปลอดภัยไซเบอร์จึงไม่ใช่เรื่องเพียงแค่เป็นวิสัยทัศน์อีกต่อไป เพราะหากไม่ลงมือสร้างขีดความสามารถด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยของเราก็จะประสบกับหายนะที่รับไม่ได้ในอนาคตอย่างแน่นอน เพราะภัยคุกคามทางไซเบอร์เริ่มปรากฏชัดที่กำลังจะมีผลกระทบต่อสถาบันหลักของประเทศไทย ดังนั้น ประเทศไทยจึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการดำเนินการบัญญัติกฎหมายที่เกี่ยวข้องในการเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ และจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเร่งด่วน เพื่อให้ทันต่อการเติบโตของภัยคุกคามด้านไซเบอร์

เอกสารฉบับนี้ มีจุดมุ่งหมายเพื่อเป็นแนวทางให้แก่ผู้เกี่ยวข้องในการร่างแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยเนื้อหาในเอกสารนี้ได้อ้างอิงจากเอกสารและงานวิชาการจากสถาบันและองค์กรที่น่าเชื่อถือในระดับสากล

พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ
ประธานกรรมการกิจการโทรคมนาคม/รองประธาน กสทช.
6 ตุลาคม 2560

สารบัญ

1. บทนำ

การขยายตัวของการโจมตีทางไซเบอร์ทั่วโลกเกิดขึ้นอย่างรวดเร็ว ทั้งในแง่ความถี่และความรุนแรง ซึ่งจะส่งผลต่อการระบาดของอาชญากรรมไซเบอร์ และจะมีผลกระทบต่อเศรษฐกิจของประเทศทุกประเทศที่กำลังเข้าสู่ยุค Industry 4.0

สำนักวิจัย Secure Decisions พบว่า ข้อมูลยังคงเป็นเป้าหมายหลักของแฮกเกอร์ โดยไมโครซอฟท์คาดการณ์ว่าปริมาณข้อมูลออนไลน์ในปี 2020 จะมีเพิ่มมากขึ้นถึง 50 เท่านับจากปัจจุบันนี้ และจะมีการสร้างซอฟต์แวร์ใหม่จำนวน 100 พันล้านรายการในแต่ละปี ซึ่งรวมถึงการพบช่องโหว่หลายพันล้านจุดด้วย

มีการคาดการณ์ด้วยว่าจะมีจำนวนอุปกรณ์ IoT มากกว่า 200 พันล้านเครื่องภายในปี 2020 โดยสำนักวิจัย ABI คาดการณ์ว่าภายในปี 2020 จะมียานยนต์ที่เชื่อมต่อกันผ่านระบบอินเทอร์เน็ตมากกว่า 20 ล้านคัน ที่จะมาพร้อมกับเทคโนโลยีรักษาความปลอดภัยภายในตัวยานยนต์ และบริษัท Telefonica ผู้ให้บริการโทรคมนาคมในประเทศสเปนแถลงว่า 90% ของรถยนต์ทั้งหมดจะสามารถออนไลน์ได้ในปี 2020 โดยเทียบกับจำนวนเพียง 2% ในปี 2012

นอกจากนี้ ยังได้มีการวิเคราะห์ว่าจะมีการเพิ่มขึ้นอย่างรวดเร็วของการเกิดกลุ่มอาชญากรรมไซเบอร์ และกิจกรรมการคุกคามทางไซเบอร์ที่ได้รับการสนับสนุนจากรัฐบาลของประเทศต่างๆ การโจมตีทางไซเบอร์ที่ขยายวงกว้างมากขึ้นกว่าที่เป็นอยู่ในปัจจุบัน และระบบป้องกันทางไซเบอร์ที่มีการสร้างขึ้นอย่างผิดพลาดจนกลายเป็นช่องโหว่ให้กับแฮกเกอร์และอาชญากรทางไซเบอร์

การประเมินความสูญเสียเกี่ยวกับอาชญากรรมทางไซเบอร์สามารถประเมินจากประเด็นต่างๆ ดังนี้ คือ ความเสียหายจากการทำลายข้อมูล เงินดิจิทัลที่ถูกขโมย การสูญเสียประสิทธิภาพในการทำงาน การโจรกรรมทรัพย์สินทางปัญญา การขโมยข้อมูลส่วนบุคคลและข้อมูลทางการเงิน การฉ้อฉล การทุจริต การหยุดชะงักทางธุรกิจภายหลังการถูกโจมตี การสืบสวนทางนิติวิทยาศาสตร์ การกู้ข้อมูลและระบบที่ถูกเจาะ และการคุกคามต่อชื่อเสียงและความไว้วางใจ เป็นต้น

โดยการคำนวณตัวเลขความเสียหายในทางไซเบอร์ทั่วโลก (ไม่รวมถึงอาชญากรรมทางไซเบอร์ที่ไม่มีการรายงาน) เป็นเรื่องที่สลับซับซ้อน ทั้งนี้เพราะผลกระทบจากการลดลงของราคาหุ้นและการประเมินมูลค่าของบริษัททั้งทางตรงและทางอ้อม, ผลกระทบที่เกิดขึ้นกับความสามารถภายหลังถูกเจาะระบบ, การหยุดชะงักในการทำธุรกรรมอีคอมเมิร์ซและธุรกรรมทางธุรกิจดิจิทัลอื่นๆ, การสูญเสียความสามารถในการแข่งขัน, การลาออกของพนักงานและการสรรหาพนักงานทดแทนที่เกี่ยวข้องกับการโจมตีทางไซเบอร์และการสูญเสียที่เกิดขึ้น, การสืบสวนอย่างต่อเนื่องเพื่อติดตามข้อมูลและเงินดิจิทัลที่ถูกขโมย และอื่นๆ โดยผลกระทบต่างๆ เหล่านี้ ยากมากที่จะประเมินเป็นตัวเลขที่แม่นยำได้

การสร้างความมั่นคงปลอดภัยไซเบอร์จึงไม่ใช่เป็นเพียงแค่วิสัยทัศน์อีกต่อไป เพราะหากไม่ลงมือสร้างขีดความสามารถด้านบุคลากรและเครื่องมือทางเทคโนโลยี ประเทศไทยของเราก็จะประสบกับหายนะที่รับไม่ได้ในอนาคตอย่างแน่นอน

2. วิเคราะห์สิ่งแวดล้อมทั่วไป

2.1 เทคโนโลยีสารสนเทศและการสื่อสาร ได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าส่ยคดิจิทัลที่มีเศรษฐกิจ สังคมและชีวิตประจำวันของประชาชน ที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก

2.2 การปฏิวัติทางดิจิทัล (Digital revolution) ทำให้เกิดตัวแปรใหม่ที่ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาล และการให้บริการสาธารณะที่จำเป็น ซึ่งปัจจุบันขึ้นอยู่กับความมั่นคงของโลกไซเบอร์และโครงสร้างพื้นฐานดิจิทัล อย่างไรก็ตามการสูญเสียความไว้วางใจในระบบดิจิทัล จะเป็นภัยคุกคามต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ

2.3 ฮาร์ดแวร์และซอฟต์แวร์ส่วนใหญ่ที่พัฒนาขึ้นเพื่ออำนวยความสะดวกในสภาพแวดล้อมแบบดิจิทัลที่มีการเชื่อมต่อกันอย่างหนาแน่นยิ่งยวด (Hyperconnected) ได้ส่งผลกระทบต่อประสิทธิภาพ ต้นทุน และขีดความสามารถของอุตสาหกรรมและการใช้ชีวิตอย่างปกติของประชาชน แต่ไม่ได้มีการออกแบบที่มีความปลอดภัยมาตั้งแต่ต้นอย่างเหมาะสม จึงทำให้ผู้โจมตีไม่ว่าจะเป็นรัฐที่เป็นฝ่ายตรงข้าม องค์กรอาชญากรรม หรือผู้ก่อการร้าย และแม้แต่บุคคลทั่วไป ก็สามารถใช้ช่องว่างระหว่างความสะดวกและความปลอดภัยในการโจมตีได้ ดังนั้นการลดช่องว่างและความเสี่ยงทางไซเบอร์จึงควรได้รับการให้ความสำคัญเป็นอันดับแรก

2.4 การขยายตัวของอินเทอร์เน็ตที่เชื่อมโยงกับคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มาสู่การใช้งาน ในระบบอัจฉริยะนั้น เป็นการขยายขอบเขตของการคุกคามทางไซเบอร์ ซึ่งระบบและเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเรา เช่น ระบบการผลิตไฟฟ้า, ระบบควบคุมการจราจรทางอากาศ, ดาวเทียม, เทคโนโลยีทางการแพทย์, โรงงานอุตสาหกรรมและระบบการขนส่ง ต่างมีการเชื่อมต่อกับอินเทอร์เน็ตที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้

2.5 ภัยคุกคามด้านไซเบอร์ที่เกิดจากช่องโหว่ที่มีและช่องว่าง ในขีดความสามารถและการป้องกันของประเทศ ทำให้รัฐบาลต้องเล็งเห็นถึงความสำคัญอย่างมากเพื่อให้สามารถตอบโต้ได้อย่างเท่าทันต่อภัยคุกคามทางไซเบอร์นี้ โดยจำเป็นที่จะต้องมีแนวทาง ในการป้องกันอย่างรอบด้าน เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ และควรมีการแก้ปัญหา ในการลงทุนและการแทรกแซงเพิ่มเติม ในภาคธุรกิจและภาคอุตสาหกรรม โดยอาศัยการประเมินดังต่อไปนี้

- ขนาดและลักษณะของภัยคุกคามทางไซเบอร์ และช่องโหว่ของประเทศ ซึ่งหมายความว่าการใช้แนวทาง ในปัจจุบัน อาจจะไม่เพียงพอที่จะทำให้ประเทศปลอดภัย
- แนวทางที่ขึ้นกับตลาด (market based approach) ทำให้เกิดการลงทุน ในภาคเอกชนเพื่อสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ แต่ไม่ได้ทำให้เกิดการเปลี่ยนแปลง ในระดับที่ต้องการ ดังนั้นรัฐบาลต้องเป็นผู้นำและแทรกแซงโดยตรง โดยการสร้างกลไกด้านการลงทุนและการนำทรัพยากรที่มีอยู่ไปใช้เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์
- การที่รัฐบาลดำเนินการเพียงฝ่ายเดียวเท่านั้น จะไม่สามารถทำให้เกิดความมั่นคงปลอดภัยไซเบอร์ได้ ในทุกด้าน ดังนั้นแนวทางสร้างความร่วมมือกับทุกภาคส่วนจึงเป็นสิ่งจำเป็น
- ประเทศไทยจำเป็นต้องมีหน่วยงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ตื่นตัวและสนับสนุนทักษะและขีดความสามารถต่างๆ ที่สามารถก้าวให้ทันและเผชิญกับภัยคุกคามที่กำลังเปลี่ยนแปลงได้

