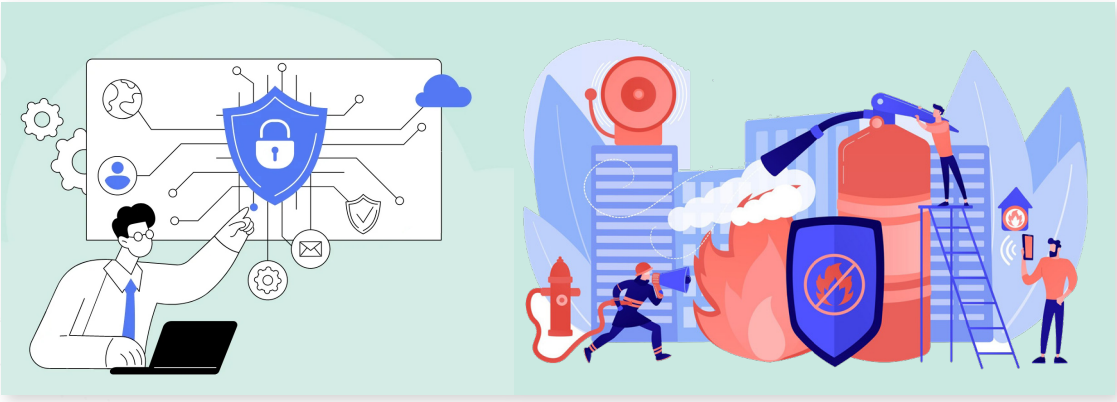
เกร็ดความรู้ที่ 1

นโยบายและแผนความมั่นคงที่ 9 การป้องกันและบรรเทาสาธารณภัย และนโยบายและแผนความมั่นคงที่ 10 การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์



เกร็ดความรู้ในส่วนนี้จะนำเสนอรายละเอียดของนโยบายและแผนความมั่นคงภายใต้นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2567 – 2570) ซึ่งต่อเนื่องจากวารสารมุมมองความมั่นคงฉบับที่ 12 – 17 ที่ได้นำเสนอไปแล้วบางส่วน โดยในวารสารมุมมองความมั่นคง ฉบับที่ 18 นี้ ขอนำเสนอเกร็ดความรู้เกี่ยวกับ นโยบายและแผนความมั่นคงที่ 9 การป้องกันและบรรเทาสาธารณภัย และนโยบายและแผนความมั่นคงที่ 10 การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

นโยบายและแผนความมั่นคงที่ 9 การป้องกันและบรรเทาสาธารณภัย

1 จุดมุ่งเน้น

การจัดการความเสี่ยงสาธารณภัยที่สำคัญอันเกิดจากภัยธรรมชาติ และภัยที่เกิดจากการกระทำของมนุษย์ และ/หรือ เป็นภัยซ้ำซ้อน ให้สามารถแก้ไขปัญหาที่เกิดขึ้นได้รวดเร็ว ทันต่อเหตุการณ์ และยั่งยืน

2 ความเชื่อมโยงกับยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

2.1 ยุทธศาสตร์ชาติ ด้านความมั่นคง

เป้าหมาย
บ้านเมืองมีความมั่นคงในทุกมิติและทุกระดับ

2.2 แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

แผนย่อยที่ 2 แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

เป้าหมาย ปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (เช่น ปัญหายาเสพติด ความมั่นคงทางไซเบอร์ การค้ามนุษย์ ฯลฯ) ได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ

3 เป้าหมาย ผลสัมฤทธิ์ และตัวชี้วัด

เป้าหมาย การยกระดับการจัดการความเสี่ยงสาธารณภัยที่สำคัญอันเกิดจากภัยธรรมชาติ และภัยที่เกิดจากการกระทำของมนุษย์ที่เกิดขึ้น และ/หรือ เป็นภัยซ้ำซ้อน (Compound Hazards) ไปสู่มาตรฐานตามหลักสากล

ผลสัมฤทธิ์ ประเทศไทยสามารถจัดการความเสี่ยง พร้อมทั้งรับมือและลดผลกระทบจากสาธารณภัยได้อย่างมีประสิทธิภาพ

