บทสรุปสำหรับผู้บริหาร
ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ได้มีการกำหนดวิสัยทัศน์การวิจัยไว้ว่า “การวิจัยและพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเพิ่มขีดความสามารถของประเทศ” ซึ่งมีพันธกิจการวิจัย ประกอบด้วย ๑) ส่งเสริมและสนับสนุนการวิจัยและพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเพิ่มขีดความสามารถของประเทศในการป้องกันและรับมือภัยคุกคามด้านไซเบอร์ทุกรูปแบบอย่างมีประสิทธิภาพ ๒) ส่งเสริมและสนับสนุนการวิจัยพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ตอบสนองความต้องการของผู้ใช้ทั้งภาครัฐและภาคเอกชนอย่างแท้จริงและลดการพึ่งพาเทคโนโลยีจากต่างประเทศ ๓) ส่งเสริมและพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งส่งเสริมและพัฒนาความร่วมมือด้านการวิจัยของนักวิจัยไทยและต่างประเทศ ๔) สนับสนุนให้มีการพัฒนายกระดับหน่วยงานที่รับผิดชอบในปัจจุบันไปสู่การเป็นศูนย์แห่งความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์ในเขตภูมิภาคเอเชียตะวันออกเฉียงใต้ ๕) ศึกษารวบรวมปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันและอนาคต รวมทั้งศึกษาความเป็นไปได้ในการแก้ไขปัญหาในรูปแบบของการวิจัยและพัฒนา และ ๖) จัดทำกรอบงบประมาณ ๕ ปี ของงานวิจัยและพัฒนาทั้งหมดที่อยู่ภายใต้แผนยุทธศาสตร์การวิจัย ดังกล่าว

ยุทธศาสตร์การวิจัย ประกอบด้วย ๑) การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านความมั่นคง และภาคบริการประชาชน ๒) การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านการเงิน การธนาคาร และพาณิชย์อิเล็กทรอนิกส์ ๓) การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานด้านสาธารณูปโภคพื้นฐาน ๔) การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานด้านการสื่อสารและโทรคมนาคม และ ๕) การวิจัยและพัฒนาการรักษาความมั่งคงปลอดภัยไซเบอร์สำหรับข้อมูลส่วนบุคคล เครือข่ายสังคมออนไลน์ และการป้องกันอาชญากรรมไซเบอร์ที่ส่งผลกระทบต่อบุคคล เศรษฐกิจ อุตสาหกรรมโดยรวม

เป้าประสงค์ของยุทธศาสตร์การวิจัย ประกอบด้วย ๑) มีแผนยุทธศาสตร์การวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีทิศทางที่ชัดเจน และครอบคลุมทุกประเด็นที่มีความสำคัญและมีความเร่งด่วนต่อการพัฒนาประเทศไทย ๒) มีการปรับปรุงกฎหมายให้ทันสมัย และมีข้อเสนอแนะเชิงนโยบายในการพัฒนายกระดับองค์กร/หน่วยงานที่รับผิดชอบในปัจจุบันให้เป็นศูนย์ความเป็นเลิศทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ประเทศไทยเป็นศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์ของภูมิภาคเอเชียตะวันออกเฉียงใต้ ๓) เกิดการบูรณาการในการทำวิจัยและพัฒนาร่วมกันระหว่างภาครัฐและภาคเอกชนทั้งในและต่างประเทศ เพื่อพัฒนาองค์ความรู้และนวัตกรรมใหม่อย่างจริงจังในการแก้ปัญหาทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันและอนาคต และ ๔) หน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชนสามารถนำองค์ความรู้และนวัตกรรมที่ได้ไปใช้งานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เกิดประโยชน์ได้จริง รวมทั้งลดการนำเข้าเทคโนโลยีทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีราคาแพงจากต่างประเทศในระยะยาว