3. แนวความคิดทางด้านยุทธศาสตร์

3.1 ความเจริญและความมั่นคงปลอดภัยของประเทศขึ้นอยู่กับดิจิทัลมากขึ้นทุกขณะ ซึ่งความท้าทายของสังคม ในยุคปัจจุบันคือการสร้างสังคมดิจิทัลที่สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ และมีองค์ความรู้และขีดความสามารถที่จำเป็น ในการสร้างโอกาสและบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ

3.2 อินเทอร์เน็ตเป็นสิ่งจำเป็นอย่างยิ่ง แต่อย่างไรก็ตามอินเทอร์เน็ตก็ยังคงมีความไม่ปลอดภัยและยังคงมีความพยายามจากผู้ไม่หวังดีอย่างต่อเนื่องที่จะ ใช้ประโยชน์จากจุดอ่อนที่มีไป ในทางที่ผิด ในการโจมตีทางไซเบอร์ ซึ่งภัยคุกคามนี้ไม่สามารถกำจัดได้ทั้งหมดโดยสิ้นเชิง แต่สามารถลดความเสี่ยงได้โดย ให้อยู่ ในระดับที่ทำ ให้สังคมยังคงดำรงต่อไปได้โดย ใช้ประโยชน์จากโอกาสอันมากมายที่เกิดจากเทคโนโลยีอินเทอร์เน็ต

3.3 ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) ที่กำหนดโดยรัฐบาล ถือว่าเป็นยุทธศาสตร์ที่มีความสำคัญ ในลำดับต้นๆ เพื่อที่จะวางแนวทาง ในการพัฒนาความมั่นคงปลอดภัยไซเบอร์ ให้เกิดขึ้นกับประเทศ อีกทั้งยังเป็นแนวทาง ในการพัฒนาบุคลากร, เครื่องมือ และโครงการที่เกี่ยวข้อง รวมไปถึงแนวทางการส่งเสริมสนับสนุนงบประมาณ

3.4 วิสัยทัศน์ที่กำหนดขึ้นต้องเป็นผลให้ประเทศปลอดภัย และสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ และก้าวไปอย่างมั่นใจและประสบความสำเร็จในโลกดิจิทัล

3.5 เพื่อให้บรรลุวิสัยทัศน์ดังกล่าว รัฐบาลจะต้องดำเนินการให้บรรลุเป้าหมาย ดังต่อไปนี้

- ป้องกัน – ประเทศจะต้องมีวิธีและเครื่องมือที่จะป้องกันจากภัยคุกคามทางไซเบอร์ที่มีพัฒนาการอยู่ตลอดเวลา เพื่อตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ และทำให้มั่นใจได้ว่า ระบบเครือข่ายและข้อมูลของประเทศจะได้รับการคุ้มครองป้องกันและมีความยืดหยุ่น โดยประชาชน ภาคธุรกิจ และหน่วยงานของรัฐ จะต้องมีความรู้และมีขีดความสามารถในการป้องกันตัวเอง
- ขัดขวาง – ต้องทำให้ประเทศไทยเป็นเป้าหมายที่ยากต่อการโจมตีทางไซเบอร์ทุกรูปแบบ ซึ่งสามารถตรวจสอบ สืบสวน และทำลายการกระทำต่างๆ ที่เข้ามาโจมตีได้ โดยทำการไล่ล่าและจับกุมผู้ที่กระทำความความผิด ซึ่งจะต้องมีแนวทางและมาตรการในการจัดการกับผู้กระทำที่ไม่เหมาะสมในโลกไซเบอร์
- พัฒนา – ประเทศไทยมีอุตสาหกรรมที่เกี่ยวกับดิจิทัลที่กำลังเติบโตขึ้น ซึ่งรัฐบาลจะต้องสนับสนุนโดยผ่านการวิจัยและพัฒนาทางวิทยาศาสตร์และเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ การสร้างบุคลากรที่มีความสามารถในทักษะเฉพาะทาง เพื่อตอบสนองต่อความต้องการของทั้งภาครัฐและเอกชน ซึ่งความเชี่ยวชาญและขีดความสามารถในการวิเคราะห์ที่ทันสมัย จะช่วยให้ประเทศไทยสามารถตอบสนองต่อความท้าทายและเอาชนะภัยคุกคามในอนาคตได้

3.6 เพื่อเป็นการสนับสนุนเป้าหมายเหล่านี้ ประเทศไทยควรจะต้องมีการดำเนินการในระดับนานาชาติ และมีมาตรการสนับสนุนในการลงทุน และร่วมเป็นพันธมิตรในการกำหนดทิศทางวิวัฒนาการทางไซเบอร์ในระดับนานาชาติ เพื่อช่วยเพิ่มความมั่นคงปลอดภัยไซเบอร์โดยรวมให้แก่ประเทศได้มากที่สุด นอกจากนี้รัฐบาลควรมีการพัฒนาความสัมพันธ์กับพันธมิตรใหม่ๆ ด้วย เพื่อพัฒนาระดับความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศเหล่านั้น และยังเป็นการปกป้องประเทศไทยอีกด้วย ซึ่งควรทำทั้งในรูปแบบทวิภาคีและพหุภาคี รวมทั้งผ่านทาง ASEAN และ UN

3.7 เพื่อให้บรรลุผลเหล่านี้ในอีก 5 ปีข้างหน้า (หากกำหนดยุทธศาสตร์ 5 ปี) รัฐบาลควรเข้าไปดำเนินการอย่างจริงจังและใช้การลงทุนที่เพิ่มขึ้น ในขณะที่ยังคงสนับสนุนให้อุตสาหกรรมยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ทั่วทั้งประเทศ โดยการร่วมมือกับหน่วยงานที่รับผิดชอบ ทั้งหน่วยงานภาครัฐและเอกชนเพื่อให้แน่ใจว่าบุคคลทั่วไป ภาคธุรกิจ และองค์กรต่างๆ จะมีพฤติกรรมที่เหมาะสมในการใช้งานอินเทอร์เน็ตได้อย่างปลอดภัย โดยมีมาตรการในการแทรกแซง (เมื่อจำเป็นและอยู่ในขอบเขตของอำนาจที่กระทำได้) เพื่อผลักดันให้มีการพัฒนาในระดับชาติ โดยเฉพาะอย่างยิ่งในเรื่องเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญของประเทศ (National Critical Infrastructure)

3.8 รัฐบาลต้องใช้ขีดความสามารถทั้งของรัฐและของภาคอุตสาหกรรม ในการพัฒนาและมีมาตรการป้องกันทางไซเบอร์ที่มีประสิทธิภาพได้อย่างจริงจัง เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศ ซึ่งมาตรการเหล่านี้ ได้แก่ การลดรูปแบบการโจมตีแบบฟิชชิ่งทั่วไปที่พบมากที่สุด โดยกรอง IP address ที่น่าสงสัย และทำการบล็อกกิจกรรมออนไลน์ที่เป็นอันตราย ปรับปรุงขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน ซึ่งจะช่วยเพิ่มความยืดหยุ่นของประเทศในการรับมือกับภัยคุกคามทางไซเบอร์

3.9 สร้างศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Center (NCSC)) ขึ้น เพื่อเป็นหน่วยงานที่ดูแลเรื่องความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยมีภารกิจในการให้ความรู้ หาช่องโหว่ของไซเบอร์ และเป็นผู้นำในเรื่องของความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

3.10 ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ทางทหารของประเทศ จะต้องทำงานอย่างใกล้ชิดกับศูนย์ NCSC เพื่อจะทำให้มั่นใจได้ว่ากองทัพของประเทศมีความยืดหยุ่นและมีการป้องกันทางไซเบอร์อย่างแข็งแกร่งที่จำเป็นต่อการรักษาความปลอดภัย และสามารถปกป้องเครือข่ายและแพลตฟอร์มของกองทัพได้ ทำให้กองทัพยังคงสามารถดำเนินการและปฏิบัติการรบได้อยู่ ถึงแม้จะมีภัยคุกคามทางไซเบอร์เกิดขึ้น ซึ่งจะทำให้แน่ใจว่ากองทัพสามารถยับยั้งการโจมตีทางไซเบอร์ที่สำคัญในระดับชาติได้

3.11 นอกจากนี้ควรมีวิธีในการตอบสนองต่อการโจมตีทางไซเบอร์เช่นเดียวกับที่มีเพื่อโต้ตอบกับการโจมตีในรูปแบบอื่นๆ โดยใช้ขีดความสามารถที่เหมาะสมที่สุด ซึ่งรวมถึงขีดความสามารถด้านการป้องกันทางไซเบอร์มิให้เกิดขึ้นด้วย

3.12 ควรมีการใช้อำนาจของรัฐในการลงทุน เพื่อจัดการกับปัญหาการขาดแคลนบุคลากรที่มีทักษะทางด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศ โดยเริ่มตั้งแต่ระดับโรงเรียนถึงมหาวิทยาลัยจนถึงวัยทำงาน

3.13 ทำการจัดตั้งศูนย์นวัตกรรมด้านไซเบอร์ เพื่อขับเคลื่อนการพัฒนาผลิตภัณฑ์ทางไซเบอร์ที่ทันสมัย และส่งเสริมให้เกิดบริษัทด้านความมั่นคงปลอดภัยไซเบอร์ใหม่ๆ ซึ่งรัฐบาลควรจะจัดสรรเงินทุนจากกองทุนเพื่อการป้องกันและนวัตกรรมด้านไซเบอร์ (Defence and Cyber Innovation Fund) ที่ควรจัดตั้งขึ้นเพื่อสนับสนุนการสร้างนวัตกรรมในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ประเทศโดยรวม

4. ขอบเขตและกระบวนการของยุทธศาสตร์

4.1 ยุทธศาสตร์นี้มีจุดมุ่งหมายเพื่อกำหนดนโยบายระดับชาติของรัฐบาล และในขณะเดียวกันได้นำเสนอวิสัยทัศน์ร่วมกัน เพื่อแลกเปลี่ยนข้อมูลระหว่างภาครัฐและเอกชน ภาคประชาสังคม ภาคการศึกษา และประชาชนทั่วไป

4.2 ยุทธศาสตร์นี้ครอบคลุมทั่วทั้งราชอาณาจักร โดยรัฐบาลจะทำให้มั่นใจว่ายุทธศาสตร์นี้มีการปรับใช้กับทุกภาคส่วน