KPI ตัวชี้วัดที่ 1 อัตราการเสียชีวิตจากภัยธรรมชาติ (อุทกภัย วาตภัย ภัยแล้ง) ต่อประชากร 100,000 คน ลดลงเมื่อเทียบกับค่าเฉลี่ยย้อนหลัง 5 ปี

KPI ตัวชี้วัดที่ 2 จำนวนผู้ได้รับผลกระทบจากภัยธรรมชาติ (อุทกภัย วาตภัย ภัยแล้ง) ต่อประชากร 100,000 คน ลดลงเมื่อเทียบกับค่าเฉลี่ยย้อนหลัง 5 ปี

KPI ตัวชี้วัดที่ 3 อัตราการเสียชีวิตจากภัยที่เกิดจากการกระทำของมนุษย์ (อัคคีภัย) ต่อประชากร 100,000 คน ลดลงเมื่อเทียบกับค่าเฉลี่ยย้อนหลัง 5 ปี

KPI ตัวชี้วัดที่ 4 การแจ้งเตือนสาธารณภัยล่วงหน้าได้ทันสถานการณ์ภายในระยะเวลาที่กำหนด (เฉพาะภัยธรรมชาติ 4 ภัย ได้แก่ อุทกภัย วาตภัย น้ำป่าไหลหลากและดินโคลนถล่ม และสึนามิ) ไม่ต่ำกว่าร้อยละ 98 ของการเกิดภัยดังกล่าวทุกปี

4 กลยุทธ์

4.1 กลยุทธ์หลักที่ 1 การลดความเสี่ยงจากสาธารณภัยให้มีประสิทธิภาพ

กลยุทธ์ย่อยที่ 1.1 พัฒนามาตรการลดความเสี่ยงจากสาธารณภัยที่เกิดขึ้น และป้องกันความเสี่ยงใหม่ให้มีประสิทธิภาพ รวมถึงภัยซ้ำซ้อน โดยเฉพาะอุทกภัย วาตภัย น้ำป่าไหลหลากและดินโคลนถล่ม สึนามิ และอัคคีภัย หรือเหตุอื่นใดซึ่งก่อให้เกิดอันตรายแก่ชีวิต ร่างกาย ของประชาชน หรือความเสียหายแก่ทรัพย์สินของประชาชน หรือของรัฐ อาทิ ภัยจากสารเคมีรั่วไหล และปัญหาน้ำมันรั่วไหลในทะเล

กลยุทธ์ย่อยที่ 1.2 พัฒนาระบบคลังข้อมูลความเสี่ยงสาธารณภัยแห่งชาติให้ทันสมัย มีคุณภาพ และได้มาตรฐาน โดยมีการแบ่งปันข้อมูลระหว่างหน่วยงาน การประสานแลกเปลี่ยน และบูรณาการข้อมูลร่วมกันด้วยเทคโนโลยี เพื่อนำมาวางแผนตัดสินใจเชิงนโยบายและแนวทางปฏิบัติที่เป็นมาตรฐาน รวมถึงการแจ้งเตือนภัย พร้อมทั้งการเข้าถึงและการใช้ประโยชน์ของทุกภาคส่วน

กลยุทธ์ย่อยที่ 1.3 เสริมสร้างความรู้ความเข้าใจ รวมถึงการรับรู้และตระหนักรู้การจัดการความเสี่ยงจากสาธารณภัยที่ถูกต้องให้กับทุกภาคส่วน ทั้งมิติการวิเคราะห์ภัยที่อาจเกิดขึ้นความล่อแหลมในพื้นที่และประเมินสภาพความเปราะบางที่อาจก่อให้เกิดอันตรายทั้งต่อชีวิตและทรัพย์สิน

