NATIONAL CYBERSECURITY STRATEGY 2017-2021

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

OFFICE OF THE NATIONAL SECURITY COUNCIL
สำนักงานสภาความมั่นคงแห่งชาติ

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พ.ศ. ๒๕๖๐ – ๒๕๖๔

สำนักงานสภาความมั่นคงแห่งชาติ
สำนักนายกรัฐมนตรี

คำนำ

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ (National Cybersecurity Strategy 2017 – 2021) โดยสำนักงานสภาความมั่นคงแห่งชาติ เป็นแนวนโยบายระดับชาติฉบับแรกของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้รับกับสภาพสังคมที่จะเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต ยุทธศาสตร์ฯ ฉบับนี้จึงมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อมเอื้ออำนวย เพื่อเสริมขีดความสามารถของไทยในด้านนี้ที่มีอยู่แล้วให้เข้มแข็งยิ่งขึ้น โดยมุ่งเน้น การมีกลไกกลางในการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภคพื้นฐานและการสร้างความตระหนักในทุกภาคส่วนและความร่วมมือกับต่างประเทศ

ยุทธศาสตร์ฯ ฉบับนี้ เป็นผลเกิดจากการระดมสมองของหน่วยงานต่าง ๆ ที่เกี่ยวข้อง รวมทั้งมีการรับฟังข้อคิดเห็นและข้อเสนอแนะจากภาคส่วนต่าง ๆ สำนักงานสภาความมั่นคงแห่งชาติจึงหวังเป็นอย่างยิ่งว่ายุทธศาสตร์ฯ ฉบับนี้ จะเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้องสำหรับการนำไปเป็นแนวทางการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์ และแสดงให้ภาคประชาชนและเอกชนได้เห็นถึงความตั้งใจจริงของภาครัฐในการป้องกันและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ โดยมีแนวนโยบายที่ชัดเจนเพื่อการนำไปปฏิบัติอย่างมีเป้าหมายและเน้นผลรูปธรรมตลอดจนให้ความสำคัญกับการมีส่วนร่วมของประชาชน

สำนักงานสภาความมั่นคงแห่งชาติ

สารบัญ

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560-2564

สภาพปัญหาและแนวโน้มของภัยคุกคาม

ด้วยปัจจุบัน เทคโนโลยีมีความก้าวหน้าไปมาก การเข้าถึงอินเทอร์เน็ตสามารถทำได้ทุกที่ทุกเวลา ทำให้ประเทศไทยเกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ โดยเฉพาะกับหน่วยงานโครงสร้างพื้นฐานสำคัญ

นอกจากนี้ การแพร่ระบาดของภัยไซเบอร์ การก่อการร้ายไซเบอร์และการทำสงครามไซเบอร์มีมากขึ้น ขณะที่การวางแผนรับมือและซ้อม ทั้งก่อนเกิดเหตุ ขณะเกิดเหตุ และหลังเกิดเหตุที่มีอยู่ไม่เพียงพอ จึงจำเป็นต้องส่งเสริมขีดความสามารถในการรับมือภัยไซเบอร์ให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิม

เป้าหมาย

- สร้างความเชื่อมั่นและความไว้วางใจในการใช้ไซเบอร์สเปซ
- มีขีดความสามารถในการรับมือภัยคุกคาม สามารถปกป้องโครงสร้างพื้นฐานสำคัญของประเทศได้
- ปกป้องผลประโยชน์และความมั่นคงของชาติ
- เปลี่ยนผ่านไปสู่เศรษฐกิจดิจิทัล
- มีการบูรณาการ ประสานความร่วมมือ แลกเปลี่ยนข้อมูลกันมากขึ้น
- พัฒนาศักยภาพหน่วยงาน และบุคลากรให้มีความพร้อมในการตอบสนองต่อการปฏิบัติการ
- สร้างความตระหนักและวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ
- การป้องกันและปราบปรามอาชญากรรมมีความเข้มแข็ง
- เพิ่มบทบาทของไทยในระดับภูมิภาคและระดับโลกในการลดความขัดแย้งทางไซเบอร์ระหว่างรัฐ

ประเด็นยุทธศาสตร์

ประเด็นยุทธศาสตร์ที่ 1
เสริมสร้างความเชื่อมั่นและไว้วางใจในทุกภาคส่วน

ประเด็นยุทธศาสตร์ที่ 2
ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ

ประเด็นยุทธศาสตร์ที่ 3
ปกป้องผลประโยชน์และความมั่นคงของชาติ

ประเด็นยุทธศาสตร์ที่ 4
เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ 5
สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศ

ประเด็นยุทธศาสตร์ที่ 6
เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ 7
ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ 8
ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในระดับภูมิภาคและระดับนานาชาติ

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พ.ศ. ๒๕๖๐ – ๒๕๖๔

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

๑. ความนำ

ปัจจุบันอินเทอร์เน็ตเป็นส่วนสำคัญในการดำรงชีวิต ไม่ว่าจะในมิติต่าง ๆ ของการดำเนินการทางเศรษฐกิจและสังคม การรักษาความมั่นคงและการป้องกันประเทศ การสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ และจะทวีความสำคัญยิ่งขึ้นในอนาคต เนื่องจากความสามารถในการพัฒนาทางเทคโนโลยีที่รวดเร็วทั้งของประเทศชั้นนำด้านเทคโนโลยีเองและความสามารถในการพัฒนาและการเข้าถึงเทคโนโลยีของประเทศที่มีความก้าวหน้าทางเทคโนโลยีในระดับรองลงมา ซึ่งความก้าวหน้าทางเทคโนโลยีในประเภทนี้ตอบสนองต่อการใช้งานเครือข่ายเทคโนโลยีสารสนเทศของคนได้เป็นจำนวนมาก ทั้งกลุ่มที่เป็นผู้ใช้งานอินเทอร์เน็ตโดยตรงหรือผู้ที่ได้รับประโยชน์จากการใช้เครือข่ายเทคโนโลยีสารสนเทศในทางอ้อม เช่น การควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐาน ทั้งยังช่วยประหยัดเวลาและลดต้นทุน จากรายงานของ ITU ปี ๒๕๕๘ พบว่า ร้อยละ ๔๖ ของครัวเรือนทั่วโลกสามารถเข้าถึงอินเทอร์เน็ตได้

สำหรับประเทศไทย มีการใช้ประโยชน์จากอินเทอร์เน็ตและระบบดิจิทัลมากขึ้นเช่นกัน จากสถิติของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center: NECTEC) ในปี พ.ศ. ๒๕๕๙ มีผู้ใช้อินเทอร์เน็ตในไทยสูงถึงเกือบ ๔๐ ล้านคน เพิ่มขึ้นจากที่เคยมีผู้ใช้ไม่ถึง ๓๐ ล้านคน ในปี พ.ศ. ๒๕๕๗ คิดเป็นร้อยละ ๑๖ ของจำนวนผู้ใช้อินเทอร์เน็ตในภูมิภาคเอเชีย

ตะวันออกเฉียงใต้ ซึ่งมีจำนวนโดยประมาณ ๒๕๐ ล้านคนซึ่งจากการสำรวจผู้ใช้อินเทอร์เน็ตทั้งจากคอมพิวเตอร์ โทรศัพท์เคลื่อนที่และผ่านทางอุปกรณ์และเทคโนโลยีต่าง ๆ ในปี ๒๕๕๘ ประเทศไทยมีประชากรผู้ใช้อินเทอร์เน็ตอายุตั้งแต่ ๖ ปีขึ้นไปจำนวนประมาณ ๒๔.๖ ล้านคน หรือคิดเป็นสัดส่วนร้อยละ ๓๙.๓ ของผู้ใช้อินเทอร์เน็ตทั้งหมด ทั้งนี้เป็นกลุ่มของวัยรุ่นอายุ ๑๙ ปีหรือน้อยกว่า คิดเป็นสัดส่วนหนึ่งในสาม (หรือคิดเป็นผู้ใช้ประมาณ ๘.๔ ล้านคน) ของผู้ใช้อินเทอร์เน็ตทั้งหมด จากการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) พบว่า ประชากรใช้เวลาโดยเฉลี่ย ๔๑.๔ ชั่วโมงต่อสัปดาห์ในการใช้อินเทอร์เน็ต โดยสมาร์ตโฟนถือเป็นช่องทางที่นิยมใช้กันมากที่สุดในการเข้าถึงอินเทอร์เน็ต คิดเป็นร้อยละ ๘๐.๙ และการใช้คอมพิวเตอร์แบบตั้งโต๊ะ (desktop) และการใช้คอมพิวเตอร์แบบพกพา (laptop) เป็นที่นิยมเป็นอันดับสองและสามตามลำดับ และเฟซบุ๊ก (Facebook) และไลน์ (LINE) เป็นสื่อสังคมออนไลน์ที่เป็นที่นิยมมากที่สุด จะเห็นว่าการเข้าถึงระบบเครือข่ายสารสนเทศและอินเทอร์เน็ตนั้นกระทำได้ง่ายขึ้น ทำให้เกิดความสะดวกสบายในการใช้ชีวิตประจำวัน แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิดและเสี่ยงที่จะเกิดภัยคุกคามต่อชีวิตเพิ่มขึ้นอีกด้วย กล่าวคือ ภัยที่เกิดจากมิจฉาชีพหรือผู้ไม่ประสงค์ดีใช้อินเทอร์เน็ตในการก่ออาชญากรรมและแสวงผลประโยชน์ในรูปแบบต่าง ๆ และภัยที่จะเกิดต่อระบบที่ควบคุมดูแลการใช้งานอินเทอร์เน็ตและระบบปฏิบัติการที่เกี่ยวข้องกับโครงสร้างสาธารณูปโภคพื้นฐานซึ่งมีผลต่อการใช้ดำรงชีวิตของประชาชนและภาคธุรกิจ ทั้งในยามปกติและยามเกิดเหตุฉุกเฉินหรือภัยที่ส่งผลกระทบต่อสังคมวัฒนธรรมและธรรมเนียมประเพณีอันดีงาม

ทั้งต่อบุคคลทั่วไป กลุ่มเด็ก สตรี และเยาวชน ตลอดจนกลุ่มผู้สูงอายุ โดยเป็นภัยที่เกิดจากกลุ่มผู้ที่คึกคะนองหรือกลุ่มผู้ที่รู้เท่าไม่ถึงการณ์ การใช้ไซเบอร์สเปซในทางที่ผิด เช่น การใช้สื่อออนไลน์เป็นเครื่องมือในการเผยแพร่แนวคิดหัวรุนแรงหรือชักชวนให้คนทั่วไปมาเข้าร่วมเป็นสมาชิกของกลุ่มเพื่อก่ออาชญากรรมหรือก่อเหตุก่อการร้าย ซึ่งการใช้ไซเบอร์สเปซเป็นเครื่องมือก่อความผิดในรูปแบบต่าง ๆ นับวันจะทวีความรุนแรง กระจายเป็นวงกว้าง ทำให้ควบคุมดูแลได้ยากขึ้น นอกจากนี้ ในด้านการเมืองและการทหารก็มีการใช้เทคโนโลยีเพื่อให้ได้มาซึ่งข้อมูลลับ หรือการใช้เทคโนโลยีเจาะโครงข่ายของชาติอื่น ตลอดจนการใช้ความก้าวหน้าทางเทคโนโลยีและทางไซเบอร์เป็นเครื่องมือหนึ่งในการทำสงครามหรือทำให้ประเทศของตนได้เปรียบในความขัดแย้ง ดังนั้น การดูแลรักษาความมั่นคงปลอดภัยให้เครือข่ายเทคโนโลยีสารสนเทศและอินเทอร์เน็ตมีความมั่นคง ใช้งานได้อย่างต่อเนื่อง สามารถป้องกันแก้ไขปัญหาการถูกเจาะโจมตีระบบและฟื้นตัวกลับมาใช้งานได้ตามปกติได้อย่างรวดเร็วและไม่ให้อินเทอร์เน็ตถูกนำไปใช้ในทางที่ผิด จึงเป็นสิ่งสำคัญอย่างยิ่งต่อการขับเคลื่อนทางเศรษฐกิจ การเมือง สังคม และการป้องกันประเทศ เพื่อให้ประเทศมีภูมิคุ้มกันทางไซเบอร์และมีความสามารถในการแข่งขันกับประเทศอื่น ๆ ในการจัดอันดับการรับมือภัยคุกคามทางไซเบอร์ จากดัชนีชี้วัดความมั่นคงปลอดภัยไซเบอร์โลก (GlobalCybersecurity Index 2017) โดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ซึ่งใช้เกณฑ์การวัดระดับความมุ่งมั่นจริงจังในห้าด้าน คือ มาตรการทางกฎหมาย มาตรการทางเทคนิค โครงสร้างองค์กร การพัฒนาศักยภาพและความร่วมมือ พบว่าประเทศไทยอยู่อันดับ ๗ ในเอเชียแปซิฟิก