4.3 ยุทธศาสตร์นี้ได้กำหนดการดำเนินการที่ควรปฏิบัติ โดยมุ่งไปที่ความร่วมมือกันระหว่างภาคเศรษฐกิจและสังคมจากหน่วยงานรัฐบาล ผู้นำในแต่ละอุตสาหกรรมและประชาชนทั่วไป โดยมีเป้าหมายเพื่อเพิ่มการรักษาความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ เพื่อให้เกิดความร่วมมือโดยทั่วกัน และจะเป็นพื้นฐานที่ประเทศใช้ในการสนับสนุนในระดับนานาชาติเพื่อส่งเสริมการกำกับดูแลอินเทอร์เน็ตที่ดี

4.4 ในยุทธศาสตร์นี้ "ความมั่นคงปลอดภัยไซเบอร์" หมายถึงการป้องกันระบบข้อมูล (ฮาร์ดแวร์, ซอฟต์แวร์ และโครงสร้างพื้นฐานที่เกี่ยวข้อง) และบริการที่จัดให้มี จากการเข้าถึงที่ไม่ได้รับอนุญาตที่เป็นอันตรายหรือใช้ในทางที่ผิด ซึ่งรวมถึงอันตรายที่เกิดขึ้นโดยเจตนา โดยผู้ดำเนินการระบบหรือโดยบังเอิญ อันเนื่องมาจากการไม่ปฏิบัติตามขั้นตอนด้านความปลอดภัย

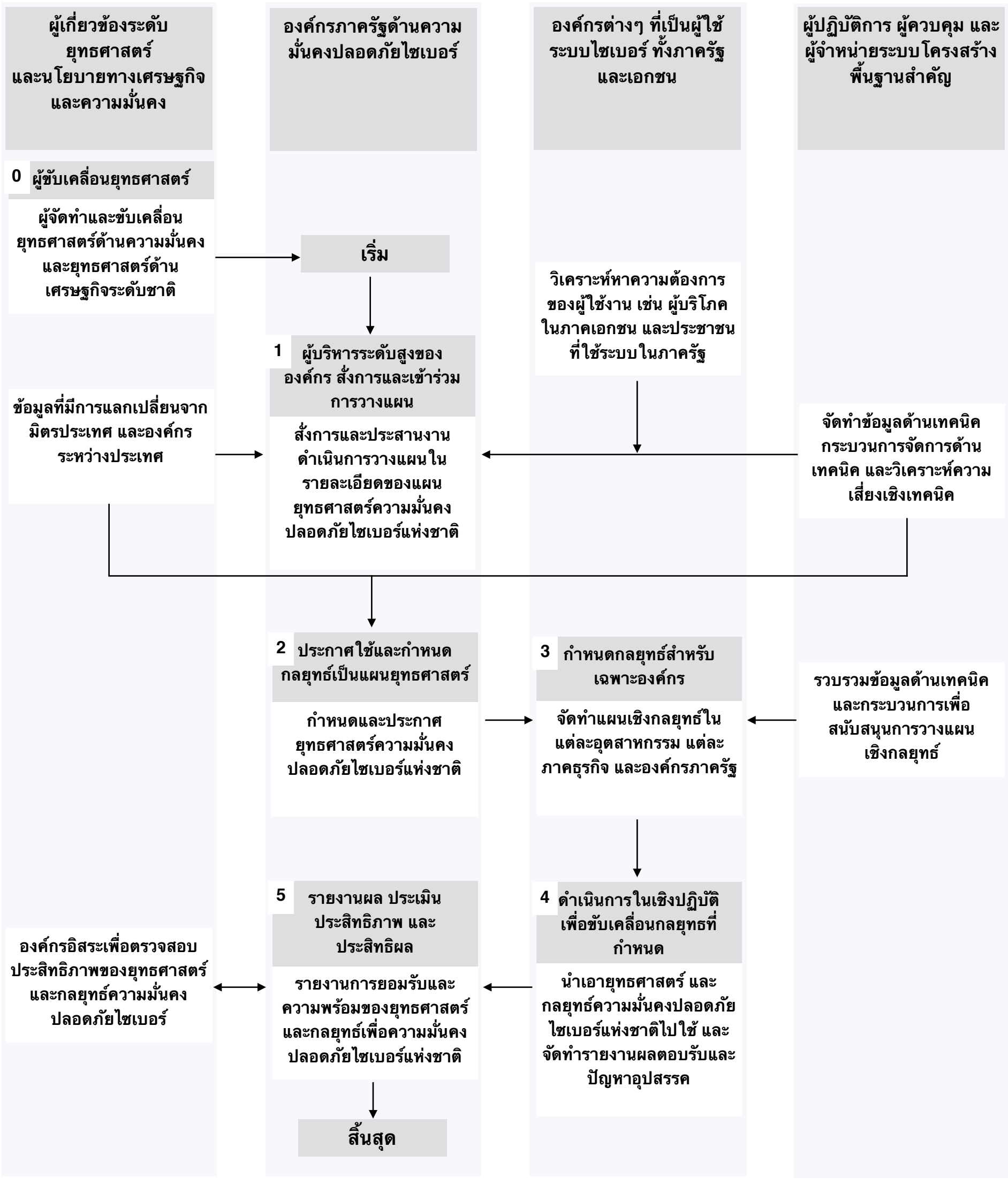
4.5 สอดคล้องกับการประเมินเกี่ยวกับภัยคุกคามของชาติ และความท้าทายที่ต้องเผชิญ โดยระบุถึง:

- การประเมินล่าสุดเกี่ยวกับบริบทเชิงกลยุทธ์ รวมถึงภัยคุกคามในปัจจุบัน และภัยคุกคามที่พัฒนาขึ้นในอนาคต
- ทบทวนจุดอ่อนและวิธีการแก้ปัญหาหรือพัฒนาในช่วงห้าปีที่ผ่านมา
- วิสัยทัศน์ของรัฐบาลเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และวัตถุประสงค์หลักเพื่อให้บรรลุเป้าหมายดังกล่าว รวมทั้งหลักการแนวทาง, บทบาทหน้าที่และความรับผิดชอบ และการแทรกแซงของรัฐบาล
- วิธีการในการนำนโยบายมาสู่การปฏิบัติ โดยการกำหนดเป้าหมายของรัฐบาลและสิ่งที่คาดหวังในการดำเนินการเป็นพันธมิตรกับทุกภาคส่วน ทั้งในระดับชาติและระดับนานาชาติ
- วิธีการประเมินความก้าวหน้าต่อวัตถุประสงค์ที่ตั้งไว้

4.6 เพื่อให้การวางยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์เป็นที่เข้าใจตรงกันของทุกฝ่ายที่เกี่ยวข้อง จึงมีความจำเป็นที่จะต้องกำหนดกระบวนการการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์อย่างชัดเจน และเพื่อความง่ายและเข้าใจตรงกัน โดยสามารถกำหนดกระบวนการดังกล่าวเป็นขั้นๆ ดังนี้

Stage 0 - Cybersecurity Strategy Driver
Stage 1 - Direct and Coordinate Elaboration
Stage 2 - Define and Issue Strategy
Stage 3 - Sector Strategies
Stage 4 - Implement Cybersecurity Strategy
Stage 5 - Report on Compliance and Efficacy

กระบวนการพัฒนายุทธศาสตร์และกลยุทธ์เพื่อความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



4.7 ขั้นตอนส่ความมั่นคงปลอดภัยทางไซเบอร์

หนึ่ง ในหัวข้อที่สำคัญ ที่ควรบรรจุไว้ในแผนยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาตินั้นคือ ข้อแนะนำเกี่ยวกับการสร้างกระบวนการขั้นตอน ที่จะนำไปสู่ความมั่นคงปลอดภัยทางไซเบอร์

แนวทางที่มีประสิทธิภาพสู่การมีความมั่นคงปลอดภัยทางไซเบอร์ต้องอาศัยการดำเนินการเป็นขั้นตอน เพื่อให้บรรลุเป้าหมาย ในการจัดการความเสี่ยงได้ โดยสามารถแบ่งเป็น 10 ขั้นตอน ดังนี้

(1) การบริหารจัดการความเสี่ยง (Risk Management Regime)

ต้องมีการบริหารจัดการความเสี่ยงทั่วทั้งองค์กร และมีการสนับสนุนอย่างจริงจังจากผู้บริหารขององค์กร ซึ่งต้องมีการสื่อสารที่ชัดเจนถึงแนวทางของการบริหารจัดการความเสี่ยงที่มีนโยบายและแนวทางการปฏิบัติที่ชัดเจน โดยควรมีเป้าหมายเพื่อให้แน่ใจว่าเจ้าหน้าที่และผู้เกี่ยวข้องทุกคน รวมถึงคู่สัญญาขององค์กรและซัพพลายเออร์ต่างๆ ได้เข้าใจและตระหนักถึงแนวทางนี้และเข้าใจถึงวิธีการตัดสินใจและความเสี่ยงต่างๆ ที่อาจจะเกิดขึ้น