กลยุทธ์ย่อยที่ 1.4 พัฒนาแนวทางการประเมินความเสี่ยงจากสาธารณภัยในทุกระดับให้สอดคล้องกับมาตรฐานหลักสากล โดยให้ความสำคัญกับการระดมทรัพยากรเข้าพื้นที่ประสบภัย การให้ความช่วยเหลือผู้ประสบภัย การลงทุนในโครงสร้างพื้นฐานและบริการสาธารณะของประเทศ การจัดการพื้นที่ตามระบบผังเมือง ระบบประกันภัย การฝึกป้องกันและบรรเทาสาธารณภัย การอพยพและศูนย์พักพิงชั่วคราว การบริหารความต่อเนื่อง โดยให้องค์การปกครองส่วนท้องถิ่น ภาคเอกชน ภาคประชาสังคม และภาคประชาชนเข้ามามีส่วนร่วมตลอดกระบวนการประเมินความเสี่ยงด้วย

กลยุทธ์ย่อยที่ 1.5 ส่งเสริมและสนับสนุนทรัพยากรและการสร้างแรงจูงใจในการดำเนินการป้องกันและบรรเทาสาธารณภัยของภาคีเครือข่าย ภาคประชาชน อาสาสมัคร และอื่น ๆ

กลยุทธ์ย่อยที่ 1.6 ส่งเสริม พัฒนา ต่อยอดงานวิจัยและองค์ความรู้ โดยประยุกต์ใช้นวัตกรรม เทคโนโลยี ภูมิปัญญาท้องถิ่นทั้งในและต่างประเทศ รวมถึงการจัดตั้งสถาบันด้านการป้องกันและบรรเทาสาธารณภัยของประเทศ เพื่อพัฒนาศักยภาพบุคลากรให้มีความเชี่ยวชาญและความเป็นมืออาชีพให้มีทักษะ ความรู้ และสมรรถนะด้านการจัดการความเสี่ยงสาธารณภัย ตลอดจนยกระดับศักยภาพการจัดการความเสี่ยงจากสาธารณภัยของประเทศ

กลยุทธ์ย่อยที่ 1.7 ส่งเสริมความเป็นหุ้นส่วนระหว่างประเทศในการจัดการความเสี่ยงสาธารณภัยและการประสานความช่วยเหลือด้านมนุษยธรรมให้ครอบคลุมมิติการพัฒนาทางเศรษฐกิจ สังคม สิ่งแวดล้อม และความมั่นคง

4.2 กลยุทธ์หลักที่ 2 การจัดการสาธารณภัยให้มีมาตรฐานตามหลักสากล

กลยุทธ์ย่อยที่ 2.1

เสริมสร้างการจัดการในภาวะฉุกเฉินแบบบูรณาการให้เป็นไปตามมาตรฐานในการปฏิบัติในภาวะฉุกเฉิน โดยเร่งกระบวนการประกาศเขตพื้นที่ประสบสาธารณภัย การใช้ระบบบัญชาการเหตุการณ์ (Incident Command System: ICS) และการใช้วงเงินทดรองราชการเพื่อช่วยเหลือผู้ประสบภัยพิบัติกรณีฉุกเฉินเพื่อบรรเทาความเดือดร้อนเฉพาะหน้าของผู้ประสบภัยพิบัติ

กลยุทธ์ย่อยที่ 2.2

กำหนดแนวทางการปฏิบัติร่วมของศูนย์ปฏิบัติการฉุกเฉิน (Emergency Operation Center: EOC) ให้เป็นระบบมาตรฐานหลักสากล และหลักธรรมาภิบาล เพื่อลดความเสี่ยงจากสาธารณภัย การเตรียมพร้อมรับมือกับสาธารณภัย และการฟื้นฟูบนฐานข้อมูลความเสียหายและความต้องการของประชาชน

กลยุทธ์ย่อยที่ 2.3

พัฒนาระบบการสื่อสารและการแลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานในการจัดการความเสี่ยงสาธารณภัยที่มีแนวโน้มขยายขอบเขตไปสู่การจัดการสาธารณภัยขนาดใหญ่ขึ้นไปให้มีประสิทธิภาพ

กลยุทธ์ย่อยที่ 2.4

พัฒนาระบบการแจ้งเตือนภัยล่วงหน้า (Early Warning) โดยใช้เทคโนโลยีสารสนเทศนวัตกรรม แบบจำลองการวิเคราะห์ข้อมูลจำนวนมาก (Data Analytics and Big Data) ปัญญาประดิษฐ์ (Artificial Intelligence: AI) รวมถึงเสริมสร้างความตระหนักรู้และการตอบสนองต่อการแจ้งเตือนภัยของชุมชนและประชาชน