ปัจจัยแห่งความสำเร็จของยุทธศาสตร์การวิจัย ประกอบด้วย ๑) มีมาตรการที่จะพัฒนาองค์ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในด้านต่างๆ ๒) ภาครัฐมีนโยบายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต่อเนื่องในปัจจัยในแต่ละด้าน และ ๓) ทุกหน่วยงานที่เกี่ยวข้องได้รับการจัดสรรงบประมาณเพื่อใช้ในการวิจัย พัฒนา สาธิต ส่งเสริม รณรงค์ เผยแพร่ และประชาสัมพันธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายใต้กรอบการดำเนินงานของแผน

ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. หลักการและเหตุผล

๑.๑ ความเป็นมาของงานวิจัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

จากผลการสำรวจของสำนักงานสถิติแห่งชาติ พบว่าในปี ๒๕๕๔ ประเทศไทยมีผู้ใช้อินเทอร์เน็ตที่มีอายุ ๖ ปีขึ้นไป จำนวน ๑๔.๘ ล้านคน หรือคิดเป็นร้อยละ ๒๓.๗ ของประชากรในประเทศ[๑] และจากจำนวนผู้ใช้อินเทอร์เน็ตทั้งในประเทศและต่างประเทศที่มีจำนวนมากจะมีกลุ่มบุคคลที่เรียกว่า “อาชญากรไซเบอร์” ที่แฝงตัวเข้ามาใช้เพื่อเจาะข้อมูล เปลี่ยนแปลงข้อมูล ทำลายข้อมูล หรือใช้พื้นที่บนโลกไซเบอร์เพื่อแสวงหาผลประโยชน์อย่างผิดกฎหมาย บริษัทไซแมนเทคเปิดเผยผลสำรวจเกี่ยวกับความเสียหายจากอาชญากรรมออนไลน์ที่เกิดขึ้นทั่วโลกในปี ๒๕๕๓ ว่ามีมูลค่าเฉลี่ย ๓.๘๘ แสนล้านดอลล่าร์สหรัฐ โดยแบ่งเป็นความสูญเสียทางการเงิน ๑.๑๔ แสนล้านดอลล่าร์สหรัฐ และค่าเสียเวลาของผู้เสียหาย ๒.๗๔ แสนล้านดอลล่าร์สหรัฐ[๒] และเปิดเผยว่าในปี ๒๕๕๔ อาชญากรทางไซเบอร์ส่งผลให้เกิดการขยายตัวของจำนวนการโจมตีทางอินเทอร์เน็ตเพิ่มสูงขึ้นถึงร้อยละ ๘๑[๓] โดยองค์กรขนาดใหญ่ที่มีพนักงานมากกว่า ๒,๕๐๐ คน จะถูกโจมตีมากที่สุด มีการตรวจพบการโจมตีและการป้องกันเฉลี่ย ๓๖.๗ ครั้งต่อวัน[๔] ทั้งนี้ธุรกิจอาชญากรรมบนโลกไซเบอร์ทั่วโลกคิดเป็นมูลค่าประมาณ ๑ ล้านล้านเหรียญสหรัฐ หรือประมาณ ๓๐ ล้านล้านบาท และภูมิภาคเอเชีย คือ ศูนย์กลางของอุตสาหกรรมดังกล่าว[๕]

๑.๒ วิเคราะห์สถานการณ์ปัจจุบันและแนวโน้มการเปลี่ยนแปลงเกี่ยวกับประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สถานการณ์ในปัจจุบันและแนวโน้มการเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวกับประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่าในช่วงหลายปีที่ผ่านมา รัฐบาลตระหนักและให้ความสำคัญกับการป้องกันและแก้ไขปัญหาไซเบอร์อย่างจริงจัง เนื่องจากความแพร่หลายของการให้และใช้บริการข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต และโครงข่ายสื่อสารโทรคมนาคม ฯลฯ ที่ครอบคลุมเกือบทุกพื้นที่ทั้งภายในประเทศและทั่วโลก ซึ่งการเชื่อมโยงถึงกันดังกล่าว หากพิจารณาจากมุมมองของผู้ที่ปฏิบัติหน้าที่รักษาความมั่นคงปลอดภัยของประเทศ ก็อาจถือเป็นปัจจัยเชิงลบที่คุกคามและส่งผลกระทบอย่างรวดเร็วและรุนแรงต่อประชาชน เศรษฐกิจ และความมั่นคงของประเทศ หากภาครัฐและหน่วยงานที่เกี่ยวข้องยังขาดความพร้อมและไม่มีมาตรการป้องกันแก้ไขที่ชัดเจนและมีประสิทธิภาพเพียงพอแล้ว ความเสียหายที่เกิดขึ้นต่อทุกภาคส่วนของสังคมนั้นก็จะมีมูลค่ามหาศาลและยากที่จะประเมินได้