(2) โครงสร้างความมั่นคงปลอดภัย (Secure configuration)
มีแนวทาง ในการระบุเทคโนโลยีพื้นฐานที่สร้างขึ้นและกระบวนการเพื่อ ให้แน่ ใจว่าการจัดการโครงสร้างสามารถช่วยปรับปรุงความมั่นคงปลอดภัยของระบบได้ดีขึ้น โดยควรพัฒนากลยุทธ์เพื่อตัดหรือปิดการ ใช้งานฟังก์ชันที่ไม่จำเป็นออกจากระบบ และแก้ไขช่องโหว่ที่พบได้อย่างรวดเร็ว ซึ่งหากไม่ทำกระบวนการนี้ ก็อาจส่งผล ให้เกิดความเสี่ยงต่อการละเมิดข้อมูลและระบบได้
(3) ความมั่นคงปลอดภัยของเครือข่าย (Network security)
การเชื่อมโยงจากเครือข่ายขององค์กรกับอินเทอร์เน็ตและเครือข่ายของพันธมิตรอื่นๆ อาจเป็นการเปิดโอกาส ให้ระบบและเทคโนโลยีขององค์กรถูกโจมตีได้ โดยองค์กรสามารถลดโอกาสที่จะทำ ให้เกิดการโจมตีได้ โดยการมีแผนและปรับ ใช้นโยบาย ในการตอบโต้ทางเทคนิคที่เหมาะสม ซึ่งโดยปกติเครือข่ายขององค์กรจะต้องมีการเชื่อมโยงกับหลายระบบขององค์กรภายนอก และยังมีการ ใช้งานบนอุปกรณ์เคลื่อนที่หรือเข้าถึงระบบจากระยะไกล รวมทั้งเชื่อมโยงกับระบบคลาวด์อีกด้วย จึงทำ ให้มีความยากลำบาก ในการควบคุมการเข้าถึงเครือข่าย ให้มีความปลอดภัย
(4) การจัดการสิทธิพิเศษของผู้ ใช้
ถ้าผู้ ใช้มีสิทธิพิเศษ ในการเข้าระบบโดยไม่จำเป็น อาจจะสร้างผลกระทบจากการ ใช้งานที่ผิดหรืออาจจะมีการละเมิดข้อมูลบัญชีผู้ ใช้นั้นๆ ดังนั้น ผู้ ใช้ทุกคนควรจะได้รับสิทธิ ในการเข้าถึงข้อมูลที่เหมาะสมกับบทบาท ในตำแหน่งงาน ควรมีการควบคุมและจัดการการ ให้สิทธิการเข้าถึงข้อมูลที่เหมาะสม
(5) สร้างความตระหนักและ ให้ความรู้แก่ผู้ ใช้
ผู้ ใช้มีบทบาทสำคัญ ในการสร้างความมั่นคงปลอดภัย ให้แก่องค์กร ดังนั้น กฎระเบียบและหลักการปฏิบัติเรื่องความมั่นคงปลอดภัย ในการ ใช้เทคโนโลยีที่มีนั้นจะช่วย ให้ผู้ ใช้สามารถทำงานด้วยตัวเองได้อย่างถูกต้องและยังช่วยองค์กร ในการรักษาความมั่นคงปลอดภัยด้วย ซึ่งสามารถทำ ให้เกิดขึ้นได้ด้วยการฝึกอบรมและมีโปรแกรม ในการสร้างความตระหนัก ในเรื่องความมั่นคงปลอดภัย ให้แก่บุคลากรทั่วทั้งองค์กร

(6) การบริหารจัดการเหตุการณ์ไม่ปกติ (Incident management)
ทุกองค์กรจะต้องเผชิญกับเหตุการณ์ไม่ปกติ การลงทุนในการสร้างนโยบายและกระบวนการบริหารจัดการเหตุการณ์ไม่ปกติอย่างมีประสิทธิภาพ จะช่วยทำให้มีความยืดหยุ่น สนับสนุนความต่อเนื่องของธุรกิจ สร้างความเชื่อมั่นต่อผู้เกี่ยวข้องทุกส่วนทั้งภายในและภายนอกองค์กรและผู้มีส่วนได้เสียต่างๆ ซึ่งจะช่วยลดผลกระทบที่อาจจะเกิดขึ้นด้วย โดยควรจะกำหนดผู้เชี่ยวชาญที่เข้ามารับผิดชอบในด้านการบริหารจัดการเหตุการณ์ไม่ปกติทั้งจากภายในและภายนอกองค์กร
(7) ป้องกันมัลแวร์ (Malware prevention)
มัลแวร์เป็นคำที่ใช้เรียกโค้ดหรือเนื้อหาที่อาจจะเป็นอันตรายและมีผลกระทบต่อระบบโดยอาจจะลดความเสี่ยงได้โดยการพัฒนาและใช้นโยบายการป้องกันมัลแวร์ที่เหมาะสมให้เป็นส่วนหนึ่งของแนวทางการป้องกันโดยรวม
(8) การเฝ้าติดตาม (Monitoring)
การเฝ้าติดตามระบบจะเป็นการสร้างขีดความสามารถในการตรวจสอบการโจมตีที่เกิดขึ้นจริงหรือมีความพยายามที่จะทำให้เกิดขึ้นต่อระบบและบริการของธุรกิจ การเฝ้าติดตามอย่างต่อเนื่องเป็นสิ่งที่จำเป็นเพื่อจะได้ตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพ นอกจากนี้ การเฝ้าติดตามทำให้องค์กรมั่นใจได้ว่า ระบบมีการใช้งานอย่างเหมาะสมสอดคล้องกับนโยบายขององค์กร ซึ่งการเฝ้าติดตามมักจะเป็นขีดความสามารถที่สำคัญที่ต้องทำให้สอดคล้องกับข้อกำหนดทางกฎระเบียบและทางกฎหมาย
(9) ควบคุมการใช้งานอุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้ (Removable media controls)
อุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้สามารถเผยแพร่มัลแวร์ได้โดยไม่ได้ตั้งใจหรืออาจจะนำข้อมูลที่สำคัญออกไปจากระบบได้ ดังนั้นต้องมีความชัดเจนหากองค์กรจะใช้อุปกรณ์เก็บข้อมูลที่สามารถถอดเคลื่อนย้ายได้โดยมีการควบคุมเรื่องความมั่นคงปลอดภัยในการใช้ที่เหมาะสม
(10) การทำงานจากที่บ้านและบนโทรศัพท์เคลื่อนที่ (Home and mobile working)
การทำงานบนโทรศัพท์เคลื่อนที่และการเข้าระบบจากระยะไกลมีประโยชน์มากในทุกองค์กร แต่ก็มีความเสี่ยงที่ต้องจัดการด้วย โดยควรมีนโยบายและกระบวนการต่างๆ ที่สนับสนุนการทำงานบนโทรศัพท์เคลื่อนที่และการเข้าระบบจากระยะไกลทั้งต่อผู้ใช้และผู้ให้บริการ และควรมีการฝึกอบรมผู้ใช้ในเรื่องความปลอดภัยในการใช้งานด้วย

5. โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure)

การกำหนดโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) นั้นมีความสำคัญอย่างยิ่ง ในการดำเนินการเพื่อ ให้เกิดความมั่นคงปลอดภัยด้านไซเบอร์ ให้แก่ประเทศ ดังนั้น ในแผนยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์จึงควรมีการบรรจุหัวข้อโครงสร้างพื้นฐานสำคัญเอาไว้ด้วย

การเติบโตขึ้นของการ ใช้งานอินเทอร์เน็ตและด้วยความเร็วบรอดแบนด์ที่เพิ่มขึ้นตลอดเวลาจะทำ ให้โลกมีการเชื่อมต่อเพิ่มมากขึ้นอย่างก้าวกระโดด เหตุการณ์ที่เกิดขึ้นอีกซีกโลกหนึ่ง ทำ ให้คนที่อีกซีกโลกหนึ่งสามารถจะรับรู้ได้ภาย ในเวลาไม่กี่นาที ปัจจุบันพัฒนาการของอินเทอร์เน็ตไม่ได้หยุดอยู่เพียงการเชื่อมต่อระหว่างคนเพื่อสื่อสารด้วยกัน แต่กำลังก้าวไปสู่การสื่อสารของทุกสิ่งทุกอย่าง (Internet of Thing: IoT) ซึ่งอินเทอร์เน็ตกำลังเชื่อมโยงเข้าไปทุกภาคส่วน โดยไม่ได้หยุดอยู่แค่โครงสร้างพื้นฐาน ในระบบสื่อสารโทรคมนาคมเท่านั้น ซึ่ง ในปัจจุบันโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เช่น ระบบประปา ระบบไฟฟ้า ระบบขนส่งมวลชน ระบบการชลประทาน ระบบบริการสาธารณสุข ระบบบริการการเงิน ฯลฯ ต่างก็มีระบบสารสนเทศและอินเทอร์เน็ตเข้าไปเป็นส่วนหนึ่งและยิ่งจะมีการเชื่อมโยงมากขึ้นทุกวัน

โดยบริการต่างๆ เหล่านี้ได้แพร่หลายอย่างรวดเร็วเพื่อให้ประชาชนสามารถเชื่อมโยงด้วยอินเทอร์เน็ตมากขึ้น และรัฐบาลในประเทศต่างๆ ให้ความสำคัญที่จะเปิดโอกาสให้ประชาชนของตนสามารถเข้าเชื่อมต่อกับอินเทอร์เน็ตได้ง่ายและสะดวกมากขึ้นเพราะโอกาสในการพัฒนาประเทศในด้านต่างๆ จะเพิ่มขึ้นและจะเป็นประโยชน์ต่อรัฐบาล, ภาคธุรกิจ, ประชาชน และประเทศชาติที่จะสามารถเพิ่มขีดความสามารถในการแข่งขันได้ อย่างไรก็ตามการเปิดให้มีการเชื่อมต่ออินเทอร์เน็ตได้ง่ายดายขึ้นย่อมมาพร้อมกับความเสี่ยงเสมอ การที่เปิดให้มีการเชื่อมโยงมากขึ้นย่อมหมายความว่ากำแพงที่ขวางกั้นขบวนการก่ออาชญากรรมผ่านระบบไซเบอร์จะลดระดับต่ำลงมา จึงทำให้กระบวนการในการบังคับใช้กฎหมายจะมีความยุ่งยากในการนำตัวผู้ต้องสงสัยเข้าสู่กระบวนการพิสูจน์ความผิดในกระบวนการยุติธรรม การก่ออาชญากรรมไซเบอร์มีผลกระทบต่อสังคมส่วนรวมอย่างยิ่งมิใช่เป็นเรื่องผลกระทบและเรื่องสิทธิส่วนบุคคล แต่จะส่งผลต่อโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) อันจะส่งผลกระทบเป็นวงกว้างอย่างรุนแรงต่อความมั่นคงของชาติได้ และด้วยโลกที่มีความเป็นโลกาภิวัตน์มากขึ้นจึงทำให้เศรษฐกิจประเทศหนึ่งถูกกระทบย่อมจะมีผลต่อประเทศอื่นๆ ทั่วโลกได้ ดังนั้นกระบวนการต่อต้านการโจมตีไซเบอร์ไม่สามารถดำเนินการโดยหน่วยงานรัฐเพียงหน่วยหนึ่งหน่วยใดโดยเฉพาะหรือบุคคุลใดบุคคลหนึ่ง แต่จะต้องเกิดขึ้นเมื่อมีกระบวนการประสานความร่วมมือ แลกเปลี่ยนข้อมูลกันทั้งในมิติหน่วยงานรัฐกับหน่วยงานรัฐ เอกชนกับเอกชน เอกชนกับหน่วยงานรัฐ หน่วยงานรัฐกับเอกชน และความร่วมมือนี้จะต้องกระทำกันในระดับนานาชาติด้วย

ดังนั้นกระบวนการต่อต้านการโจมตีไซเบอร์จะต้องมีการกำหนดขอบเขตไว้ 4 ระดับคือระดับนานาชาติ, ระดับประเทศ, ระดับกลุ่มอุตสาหกรรม และระดับส่วนบุคคล โดยในระดับส่วนบุคคลจะต้องพึงระลึกไว้เสมอว่าตนเองจะต้องมีความรับผิดชอบและต้องตระหนักถึงภัยที่จะถูกโจมตีทางไซเบอร์และเป็นช่องทางนำไปสู่การโจมตีในระดับที่สูงขึ้นเพื่อขยายผลต่อไป