กลยุทธ์ย่อยที่ 2.5

กำหนดแนวทางการปฏิบัติร่วมของศูนย์ปฏิบัติการฉุกเฉิน (Emergency Operation Center: EOC) ให้เป็นระบบมาตรฐานหลักสากล และหลักธรรมาภิบาล เพื่อลดความเสี่ยงจากสาธารณภัย การเตรียมพร้อมรับมือกับสาธารณภัย และการฟื้นฟูบนฐานข้อมูลความเสียหายและความต้องการของประชาชน

5 หน่วยงานเจ้าภาพรับผิดชอบบูรณาการขับเคลื่อน

กระทรวงมหาดไทย (กรมป้องกันและบรรเทาสาธารณภัย)

6 การถ่ายทอดและขับเคลื่อนนโยบายและแผนความมั่นคงที่ 9 ไปสู่การปฏิบัติ

6.1 การจัดทำแผนการป้องกันและบรรเทาสาธารณภัยแห่งชาติ พ.ศ. 2564 – 2570

เมื่อวันที่ 5 กรกฎาคม 2565 คณะรัฐมนตรีมีมติอนุมัติแผนการป้องกันและบรรเทาสาธารณภัยแห่งชาติ พ.ศ. 2564 – 2570 เพื่อให้กระทรวง กรม องค์กร หน่วยงานของภาครัฐ รัฐวิสาหกิจ จังหวัด อำเภอ องค์กรปกครองส่วนท้องถิ่น ภาคเอกชน และภาคส่วนต่าง ๆ ดำเนินการขับเคลื่อนแผนไปสู่การปฏิบัติ เพื่อจัดการความเสี่ยงจากสาธารณภัยของประเทศอย่างมีประสิทธิภาพ ภายใต้ยุทธศาสตร์สำคัญ คือ การจัดการความเสี่ยงจากสาธารณภัย ซึ่งประกอบด้วย ส่วนแรก การลดความเสี่ยงจากสาธารณภัยให้มีประสิทธิภาพ และส่วนที่สอง การจัดการสาธารณภัยให้มีมาตรฐาน โดยมีเป้าหมายสำคัญเพื่อให้ประเทศมีมาตรฐานในการจัดการ และพร้อมรับสถานการณ์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยที่ประชาชนมีองค์ความรู้ ภูมิคุ้มกัน รู้เท่าทันภัย เพื่อมุ่งสู่ “การรู้ รับ – ปรับตัว – ฟื้นตัวเร็ว – อย่างยั่งยืน” (Resilience) โดยกำหนด 5 ยุทธศาสตร์รองรับ ประกอบด้วย ยุทธศาสตร์การมุ่งเน้นการลดความเสี่ยงจากสาธารณภัย ยุทธศาสตร์การเพิ่มประสิทธิภาพระบบบริหารจัดการและประยุกต์ใช้นวัตกรรมด้านสาธารณภัย ยุทธศาสตร์การส่งเสริมความเป็นหุ้นส่วนระหว่างประเทศในการจัดการความเสี่ยงจากสาธารณภัย และยุทธศาสตร์การจัดการในภาวะฉุกเฉินแบบบูรณาการ และยุทธศาสตร์การเพิ่มประสิทธิภาพการฟื้นฟูอย่างยั่งยืน (รายละเอียดที่ แผนการป้องกันและบรรเทาสาธารณภัยแห่งชาติ พ.ศ. 2564 – 2570 www.disaster.go.th)

6.2
การฝึกซ้อมการบริหารวิกฤตการณ์ระดับชาติ (Crisis Management Exercise: C-MEX)