และอันดับ ๒๒ ของประเทศสมาชิกของ ITU และเมื่อพิจารณาถึงการวัดขีดความสามารถในการแข่งขันของประเทศต่าง ๆ ในโลก โดย World Economic Forum พบว่า จากรายงานดัชนีความสามารถในการแข่งขันในโลกปี ๒๕๕๘ – ๒๕๕๙ โดยรวมแล้ว อันดับของไทยลดจากอันดับ ๓๑ ไปเป็นอันดับที่ ๓๒ แต่หากพิจารณาเกณฑ์ของโครงสร้างพื้นฐานโดยเฉพาะจำนวนเลขหมายโทรศัพท์เคลื่อนที่ต่อประชากร ๑๐๐ คน จะพบว่าไทยอยู่ในอันดับที่ ๓๑ จากอันดับที่ ๓๔ ในรายงานปี ๒๕๕๗-๒๕๕๘ โดยในด้านความพร้อมทางเทคโนโลยีในด้านการเป็นสมาชิกอินเทอร์เน็ตความเร็วสูงต่อประชากร ๑๐๐ คน ยังคงอยู่ในระดับที่สูงขึ้น ปริมาณการใช้อินเทอร์เน็ตแบนด์วิดท์ (Bandwidth) ไปต่างประเทศต่อผู้ใช้หนึ่งคนสูงขึ้น และสมาชิกเครือข่ายโทรศัพท์เคลื่อนที่ที่ใช้อินเทอร์เน็ตความเร็วสูงต่อประชากร ๑๐๐ คนก็เพิ่มขึ้น จากเดิม ๕๒.๓ คนเป็น ๗๙.๙ คน ทำให้ไทยอยู่ในอันดับที่ ๒๓ จากเดิมที่เคยอยู่ในอันดับที่ ๓๘ และจากสถิติการใช้อินเทอร์เน็ตจากอุปกรณ์และเทคโนโลยีต่าง ๆ ที่ได้กล่าวไว้ข้างต้น แสดงให้เห็นว่าคนไทยหันมาพึ่งพิงเทคโนโลยีและการใช้งานอินเทอร์เน็ตเพิ่มขึ้น ทั้งการใช้ในเรื่องส่วนตัวและเรื่องทางธุรกิจ ดังนั้น จึงจำเป็นอย่างยิ่งที่ไทยควรให้ความสำคัญกับการกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ระดับชาติที่มีความชัดเจนและปฏิบัติได้ผลเป็นรูปธรรม นำไปสู่การรับมือภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพทันต่อสถานการณ์ ทั้งด้านการบริหารจัดการภายในประเทศและความร่วมมือกับต่างประเทศ เนื่องจากปัญหาภัยคุกคามทางไซเบอร์นั้นเป็นภัยที่ไม่ได้เฉพาะเจาะจงอยู่ในประเทศอีกต่อไปแล้ว เช่น การเจาะระบบธนาคารกลางของบังกลาเทศโดยการใช้มัลแวร์โจมตีระบบ SWIFT ส่งผลให้เกิด

ความเสียหายมูลค่ากว่า ๘๑ ล้านดอลลาร์ ซึ่งมีการถ่ายโอนเงินไปยังศรีลังกาและฟิลิปปินส์ ซึ่งเป็นตัวอย่างที่สะท้อนภัยคุกคามทางไซเบอร์ที่หากประเทศไทยมีนโยบายและมาตรการที่เข้มแข็งจะนำไปสู่การรักษาความมั่นคงปลอดภัยไซเบอร์อย่างยั่งยืนของไทยและต่างประเทศอีกด้วย

๒. การประเมินความพร้อม สภาพปัญหา และแนวโน้มของภัยคุกคามทางไซเบอร์

๒.๑ การประเมินความพร้อม

หากประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ เป็น ๕ ด้านหลัก ๆ ด้วยกัน กล่าวคือ ความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ความพร้อมทางด้านบุคลากร ความพร้อมของระบบและเทคโนโลยี และความพร้อมด้านงานสืบสวน งานการข่าว และการข่าวกรองทางไซเบอร์ พบว่า

๒.๑.๑ ความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ

ประเทศไทยได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์มาอย่างต่อเนื่อง โดยกฎหมายหลายฉบับได้กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เอาไว้ แบ่งออกได้เป็น ๓ กลุ่ม คือ

๑) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งได้กำหนดมาตรการสำคัญ ๆ ด้านความมั่นคงปลอดภัย เอาไว้เพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือเมื่อมีการใช้ระบบคอมพิวเตอร์หรือระบบ

อินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งครอบคลุมทั้งในการพาณิชย์อิเล็กทรอนิกส์ รวมไปจนถึงการให้บริการทางอิเล็กทรอนิกส์ของรัฐ หรือในงานรัฐบาลอิเล็กทรอนิกส์นั้นมีความมั่นคงปลอดภัย ตลอดจนกำหนดให้หน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure Protection) ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย และต่อมาก็ได้มีการตรากฎหมายจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ซึ่งได้กำหนดอำนาจหน้าที่สำคัญเพิ่มเติมอีกประการ คือ การยกระดับทักษะผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งทำหน้าที่ดูแลศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)

๒) กฎหมายระดับอนุบัญญัติ หรือกฎหมายลูกที่กำหนดมาตรการในการกำกับดูแลตลาดเงินโดยธนาคารแห่งประเทศไทย และตลาดทุนโดยสำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย รวมทั้งในการกำกับดูแลธุรกิจประกันภัยโดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อให้บริการของผู้ประกอบการในภาคเศรษฐกิจที่มีการกำกับดูแลนั้นมีความมั่นคงปลอดภัย

๓) กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์ โดยมีกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติ

สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นหน่วยงานรองรับการดำเนินงาน

อย่างไรก็ตาม การกำหนดมาตรการด้านความมั่นคงปลอดภัยเอาไว้ในกฎหมายที่เกี่ยวข้องได้เน้นให้ความสำคัญในด้านมาตรการป้องกันหรือลดความเสี่ยง การสร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย และการกำหนดฐานความผิดและบทลงโทษ ซึ่งอาจครอบคลุมเพียงบางมิติของการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น จึงยังจำเป็นต้องยกระดับความเข้มแข็งเพื่อเตรียมความพร้อมของประเทศด้านดังกล่าวให้ครอบคลุมถึงมิติของการเฝ้าระวังภัยคุกคาม หรือการดำเนินการใด ๆ ที่จำเป็นเมื่อมีการโจมตี หรือเมื่อเกิดวิกฤติต่อความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการกำหนดมาตรการในการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เมื่อต้องเผชิญกับการโจมตี หรือภาวะวิกฤติดังกล่าวที่อาจส่งผลกระทบอย่างมีนัยสำคัญและรุนแรง อันส่งผลกระทบต่อความมั่นคงของประเทศในภาพรวม

นอกจากนั้น ยังขาดแนวทางปฏิบัติ และบรรทัดฐานในการบริหารจัดการไซเบอร์สเปซที่ชัดเจนในระดับภูมิภาคและระดับระหว่างประเทศ ซึ่งไทยเองก็ควรให้ความสำคัญกับการสนับสนุนให้มีบรรทัดฐานและแนวทางปฏิบัติระหว่างประเทศที่เป็นที่ยอมรับ เพื่อส่งเสริมความร่วมมือระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกันความขัดแย้งทางไซเบอร์ระหว่างรัฐอันอาจเกิดขึ้นได้ในอนาคต จึงจำเป็นต้องมีการผลักดันการจัดทำกรอบนโยบายหรือยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร่งด่วนต่อไป

๒.๑.๒ ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์

ปัจจุบัน แม้ประเทศไทยจะให้ความสำคัญในเรื่องความมั่นคงปลอดภัยไซเบอร์มากขึ้นตามลำดับ และได้มีการดำเนินงานของหน่วยปฏิบัติหลาย ๆ หน่วย เช่น การทำงานของศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ (The Computer Emergency Response Team) หรือไทยเซิร์ต (ThaiCERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ช่วยในการปกป้องและประสานการทำงานด้านความมั่นคงปลอดภัยไซเบอร์และเริ่มมีการทำงานในรูปแบบ CERT ในองค์กรที่ทำหน้าที่กำกับดูและองค์การภาคเอกชนบ้างแล้วก็ตาม หรือมีการดำเนินงานของกองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยี ศูนย์เทคโนโลยีสารสนเทศภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือธนาคารแห่งประเทศไทย แล้วก็ตาม แต่รูปแบบการทำงานดังกล่าวก็เป็นการทำงานในเชิงป้องกันและตั้งรับเมื่อมีภัยคุกคามทางไซเบอร์เท่านั้น จึงได้มีการจัดตั้งศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม หรือกองทัพไทยเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในเชิงรุกให้มากขึ้น

อย่างไรก็ตาม หากมองในภาพรวมของประเทศ ก็ยังจำเป็นต้องผลักดันให้มีกลไกการประสานงานและเชื่อมโยงระหว่างฝ่าย

นโยบายกับหน่วยงานปฏิบัติ และมีการดำเนินการอย่างเป็นรูปธรรม โดยเฉพาะในงานด้านการข่าวและการข่าวกรองทางไซเบอร์ซึ่งมีส่วนสำคัญอย่างมากต่อการปฏิบัติภารกิจของเจ้าหน้าที่ในด้านการติดตาม ประเมินสถานการณ์และตัดสินใจ อีกทั้งจำเป็นต้องเพิ่มกลไกในการตรวจสอบและติดตามประเมินผล ซึ่งประเทศไทยยังไม่มีหน่วยงานหลักที่มีอำนาจและหน้าที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศโดยตรง จึงมีความจำเป็นอย่างยิ่งที่ต้องมีศูนย์กลางในการดำเนินการเรื่องนี้โดยตรง เพื่อให้สามารถยกระดับการป้องกันและรับมือกับภัยคุกคามและการโจมตีทางไซเบอร์ที่มีแนวโน้มว่าจะซับซ้อนและมีความรุนแรงเพิ่มมากขึ้นตามลำดับ