ด้วยความท้าทายต่อนโยบายสาธารณะของรัฐบาลเพื่อเปิดโอกาสให้ประชาชนสามารถเข้าถึงอินเทอร์เน็ตได้โดยสะดวก แต่ยังสามารถรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) จึงทำให้รัฐบาลควรจะดำเนินการใน 3 ประเด็นหลักๆ ดังนี้

(1) เปลี่ยนแนวความคิดที่พยายามสร้างกำแพงกันไม่ให้แฮกเกอร์เข้ามาในระบบ (Blocking Concept) เพราะเหล่าแฮกเกอร์จะหาช่องว่างของกำแพงเพื่อเจาะเข้ามาได้ในที่สุด ดังนั้นจึงควรจะหาวิธีการตรวจสอบและตอบโต้กับบุคคลเหล่านี้เป็นหลัก รวมทั้งมีมาตรการเตือนภัยหรือบรรเทาผลกระทบจากการโจมตี

(2) วิเคราะห์ข้อมูลในส่วนที่มีความสำคัญและส่งผลกระทบอย่างรุนแรง และต้องนำข้อมูลในส่วนนี้ไปเก็บรักษาไว้ในที่ที่มีความปลอดภัยสูง ถึงแม้ว่าเหล่าแฮกเกอร์สามารถเจาะระบบเข้ามาได้ แต่ถ้าข้อมูลปลอดภัยโดยมีกระบวนการสามารถกู้คืนกลับมาใช้ได้ ข้อมูลเหล่านี้จะทำให้โครงสร้างพื้นฐานสำคัญจะสามารถกลับมาให้บริการได้อย่างต่อเนื่องต่อไป

(3) การสร้างความตระหนักรู้ (Awareness) ให้กับผู้เกี่ยวข้องทั้งหมด เพราะทุกๆ จุดที่มีการเชื่อมต่อจะเป็นจุดเสี่ยงให้ถูกโจมตีไซเบอร์ได้เสมอ เพียงแค่การใช้งานสมาร์ทโฟนส่วนบุคคลอาจนำไปสู่การโจมตีโครงสร้างพื้นฐานสำคัญของประเทศได้ ดังนั้นหน้าที่ในการลดความเสี่ยงและลดผลกระทบการโจมตีเหล่านี้ไม่ใช่เป็นหน้าที่ของคนใดคนหนึ่ง หรือหน่วยงานใดหน่วยงานหนึ่งเท่านั้น

โลกกำลังเข้าสู่การเปลี่ยนแปลงในบริบทใหม่ จากเดิมโลกที่แคบและเล็กประชาชนมีส่วนร่วมในกิจการรวมทั้งการรับรู้ที่สำคัญของประเทศที่น้อยมาก รวมทั้งบริการจากโครงสร้างพื้นฐานสำคัญของประเทศในระดับต่ำ ซึ่งในปัจจุบันโลกกำลังจะเดินไปสู่การเชื่อมโยงทุกสิ่งทุกอย่างเข้าหากัน ประชาชนมีโอกาสที่จะมีส่วนร่วมและรับรู้ข้อมูลมากขึ้น รัฐบาลหลายประเทศพยายามฝืนกระแสการเปลี่ยนแปลงนี้แต่ไม่สามารถทัดทานในท้ายที่สุดได้ ดังนั้นแนวความคิดที่รัฐจะเป็นผู้ดำเนินการเองทั้งหมด ด้วยนโยบายการควบคุมและสั่งการ (Command and Control Role) ที่สามารถทำได้ในอดีตที่ผ่านมา อาจไม่สามารถใช้ได้ในโลกยุคปัจจุบัน ดังนั้นในอนาคตรัฐจำเป็นจะต้องเปลี่ยนบทบาทจากผู้ควบคุมและสั่งการมาเป็นบทบาทการเป็นผู้สนับสนุน (Supportive Role) เพื่อให้ทุกภาคส่วนมีส่วนร่วมในการดำเนินการที่สำคัญของประเทศต่อไป โดยเรื่องการต่อต้านการโจมตีไซเบอร์เพื่อการรักษาโครงสร้างพื้นฐานสำคัญก็เป็นประเด็นสำคัญที่รัฐจำเป็นจะต้องมีการเปลี่ยนแนวความคิดให้สอดคล้องกับการเปลี่ยนแปลงบริบทของโลกต่อไป

โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) คืออะไร

คำจัดกัดความ “โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure)” อาจมีการนิยามไว้ในหลายความหมายจนไม่สามารถใช้นิยามเดียวเพื่ออธิบายให้มีความเข้าใจได้เหมือนกันทั่วโลก ดังนั้นในที่นี้จะขอเลือกนิยามที่มีการอธิบายอยู่บ่อยครั้งกล่าวคือ “โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure)” หมายถึงโครงสร้างของการบริการพื้นฐานที่เมื่อโครงสร้างเหล่านี้เกิดการทำงานที่ผิดปกติหรือไม่สามารถให้บริการได้เพียงแค่ช่วงเวลาหนึ่งเท่านั้น จะส่งผลกระทบต่อกลุ่มอุตสาหกรรมหรือองค์กรใดองค์กรหนึ่ง ซึ่งผลกระทบนี้จะนำไปสู่ความมั่นคงและปลอดภัยของประชาชนทั้งสังคมและเศรษฐกิจในวงกว้าง ซึ่งกลุ่มประชาชนนี้อาจเป็นประชาชนของประเทศใดประเทศหนึ่ง หรืออาจขยายผลกระทบไปสู่ประชาชนของกลุ่มประเทศได้ด้วย

ถ้าโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เกิดปัญหาในการดำเนินการผลกระทบจะไม่ใช่เฉพาะกลุ่มอุตสาหกรรมนั้นเพียงอย่างเดียว แต่จะส่งผลกระทบอย่างรุนแรงต่ออุตสาหกรรมอื่นๆ อีกด้วย เช่นโครงสร้างของระบบลอจิสติกส์ผ่านระบบรางเกิดปัญหาขึ้นย่อมส่งผลกระทบต่ออุตสาหกรรมการเกษตรที่ทำให้สินค้าพืชผักเน่าเสียก่อนนำส่งไปขายให้กับประชาชนได้ หรือในกรณีที่ระบบขนส่งน้ำมันทางท่อเกิดเสียหาย มีการปล่อยน้ำมันลงในเขตชุมชนอาจส่งผลกระทบต่อชุมชนและระบบนิเวศในชุมชน เช่น ถ้ามีน้ำมันไหลลงในเขตชุมชนชาวประมง จะทำให้ชาวประมงไม่สามารถประกอบอาชีพต่อไปได้ หรือระบบธุรกรรมทางการเงินเกิดสะดุดหยุดลง จะส่งผลต่อกลุ่มธุรกิจอุตสาหกรรมอื่นๆ ไม่สามารถติดต่อซื้อขายทำธุรกิจกันได้

ด้วยบทบาทของระบบสารสนเทศที่เป็นส่วนประกอบที่สำคัญ โดยเฉพาะอย่างยิ่งในโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) เช่น ในโครงสร้างพื้นฐานสำคัญที่เกี่ยวกับบริการน้ำประปา หรือบริการพลังงานมักจะมีระบบสารสนเทศที่ใช้ในการควบคุม SCADA (Supervisory Control and Data Acquisition) โดยในระยะแรกของ SCADA อุปกรณ์ต่างๆ รวมทั้งซอฟต์แวร์ค่อนข้างจะมีการเปิดเผยให้ภายนอกได้รับรู้อยู่ในวงจำกัด จึงมีความปลอดภัยจากการคุกคามได้ระดับหนึ่ง แต่เมื่อเวลาผ่านไปและปัจจัยต่างๆ ทางธุรกิจมีเงื่อนไขมากขึ้น จนเป็นเหตุให้ระบบ SCADA จำเป็นที่จะต้องเชื่อมต่อกับระบบสารสนเทศอื่นๆ ด้วยเงื่อนไขนี้ทำให้ระบบ SCADA มีปัจจัยความเสี่ยงที่จะถูกโจมตีสร้างความเสียหายให้โครงสร้างพื้นฐานสำคัญเพิ่มมากขึ้น ดังนั้นอาจกล่าวโดยสรุปได้ว่า ระบบสารสนเทศในโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) มีความสำคัญเพิ่มมากขึ้น ทั้งนี้การโจมตีทางไซเบอร์ไม่ได้มุ่งหวังแต่เพียงโครงข่ายการสื่อสารแต่เพียงเท่านั้น แต่จะสามารถขยายวงไปสู่โครงสร้างพื้นฐานสำคัญชนิดอื่นๆ ได้ทั้งหมดผ่านทางช่องการเชื่อมต่อของระบบสารสนเทศในโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) โดยการโจมตีเหล่านี้จะสร้างผลกระทบอย่างรุนแรงต่อสวัสดิภาพของประชาชนในประเทศ และความปลอดภัยในชีวิตและทรัพย์สินของประชาชนในประเทศได้ ถ้าประเทศเกิดปัญหาที่ประชาชนไม่สามารถทำธุรกรรมทางการเงิน สาธารณูปโภคพื้นฐานใช้ไม่ได้ ผู้เจ็บป่วยเข้าสู่บริการสาธารณสุขไม่ได้ เนื่องจากไม่มีข้อมูลประวัติของคนไข้ ระบบขนส่งไม่สามารถใช้งานได้ เป็นเวลาเพียงไม่กี่นาทีก็สามารถสร้างความโกลาหลให้กับประเทศได้ ซึ่งจะเป็นการทำลายความมั่นคงได้ทั้งทางสังคมและเศรษฐกิจของประเทศได้ในเวลาชั่วพริบตา

การกำหนดชนิดของโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure) ในแต่ละประเทศ