ตั้งแต่ปี พ.ศ. 2550 สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ร่วมกับ กระทรวงมหาดไทย (กรมป้องกันและบรรเทาสาธารณภัย) กระทรวงกลาโหม (ศูนย์บรรเทาสาธารณภัยกระทรวงกลาโหมและเหล่าทัพ) กระทรวงสาธารณสุข ได้จัดการฝึกการบริหารวิกฤตการณ์ระดับชาติ (C-MEX 07) และมีการพัฒนาโจทย์การฝึกอย่างต่อเนื่องเพื่อเตรียมความพร้อมในการเผชิญกับสาธารณภัย (พ.ศ. 2566 – 2570) ซึ่งเป็นนโยบายฉบับปัจจุบันได้กำหนดให้มีนโยบายและแผนความมั่นคงที่ 14 เรื่องการพัฒนาศักยภาพการเตรียมพร้อมแห่งชาติ และการบริหารจัดการวิกฤตการณ์ระดับชาติ โดยมุ่งเน้นการพัฒนาศักยภาพการเตรียมพร้อมเพื่อป้องกันและตอบสนองต่อภัยคุกคาม รวมทั้งการบูรณาการทรัพยากรของประเทศเพื่อใช้ในการเผชิญกับวิกฤตการณ์ระดับชาติ ดังนั้น การจัดการฝึกการบริหารวิกฤตการณ์ทั้งในระดับชาติ ระดับหน่วยงาน และระดับท้องถิ่นเป็นประจำและต่อเนื่อง นับได้ว่าเป็นกลยุทธ์หนึ่งในการทดสอบประสิทธิภาพและเป็นการเตรียมความพร้อมของหน่วยงาน โดยเฉพาะระบบบัญชาการเหตุการณ์ ระบบบัญชีทรัพยากรของหน่วยงานของรัฐและภาคส่วนต่าง ๆ เพื่อให้สามารถเผชิญกับภัยคุกคามได้ในแต่ละประเภทภัยหรือลักษณะของภัยที่เกิดขึ้น

นโยบายและแผนความมั่นคงที่ 10 การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมาย “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ในขณะที่ “ไซเบอร์” หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป โดยการดำเนินงานของสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) กำหนดนโยบายและแผนความมั่นคงที่ 10 การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ เป็นประเด็นหนึ่งภายใต้นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ และได้นำเสนอเป็นบทความเกี่ยวกับมุมมองความมั่นคงทางไซเบอร์จากการเข้าร่วมประชุมสัมมนาและศึกษาค้นคว้าเพื่อถ่ายทอดในวารสารมุมมองความมั่นคงในฉบับก่อนหน้านี้ โดยนโยบายและแผนความมั่นคงที่ 10 มีสาระสำคัญ ดังนี้

1 จุดมุ่งเน้น

ประเทศไทยสามารถเพิ่มประสิทธิภาพการป้องกันการโจมตีทางไซเบอร์ การยกระดับมาตรฐานรักษาความมั่นคงปลอดภัยไซเบอร์ และลดการก่ออาชญากรรมทางไซเบอร์

2 ความเชื่อมโยงกับยุทธศาสตร์ชาติ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

2.1 ยุทธศาสตร์ชาติ ด้านความมั่นคง

เป้าหมาย
บ้านเมืองมีความมั่นคงในทุกมิติและทุกระดับ

2.2 แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

แผนย่อยที่ 2 แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

เป้าหมาย ปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (เช่น ปัญหายาเสพติด ความมั่นคงทางไซเบอร์ การค้ามนุษย์ ฯลฯ) ได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ

3 เป้าหมาย ผลสัมฤทธิ์ และตัวชี้วัด

เป้าหมาย ประเทศไทยมีความพร้อมต่อการป้องกัน รับมือความเสี่ยงกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ ทั้งการป้องกันการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์

ผลสัมฤทธิ์ หน่วยงานระดับชาติ กลุ่มภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระดับหน่วยงานมีความพร้อมและมาตรการและแนวทางปฏิบัติในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เท่าทันเหตุการณ์สอดคล้องกับมาตรฐานสากล รวมถึงมีกลไกและแนวทางในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ และการพัฒนาการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์

KPI ตัวชี้วัดที่ 1 การพัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องมาตรฐานสากล เพิ่มขึ้นร้อยละ 90 ภายในปี 2570