๒.๑.๓ ความพร้อมทางด้านบุคลากร

ความพร้อมทางด้านบุคลากรถือเป็นสิ่งที่สำคัญอย่างยิ่ง ทั้งในด้านความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ทั้งระดับนโยบายและปฏิบัติ และด้านความรู้ความเชี่ยวชาญเฉพาะทาง ซึ่งจากการสำรวจพบว่ากว่าร้อยละ ๕๐ หน่วยงานรัฐและเอกชนยังไม่ได้ให้ความสำคัญกับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ และร้อยละ ๗๙ ของหน่วยงานจะมีข้อจำกัดในการสร้างแรงจูงใจให้บุคลากรเสริมศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากล ซึ่งประเทศไทยควรกำหนดทิศทางและให้ความสำคัญกับการส่งเสริมและสนับสนุนการพัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เพื่อเตรียมการรับมือกับภัยคุกคามที่อาจเกิดขึ้นในรูปแบบต่าง ๆ ได้อย่างครอบคลุมและมีประสิทธิภาพยิ่งขึ้น

๒.๑.๔ ความพร้อมของระบบและเทคโนโลยี

ไทยยังขาดระบบการบริหารจัดการเครือข่ายเพื่อเสริมความมั่นคงของประเทศและยังต้องพึ่งพาต่างประเทศอย่างสูงในด้านนี้ ไทยจึงควรหันมาให้ความสำคัญกับการพัฒนาระบบและเทคโนโลยีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง เพื่อลดการพึ่งพาต่างชาติและเพื่อการรักษาผลประโยชน์ของชาติและความมั่นคงของชาติอย่างรอบคอบรัดกุมและได้มาตรฐาน ควบคู่ไปกับการเสริมสร้างระบบและเทคโนโลยีที่นำเข้ามาจากต่างประเทศ

๒.๑.๕ ความพร้อมด้านงานสืบสวน

งานข่าวและข่าวกรองทางไซเบอร์ปัจจุบันยังขาดการบูรณาการและการให้ความสำคัญกับการพัฒนาขีดความสามารถศักยภาพด้านงานข่าวกรองทางไซเบอร์ซึ่งมีส่วนสำคัญอย่างยิ่งในการทำความเข้าใจกับภัยคุกคามรูปแบบใหม่ ๆ โดยเฉพาะภัยคุกคามทางไซเบอร์ อันจะช่วยเสริมงานด้านการสืบสวนและงานข่าวโดยรวมอีกด้วย

๒.๒ สภาพปัญหาและแนวโน้มของภัยคุกคามไซเบอร์

๒.๒.๑ ในปัจจุบัน เทคโนโลยีของอุปกรณ์อิเล็กทรอนิกส์ก้าวหน้าไปมาก อุปกรณ์สื่อสารที่สามารถเข้าถึงอินเทอร์เน็ตมีขนาดเล็กลงหรือมีให้เลือกใช้ได้หลากหลาย และมีอุปกรณ์ที่ใช้ในชีวิตประจำวันที่ต้องอาศัยอินเทอร์เน็ตมากขึ้น เช่น โทรศัพท์ จีพีเอส กล้องถ่ายรูป อุปกรณ์การแพทย์ ในขณะเดียวกันก็เป็นจุดอ่อนที่ทำให้เสี่ยงต่อการเกิดภัยทางไซเบอร์ได้ง่ายขึ้นไม่ว่าผู้ใช้งานหรือผู้โจมตีจะอยู่ ณ จุดใดของโลก อีกทั้งพบว่าผู้ใช้งานมักให้ความสำคัญกับความปลอดภัยเป็นอันดับรอง และเน้นความสะดวกสบายเป็นหลัก

๒.๒.๒ ความเสี่ยงต่อการถูกโจมตีในหลายลักษณะ ทั้งต่อโครงสร้างพื้นฐานสำคัญของประเทศ เช่น ไฟฟ้า ประปา ท่อก๊าซ โดยใช้มัลแวร์โจมตีระบบตรวจสอบและควบคุมการทำงานของระบบสาธารณูปโภคหรือต่อบริการสาธารณะ เช่น การข่มขู่โจมตี ระงับการให้บริการเว็บไซต์โดยใช้เทคนิค DoS/DDoS (Denial of Service/Distributed Denial of Service) จนประชาชนไม่สามารถเข้าถึงเว็บไซต์ที่ต้องการใช้บริการได้ เป็นต้น รวมถึงการส่งมัลแวร์ประเภท Ransomware ไปเข้ารหัสลับเอกสารสำคัญในคอมพิวเตอร์ของเหยื่อเพื่อเรียกร้องให้จ่ายค่าไถ่ก็เป็นการโจมตีอีกลักษณะหนึ่ง

๒.๒.๓ ตลาดการเงินโลกไร้พรมแดนซึ่งเป็นผลจากเทคโนโลยีและนวัตกรรมทางการเงินมีความก้าวหน้าอย่างรวดเร็วทำให้มีการพัฒนาเครื่องมือทางการเงินใหม่ ๆ เช่น Application ทางการเงิน Crowd Funding และ Financial Platform เป็นต้น รวมทั้งต้องเตรียมความพร้อมในด้านต่าง ๆ เพื่อรองรับต่อการเปลี่ยนแปลงที่เกิดขึ้น เช่น การปรับปรุงกฎระเบียบในการกำกับดูแลภาคการเงิน การสร้างความเชื่อมั่นให้แก่ผู้ใช้บริการในเรื่องความปลอดภัยของข้อมูลส่วนตัวผ่านระบบเทคโนโลยีสารสนเทศการป้องกันความเสี่ยงจากความเชื่อมโยงทางการเงิน การเคลื่อนย้ายเงินทุน และปริมาณธุรกรรมที่เพิ่มขึ้น

๒.๒.๔ หน่วยงานภายในประเทศยังไม่ให้ความสำคัญกับการวางแผนรับมือและซ้อมทั้งก่อนเกิดเหตุ ขณะเกิดเหตุ และหลังเกิดเหตุที่ได้มาตรฐาน โดยเฉพาะความสามารถในการฟื้นตัว (Resilience) หลังเกิดภัยคุกคามทางไซเบอร์ซึ่งมีความสำคัญอย่างยิ่งต่อการรักษาความต่อเนื่องของการปฏิบัติการในมิติต่าง ๆ โดยจะช่วยลดผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ให้น้อยลง

๒.๒.๕ การก่อการร้ายไซเบอร์และการทำสงครามไซเบอร์ (Cyber terrorism/Cyber warfare) ไทยเป็นประเทศหนึ่งที่มีความเสี่ยงที่จะตกเป็นพื้นที่กระทำการก่อการร้ายทางไซเบอร์โดยรัฐหรือบุคคล/กลุ่มบุคคล ตลอดจนกลุ่มผู้ก่อการร้าย ซึ่งการก่อการร้ายทางไซเบอร์ยังหมายรวมถึงการนำสื่อออนไลน์ไปใช้เป็นเครื่องมือในการเผยแพร่แนวคิดที่นิยมการใช้ความรุนแรงหรือการสอนการก่อการร้าย การจัดหาอาวุธและวัสดุที่ใช้ประกอบเป็นอาวุธรวมทั้งสอนวิธีการทำ การหาสมาชิกมาร่วมอุดมการณ์และก่อการอีกด้วย ซึ่งสำหรับไทยนั้น ต้องคอยเฝ้าระวังกลุ่มเสี่ยงที่อาจถูกชักจูงไปในการดังกล่าว และในด้าน Cyber Warfare นั้น ไทยต้องพัฒนาขีดความสามารถในการควบคุมมิติทางไซเบอร์ที่จะมีผลต่อการทำสงคราม เพื่อสามารถปกป้องผลประโยชน์แห่งชาติและรักษาความมั่นคงแห่งชาติที่เกิดจากภัยคุกคามในรูปแบบใหม่นี้

๒.๒.๖ ปัญหาการขาดความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะการใช้อินเทอร์เน็ต โดยพบว่าผู้ใช้งานอินเทอร์เน็ตมักให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยเป็นอันดับรองและเน้นความสะดวกสบายเป็นหลัก จึงต้องสร้างความตระหนักรู้ให้กับประชาชนทั่วไปและผู้ใช้งานอินเทอร์เน็ตในทุกระดับทราบถึงภัยคุกคามทางไซเบอร์และวิธีรับมือกับปัญหานี้

๒.๒.๗ การแพร่ระบาดของภัยไซเบอร์เกิดความเสี่ยงด้านความปลอดภัยไซเบอร์ตามมาอีกหลายรูปแบบ เช่น การสร้างความเสียหายแก่ระบบ การจารกรรมข้อมูลบนระบบคอมพิวเตอร์ (ข้อมูลการค้าการเงิน หรือข้อมูลส่วนตัว) หรือแม้แต่การโจมตีโครงสร้างพื้นฐานที่มีความสำคัญยิ่งยวดที่สามารถทำให้ระบบเศรษฐกิจหยุดชะงักและได้รับความ

เสียหายหรือเกิดอันตรายต่อชีวิตและทรัพย์สินของผู้คน โดยที่ภัยไซเบอร์เหล่านี้ล้วนแล้วแต่พัฒนาอย่างรวดเร็วตามความก้าวหน้าของเทคโนโลยี

โดยรวมแล้ว สถานการณ์ความพร้อมของประเทศเกี่ยวกับการรับมือและจัดการความเสี่ยงกับภาวะภัยคุกคามทางไซเบอร์ยังมีข้อจำกัดในหลายด้าน ในขณะที่ความซับซ้อนของภัยคุกคามที่เกิดขึ้นมีความแปลกใหม่ตลอดเวลา ดูได้จากเหตุการณ์การค้นพบช่องโหว่ในระบบปฏิบัติการ แอปพลิเคชัน หรือแม้แต่ซอฟต์แวร์ของอุปกรณ์ประเภท IoT (Internet of Things) ที่เริ่มมีการใช้งานอย่างแพร่หลายในช่วงหลายปีที่ผ่านมา ทำให้แฮกเกอร์สามารถลักลอบติดตั้งมัลแวร์หรือโปรแกรมประสงค์ร้ายบนคอมพิวเตอร์ที่มีช่องโหว่และฝังรหัสอันตราย สามารถสร้างความเสียหายให้กับข้อมูลของเหยื่อ เช่น WannaCry Ransomware ซึ่งเป็นมัลแวร์เรียกค่าไถ่ข้อมูลด้วยการเข้ารหัสลับ ทำให้ผู้ใช้ไม่สามารถเปิดข้อมูลใช้งานได้ และพบว่าแพร่กระจายได้ด้วยตัวเองผ่านการโจมตีช่องโหว่ของระบบปฏิบัติการ Windows ทำให้การระบาดเป็นไปอย่างรวดเร็วในวงกว้างกว่าเดิม หรือ Mirai Botnet ซึ่งเป็นมัลแวร์โจมตีอุปกรณ์ประเภท IoT ที่แฮกเกอร์สามารถสั่งการให้โจมตีระบบคอมพิวเตอร์ของผู้อื่นที่อยู่ในเครือข่ายคอมพิวเตอร์ในลักษณะ DDoS (Distributed Denial-of-Service) และทำให้บริการเครือข่ายอินเทอร์เน็ตและบริการที่ตกเป็นเป้าโจมตีขาดสภาพความพร้อมให้บริการ

นอกจากนี้ จากรายงานสถิติจากหลายแห่ง ได้ระบุว่าประเทศไทยยังมีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น สถาบันนานาชาติในการจัดอันดับความสามารถในการแข่งขันของประเทศสมาชิก หรือ International Institute for Management Development (IMD)