Australia	หมายถึงโครงสร้างทางกายภาพที่เมื่อโครงสร้างเหล่านี้เกิดการทำงานที่ผิดปกติหรือไม่สามารถให้บริการได้เพียงแค่ช่วงเวลาหนึ่งเท่านั้น จะส่งผลกระทบอย่างรุนแรงต่อประเทศทั้งทางด้านสังคมและเศรษฐกิจ หรือมีผลกระทบต่อความสามารถในการป้องกันและรักษาความมั่นคงของประเทศได้ โดยได้กำหนดโครงสร้างพื้นฐานในกลุ่มอุตสาหกรรมเหล่านี้ได้แก่ 7 กลุ่มธุรกิจ banking and finance, communications, energy, food and grocery, health, transport, water services
Canada	หมายถึง กระบวนการ ระบบ เครื่องอำนวยความสะดวก เทคโนโลยี เครือข่าย ทรัพย์สิน และบริการต่างๆ ที่จำเป็นต่อสุขภาพอนามัย ความปลอดภัย ความมั่นคง หรือการกินดีอยู่ดีของประชาชน รวมทั้งการบริหารงานที่ดีของรัฐบาล โครงสร้างพื้นฐานสำคัญอาจตั้งอยู่อย่างเป็นเอกเทศ หรือมีการเชื่อมโยงทั้งภายในและภายนอกทั้งในระดับท้องถิ่นและระดับประเทศ การทำงานที่ผิดปกติหรือไม่สามารถให้บริการได้จะเป็นผลให้เกิดวิกฤติต่อการสูญเสียชีวิตหรือผลกระทบทางด้านเศรษฐกิจและสร้างผลร้ายต่อความมั่นคงของชาติได้ โดยมี 10 กลุ่มธุรกิจ Health, Food, Finance, Water, Information and Communication Technology, Safety, Energy and utilities, Manufacturing, Government, Transportation

European Union	หมายถึงทรัพย์สิน ระบบ หรือส่วนประกอบที่ตั้งอยู่ ในชาติสมาชิก อันเป็นผลสำคัญต่อการดูแลรักษาเพื่อ ให้เกิดการทำงาน ให้กับประชาชนมีความเป็นอยู่ที่ดีทั้งทางด้านสังคมและเศรษฐกิจ โดยครอบคลุม ในด้านสุขภาพอนามัย ความปลอดภัย ความมั่นคง โครงสร้างพื้นฐานสำคัญเหล่านี้เกิดการทำงานที่ผิดปกติหรือไม่สามารถ ให้บริการได้ จะส่งผลกระทบอย่างรุนแรงต่อชาติสมาชิก โดยมีทั้งหมด 11 กลุ่มธุรกิจ Energy, Nuclear industry, Information Communication Technologies(ICT), Water, Food, Health, Financial, Transport, Chemical industry, Space, Research facilities
United Kingdom	ประกอบไปด้วยทรัพย์สิน บริการและระบบที่สนับสนุนต่อระบบเศรษฐกิจ การเมืองและวิถีชีวิตของประชาชน ซึ่งความเสียหายที่จะเกิดขึ้นกับสิ่งเหล่านี้จะนำมาซึ่งประเด็นดังต่อไปนี้ 1. ความสูญเสีย ในชีวิตของประชากรจำนวนมาก 2. ส่งผลกระทบอย่างรุนแรงต่อเศรษฐกิจของประเทศ 3. เป็นเรื่องที่น่าวิตกอย่างฉับพลันทัน ใดต่อการบริหารงานของประเทศ โดยมีทั้งหมด 9 กลุ่มธุรกิจ Communications, Emergency Services, Energy, Financial Services, Food, Government, Health, Transport, Water

United States	ระบบหรือทรัพย์สินทั้งแบบมีจริงตามกายภาพ (Physical) หรือเป็นแบบเสมือน (Virtual) ที่มีความสำคัญกับประเทศ เพราะการทำ ให้เกิดการหยุดชะงันหรือทำงานได้ไม่เต็มประสิทธิภาพของระบบหรือทรัพย์สินเหล่านี้จะมีผลกระทบที่สร้างความอ่อนแอ ให้กับความปลอดภัย เสถียรภาพทางเศรษฐกิจ สุขภาพอนามัยของประชาชน หรือผลรวมของปัจจัยเหล่านี้ โดยมีทั้งหมด 16 กลุ่มธุรกิจ • Chemical Sector • Commercial Facilities Sector • Communications Sector • Critical Manufacturing Sector • Dams Sector • Defense Industrial Base Sector • Emergency Services Sector • Energy Sector • Financial Services Sector • Food and Agriculture Sector • Government Facilities Sector • Healthcare and Public Health Sector • Information Technology Sector • Nuclear Reactors, Materials, and Waste Sector • Transportation Systems Sector • Water and Wastewater Systems Sector

Japan	ในแผน Critical Infrastructure Protection : CIIP ฉบับที่ 3 ได้มีการกำหนดกลุ่มธุรกิจไว้ 13 กลุ่มคือ • Information and Communications • Finance • Aviation • Railways • Electricity • Gas • Government and Administrative Services • Medical Services • Water • Logistics • Chemistry • Credit Card • Petroleum

6. แนวโน้มความเสี่ยงด้านภัยคุกคามทางไซเบอร์

6.1 ระดับการเปลี่ยนแปลงทางเทคโนโลยีและผลกระทบจากเทคโนโลยีก็ได้ปรากฏให้เห็นชัดขึ้น มีเทคโนโลยีใหม่ๆ เกิดขึ้นมากมาย และการที่มีเทคโนโลยีอินเทอร์เน็ตแพร่หลายทั่วโลกโดยเฉพาะอย่างยิ่งในประเทศกำลังพัฒนา ยิ่งเพิ่มโอกาสในการพัฒนาเศรษฐกิจและสังคมมากขึ้น การพัฒนาเหล่านี้ได้นำมาซึ่งข้อได้เปรียบที่สำคัญต่อสังคมที่มีการเชื่อมต่อในทุกวันนี้ แต่จากการที่ประเทศไทยยังคงต้องพึ่งพาเครือข่ายในต่างประเทศ จึงเป็นโอกาสสำหรับผู้ที่พยายามจะละเมิดต่อระบบและข้อมูลของประเทศ ซึ่งการกระทำทางไซเบอร์ที่อันตรายนั้นไม่มีขอบเขตระหว่างประเทศ

ผู้บุกรุกที่เป็นภาครัฐกำลังทดลองใช้ขีดความสามารถในการโจมตีทางไซเบอร์ โดยอาชญากรไซเบอร์ได้มีความพยายามขยายแนวทางการดำเนินงานเชิงกลยุทธ์ของตนเพื่อให้ได้ผลประโยชน์มากขึ้นจากพลเมือง องค์กรและสถาบันต่างๆ ของประเทศ ผู้ก่อการร้ายและผู้สนับสนุนต่างๆ กำลังดำเนินการโจมตีในระดับต่ำอย่างต่อเนื่องและต้องการที่จะทำในสิ่งที่มีผลกระทบมากขึ้น

6.2 อาชญากรรมทางไซเบอร์มีความผิดทางอาญาสองรูปแบบ ได้แก่:

- อาชญากรรมที่ขึ้นกับไซเบอร์ (cyber-dependent crimes) คืออาชญากรรมที่เกิดขึ้นจากการใช้อุปกรณ์ทางเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งอุปกรณ์ดังกล่าวเป็นทั้งเครื่องมือ ในการก่ออาชญากรรมและเป้าหมายของอาชญากรรม (เช่น การพัฒนาและแพร่กระจายมัลแวร์สำหรับหวังผลทางการเงิน, การแฮกเพื่อโจรกรรมข้อมูลและทำ ให้เกิดความเสียหาย, การบิดเบือนหรือทำลายข้อมูลและ / หรือเครือข่ายหรือกิจกรรม)
- อาชญากรรมแบบที่ ใช้ไซเบอร์ (cyber-enabled crimes) เป็นอาชญากรรมแบบดั้งเดิมที่สามารถเพิ่มขนาดหรือเข้าถึงได้โดย ใช้คอมพิวเตอร์ เครือข่ายคอมพิวเตอร์หรือ ICT รูปแบบอื่นๆ (เช่น การฉ้อโกงบนโลกไซเบอร์และการโจรกรรมข้อมูล)

6.3 อาชญากรรมทางไซเบอร์ที่ร้ายแรงที่สุดที่เกิดขึ้น ในประเทศไทยส่วน ใหญ่คือการหลอกลวง, การขโมย และการขูดรีดเงิน (fraud, theft and extortion) อย่างไรก็ตามภัยคุกคามนี้ก็เกิดจากประเทศและภูมิภาคอื่นๆ เช่นกัน

6.4 ถึงแม้ว่าจะสามารถระบุผู้ที่ต้องรับผิดชอบต่อการกระทำทางอาชญากรรมไซเบอร์ที่สร้างความเสียหายต่อประเทศได้นั้น แต่ก็มีความยากลำบากสำหรับประเทศและหน่วยงานบังคับ ใช้กฎหมายระหว่างประเทศ ในการฟ้องร้องเมื่อบุคคลเหล่านั้นอยู่ ในเขตอำนาจศาลที่มีข้อจำกัดหรือไม่มีข้อตกลง ในเรื่องการส่งผู้ร้ายข้ามแดน

6.5 กลุ่มแฮกเกอร์หลักๆ จากทั่วทุกมุมโลกได้ทำการพัฒนาและ ใช้งานมัลแวร์ขั้นสูงที่เผยแพร่ต่อคอมพิวเตอร์และเครือข่ายของประชากรโลก, อุตสาหกรรม และรัฐบาลของประเทศต่างๆ ซึ่งผลกระทบได้กระจายไปทั่วรวมทั้งประเทศไทย โดยการโจมตีเหล่านี้มีความก้าวร้าวและเผชิญหน้ามากขึ้นซึ่งเห็นได้จากการ ใช้ ransomware เพิ่มมากขึ้นและภัยคุกคามจากการโจมตีระบบเครือข่ายแบบ Distributed denial of service (DDoS)

6.6 ขณะที่กลุ่มแฮกเกอร์หลักๆ ในระดับโลกอาจก่อ ให้เกิดภัยคุกคามที่สำคัญต่อการเติบโตและความมั่นคง แต่เรื่องที่น่าห่วง ใยไม่แพ้กันคือภัยคุกคามจากการกระทำของอาชญากรรมไซเบอร์ที่มีความซับซ้อนน้อยกว่า แต่แพร่กระจาย ในกลุ่มบุคคลหรือองค์กรขนาดเล็ก

6.7 เรามักเห็นความพยายามของรัฐและกลุ่มที่ได้รับการสนับสนุนจากรัฐ ในการเจาะเครือข่ายของประเทศเพื่อประโยชน์ทางด้านการเมือง, การทูต, การจารกรรมเทคโนโลยี, การค้าและผลประโยชน์ทางยุทธศาสตร์ โดยมุ่งเน้นไปที่รัฐบาลและการป้องกันประเทศ การเงิน พลังงานและโทรคมนาคม

6.8 ความสามารถและผลกระทบของโครงการไซเบอร์ของรัฐ ในแต่ละประเทศแตกต่างกันไป ประเทศที่ก้าวหน้าที่สุดยังคงเพิ่มขีดความสามารถ ในการรวมการเข้ารหัสและการ ให้บริการการระบุตัวตนลง ในเครื่องมือของตนเพื่อที่จะรักษาข้อมูลที่เป็นความลับ แม้ว่าจะมีขีดความสามารถทางเทคนิค ในการ ใช้การโจมตีที่ซับซ้อน แต่ก็มักจะสามารถบรรลุเป้าหมายได้โดย ใช้เครื่องมือและเทคนิคขั้นพื้นฐานต่อเป้าหมายที่อ่อนแอ