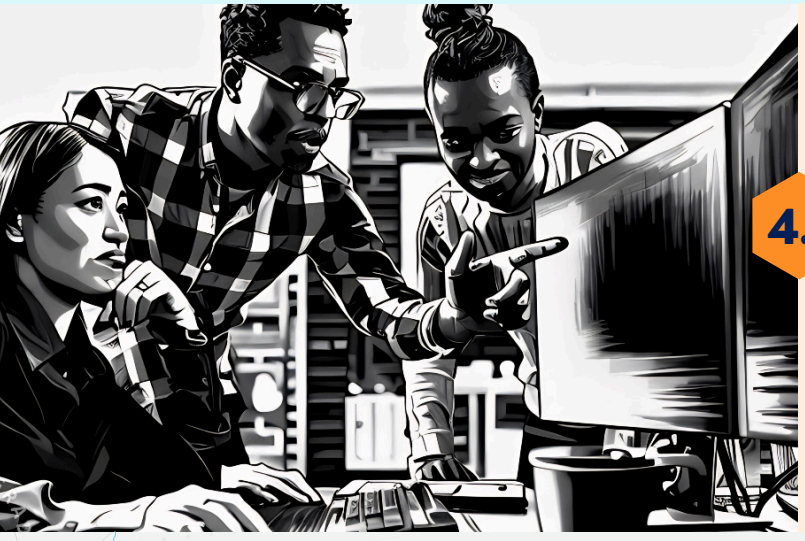
KPI ตัวชี้วัดที่ 2 การแก้ไขเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีประสิทธิภาพ เพิ่มขึ้นร้อยละ 90 ภายในปี 2570

KPI ตัวชี้วัดที่ 3

การจัดทำหรือพัฒนากลไก มาตรการ และแนวทางในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ รวมถึงการพัฒนาการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ เพิ่มขึ้นร้อยละ 60 ภายในปี 2570

KPI ตัวชี้วัดที่ 4

สถิติคดีเกี่ยวกับอาชญากรรมทางไซเบอร์ลดลงร้อยละ 30 เมื่อเทียบกับปีก่อนหน้า



4 กลยุทธ์

4.1 กลยุทธ์หลักที่ 1 การป้องกัน รับมือ และลดความเสี่ยงกับภัยคุกคามทางไซเบอร์ที่กระทบต่อระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ย่อยที่ 1.1

เสริมสร้างศักยภาพของกลไกและหน่วยงานระดับชาติ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team: NCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) โดยมีการเชื่อมโยงการทำงานระหว่างกันอย่างเป็นระบบ เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ และแก้ไขเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

กลยุทธ์ย่อยที่ 1.2

ส่งเสริมให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรฐานและแนวทางปฏิบัติในการป้องกัน รับมือ ลดความเสี่ยง รักษา และฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ที่เท่าทันต่อเหตุการณ์ที่สอดคล้องกับมาตรฐานสากล

กลยุทธ์ย่อยที่ 1.3

บูรณาการความร่วมมือภายในประเทศระหว่างหน่วยงานภาครัฐ ทั้งฝ่ายทหาร พลเรือน ตำรวจ ภาคเอกชน และภาคส่วนที่เกี่ยวข้องให้เป็นเครือข่ายความร่วมมือที่เข้มแข็ง ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงสงครามไซเบอร์

กลยุทธ์ย่อยที่ 1.4

ส่งเสริมความร่วมมือระหว่างประเทศในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับทวิภาคีและพหุภาคี โดยแลกเปลี่ยนข้อมูลข่าวสาร ข่าวกรอง และความรู้ที่ทันต่อเหตุการณ์และเสริมสร้างความสัมพันธ์ที่ดีในทุกระดับ เพื่อให้สามารถป้องกัน ลดความเสี่ยง รวมถึงรับมือกับภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้อย่างทันท่วงที

กลยุทธ์ย่อยที่ 1.5

ส่งเสริมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้อง พร้อมทั้งพัฒนาทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่ เจ้าหน้าที่ หรือบุคลากรของทุกภาคส่วนที่เกี่ยวข้อง

กลยุทธ์ย่อยที่ 1.6

ส่งเสริมการเผยแพร่ความรู้เพื่อสร้างความตระหนักถึงความสำคัญของภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แก่องค์กรและบุคลากรภาครัฐ ภาคเอกชน และภาคประชาสังคมที่เกี่ยวข้อง