ได้มีรายงาน World Digital Competitiveness Rankings ประเมินจัดอันดับ ๖๓ เขตเศรษฐกิจ พบว่า อันดับความสามารถในการแข่งขันทางดิจิทัลของไทยในปี ๒๕๕๙ อยู่อันดับที่ ๔๑ จากอันดับที่ ๓๙ ในปี ๒๕๕๘ และในด้านความรู้อยู่ที่อันดับ ๔๔ จากเดิมที่อันดับ ๔๒ แม้ว่าความพร้อมในอนาคตโดยรวมอยู่ที่อันดับ ๔๕ จากเดิมที่อันดับ ๔๘ แต่พบว่ายังมีจุดอ่อนในด้าน IT integration อยู่ที่อันดับ ๕๕ แม้ว่าอันดับจะดีขึ้นจากอันดับที่ ๕๗ ในปี ๒๕๕๘ ก็ตาม แต่ด้าน E-Government ไทยอยู่ในอันดับที่ ๕๕ และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่อันดับที่ ๓๘

โดยสรุปแล้ว ไทยนั้นมีความพร้อมรับมือภัยคุกคามทางไซเบอร์อยู่แล้วในระดับหนึ่ง แต่ก็ยังสามารถพัฒนาขีดความสามารถในการรับมือให้มีประสิทธิภาพยิ่งขึ้นกว่าเดิมได้เพื่อให้ทันต่อสถานการณ์ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว โดยเฉพาะในด้านการรับมือกับการถูกโจมตีระบบ การส่งเสริมความรู้ความเข้าใจและความตระหนักโดยรวมด้านความมั่นคงปลอดภัยไซเบอร์ และการจัดการบูรณาการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในภาครัฐเองและระหว่างรัฐกับภาคส่วนอื่น ๆ ดังที่ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ ได้ระบุแนวทางการดำเนินการเอาไว้

กรอบแนวคิด

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ ได้นำแนวทางจากกรอบยุทธศาสตร์ชาติ ๒๐ ปี ซึ่งกำหนดไว้ในส่วนของยุทธศาสตร์ด้านความมั่นคงข้อ (๕) พัฒนาระบบกลไก มาตรการและความร่วมมือระหว่างประเทศทุกระดับ เพื่อป้องกัน

และแก้ไขปัญหาภัยคุกคามข้ามชาติ ลดผลกระทบจากภัยก่อการร้ายและเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ และข้อ (๖) พัฒนาเสริมสร้างศักยภาพกองทัพ ปรับโครงสร้างกำลังและยุทโธปกรณ์ที่เหมาะสม พัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ พร้อมสร้างความร่วมมือ กับประเทศเพื่อนบ้าน

นอกจากนี้ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ก็ได้ระบุให้ภัยคุกคามทางไซเบอร์เป็นหนึ่งในภัยคุกคามความมั่นคง โดยกำหนดแนวทางในประเด็นที่ ๓.๗.๑๕ การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ โดยได้กำหนดเป้าหมายเชิงยุทธศาสตร์ ตัวชี้วัด และกลยุทธ์ ดังนี้

เป้าหมายเชิงยุทธศาสตร์

ประเทศเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

ตัวชี้วัด

๑) ระดับความพร้อมของไทยในการป้องกันความเสี่ยงจากการโจมตีด้านไซเบอร์ที่สอดคล้องกับหลักสากล

๒) ระบบป้องกันทางไซเบอร์ที่มีประสิทธิภาพ สามารถปกป้องข้อมูลอิเล็กทรอนิกส์ของรัฐบาล ตลอดจนโครงสร้างพื้นฐานสำคัญทางไซเบอร์

กลยุทธ์

๑) พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือน และตำรวจ และภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล

๒) พัฒนากรอบความร่วมมือระหว่างประเทศและอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

๓) พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญของภัยคุกคามความมั่นคงทางไซเบอร์

๔) ปกป้อง ป้องกัน ภัยคุกคามทางไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ

๕) พัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์

๖) ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน/บุคลากรที่เกี่ยวข้องให้มีความรู้ ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

ในส่วนของแผนพัฒนาฯ ฉบับที่ ๑๒ ได้ระบุไว้ในยุทธศาสตร์ที่ ๕ ถึงการเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน โดยระบุไว้ในเป้าหมายที่ ๕ ว่า ประเทศไทยมีความพร้อมต่อการรับมือภัยคุกคาม ทั้งภัยคุกคามทางทหารและภัยคุกคามอื่น ๆ ซึ่งมี ๓ ตัวชี้วัด ประกอบด้วย ตัวชี้วัดที่ ๕.๑ ระยะเวลาในการระดมสรรพกำลังเมื่อเกิดภัยคุกคาม ตัวชี้วัดที่ ๕.๒ อันดับความเสี่ยงจากการก่อการร้าย

ต่ำกว่าอันดับที่ ๒๐ ของโลก (ดัชนีความเสี่ยงของโลกของ WEF) และตัวชี้วัดที่ ๕.๓ อันดับความเสี่ยงจากการโจมตีด้านไซเบอร์ต่ำกว่าอันดับที่ ๑๐ ของโลก (ดัชนีความปลอดภัยไซเบอร์ของโลกของ International Telecommunication Union: ITU) และในยุทธศาสตร์ที่ ๗ กล่าวถึงการพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ โดยในเป้าหมายที่ ๕ เรื่องการพัฒนาเศรษฐกิจดิจิทัลเพื่อขยายโครงข่ายอินเทอร์เน็ตความเร็วสูงให้ครอบคลุมทั่วทั้งประเทศ และสร้างผู้ประกอบการธุรกิจดิจิทัลรายใหม่เพิ่มขึ้น รวมทั้งพัฒนาระบบความมั่นคงปลอดภัยทางไซเบอร์ให้มีประสิทธิภาพและสอดคล้องตามมาตรฐานสากลเพื่อรับมือภัยคุกคามทางออนไลน์ โดยมีตัวชี้วัดที่สำคัญ คือ จำนวนหน่วยงานภาครัฐมีระบบความมั่นคงปลอดภัยทางไซเบอร์ที่เพิ่มขึ้น รวมทั้งสร้างความมั่นคงปลอดภัยทางไซเบอร์ โดยจัดตั้งศูนย์การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์เพื่อดูแลปัญหาและรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปตามความก้าวหน้าของเทคโนโลยีโดยเฉพาะความมั่นคงปลอดภัยในภาคการเงินและความปลอดภัยของข้อมูลส่วนบุคคล โดยมีแนวทางการพัฒนาคือให้ปรับปรุงโครงสร้างพื้นฐานโทรคมนาคมของประเทศให้ทั่วถึงและมีประสิทธิภาพ ส่งเสริมการใช้เทคโนโลยีดิจิทัลในการสร้างมูลค่าเพิ่มทางธุรกิจการส่งเสริมนวัตกรรมการวิจัยและพัฒนาอุตสาหกรรมดิจิทัลและเทคโนโลยีอวกาศของไทย พัฒนาความรู้และทักษะของประชาชน และให้สร้างความมั่นคงปลอดภัยทางไซเบอร์

อีกทั้งในแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมได้ระบุในยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล มุ่งเน้นการมีกฎหมาย กฎระเบียบ กติกา และมาตรฐานที่มีประสิทธิภาพ ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรค

เพิ่มประสิทธิภาพในการประกอบกิจกรรมและทำธุรกรรมออนไลน์ต่าง ๆ รวมถึงสร้างความมั่นคงปลอดภัยและความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัลในทุกภาคส่วน เพื่อรองรับการเติบโตของเทคโนโลยีดิจิทัลและการใช้งานที่เพิ่มขึ้นในอนาคต เช่น การสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์ สร้างความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารเพื่อสร้างความเชื่อมั่นให้กับภาคธุรกิจและประชาชนในการสื่อสารและการทำธุรกรรมออนไลน์ การกำหนดมาตรการการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์ที่เหมาะสมและสอดคล้องตามมาตรฐานสากล โดยเฉพาะการปกป้องโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (critical infrastructure) เช่น โครงสร้างพื้นฐานทางไฟฟ้า โครงสร้างพื้นฐานทางการเงิน ให้มีความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน การสร้างเครือข่ายแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ พร้อมกำหนดหน่วยงานรับแจ้งเหตุและสร้างกลไกการบังคับใช้กฎหมายที่มีประสิทธิภาพในการป้องกันปราบปรามการกระทำความผิดที่มีผลต่อระบบความมั่นคงปลอดภัยดิจิทัล

นอกจากนี้ ในการประชุมสุดยอดอาเซียน ครั้งที่ ๒๘ และ ๒๙ ณ กรุงเวียงจันทน์ เมื่อปี พ.ศ. ๒๕๕๙ นายกรัฐมนตรียังได้เสนอให้ประเทศสมาชิกอาเซียนจัดตั้งหน่วยงานติดตามและเฝ้าระวังภัยคุกคามไซเบอร์เป็นการเฉพาะ กำหนดมาตรการด้านกฎหมายร่วมกัน ตลอดจนส่งเสริมเครือข่ายความร่วมมือระหว่างบุคลากรและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจนำไปสู่การจัดตั้งศูนย์ไซเบอร์อาเซียน ซึ่งสะท้อนถึงความสำคัญที่รัฐบาลไทยมีให้กับการรักษาความมั่นคงปลอดภัยไซเบอร์และความร่วมมือกับต่างประเทศ

ซึ่งจากกรอบยุทธศาสตร์ชาติ ๒๐ ปี นโยบายและแผนระดับชาติ ว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) แผนพัฒนาฯ ฉบับที่ ๑๒ และแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม แนวคิดของนายกรัฐมนตรีที่นำเสนอในระหว่างการประชุมสุดยอดอาเซียน ประกอบกับการประเมินสถานการณ์ภัยคุกคามไซเบอร์และความพร้อมของไทยที่กล่าวไว้ข้างต้น จึงได้ประมวลเป็นยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ เพื่อเป็นกรอบการดำเนินงานที่ใช้กับทุกภาคส่วน ทั้งภาครัฐ ภาคธุรกิจ และภาคประชาชน โดยเน้นความสมดุลระหว่างสิทธิเสรีภาพของประชาชนและการใช้อำนาจของรัฐเชิงนโยบายในการควบคุมและรักษาความสงบเรียบร้อยของสังคม

วิสัยทัศน์

ไซเบอร์สเปซของไทยมีความมั่นคงปลอดภัย ทุกภาคส่วนมั่นใจมีความพร้อมรับมือกับภัยคุกคามทางไซเบอร์และร่วมมือกันใช้ไซเบอร์อย่างสร้างสรรค์ เพื่อส่งเสริมความมั่นคงทางเศรษฐกิจและคุณภาพชีวิตที่ดี

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

<u>วัตถุประสงค์</u>

๑. เพื่อสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนต่อการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

๒. เพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

๓. เพื่อปกป้องผลประโยชน์และความมั่นคงของชาติจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

๔. เพื่อเสริมสร้างเศรษฐกิจดิจิทัล

๕. เพื่อบูรณาการและประสานความร่วมมือ รวมทั้งการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างหน่วยงาน

๖. เพื่อพัฒนาศักยภาพของหน่วยงานและเพิ่มขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๗. เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ

๘. เพื่อส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

๙. เพื่อส่งเสริมบทบาทของไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

<u>เป้าหมาย</u>

- ภาคส่วนต่าง ๆ เชื่อมั่นและไว้วางใจในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ
- โครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและประเทศโดยรวมมีขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์
- ผลประโยชน์และความมั่นคงของชาติได้รับการปกป้องจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่
- ประเทศเปลี่ยนผ่านสู่เศรษฐกิจที่ใช้เทคโนโลยีดิจิทัลได้อย่างราบรื่นและยั่งยืน
- ทุกภาคส่วนมีความตระหนักถึงภัยคุกคามทางไซเบอร์และร่วมมือกันด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- ประเทศไทยมีวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ
- มีการบูรณาการและการประสานความร่วมมือ รวมทั้งการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน
- งานด้านการป้องกันและปราบปรามอาชญากรรมมีความเข้มแข็ง การสืบสวนและงานข่าวมีคุณภาพและมั่นคงปลอดภัย
- หน่วยงานมีความพร้อมสามารถตอบสนองการปฏิบัติการได้อย่างถูกต้องและรวดเร็ว
- บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์มีความเชี่ยวชาญและมีศักยภาพในการปฏิบัติงาน
- ไทยมีบทบาทในการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติและการลดความขัดแย้งทางไซเบอร์ระหว่างรัฐ