6.9 มีหลายประเทศที่มีขีดความสามารถทางเทคนิคที่ก่อ ให้เกิดภัยคุกคามอย่างร้ายแรงต่อความมั่นคงและการเติบโตโดยรวมของประเทศไทยได้ และมีอีกหลายประเทศกำลังพัฒนาโปรแกรมทางไซเบอร์ที่มีความซับซ้อนซึ่งอาจเป็นภัยคุกคามต่อประเทศไทย ในอนาคตอันใกล้นี้ หลายประเทศที่มีความพยายาม ในการพัฒนาขีดความสามารถ ในการสอดแนมทางไซเบอร์สามารถซื้อเครื่องมือที่หาซื้อได้ทั่วไปสำหรับหาประโยชน์จากเครือข่ายคอมพิวเตอร์ เช่น ใช้ ในการโจรกรรมทางไซเบอร์

6.10 นอกจากภัยคุกคามจากการโจรกรรมแล้ว ยังมีกลุ่มแฮกเกอร์ที่เป็นภัยคุกคามจากต่างประเทศจำนวนหนึ่งที่มีการพัฒนาและ ใช้ขีดความสามารถทางไซเบอร์ที่ไม่เหมาะสม รวมทั้ง ใช้ไป ในทางมุ่งทำลายด้วย ซึ่งขีดความสามารถเหล่านี้คุกคามต่อความมั่นคงของโครงสร้างพื้นฐานสำคัญและระบบการควบคุมอุตสาหกรรมที่สำคัญของประเทศ บางประเทศอาจ ใช้ขีดความสามารถเหล่านี้ ในการฝ่าฝืนกฎหมายระหว่างประเทศโดยเชื่อว่าพวกเขาสามารถทำเช่นนั้นได้โดยได้รับการยกเว้นโทษ

6.11 กลุ่มผู้ก่อการร้ายยังคงมุ่งมั่นที่จะสร้างความเสียหายจากการกระทำทางไซเบอร์ที่เป็นอันตรายต่อประเทศและผลประโยชน์ของประเทศ โดยมีแนวโน้มว่าผลกระทบของกิจกรรมที่ ใช้ขีดความสามารถต่ำต่อประเทศ ในปัจจุบันนั้นถือเป็นอัตราส่วนที่สูงมาก เพียงการเปลี่ยนข้อมูล (defacements) และการแฮกข้อมูลส่วนตัวที่รั่วไหลทางออนไลน์ ช่วย ให้กลุ่มผู้ก่อการร้าย ได้รับความสน ใจจากสื่อมวลชนและข่มขู่ผู้ที่ตกเป็นเหยื่อได้

6.12 การประเมินผลในปัจจุบันคือการโจมตีทางกายภาพยังเป็นการโจมตีที่ผู้ก่อการร้ายจะยังคงให้ความสำคัญมากกว่าการโจมตีทางไซเบอร์ในช่วงเวลานี้ โดยมีการคาดว่าในอนาคตอันใกล้ศักยภาพของผู้มีความเชี่ยวชาญและทักษะในด้านไซเบอร์จำนวนมากจะปรากฏออกมาให้เห็นมากขึ้น เช่นเดียวกับความเสี่ยงที่องค์กรผู้ก่อการร้ายจะพยายามแสวงหาแหล่งข้อมูลภายใน ผู้ก่อการร้ายอาจใช้ขีดความสามารถในโลกไซเบอร์ใดๆ เพื่อให้บรรลุผลสูงสุด ดังนั้นแม้การเพิ่มขึ้นของขีดความสามารถในการก่อการร้ายในระดับปานกลางอาจเป็นภัยคุกคามที่สำคัญต่อประเทศและผลประโยชน์ของประเทศได้
6.13 กลุ่ม Hacktivist จะขับเคลื่อนตามวาระหรือประเด็นต่างๆ ที่มี ด้วยการสร้างและเลือกเป้าหมาย โดยกิจกรรมทางไซเบอร์ของ Hacktivist ส่วนใหญ่จะก่อกวนในรูปแบบของ defacement หรือ DDoS

ภัยคุกคามจากอินไซเดอร์หรือคนภายใน ยังคงเป็นความเสี่ยงด้านไซเบอร์ต่อองค์กรในประเทศ คนภายในที่เป็นบุคลากรที่น่าเชื่อถือขององค์กรและมีสิทธิเข้าถึงระบบและข้อมูลที่สำคัญถือเป็นภัยคุกคามที่น่ากลัวที่สุด ซึ่งอาจทำให้เกิดความเสียหายทางการเงินและชื่อเสียงขององค์กรจากการขโมยข้อมูลสำคัญและทรัพย์สินทางปัญญา

สิ่งที่น่ากังวลไม่น้อยกว่ากันคือ บุคคลภายในหรือพนักงานที่ทำให้เกิดอันตรายทางไซเบอร์โดยไม่ตั้งใจจากการเปิดอีเมลฟิชชิ่ง หรือใช้ USB ที่ติดไวรัส หรือละเลยขั้นตอนด้านความปลอดภัยและดาวน์โหลดเนื้อหาที่ไม่ปลอดภัยจากอินเทอร์เน็ต ถึงแม้พวกเขาจะไม่ได้ตั้งใจทำให้เกิดความเสียหายทางไซเบอร์ต่อองค์กร แต่การมีสิทธิในการเข้าถึงระบบและข้อมูลหมายความว่าการกระทำของพวกเขาอาจก่อให้เกิดความเสียหายเช่นเดียวกับอินไซเดอร์ ซึ่งบุคคลเหล่านี้มักตกเป็นเหยื่อที่สามารถเข้าถึงเครือข่ายขององค์กรหรือทำตามคำแนะนำโดยบริสุทธิ์ใจแต่สร้างประโยชน์ให้แก่ผู้หลอกลวง

ความเสี่ยงทางไซเบอร์โดยรวมต่อองค์กรจากภัยคุกคามจากอินไซเดอร์ไม่ได้เป็นเพียงเรื่องเกี่ยวกับการเข้าถึงระบบสารสนเทศและเนื้อหาโดยไม่ได้รับอนุญาตเท่านั้น การควบคุมความปลอดภัยทางกายภาพเพื่อปกป้องระบบจากการเข้าถึงที่ไม่เหมาะสมหรือการลบข้อมูลสำคัญหรือข้อมูลที่มีเจ้าของในรูปแบบต่างๆ ต่างมีความสำคัญเท่าเทียมกัน

6.14 กลุ่มแฮกเกอร์มือใหม่ที่ยังขาดความชำนาญในการเจาะระบบคอมพิวเตอร์ โดยใช้โปรแกรมที่พัฒนาโดยคนอื่นมาใช้โจมตีทางไซเบอร์ ซึ่งไม่ได้เป็นภัยคุกคามที่สำคัญต่อเศรษฐกิจหรือสังคมในวงกว้าง แต่พวกเขามีสิทธิเข้าถึงคู่มือการเจาะข้อมูลและเครื่องมือต่างๆ บนอินเทอร์เน็ต เนื่องจากช่องโหว่ที่พบในระบบที่ใช้อินเทอร์เน็ตซึ่งถูกนำมาใช้โดยองค์กรหลายแห่ง ซึ่งบางครั้งการกระทำของ "Script Kiddies" อาจทำให้เกิดผลเสียหายร้ายแรงต่อองค์กรได้

6.15 ประชาชนส่วนใหญ่เข้าใจเรื่องความมั่นคงปลอดภัยทางไซเบอร์ในมุมมองของการปกป้องอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ เดสก์ท็อป หรือแล็ปท็อป เป็นต้น ตั้งแต่นั้นมาอินเทอร์เน็ตก็ได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น แต่แนวโน้มเทคโนโลยี Internet of Things กำลังสร้างโอกาสใหม่ๆ ในการแสวงหาผลประโยชน์รวมทั้งผลกระทบที่อาจเกิดขึ้นตามมาจากการโจมตีที่ทำให้เกิดความเสียหายทางกายภาพแก่บุคคลหรืออาจจถึงชีวิตได้

6.16 การใช้การเชื่อมต่อในกระบวนการควบคุมอุตสาหกรรมในระบบที่สำคัญได้เพิ่มขึ้นอย่างรวดเร็วในหลากหลายอุตสาหกรรมไม่ว่าจะเป็นพลังงาน การทำเหมืองแร่ เกษตรกรรม และการบิน เพิ่มความเสี่ยงให้สูงขึ้นโดยอาจจะถูกแฮกและดัดแปลงจนมีผลกระทบร้ายแรงตามมา

6.17 ดังนั้นประชาชนจึงไม่เพียงแต่เสี่ยงต่ออันตรายจากโลกไซเบอร์ที่เกิดจากอุปกรณ์ที่ขาดความปลอดภัยทางไซเบอร์เท่านั้น แต่ยังมีความเสี่ยงจากภัยคุกคามต่อระบบที่มีการเชื่อมต่อ ซึ่งเป็นพื้นฐานของสังคม สุขภาพ และสวัสดิการของประชาชนในทุกวันนี้

6.18 การตระหนักถึงช่องโหว่ทางเทคนิคทั้งในซอฟต์แวร์และเครือข่าย และความต้องการสำหรับการใช้ไซเบอร์ที่ถูกต้องในประเทศได้เพิ่มขึ้นตลอดในช่วงห้าปีที่ผ่านมา ส่วนหนึ่งเป็นผลมาจากการริเริ่มของรัฐบาลในเรื่องความมั่นคงปลอดภัยไซเบอร์ และยังเกิดจากการเพิ่มขึ้นของเหตุการณ์สำคัญทางไซเบอร์ที่ส่งผลต่อรัฐบาล และบริษัทต่างๆ ด้วย ซึ่งการโจมตีทางไซเบอร์ไม่ได้ซับซ้อนหรือหลีกเลี่ยงไม่ได้เสมอไปแต่มักเป็นผลมาจากการใช้ประโยชน์ที่ไม่ถูกต้อง ซึ่งสามารถแก้ไขได้ไม่ยากและบ่อยครั้งที่สามารถป้องกันช่องโหว่ได้