อย่างไรก็ดี ด้านทิศทางของการวิจัยและพัฒนาเพื่อสนับสนุนการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมายังไม่ตอบสนองต่อความสำคัญดังกล่าว ดังนั้น การกำหนดยุทธศาสตร์

---

[๑] สรุปผลที่สำคัญจากการสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. ๒๕๕๔ (ICT Household 2011) , สำนักงานสถิติแห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

[๒] Cybercrime Report 2011, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads /en-us/NCR-DataSheet.pdf

[๓] ข่าว “เผยรายงานภัยคุกคามบนอินเทอร์เน็ตการโจมตีเพิ่มขึ้นร้อยละ ๘๑”, GLOBAL BUSINESS ประจำวันที่ ๕-๑๙ มิถุนายน พ.ศ. ๒๕๕๕

[๔] Symantec Intelligence Report: November 2011, http://www.symantec.com/connect/sites/default/files/SYMCINT _2011_11_ November_ FINAL-en.pdf

[๕] คอลัมน์ “ความปลอดภัยบนโลกอินเทอร์เน็ต”, นิตยสาร Asia Pacific Defense FORUM, ชุดที่ ๓๗ ฉบับที่ ๑/๒๕๕๕

การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะต้องมีความครอบคลุม ชัดเจน และมองเป็นภาพรวมเชิงบูรณาการกับทุกภาคส่วนที่เกี่ยวข้อง

๑.๓ ผลงานวิจัยที่เคยมีมาแล้วในอดีต ช่องว่างการวิจัย และประเด็นที่สำคัญของการวิจัยที่เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นที่ต้องการของประเทศ

จากผลการศึกษาปัญหาอาชญากรรมไซเบอร์รูปแบบต่างๆ ได้แผ่ขยายไปทั่วโลกพบว่าเกิดผลกระทบต่อบุคคล องค์กร และประเทศ ทั้งในมิติเศรษฐกิจ สังคม และความมั่นคงของชาติ ยกตัวอย่างเช่น ประเทศสหรัฐอเมริกาพบปัญหาการค้าภาพลามกอนาจารบนอินเทอร์เน็ต และปัญหาการล่อลวงเด็กและเยาวชนผ่านการสื่อสารทางอินเทอร์เน็ต รวมถึงปัญหาการโจรกรรมข้อมูลบัตรเครดิต เช่น บัตรวีซ่าและมาสเตอร์การ์ดของลูกค้าในประเทศสหรัฐอเมริกากว่า ๑๐ ล้านราย[๖] ในทวีปเอเชีย มีการพบปัญหาการก่อกวนระบบเครือข่ายตลาดหลักทรัพย์ฮ่องกง จนทำให้เกิดผลกระทบอย่างมหาศาลต่อระบบการเงิน บุคคล และบริษัทหลายร้อยราย เนื่องจากการซื้อขายหุ้นในตลาดหลักทรัพย์ฮ่องกงหยุดชะงัก[๗] ในขณะที่ประเทศญี่ปุ่นเกิดกรณีแฮ็กเกอร์โจมตีเว็บไซต์ของกระทรวงการคลัง ศาลฎีกา และศาลทรัพย์สินทางปัญญา โดยมีจุดประสงค์เพื่อต่อต้านการออกกฎหมายป้องกันการดาวน์โหลดสินค้าลิขสิทธิ์ ส่งผลให้เว็บไซต์ดังกล่าวต้องปิดตัวลงชั่วคราว[๘]