4.2 กลยุทธ์หลักที่ 2 การเสริมสร้างขีดความสามารถในการป้องกันและแก้ไขปัญหาการใช้ไซเบอร์เป็นช่องทางในการก่ออาชญากรรมทางไซเบอร์

กลยุทธ์ย่อยที่ 2.1

พัฒนากลไก มาตรการ และแนวทางที่เกี่ยวข้องกับการป้องกันและปราบปรามที่ครอบคลุมถึงการพัฒนาการเฝ้าระวังความเสี่ยงในการก่ออาชญากรรมทางไซเบอร์ การแจ้งเตือนเพื่อลดความเสี่ยงการก่ออาชญากรรมทางไซเบอร์ รวมถึงการติดตาม วิเคราะห์และการประมวลผลข้อมูล ตลอดจนพัฒนาการสืบสวนอาชญากรรมทางไซเบอร์ด้วยการนำเทคโนโลยีมาใช้ประโยชน์

กลยุทธ์ย่อยที่ 2.2

ส่งเสริมความร่วมมือหรือให้ความช่วยเหลือระหว่างหน่วยงาน ทั้งภายในประเทศและต่างประเทศ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากการก่ออาชญากรรมทางไซเบอร์ร่วมกัน

กลยุทธ์ย่อยที่ 2.2

เสริมสร้างความตระหนักรู้และพัฒนาขีดความสามารถแก่องค์กรและบุคลากรภาครัฐ ภาคเอกชน และภาคประชาสังคมที่เกี่ยวข้องให้มีความรู้ในการป้องกันตนเองจากอาชญากรรมทางไซเบอร์

5 หน่วยงานเจ้าภาพรับผิดชอบบูรณาการขับเคลื่อน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

6 การถ่ายทอดและขับเคลื่อนนโยบายและแผนความมั่นคงที่ 10 ไปสู่การปฏิบัติ

6.1

การมีกฎหมายและนโยบายที่เกี่ยวข้อง อาทิ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีการตอบสนองภัยทางไซเบอร์ 3 ระดับ คือ ระดับความไม่ร้ายแรง ระดับร้ายแรง และระดับวิกฤต นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งการพัฒนาบุคลากร การสร้างการตระหนักรู้ การลดความเสี่ยง การพัฒนาทักษะ การศึกษาวิจัย การบูรณาการความร่วมมือเพื่อเตรียมความพร้อมการรับมือและสามารถฟื้นคืนสู่สภาพปกติ (Resilience) โดยเฉพาะโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) การแต่งตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team (National-CERT)) ตลอดจนมีประกาศ กมช. เรื่องมาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566 เพื่อรับมือกับภัยคุกคามทางไซเบอร์

6.2

การเสริมสร้างความรู้ความเข้าใจและการตระหนักรู้ให้แก่บุคลากรทางด้านไซเบอร์ของหน่วยงานกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งการอบรมระยะสั้น และเร่งรัดพัฒนาผู้เชี่ยวชาญด้าน Cybersecurity การประสานความร่วมมือกับหน่วยงาน องค์กร ทั้งในและต่างประเทศ การฝึก Thailand’s National Cyber Exercise

6.3

ความร่วมมือกับสหภาพยุโรปภายใต้ ESIWA Project (Enhancing Security Cooperation in and with Asia) ได้ให้ความสำคัญกับประเด็นความมั่นคงทางไซเบอร์ โดยความร่วมมือที่ผ่านมาเมื่อวันที่ 24 ตุลาคม 2566 สมช. ร่วมกับ ESIWA Project จัดการสัมมนา Sharing Good Practices to Respond of Cybercrime เพื่อถ่ายทอดความรู้และประสบการณ์เกี่ยวกับกฎหมายระหว่างประเทศและกฎหมายประเทศไทย ความรู้และทักษะที่จำเป็นในการปฏิบัติงาน การเสริมสร้างความร่วมมือโดยการแลกเปลี่ยนการปฏิบัติที่ดี (Best Practice) ซึ่งในระยะต่อไปจะได้พัฒนาและกระชับความร่วมมือในเรื่องดังกล่าวต่อไป