ส่วน ใหญ่แล้วก็ยังคงเป็นเพราะจุดอ่อนของผู้เสียหายมากกว่าที่จะเป็นเพราะความเฉลียวฉลาดของผู้โจมตี นั่นคือปัจจัยสำคัญที่มีต่อความสำเร็จของการโจมตีทางไซเบอร์ ซึ่งการปรับลดความเสี่ยงของระบบและข้อมูลที่สำคัญจากการโจมตีทางไซเบอร์โดยมีการลงทุนอย่างพอเพียง ในการสร้างบุคลากร เทคโนโลยีและธรรมาภิบาล จะช่วยลดความเสี่ยงจากภัยทางไซเบอร์ที่อาจเกิดขึ้นได้

6.19 การขาดทักษะและความรู้เพื่อตอบสนองความต้องการด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้งของภาครัฐและเอกชนเกิดมาจากการที่ เจ้าหน้าที่และพนักงานส่วน ใหญ่ไม่ได้ตระหนักถึงเรื่องความมั่นคงปลอดภัยทางไซเบอร์และยังไม่เข้า ใจถึงความรับผิดชอบของตน ในเรื่องนี้ ส่วนหนึ่งอาจจะมาจากการขาดการฝึกอบรมอย่างจริงจังและสาธารณชนยังไม่ได้ตระหนักถึงปัญหาไซเบอร์อย่างเพียงพอด้วย

6.20 นอกจากนี้เรายังต้องพัฒนาทักษะและความเชี่ยวชาญเฉพาะด้านซึ่งจะช่วยให้ประเทศสามารถก้าวทันต่อเทคโนโลยีที่พัฒนาไปอย่างรวดเร็วและจัดการความเสี่ยงด้านไซเบอร์ที่เกี่ยวข้องได้ ซึ่งช่องว่างทางทักษะนี้เป็นช่องโหว่ของชาติที่ต้องได้รับการแก้ไขอย่างเร่งด่วน

6.21 หลายองค์กร ในประเทศยังคง ใช้ระบบเดิมที่อ่อนแอต่อไปจนกว่าจะมีการปรับปรุงระบบสารสนเทศ ประกอบกับซอฟต์แวร์ ในระบบเหล่านี้เป็นรุ่นเก่าที่ไม่ได้รับการติดตั้งซอฟต์แวร์ที่ป้องกันการโจมตีไว้ ซึ่งมักมีช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์ได้อย่างง่ายดาย

6.22 ข้อมูลที่เกี่ยวกับวิธีการเจาะข้อมูลและเครื่องมือที่ ใช้ ในการโจมตีสามารถหาได้ง่าย ในอินเทอร์เน็ต รวมทั้งข้อมูลส่วนตัวก็เปิดกว้างและสามารถเข้าถึงได้ง่ายเช่นกัน ทำ ให้ผู้โจมตีสามารถนำไป ใช้ประโยชน์ได้ ดังนั้นทุกคนต้องตระหนักถึงขอบเขตของการเปิดเผยรายละเอียดส่วนบุคคลและระบบขององค์กรบนอินเทอร์เน็ต ในระดับที่ป้องกันตัวเองจากช่องโหว่ที่อาจจะมีจนทำ ให้ผู้ไม่หวังดีนำไป ใช้ประโยชน์ ในทางอาชญากรรมไซเบอร์ได้

ข้อเสนอแนะ

โลกกำลังเข้าสู่การเปลี่ยนแปลงในบริบทใหม่ จากเดิมโลกที่แคบและเล็ก ประชาชนมีส่วนร่วมในกิจการรวมทั้งการรับรู้ที่สำคัญของประเทศน้อยมาก รวมทั้งบริการจากโครงสร้างพื้นฐานสำคัญของประเทศที่กำลังจะเดินไปสู่การเชื่อมโยงทุกสิ่งทุกอย่างเข้าหากัน ประชาชนมีโอกาสที่จะมีส่วนร่วมและรับรู้ข้อมูลมากขึ้น อย่างไรก็ตามรัฐบาลในหลายประเทศพยายามฝืนกระแสการเปลี่ยนแปลงนี้ แต่ไม่สามารถทัดทานในท้ายที่สุดได้ ดังนั้นแนวความคิดที่รัฐจะเป็นผู้ดำเนินการเองทั้งหมด ด้วยนโยบายการควบคุมและสั่งการ (Command and Control Role) ที่สามารถทำได้ในอดีตที่ผ่านมา อาจไม่สามารถใช้ได้ในโลกยุคปัจจุบันและในอนาคตรัฐจำเป็นจะต้องเปลี่ยนบทบาทจากผู้ควบคุมและสั่งการ มาเป็นบทบาทการเป็นผู้สนับสนุน (Supportive Role) เพื่อให้ทุกภาคส่วนมีส่วนร่วมในการดำเนินการที่สำคัญของประเทศต่อไป โดยเรื่องการต่อต้านการโจมตีไซเบอร์เพื่อการรักษาโครงสร้างพื้นฐานสำคัญก็เป็นประเด็นสำคัญยิ่งที่รัฐจำเป็นที่จะต้องมีการเปลี่ยนแนวความคิดให้สอดคล้องกับการเปลี่ยนแปลงบริบทของโลกต่อไป

ประเทศไทยเป็นประเทศที่มีผู้ใช้สมาร์ทโฟนและอุปกรณ์สื่อสารเคลื่อนที่ในลักษณะ IoT จำนวนมหาศาล รวมไปถึงประชาชนนิยมใช้ social media จำนวนมากจนติดอันดับต้นๆ ของโลก จึงทำให้มีความเสี่ยงด้านไซเบอร์อย่างมาก ดังนั้นประเทศไทยจะต้องเร่งดำเนินการที่เกี่ยวข้องกับการออกกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์และกฎหมายด้านความเป็นส่วนตัวบนไซเบอร์ รวมทั้งกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมีการจัดตั้งหน่วยงานและคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อย่างเร่งด่วน

คณะกรรมการยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติดังกล่าว ควรเป็นการจัดตั้งแบบ Top down ด้วยการจัดตั้งองค์กรระดับสำนักงานแห่งชาติเพื่อดำเนินการ และไม่ควรมอบหมายกระทรวงใดกระทรวงหนึ่งเป็นผู้ดำเนินการ เนื่องจากภัยคุกคามรูปแบบใหม่นี้เป็นภัยคุกคามที่มีรูปแบบผสมที่ซับซ้อน ทั้งในมิติของสังคม เศรษฐกิจ การเมือง และการทหาร จึงต้องใช้ผู้เชี่ยวชาญที่หลากหลายซึ่งไม่ใช่ผู้เชี่ยวชาญด้านเทคโนโลยีเท่านั้น

เอกสารอ้างอิง

[1] Framework for Improving Critical Infrastructure Cybersecurity, version 1, National Institute of Standards and Technology, Feb 12, 2014.

[2] ITU National Cybersecurity Strategy Guide, International Telecommunication Union, Switzerland, Geneva, 2012.

[3] National Cybersecurity Strategy 2016 to 2021, Cabinet office, National Security and Intelligence, Nov 1, 2016.

พันเอก ดร. เศรษฐพงค์ มะลิสุวรรณ

กรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติโทรคมนาคม (กสทช.)

ประวัติการศึกษา

- มัธยมปลายจากโรงเรียนเตรียมอุดมศึกษา
- ปริญญาตรี: วิศวกรรมไฟฟ้าสื่อสาร (เกียรตินิยมเหรียญทอง)โรงเรียนนายร้อยพระจุลจอมเกล้า (นักเรียนเตรียมทหารรุ่น 26, จปร. รุ่น 37)
- ปริญญาโท: วิศวกรรมศาสตรมหาบัณฑิต (MS in EE) (วิศวกรรมไฟฟ้าสื่อสาร) Georgia Tech สหรัฐอเมริกา
- ปริญญาโท: วิศวกรรมศาสตรมหาบัณฑิต (MS in EE) (วิศวกรรมโทรคมนาคม) The George Washington University สหรัฐอเมริกา
- ปริญญาเอก: วิศวกรรมศาสตรดุษฎีบัณฑิต (Ph.D. in EE) (วิศวกรรมโทรคมนาคม) Florida Atlantic University สหรัฐอเมริกา

เกียรติประวัติ

- เกียรตินิยมอันดับ 1 เหรียญทอง ปริญญาตรีสาขาวิศวกรรมไฟฟ้าสื่อสารโทรคมนาคมจากโรงเรียนนายร้อยพระจุลจอมเกล้า
- ได้รับทุนการศึกษาจากกระทรวงกลาโหม ประเทศสหรัฐอเมริกา เพื่อศึกษาใน หลักสูตรการต่อต้านก่อการร้ายสากล (Counter Terrorism Fellowship Program), National Defense University ประเทศสหรัฐอเมริกา
- โล่เกียรติยศจากโรงเรียนนายร้อยพระจุลจอมเกล้าคะแนนสูงสุดในวิชาผู้นำทหาร
- เกียรตินิยมปริญญาเอก Outstanding Academic Achievement จาก Tau Beta Pi Engineering Honor Society และ Phi Kappa Phi Honor Society
- รางวัลเกียรติยศจักรดาว ประจำปี พ.ศ.2556 จากมูลนิธิศิษย์เก่าโรงเรียนเตรียมทหาร
- ได้รับการจัดอันดับ 1 ใน 25 Young Executivesที่ประสบความสำเร็จสูงสุดในปี 2555 จากนิตยสาร GM
- ประกาศเกียรติคุณ “โครงการวิทยาศาสตร์สู่ความเป็นเลิศ” พ.ศ. 2556 จากคณะกรรมาธิการวิทยาศาสตร์เทคโนโลยีการสื่อสาร และ โทรคมนาคม วุฒิสภา
- ได้รับการจัดอันดับ 1 ใน 30 นักยุทธศาสตร์แห่งปีที่อยู่ในระดับผู้นำองค์กร ปี พ.ศ. 2556 จากนิตยสาร Strategy+Marketing Magazine
- รับพระราชทานรางวัลเทพทอง ครั้งที่ 16 ในฐานะองค์กรดีเด่น ประจำปี 2557
- ได้รับรางวัล “ผู้นำเสนองานวิจัยดีเด่น” จากสถาบันวิชาการป้องกันประเทศ ประจำปีงบประมาณ 2558
- ประกาศเกียรติคุณรางวัล “คนดี ความดี แทนคุณแผ่นดิน” พ.ศ.2558 สาขาการสื่อสารโทรคมนาคมจากคณะกรรมการรางวัลไทย
- ได้รับโล่เกียรติยศ “ผู้นำและผู้ทำคุณประโยชน์เพื่อผู้ด้อยโอกาส” ประจำปี พ.ศ.2558 จากสมาคมโทรคมนาคมเพื่อสิทธิเสรีภาพของผู้ด้อยโอกาส

WE'RE SMARTER

WHEN WE'RE CONNECTED