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

เป้าหมาย

๑. รัฐบาลให้ความสำคัญและสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ภาคธุรกิจและประชาชนมั่นใจในการใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ตและไซเบอร์สเปซที่ได้มาตรฐาน ทั้งจากการใช้บริการภาครัฐ ภาคธุรกิจและส่วนบุคคล

ตัวชี้วัด

๑. รัฐบาลสนับสนุนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้มีผลบังคับใช้โดยเร็ว

๒. ระดับความมั่นใจของเอกชนและประชาชนในการใช้เทคโนโลยีดิจิทัลและไซเบอร์สเปซ

แนวทางการดำเนินการ

๑.๑ ระดับนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้การสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒ พัฒนาโครงสร้างองค์กรในภาครัฐ เพื่อรองรับสังคมดิจิทัลและรับมือภัยคุกคามทางไซเบอร์ เพื่อเสริมสร้างความไว้วางใจแก่ภาคส่วนต่าง ๆ ที่ติดต่อประสานงานกับรัฐ

๑.๓ ส่งเสริมการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ตเพื่อการบริการประชาชนของหน่วยงานรัฐ และประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบและมั่นใจในการใช้บริการของหน่วยงานของรัฐ

๑.๔ ส่งเสริมให้ภาครัฐมีความโปร่งใส โดยใช้เทคโนโลยีและดำเนินกิจกรรมทางไซเบอร์โดยคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพตลอดจนความเป็นส่วนตัวของผู้ใช้บริการออนไลน์ของภาครัฐ

๑.๕ สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่าง ๆ นอกเหนือจากภาครัฐ โดยเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐในการพัฒนาและปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์ เพื่อให้ตรงตามความประสงค์ของผู้รับบริการ

๑.๖ ส่งเสริมให้ภาคเอกชนในธุรกิจสาขาต่าง ๆ ในทุกระดับดำเนินธุรกิจโดยใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ต และไซเบอร์สเปซในวงกว้างและได้มาตรฐาน โดยประชาสัมพันธ์เชิงรุกและขอความร่วมมือจากภาคเอกชน

<u>ประเด็นยุทธศาสตร์ที่ ๒</u> ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

เป้าหมาย

๑. ประเทศไทยมีการบูรณาการการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. ประเทศไทยมีหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ และมีการกำหนดบทบาทและหน้าที่หน่วยงานต่าง ๆ ของรัฐอย่างชัดเจน เพื่อดูแลการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน

๓. มีการทำงานขององค์กรต่าง ๆ ในรูปแบบที่สามารถทำงานที่พร้อมรับมือกับภัยคุกคามทางไซเบอร์ในแบบ CERT มากขึ้น

ตัวชี้วัด

๑. การจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. การจัดทำรายงานการเตรียมความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ถือว่าเป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ

๓. จำนวนองค์กรที่มีการจัดทำแผนปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ

๔. มีการทำงานในรูปแบบการทำงานของ CERT ในกลุ่มหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศเพิ่มจำนวนมากขึ้นเพื่อให้มีการทำงานแบบบูรณาการกับหน่วยงานกลางที่จะจัดตั้งขึ้น

แนวทางการดำเนินการ

๒.๑ จัดทำกรอบนโยบาย/ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔ สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ

และทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อการปรับปรุงนโยบายให้ทันกับสถานการณ์ที่เปลี่ยนไป

๒.๒ ให้มีการจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติเพื่อทำหน้าที่เป็นศูนย์กลางระดับนโยบายที่ขึ้นตรงต่อนายกรัฐมนตรี โดยเป็นศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์ และประสานการปฏิบัติ ทั้งในด้านการประสานงาน เฝ้าระวัง ตอบสนอง บริหารจัดการภัยคุกคามทางไซเบอร์ สร้างความตระหนักตลอดจนประสานความร่วมมือทั้งในและต่างประเทศและส่งเสริมการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานต่าง ๆ โดยอาจพิจารณาจัดตั้งหน่วยปฏิบัติขึ้นมาสนับสนุนตามความเหมาะสม

๒.๓ จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งของภาครัฐและเอกชน พร้อมจัดลำดับความสำคัญ เพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ

๒.๔ กำหนดบทบาทและหน้าที่ของหน่วยงานต่าง ๆ ของรัฐในด้านการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศอย่างชัดเจน เพื่อการรับมือกับภัยคุกคามทางไซเบอร์ทั้งในยามปกติ ยามเกิดเหตุ การฟื้นตัว และฟื้นฟูหลังเกิดเหตุ รวมทั้งการเยียวยาแก้ไขผลกระทบ รวมทั้งมีกลไกประสานความร่วมมือกับภาคเอกชนและผู้มีส่วนเกี่ยวข้องเพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของไทยจากภัยคุกคามทางไซเบอร์

๒.๕ ส่งเสริมการจัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งในภาครัฐและเอกชน

โดยให้แต่ละองค์กรยึดถือหลักการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของหน่วยงานตนเองโดยอาศัยศักยภาพของหน่วยก่อน และในกรณีที่สถานการณ์ยกระดับหรือเป็นเหตุฉุกเฉินที่เกินความสามารถของหน่วย ก็สามารถประสานขอความสนับสนุนได้ทันต่อสถานการณ์

๒.๖ ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือกับสถานการณ์ทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ

๒.๗ ร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติ และข้อกำหนด เพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์โดยพิจารณากำหนดบทคุ้มครองและบทลงโทษที่เหมาะสม

๒.๘ พัฒนาศักยภาพของบุคลากรในภาครัฐผ่านการศึกษาฝึกอบรมในรูปแบบต่าง ๆ และส่งเสริมการถ่ายทอดความรู้ภายในภาครัฐหรือระหว่างภาครัฐกับเอกชน ตลอดจนให้ความสำคัญกับการพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม เพื่อเป็นการรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระบบราชการ

๒.๙ พัฒนาศักยภาพทางการวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแสวงหาความร่วมมือกับเอกชนและต่างประเทศเพื่อสามารถเข้าถึงแหล่งเทคโนโลยี แหล่งเงินทุนและพัฒนาตลาดสำหรับอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์และนำไปสู่การลดการพึ่งพาจากต่างประเทศ

๒.๑๐ ส่งเสริมการมีส่วนร่วมของภาคเอกชนอย่างจริงจังในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านการพัฒนาองค์ความรู้

และเทคโนโลยี การพัฒนาบุคลากร การรักษาความมั่นคงปลอดภัย เพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม

๒.๑๑ พัฒนามาตรฐานและกระตุ้นให้มีกลไกการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ

๒.๑๒ ส่งเสริมให้มีการทำงานด้วยการปรับใช้มาตรการทางเทคนิคในลักษณะการทำงานแบบศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ หรือ CERT โดยเฉพาะอย่างยิ่งในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้มีการประสานการทำงานรับมือกับภัยคุกคามทางไซเบอร์ในทางปฏิบัติให้มีความเข้มแข็งมากยิ่งขึ้น

<u>ประเด็นยุทธศาสตร์ที่ ๓</u> ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

เป้าหมาย

๑. มีการวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ทันสมัย ครอบคลุมรอบด้าน ต่อเนื่อง และถูกต้องแม่นยำ เพื่อประโยชน์ในการตัดสินใจทางนโยบายและปฏิบัติที่เหมาะสม

๒. กองทัพและหน่วยงานความมั่นคงที่เกี่ยวข้องมีความพร้อมรับมือภัยคุกคามทางไซเบอร์ทั้งในรูปแบบเดิมและภัยคุกคามในรูปแบบใหม่ ๆ

๓. มีแผนเผชิญภัยคุกคามทางไซเบอร์เมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

ตัวชี้วัด

๑. จำนวนหน่วยงานความมั่นคงที่เกี่ยวข้องที่จัดทำนโยบาย/ยุทธศาสตร์/แผนงานด้านการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งภัยรูปแบบเดิมและภัยรูปแบบใหม่

๒. ความถี่การปรับปรุงวิเคราะห์สถานการณ์ภัยคุกคามทางไซเบอร์ให้ทันสมัยเทียบกับความถี่ในการแลกเปลี่ยนข้อมูลและผลการวิเคราะห์

๓. จัดให้มีการซ้อมแผนเผชิญภัยคุกคามทางไซเบอร์เมื่อเกิดวิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์ โดยเน้นการฝึกร่วมระหว่างกองทัพกับหน่วยที่เกี่ยวข้อง

แนวทางการดำเนินการ

๓.๑ ศึกษา ติดตาม และวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งภัยคุกคามในรูปแบบเดิมและรูปแบบใหม่ เพื่อทราบถึงแนวโน้มความเป็นไปได้ที่ผลประโยชน์และความมั่นคงของชาติจะได้รับผลกระทบและเพื่อหาทางป้องกันไม่ให้เกิดเหตุหรือลดความเสียหายให้น้อยลงมากที่สุด

๓.๒ หน่วยงานความมั่นคงที่เกี่ยวข้องพิจารณาจัดทำนโยบาย/ยุทธศาสตร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์และบริหารจัดการการเก็บรักษาข้อมูล ป้องกันการโจมตีหรือเจาะระบบ การใช้เครื่องมือทางไซเบอร์ในความขัดแย้ง รวมทั้งประเมินสถานการณ์และทบทวนนโยบาย/ยุทธศาสตร์ด้านไซเบอร์ให้ทันสมัย

๓.๓ กำหนดบทบาทให้กองทัพดูแลรับผิดชอบการป้องกันประเทศในมิติทางไซเบอร์และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการมอบหมายจากรัฐบาลโดยเฉพาะเมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

<u>ประเด็นยุทธศาสตร์ที่ ๔</u> เสริมสร้างระบบเศรษฐกิจดิจิทัล

เป้าหมาย

๑. ประเทศไทยเปลี่ยนผ่านเข้าสู่เศรษฐกิจดิจิทัลอย่างราบรื่นและมีความยั่งยืน

๒. มีการใช้เทคโนโลยีดิจิทัลในวงกว้างมากขึ้นในภาคเอกชน

๓. มียุทธศาสตร์/แผนงาน กฎระเบียบที่มีประสิทธิภาพ เหมาะสมต่อระบบเศรษฐกิจดิจิทัลได้มาตรฐาน และเอกชนมีส่วนร่วม

ตัวชี้วัด

๑. จำนวนบริษัท/กิจการที่ใช้เทคโนโลยีดิจิทัล

๒. การจัดทำยุทธศาสตร์/แผนงาน/แผนแม่บท/กฎระเบียบที่สอดคล้องสนับสนุนเศรษฐกิจดิจิทัล

แนวทางการดำเนินการ

๔.๑ ส่งเสริมการพัฒนาขีดความสามารถหรือการดำเนินการที่สนับสนุนต่อการเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลอย่างสมดุล ราบรื่น มีคุณภาพและนำไปสู่เศรษฐกิจดิจิทัลที่ยั่งยืน