สำหรับสถานการณ์ภัยคุกคามไซเบอร์ในประเทศไทย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team : ThaiCERT) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รวบรวมและเผยแพร่ข้อมูลสถิติภัยคุกคามที่ได้รับแจ้ง โดยแบ่งเป็นภัยคุกคาม ๘ ประเภท[๙] ดังแผนภาพต่อไปนี้

---

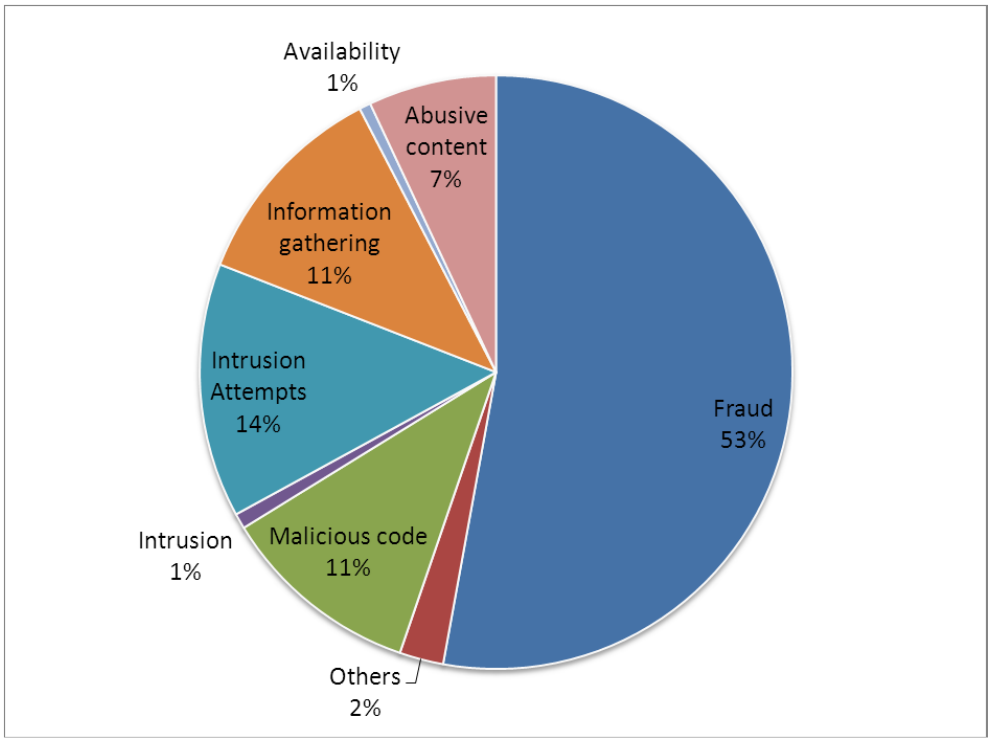
[๖] ข่าว “ฉกข้อมูลลูกค้าบัตรเครดิตวีซ่ามาสเตอร์การ์ดกว่า ๑๐ ล้านราย”, http://www.dailynews.co.th ประจำวันที่ ๑๐ เมษายน ๒๕๕๕

[๗] ข่าว “โคเรโร เน็ตเวิร์ค ซีเคียวริตี้รายงานเกี่ยวกับ ๕ อันดับแรก ที่ถูกจู่โจมระบบเครือข่ายหรือเซิร์ฟเวอร์มากที่สุด ในปี ๒๕๕๔ มีการโจมตีระบบเครือข่ายหรือเซิร์ฟเวอร์รูปแบบใหม่ๆ ที่เก่งกาจมากขึ้นในชั้นบนสุดของกระบวนการรับส่งข้อมูล”, http://www.thairath.co.th ประจำวันที่ ๑๕ กรกฎาคม ๒๕๕๕.

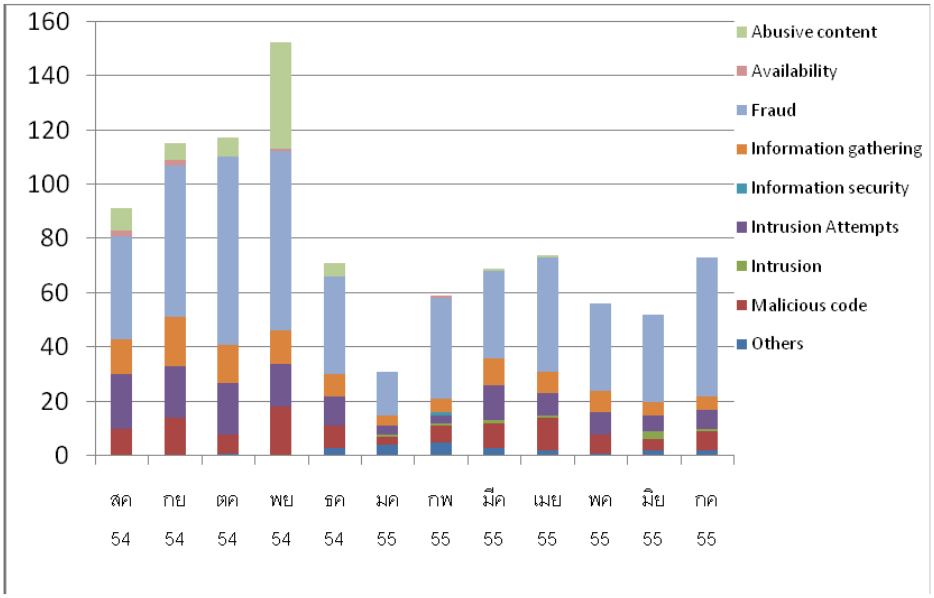
[๘] ข่าว**“จับแก๊งค้าข้อมูลเครดิตข้ามชาติเอฟบีไอโวป้องกันความเสียหายได้กว่า ๖ พันล้าน”**, หนังสือพิมพ์คมชัดลึก ฉบับวันที่ ๒๘ มิถุนายน ๒๕๕๕.

[๙] อ้างอิงตาม http://www.ecsirt.net/cec/service/documents/wp๔-clearinghouse-policy-v๑๒.html#HEAD๖

แผนภาพที่ ๑ สถิติภัยคุกคามที่ ThaiCERT ได้รับแจ้งในช่วงสิงหาคม ๒๕๕๔-กรกฎาคม ๒๕๕๕ (จำแนกตามประเภท)[๑๐]



แผนภาพที่ ๒ สถิติภัยคุกคามที่ ThaiCERT ได้รับแจ้งในช่วงสิงหาคม ๒๕๕๔-กรกฎาคม ๒๕๕๕ (จำนวนครั้ง)[๑๑]



[๑๐] อ้างอิงตาม http://www.thaicert.or.th/statistics.html

[๑๑] อ้างอิงตาม http://www.thaicert.or.th/statistics.html

แผนภาพข้างต้นแสดงให้เห็นว่า ประเทศไทยประสบปัญหาอาชญากรรมไซเบอร์หลากหลายรูปแบบ ซึ่งสถิติภัยคุกคามที่ ThaiCERT รับแจ้งแยกตามประเภทภัยคุกคาม ตั้งแต่เดือนสิงหาคม ๒๕๕๔-กรกฎาคม ๒๕๕๕ พบว่า การฉ้อฉลหลอกลวงเพื่อผลประโยชน์ (Fraud) ยังเป็นภัยคุกคามที่ได้รับแจ้งมากที่สุด ตามมาด้วยการพยายามบุกรุกเข้าระบบ (Intrusion Attempts) ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) โปรแกรมไม่พึงประสงค์ (Malicious Code) และเนื้อหาที่เป็นภัยคุกคาม (Abusive Content) ตามลำดับ ซึ่งประเภทของภัยคุกคามดังกล่าวเป็นสิ่งที่สมควรนำไปกำหนดประเด็นการวิจัยเพื่อให้ได้ข้อค้นพบเกี่ยวกับข้อเสนอแนะในระดับนโยบาย และระดับปฏิบัติสำหรับการป้องกันและแก้ไขปัญหาต่อไป