๔.๒ สนับสนุนการมีส่วนร่วมของภาคเอกชนในการส่งเสริมเศรษฐกิจดิจิทัลกับภาครัฐ ทั้งในกลุ่มผู้ที่ใช้เทคโนโลยีดิจิทัลเพื่อดำเนินธุรกิจอยู่แล้ว และส่งเสริมการใช้เทคโนโลยีดิจิทัลในวงกว้าง

๔.๓ พัฒนา ปรับปรุงยุทธศาสตร์ แผนหรือแผนงาน ตลอดจนกฎหมาย ระเบียบปฏิบัติ ที่เหมาะสมสอดคล้องและเอื้ออำนวยต่อเศรษฐกิจดิจิทัล พร้อมทั้งมีการประเมินผลและทบทวนอย่างสม่ำเสมอ โดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์ แผนหรือแผนงานดังกล่าว

<u>ประเด็นยุทธศาสตร์ที่ ๕</u> สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมาย

๑. ประชาชนทั่วไปทุกระดับทุกเพศและวัยที่เป็นผู้ใช้อินเทอร์เน็ตมีความตระหนักถึงภัยคุกคามทางไซเบอร์ และมีความรู้เรื่องการรักษาความปลอดภัยทางไซเบอร์

๒. รัฐ ภาคเอกชน และประชาสังคมร่วมมือกันในการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. ช่องทาง/กลไกการสื่อสารแนวนโยบายสู่การปฏิบัติในภาคเอกชนและภาคประชาสังคม

ตัวชี้วัด

๑. การจัดทำคู่มือเผยแพร่ความรู้เกี่ยวกับด้านไซเบอร์และการประเมินผล

๒. จำนวนครั้งการประชาสัมพันธ์ผ่านสื่อประเภทต่าง ๆ/กลไกต่าง ๆ

๓. การจัดฝึกอบรมให้ความรู้แก่ประชาชนผู้ใช้อินเทอร์เน็ตและการประเมินผล

แนวทางการดำเนินการ

๕.๑ ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วนโดยทั่วถึงกันผ่านสื่อและกลไกต่าง ๆ ของภาครัฐ ภาคเอกชน และภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการใช้เทคโนโลยีดิจิทัลและการดำเนินกิจกรรมทางไซเบอร์อย่างปลอดภัยและเกิดประโยชน์ และส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่ม ทั้งในระดับบุคคลและองค์กร

๕.๒ ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถานศึกษา เช่น มหาวิทยาลัยและสถาบันคลังสมอง ในด้านการแลกเปลี่ยนความรู้ การวิจัยร่วมกันและ/หรือการนำเสนองานวิจัยตลอดจนการจัดทำคู่มือเผยแพร่ความรู้เกี่ยวข้องกับด้านไซเบอร์

๕.๓ ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐาน ทั้งสายสามัญ

และอาชีวะ โดยให้เนื้อหาของหลักสูตรมีความแตกต่างกันไปในแต่ละระดับการศึกษา

๕.๔ ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่ประชาชนผู้ใช้อินเทอร์เน็ตทั่วไป ผู้สูงอายุ เด็ก สตรีและเยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับสถานศึกษา องค์การบริหารส่วนท้องถิ่นและหน่วยงานที่เกี่ยวข้องเพื่อเผยแพร่ความรู้และสร้างความตระหนักอย่างเป็นระบบและต่อเนื่อง

๕.๕ ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชนและภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์รวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชนและภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหา ประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์

<u>ประเด็นยุทธศาสตร์ที่ ๖</u> เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

เป้าหมาย

๑. ให้มีกลไกที่มีการปลูกฝังจิตสำนึกที่ดีในการใช้ไซเบอร์สเปซไปในทางที่เหมาะสม และเคารพสิทธิและเสรีภาพขั้นพื้นฐานของผู้อื่นบนโลกไซเบอร์

๒. ส่งเสริมให้เกิดเครือข่ายผู้ใช้อินเทอร์เน็ตที่ช่วยกันดูแลการใช้ไซเบอร์สเปซไปในทางที่เหมาะสม

๓. ส่งเสริมการเรียนรู้ โดยเฉพาะอย่างยิ่งในกลุ่มเด็กและเยาวชนให้รู้เท่าทันและมีความตระหนักเกี่ยวกับภัยคุกคามที่กระทบต่อความมั่นคงปลอดภัยของไซเบอร์สเปซ

ตัวชี้วัด

๑. การจัดโครงการ “Cyberspace Watch” ในหลายระดับ เช่น โครงการของชุมชน ท้องถิ่น สถาบันการศึกษา

๒. การจัดอบรมเครือข่ายผู้ใช้อินเทอร์เน็ต ทั้งในการประสานความร่วมมือในการดูแลและปลูกฝังจิตสำนึกเพื่อให้มีการใช้ไซเบอร์สเปซในทางที่เหมาะสม

แนวทางการดำเนินการ

๖.๑ ส่งเสริมค่านิยมอันดีงามของชาติบนโลกไซเบอร์ โดยส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนไปเพื่อการธำรงไว้ซึ่ง ชาติ ศาสนา และพระมหากษัตริย์

๖.๒ ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซด้วยความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย

<u>ประเด็นยุทธศาสตร์ที่ ๗</u> ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

เป้าหมาย

๑. บุคลากรด้านการสืบสวนและงานข่าวมีขีดความสามารถสูงขึ้น

๒. หน่วยงานของไทยมีเทคโนโลยีที่ทันสมัยยิ่งขึ้นในการช่วยในงานสืบสวนและงานข่าว

ตัวชี้วัด

๑. การจัดการฝึกอบรม/พัฒนาขีดความสามารถด้านไซเบอร์เพื่อการสืบสวนและงานข่าว

๒. แผนงาน/โครงการจัดหาเทคโนโลยีที่ทันสมัยสำหรับงานสืบสวนและงานข่าว

แนวทางการดำเนินการ

๗.๑ ยกระดับและกำหนดบทบาทของผู้บังคับใช้กฎหมาย ซึ่งได้แก่ เจ้าหน้าที่ตำรวจและเจ้าหน้าที่กรมสอบสวนคดีพิเศษและเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้องในการสืบสวนทางไซเบอร์เพื่อค้นหาตัวผู้กระทำผิดมาลงโทษ

๗.๒ ส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวนและงานข่าว ตลอดจนส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยในงานสืบสวนและงานข่าว

๗.๓ ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรม เพื่อเพิ่มประสิทธิภาพการจัดการภัยคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์

๗.๔ ส่งเสริมความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ตลอดจนประสบการณ์และแนวปฏิบัติที่ดีกับต่างประเทศ ทั้งในระดับทวิภาคีและกับองค์การระหว่างประเทศที่เกี่ยวข้อง อาทิ ตำรวจสากล เพื่อการพัฒนาขีดความสามารถในการป้องกันและปราบปรามอาชญากรรมของไทย โดยเฉพาะประโยชน์ในการสืบสวนและการข่าว

๗.๕ ส่งเสริมและสนับสนุนการพัฒนาระเบียบ และกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๘ ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

เป้าหมาย

๑. ไทยมีบทบาทที่สร้างสรรค์ในการพัฒนาหรือผลักดันให้เกิดบรรทัดฐาน มาตรฐาน และการสร้างความวางใจหรือความเชื่อมั่นในการร่วมกันใช้ไซเบอร์สเปซ ทั้งในระดับภูมิภาคและระดับระหว่างประเทศ

๒. มีการแลกเปลี่ยนองค์ความรู้และแนวปฏิบัติที่ดีกับต่างประเทศอย่างต่อเนื่อง

ตัวชี้วัด

๑. การประชุมหารือเกี่ยวกับบรรทัดฐาน มาตรฐาน และการสร้างความไว้เนื้อเชื่อใจในไซเบอร์สเปซ

๒. การสร้างเครือข่ายด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับภูมิภาคและระดับระหว่างประเทศ

แนวทางการดำเนินการ

๘.๑ สนับสนุนให้มีการใช้ไซเบอร์สเปซในทางสันติ โดยไม่ใช้เทคโนโลยีสารสนเทศเพื่อการสร้างความขัดแย้ง ตลอดจนร่วมมือกับมิตรประเทศในการต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการก่ออาชญากรรมข้ามชาติหรือการกระทำที่สร้างความเสียหาย

๘.๒ สนับสนุนการแลกเปลี่ยนองค์ความรู้ ข้อมูล แนวปฏิบัติที่ดีด้านไซเบอร์กับต่างประเทศ ทั้งในระดับทวิภาคีระดับภูมิภาคและระดับพหุภาคี

๘.๓ มีช่องทางการสื่อสารแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ชัดเจนในการร่วมมือกับต่างประเทศในการตอบสนองและรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

๘.๔ มีบทบาทในการส่งเสริมการหารือเกี่ยวกับบรรทัดฐาน มาตรฐาน และมาตรการสร้างความไว้วางใจหรือความเชื่อมั่นระหว่างประเทศในมิติไซเบอร์ รวมถึงการมีท่าทีร่วมกันในระดับภูมิภาค เพื่อให้บรรทัดฐานระหว่างประเทศเป็นที่ยอมรับและสะท้อนผลประโยชน์ของไทยและประเทศในภูมิภาค

ปัจจัยแห่งความสำเร็จ

๑. รัฐบาลให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและผลักดันให้เกิดผลเป็นรูปธรรมอย่างจริงจัง

๒. หน่วยงานต่าง ๆ นำแนวทางตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปปฏิบัติ และจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานตัวเอง และปฏิบัติตามแผนฯ อย่างจริงจัง

๓. ทุกภาคส่วนที่เกี่ยวข้อง ทั้งภาครัฐ เอกชน และภาคประชาชนให้ความร่วมมือและมีส่วนร่วมในการสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. จัดให้มีการทบทวนประเมินผลการดำเนินการตามยุทธศาสตร์ทุก ๒ ปี

ตารางประสานสอดคล้อง
แสดงความเชื่อมโยงภารกิจงาน นโยบาย
ยุทธศาสตร์ แผนหลักที่เกี่ยวข้องกับ
ยุทธศาสตร์การรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ
พ.ศ. ๒๕๖๐ – ๒๕๖๔

ตารางประสานสอดคล้องแสดงความเชื่อมโยงภารกิจงาน นโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง กับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)

ยุทธศาสตร์ด้านความมั่นคง : ข้อ ๕ พัฒนาระบบ กลไก มาตรการและความร่วมมือระหว่างประเทศทุกระดับ เพื่อป้องกันและแก้ไขปัญหาภัยคุกคามข้ามชาติ ลดผลกระทบจากภัยก่อการร้าย และเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ และข้อ ๖ พัฒนาเสริมสร้างศักยภาพกองทัพ ปรับโครงสร้างกำลังและยุทโธปกรณ์ที่เหมาะสม พัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ พร้อมสร้างความร่วมมือกับประเทศเพื่อนบ้าน

นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๐ – ๒๕๖๔) ได้ระบุให้ภัยคุกคามทางไซเบอร์เป็นหนึ่งในภัยคุกคามความมั่นคงโดยกำหนดแนวทางไว้ในประเด็นที่ ๓.๗.๑๕ การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ได้กำหนดเป้าหมายเชิงยุทธศาสตร์ คือ ประเทศเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และมีกลยุทธ์ ในด้าน ๑) พัฒนาขีดความสามารถทั้งองค์กรภาครัฐ ทั้งฝ่ายทหาร พลเรือน และตำรวจ และภาคส่วนต่างๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคมดิจิทัล ๒) พัฒนากรอบความร่วมมือระหว่างประเทศ และอาเซียนเพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ๓) พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญของภัยคุกคามความมั่นคงทางไซเบอร์ ๔) ปกป้อง ป้องกัน ภัยคุกคามทางไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ และเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วนทั้งภายในและภายนอกประเทศ ๕) พัฒนาการบังคับใช้กฎหมาย ระเบียบต่างๆ เพื่อความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ ๖) ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน/บุคลากรที่เกี่ยวข้องให้มีความรู้ ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน โดยเป้าหมายคือ ประเทศไทยมีความพร้อมต่อการรับมือภัยคุกคาม ทั้งภัยคุกคามทางทหารและภัยคุกคามอื่นๆ

ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์ โดยมีแนวทางการพัฒนาคือให้ปรับปรุงโครงสร้างพื้นฐานโทรคมนาคมของประเทศให้ทั่วถึงและมีประสิทธิภาพ ส่งเสริมการใช้เทคโนโลยีดิจิทัลในการสร้างมูลค่าเพิ่มทางธุรกิจ การส่งเสริมนวัตกรรมการวิจัยและพัฒนาอุตสาหกรรมดิจิทัลและเทคโนโลยีอวกาศของไทย พัฒนาความรู้และทักษะของประชาชน และให้สร้างความมั่นคงปลอดภัยทางไซเบอร์

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

ยุทธศาสตร์ที่ ๓ สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล เป็นการสร้างสังคมดิจิทัลที่มีคุณภาพ (digital society) เพื่อให้เกิดการใช้เทคโนโลยีดิจิทัลอย่างสร้างสรรค์ โดยประชาชนทุกคนมีความตระหนัก ความรู้ ความเข้าใจ ทักษะในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์ (Digital Literacy)

ยุทธศาสตร์ที่ ๕ พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล เป็นการสร้างและพัฒนาบุคลากรผู้ทำงานให้มีความสามารถในการสร้างสรรค์และใช้เทคโนโลยีดิจิทัลอย่างชาญฉลาดในการประกอบอาชีพ รวมถึงการพัฒนาทักษะด้านเทคโนโลยีดิจิทัลในบุคลากรภาครัฐ ภาคเอกชน ทั้งที่ประกอบอาชีพในสาขาเทคโนโลยีดิจิทัลโดยตรงและทุกสาขาอาชีพ ให้มีความรู้ความสามารถและความเชี่ยวชาญตามระดับมาตรฐานสากล

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล โดยมุ่งเน้นการสร้างความมั่นคงปลอดภัย และความเชื่อมั่นในการทำธุรกรรมด้วยเทคโนโลยีดิจิทัลให้กับผู้ประกอบการ ผู้ทำงาน และผู้ใช้บริการ ซึ่งถือได้ว่าเป็นปัจจัยพื้นฐานที่ช่วยขับเคลื่อนประเทศสู่ยุคเศรษฐกิจดิจิทัล และเป็น บทบาทหน้าที่หลักของภาครัฐในการอำนวยความสะดวกให้กับทุกภาคส่วน โดยภารกิจสำคัญยิ่งยวดของยุทธศาสตร์นี้ จะครอบคลุมเรื่องมาตรฐาน (standard) การคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคล (privacy) การรักษาความมั่นคงปลอดภัย (cyber security)

ณ วันที่ ๒๔ มกราคม ๒๕๖๑

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๐ – ๒๕๖๔

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๑. **เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ**	๑.๑ ระดับนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้การสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	ดศ.*	สพธอ.* สมช. ก.พ.ร.	- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙) - นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔
	๑.๒ พัฒนาโครงสร้างองค์กรในภาครัฐ เพื่อรองรับสังคมดิจิทัลและรับมือภัยคุกคามทางไซเบอร์ เพื่อเสริมสร้างความไว้วางใจแก่ภาคส่วนต่างๆ ที่ติดต่อประสานงานกับรัฐ	ดศ.	สพธอ. ก.พ.ร.	- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒ - แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม - แผนปฏิบัติการเพื่อขับเคลื่อนการพัฒนารายยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจ และสังคม ระยะ ๕ ปี (พ.ศ. ๒๕๖๐ – ๒๕๖๔)
	๑.๓ ส่งเสริมการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ตเพื่อการบริการประชาชนของหน่วยงานรัฐ และประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบและมั่นใจในการใช้บริการของหน่วยงานของรัฐ	ดศ.	สพธอ. สรอ.	
	๑.๔ ส่งเสริมให้ภาครัฐมีความโปร่งใส โดยใช้เทคโนโลยีและดำเนินกิจกรรมทางไซเบอร์โดยคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพตลอดจนความเป็นส่วนตัวของผู้ใช้บริการออนไลน์ของภาครัฐ	ดศ.	สพธอ. สรอ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๑.๕ สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่างๆ นอกเหนือจากภาครัฐ โดยเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐในการพัฒนาและปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์ เพื่อให้ตรงตามความประสงค์ของผู้รับบริการ	ดศ.	สพธอ. สรอ.	
	๑.๖ ส่งเสริมให้ภาคเอกชนในธุรกิจสาขาต่าง ๆ ในทุกระดับดำเนินธุรกิจโดยใช้เทคโนโลยีดิจิทัล อินเทอร์เน็ตและไซเบอร์สเปซในวงกว้างและได้มาตรฐาน โดยประชาสัมพันธ์เชิงรุกและขอความร่วมมือจากภาคเอกชน	ดศ.	สพธอ. สรอ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๒. **ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์**	๒.๑ จัดทำกรอบนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศและทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อการปรับปรุงนโยบายให้ทันกับสถานการณ์ที่เปลี่ยนไป	ดศ.	สพธอ. มท. สมช. คค. ภาคเอกชน สรอ. สธ. พน. ธปท. ปปง. สถาบันการเงิน	**- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)** **- นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔** **- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒** **- แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม** **- แผนปฏิบัติการเพื่อขับเคลื่อนการพัฒนารายยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจ และสังคม ระยะ ๕ ปี (พ.ศ. ๒๕๖๐ – ๒๕๖๔)**
	๒.๒ พิจารณาจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติเพื่อทำหน้าที่เป็นศูนย์กลางระดับนโยบายที่ขึ้นตรงต่อนายกรัฐมนตรี โดยเป็นศูนย์กลางข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ และประสานการปฏิบัติ ทั้งในด้านการประสานงานเฝ้าระวัง ตอบโต้ บริหารจัดการภัยคุกคามทางไซเบอร์ สร้างความตระหนัก ตลอดจนประสานความร่วมมือทั้งในและต่างประเทศและส่งเสริมการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานต่างๆ โดยอาจพิจารณาจัดตั้งหน่วยปฏิบัติขึ้นมาสนับสนุนตามความเหมาะสม	ดศ.	สพธอ. สมช. ก.พ. คค. สรอ. กสทช.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดศ. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๒.๓ จัดทำรายการโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งของภาครัฐและเอกชน พร้อมจัดลำดับความสำคัญ เพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ	ดศ	สพธอ. สมช. คค. สรอ. กสทช. ธปท. ภาคเอกชน	
	๒.๔ กำหนดบทบาทและหน้าที่ของหน่วยงานต่าง ๆ ของรัฐในด้านการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การรับมือกับภัยคุกคามทางไซเบอร์ทั้งในยามปกติ ยามเกิดเหตุ การฟื้นตัวและฟื้นฟูหลังเกิดเหตุ รวมทั้งการเยียวยาแก้ไขผลกระทบ รวมทั้งมีกลไกประสานความร่วมมือกับภาคเอกชนและผู้มีส่วนเกี่ยวข้องเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของไทยจากภัยคุกคามทางไซเบอร์	ดศ.	สพธอ. สถาบันการเงิน สรอ. สมช.	
	๒.๕ ส่งเสริมการจัดทำแผนการคุ้มกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งในภาครัฐและเอกชน โดยให้แต่ละองค์กรยึดถือหลักการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงานตนเองโดยอาศัยศักยภาพของหน่วยก่อน และในกรณีที่สถานการณ์ยกระดับหรือเป็นเหตุฉุกเฉินที่เกินความสามารถของหน่วย ก็สามารถประสานขอความสนับสนุนได้ทันต่อสถานการณ์	ดศ.	สพธอ. ธปท. ปปง. ภาคเอกชน สถาบันการเงิน	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๒.๖ ส่งเสริมการจัดการฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือสถานทาง ไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งในสภาวะวิกฤติ	ดศ.	สพธอ.	
	๒.๗ ร่างและปรับปรุงกฎหมาย ระเบียบปฏิบัติ และข้อกำหนดเพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณากำหนดบทคุ้มครองและบทลงโทษที่เหมาะสม	ดศ.	สพธอ. อส. ยธ. สคก.	
	๒.๘ พัฒนาศักยภาพของบุคลากรในภาครัฐผ่านการศึกษาฝึกอบรมในรูปแบบต่าง ๆ และส่งเสริมการถ่ายทอดความรู้ภายในภาครัฐหรือระหว่างภาครัฐกับเอกชน ตลอดจนให้ความสำคัญกับการพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม เพื่อเป็นการรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระบบราชการ	ดศ.	สพธอ. สรอ. ศธ. ก.พ.ร.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๒.๙ พัฒนาศักยภาพทางการวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยให้ภาครัฐมีบทบาทนำในการวิจัยและพัฒนาตลอดจนแสวงหาความร่วมมือกับเอกชนและต่างประเทศ เพื่อสามารถเข้าถึงแหล่งเทคโนโลยี แหล่งเงินทุนและพัฒนาตลาดสำหรับอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ และนำไปสู่การลดการพึ่งพาจากต่างประเทศ	ดศ.	สพธอ. ศธ. วท.	
	๒.๑๐ ส่งเสริมการมีส่วนร่วมของภาคเอกชนอย่างจริงจังในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในด้านการพัฒนาองค์ความรู้และเทคโนโลยี การพัฒนาบุคลากร การรักษาความปลอดภัย เพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม	ดศ.	สพธอ. ศธ. วท. ภาคเอกชน	
	๒.๑๑ พัฒนามาตรฐานและกระตุ้นให้มีกลไกการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ	ดศ.	สพธอ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๒.๑๒ ส่งเสริมให้มีการทำงานด้วยการปรับใช้มาตรการทางเทคนิคในลักษณะการทำงานแบบศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ หรือ CERT โดยเฉพาะอย่างยิ่งในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้มีการประสานการทำงานรับมือกับภัยคุกคามทางไซเบอร์ในทางปฏิบัติให้มีความเข้มแข็งมากยิ่งขึ้น	ดศ.	สพธอ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๓. **ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่**	๓.๑ ศึกษา ติดตามและวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งภัยคุกคามในรูปแบบเดิมและรูปแบบใหม่ เพื่อทราบถึงแนวโน้มความเป็นไปได้ที่ผลประโยชน์และความมั่นคงของชาติจะได้รับผลกระทบและเพื่อหาทางป้องกันไม่ให้เกิดเหตุหรือลดความเสียหายให้น้อยลงมากที่สุด	ดศ.	สพธอ. สมช. กห. สขช. ปอท. กสพ. บก.ทท.	**- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)** **- นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔**
	๓.๒ หน่วยงานความมั่นคงที่เกี่ยวข้องพิจารณาจัดทำนโยบาย/ยุทธศาสตร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์และบริหารจัดการการเก็บรักษาข้อมูล ป้องกันการโจมตีหรือเจาะระบบ การใช้เครื่องมือทางไซเบอร์ในความขัดแย้ง รวมทั้งประเมินสถานการณ์และทบทวนนโยบาย/ยุทธศาสตร์ด้านไซเบอร์ให้ทันสมัย	ดศ.	สพธอ. สมช. กห. สขช. ปอท. กสพ. บก.ทท.	
	๓.๓ กำหนดบทบาทให้กองทัพดูแลรับผิดชอบการป้องกันประเทศในมิติทางไซเบอร์และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการมอบหมายจากรัฐบาล โดยเฉพาะเมื่อเกิดสถานการณ์วิกฤติทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์	กห.	หน่วยงานในสังกัด กห.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๔. **เสริมสร้างระบบเศรษฐกิจดิจิทัล**	๔.๑ ส่งเสริมการพัฒนาขีดความสามารถหรือการดำเนินการที่สนับสนุนต่อการเปลี่ยนผ่านสู่เศรษฐกิจดิจิทัลอย่างสมดุล ราบรื่น มีคุณภาพและนำไปสู่เศรษฐกิจดิจิทัลที่ยั่งยืน	ดศ.	พณ. สพธอ. สศช. ภาคเอกชน	**- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒** **- แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม** **- แผนปฏิบัติการเพื่อขับเคลื่อนการพัฒนารายยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจ และสังคม ระยะ ๕ ปี (พ.ศ. ๒๕๖๐ – ๒๕๖๔)**
	๔.๒ สนับสนุนการมีส่วนร่วมของภาคเอกชนในการส่งเสริมเศรษฐกิจดิจิทัลกับภาครัฐ ทั้งในกลุ่มผู้ที่ใช้เทคโนโลยีดิจิทัลเพื่อดำเนินธุรกิจอยู่แล้ว และส่งเสริมการใช้เทคโนโลยีดิจิทัลในวงกว้าง	ดศ.	พณ. สพธอ. ภาคเอกชน	
	๔.๓ พัฒนา ปรับปรุงยุทธศาสตร์ แผนหรือแผนงาน ตลอดจนกฎหมาย ระเบียบปฏิบัติที่เหมาะสมสอดคล้องและเอื้ออำนวยต่อเศรษฐกิจดิจิทัล พร้อมทั้งมีการประเมินผลและทบทวนอย่างสม่ำเสมอ โดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์ แผนหรือแผนงานดังกล่าว	ดศ.	พณ. สพธอ. อส. ยธ. ภาคเอกชน	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๕. สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๕.๑ ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วนโดยทั่วถึงกันผ่านสื่อและกลไกต่าง ๆ ของภาครัฐ ภาคเอกชนและภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อการใช้เทคโนโลยีดิจิทัลและการดำเนินกิจกรรมทางไซเบอร์อย่างปลอดภัยและเกิดประโยชน์ และส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่ม ทั้งในระดับบุคคลและองค์กร	ดศ.	สพธอ. มท. ศธ. วท. กปส. พม.	**- นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๔** **- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒** **- แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม**
	๕.๒ ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถานศึกษา เช่น มหาวิทยาลัยและสถาบันคลังสมอง ในด้านการแลกเปลี่ยนความรู้ การวิจัยร่วมกันและ/หรือการนำเสนองานวิจัยตลอดจนการจัดทำคู่มือเผยแพร่ความรู้เกี่ยวข้องกับด้านไซเบอร์	ดศ.	สพธอ. ศธ. วท.	
	๕.๓ ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐานทั้งสายสามัญและอาชีวะ โดยให้เนื้อหาของหลักสูตรมีความแตกต่างกันไปในแต่ละระดับการศึกษา	ดศ.	สพธอ. ศธ. วท.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๕.๔ ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่ประชาชนผู้ใช้อินเทอร์เน็ตทั่วไป ผู้สูงอายุ เด็ก สตรีและเยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับสถานศึกษา องค์การบริหารส่วนท้องถิ่นและหน่วยงานที่เกี่ยวข้องเพื่อเผยแพร่ความรู้และสร้างความตระหนักอย่างเป็นระบบและต่อเนื่อง	ดศ.	สพธอ. ศธ. วท. กทม. มท.	
	๕.๕ ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชนและภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์รวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชนและภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหา ประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบาย ตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์	ดศ.	สพธอ. มท. ภาคเอกชน ศธ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๖. **เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม**	๖.๑ ส่งเสริมค่านิยมอันดีงามของชาติบนโลกไซเบอร์ โดยส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนไปเพื่อการธำรงไว้ซึ่งชาติ ศาสนา และพระมหากษัตริย์	ดศ.	สพธอ. มท. พม. ศธ. ยธ. ตร. หน่วยงานที่เกี่ยวข้อง	**- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)** **- นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔** **- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒** **- แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม** **- แผนปฏิบัติการเพื่อขับเคลื่อนการพัฒนารายยุทธศาสตร์ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ระยะ ๕ ปี (พ.ศ. ๒๕๖๐ – ๒๕๖๔)**
	๖.๒ ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซด้วยความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์ และไม่ละเมิดกฎหมาย	ดศ.	สพธอ. มท. พม. ศธ. ยธ. ตร. หน่วยเกี่ยวข้อง	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
๗. **ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม**	๗.๑ ยกระดับและกำหนดบทบาทของผู้บังคับใช้กฎหมาย ซึ่งได้แก่ เจ้าหน้าที่ตำรวจและเจ้าหน้าที่กรมสอบสวนคดีพิเศษ และเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้องในการสืบสวนทางไซเบอร์เพื่อค้นหาตัวผู้กระทำผิดมาลงโทษ	ตร.	กสพ. ยธ. สขช. อส. หน่วยเกี่ยวข้องในกระบวนการยุติธรรม เช่น ปปง. ป.ป.ท. ป.ป.ช. สนง.ศาลยุติธรรม	**- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)** **- นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔** **- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒** **- แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม** **- แผนแม่บทการบริหารงานยุติธรรมแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๑**
	๗.๒ ส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวนและงานข่าว ตลอดจนส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยในงานสืบสวนและงานข่าว	ตร.	กสพ. ปปง. สขช.	
	๗.๓ ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรม เพื่อเพิ่มประสิทธิภาพการจัดการภัยคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์	ตร.	กสพ. ปปง. สขช. กต.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๗.๔ ส่งเสริมความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ตลอดจนประสบการณ์และแนวปฏิบัติที่ดีกับต่างประเทศ ทั้งในระดับทวิภาคีและกับองค์การระหว่างประเทศที่เกี่ยวข้อง อาทิ ตำรวจสากล เพื่อการพัฒนาขีดความสามารถในการป้องกันและปราบปรามอาชญากรรมของไทย โดยเฉพาะประโยชน์ในการสืบสวนและการข่าว	ตร.	สขช.	
	๗.๕ ส่งเสริมและสนับสนุนการพัฒนาระเบียบ และกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์	ตร.	สขช. กสพ.	
๘. **ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ**	๘.๑ สนับสนุนให้มีการใช้ไซเบอร์สเปซในทางสันติ โดยไม่ใช้เทคโนโลยีสารสนเทศเพื่อการสร้างความขัดแย้ง ตลอดจนร่วมมือกับมิตรประเทศในการต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการก่ออาชญากรรมข้ามชาติหรือการกระทำที่สร้างความเสียหาย	ดศ.	กห. กต. สพธอ. สมช. ตร. สขช.	**- ร่างยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ. ๒๕๖๐ - ๒๕๗๙)** **- นโยบายความมั่นคงแห่งชาติ พ.ศ. ๒๕๕๘ – ๒๕๖๔** **- แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒**
	๘.๒ สนับสนุนการแลกเปลี่ยนองค์ความรู้ ข้อมูล แนวปฏิบัติที่ดีด้านไซเบอร์กับต่างประเทศ ทั้งในระดับทวิภาคี ระดับภูมิภาคและระดับพหุภาคี	ดศ.	กห. กต. สพธอ. สมช.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

ยุทธศาสตร์	แนวทางการดำเนินการ	หน่วยรับผิดชอบ		ความเชื่อมโยงกับนโยบาย ยุทธศาสตร์ แผนหลักที่เกี่ยวข้อง
		หลัก	รอง	
	๘.๓ มีช่องทางการสื่อสารแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ชัดเจนในการร่วมมือกับต่างประเทศในการตอบโต้และรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์	ดศ.	กต. สพธอ.	
	๘.๔ มีบทบาทในการส่งเสริมการหารือเกี่ยวกับบรรทัดฐาน มาตรฐาน มาตรการสร้างความไว้เนื้อเชื่อใจระหว่างประเทศในมิติไซเบอร์ รวมถึงการมีท่าทีร่วมกันในระดับภูมิภาค เพื่อให้บรรทัดฐานระหว่างประเทศเป็นที่ยอมรับและสะท้อนผลประโยชน์ของไทยและประเทศในภูมิภาค	ดศ.	กต. สพธอ.	

***ทั้งนี้ ตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับนี้ ดท. และ สพธอ. เป็นหน่วยงานหลักและหน่วยงานรองจนกว่าจะมีการจัดตั้งหน่วยงานกลางใหม่มาทำหน้าที่แทน**

สารบัญอักษรย่อรายชื่อหน่วยงาน

อักษรย่อ	คำอธิบาย
กต.	กระทรวงการต่างประเทศ
กทม.	กรุงเทพมหานคร
กปส.	กรมประชาสัมพันธ์
ก.พ.	สำนักงานคณะกรรมการข้าราชการพลเรือน
ก.พ.ร.	สำนักงานคณะกรรมการพัฒนาระบบราชการ
กสทช.	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
กสพ.	กรมสอบสวนคดีพิเศษ
กห.	กระทรวงกลาโหม
คค.	กระทรวงคมนาคม
ดศ.	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ตร.	สำนักงานตำรวจแห่งชาติ
ธปท.	ธนาคารแห่งประเทศไทย
บก.ทท.	กองบัญชาการกองทัพไทย
ปปง.	สำนักงานป้องกันและปราบปรามการฟอกเงิน
ป.ป.ช.	คณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
ป.ป.ท.	สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

อักษรย่อ	คำอธิบาย
ปอท.	กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ
พณ.	กระทรวงพาณิชย์
พน.	กระทรวงพลังงาน
พม.	กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
มท.	กระทรวงมหาดไทย
ยธ.	กระทรวงยุติธรรม
วท.	กระทรวงวิทยาศาสตร์และเทคโนโลยี
ศธ.	กระทรวงศึกษาธิการ
สขช.	สำนักข่าวกรองแห่งชาติ
สคก.	สำนักงานคณะกรรมการกฤษฎีกา
สธ.	กระทรวงสาธารณสุข
สนง.ศาลยุติธรรม	สำนักงานศาลยุติธรรม
สพธอ.	สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
สมช.	สำนักงานสภาความมั่นคงแห่งชาติ
สรอ.	สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
สศช.	สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ
อส.	สำนักงานอัยการสูงสุด

สำนักงานสภาความมั่นคงแห่งชาติ
เลขที่ ๑ ทำเนียบรัฐบาล ถนนพิษณุโลก
เขตดุสิต กรุงเทพมหานคร ๑๐๓๐๐

พิมพ์ครั้งแรก มิถุนายน ๒๕๖๑
จำนวนพิมพ์ ๕,๐๐๐ เล่ม
ลิขสิทธิ์โดย สำนักยุทธศาสตร์ความมั่นคงเกี่ยวกับภัยคุกคามข้ามชาติ
สำนักงานสภาความมั่นคงแห่งชาติ
ออกแบบปกและรูปเล่ม นางสาวพิมพ์กานต์ คล่องสั่งสอน
พิมพ์ที่ สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา
ถนนสามเสน เขตดุสิต กรุงเทพมหานคร ๑๐๓๐๐
โทรศัพท์ ๐ ๒๒๔๓ ๐๖๑๓
โทรสาร ๐ ๒๒๔๓ ๑๘๒๐