ดังนั้น จึงมีความจำเป็นเร่งด่วนที่จะต้องจัดทำแผนยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีองค์ประกอบสำคัญที่จะนำไปสู่การวางแนวทางและจัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติอย่างเป็นรูปธรรม เพื่อสร้างเสถียรภาพในการติดต่อสื่อสารและการทำธุรกรรมที่เกี่ยวข้องกับด้านไซเบอร์ทั้งในระดับบุคคลและองค์กรทั้งภาครัฐและภาคเอกชน อันจะนำไปสู่การรักษาผลประโยชน์ทางด้านเศรษฐกิจ ความปลอดภัยของสังคม และความมั่นคงของประเทศไทยทั้งในปัจจุบันและอนาคตอย่างยั่งยืน

๑.๔ ผู้มีส่วนได้ส่วนเสียและจุดแข็งจุดอ่อนในประเด็นการพัฒนาและการวิจัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นที่ต้องการของประเทศ

ปัญหาอาชญากรรมไซเบอร์ที่เกิดขึ้นในปัจจุบันมีผู้มีส่วนได้ส่วนเสียโดยตรง คือ ผู้ใช้บริการหน่วยงานของรัฐและเอกชน ที่จำเป็นต้องใช้ระบบเทคโนโลยีสารสนเทศ ซึ่งยังมีจุดอ่อนที่ยังไม่มีมาตรการที่จะพัฒนาองค์ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๕ นโยบายและยุทธศาสตร์ซึ่งเป็นที่มาของยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นที่ต้องการของประเทศ

การจัดทำนโยบายและยุทธศาสตร์การวิจัยของชาติ ฉบับที่ ๘ (พ.ศ. ๒๕๕๕-๒๕๕๙) โดยสำนักงานคณะกรรมการวิจัยแห่งชาติ (วช.) ได้ตระหนักถึงความสำคัญของการบูรณาการด้านการวิจัยให้สอดคล้องกับแนวนโยบายและยุทธศาสตร์การพัฒนาประเทศ ควบคู่กับการวิจัยเพื่อความเป็นเลิศทางวิชาการเป็นหลัก เพื่อการนำไปใช้ให้เกิดผลทั้งการแก้ไขปัญหาและการพัฒนาประเทศอย่างสมดุลและยั่งยืน โดยให้ทุกภาคส่วนเข้ามามีส่วนร่วมในการวิจัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) ถือเป็นแนวทางการพัฒนาประเทศที่สำคัญทางด้านการพัฒนาวิทยาศาสตร์และเทคโนโลยี วช. จึงได้นำเนื้อหาสำคัญของพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยได้กำหนดยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้สนับสนุนและแก้ปัญหาการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยไซเบอร์ ผลการวิจัยเพื่อนำมาประยุกต์ใช้กับภาคส่วนต่างๆ ของประเทศ อาทิ ภาครัฐ ภาคเอกชน และภาคประชาชน ฯลฯ สำหรับยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ วช. ได้ยึดเนื้อหาของแนวนโยบายและยุทธศาสตร์การพัฒนาประเทศที่สำคัญเพื่อความสอดคล้องกับทิศทางการพัฒนาประเทศที่เป็นปัจจุบัน คือ ยุทธศาสตร์ประเทศ (Country Strategy) แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๑ (พ.ศ. ๒๕๕๕-๒๕๕๙) นโยบายรัฐบาล (นางสาวยิ่งลักษณ์ ชินวัตร นายกรัฐมนตรี) และยุทธศาสตร์การจัดสรรงบประมาณรายจ่ายประจำปี ๒๕๕๕-๒๕๕๗

๒. วิสัยทัศน์การวิจัย

การวิจัยและพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเพิ่มขีดความสามารถของประเทศ

๓. พันธกิจการวิจัย

๓.๑ ส่งเสริมและสนับสนุนการวิจัยและพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเพิ่มขีดความสามารถของประเทศในการป้องกันและรับมือภัยคุกคามด้านไซเบอร์ทุกรูปแบบอย่างมีประสิทธิภาพ ซึ่งรวมถึงด้านสงครามไซเบอร์ (Cyber Warfare) ทั้งในเชิงรุกและเชิงรับ และการกู้คืนข้อมูล ระบบ/เครือข่ายเมื่อเกิดภัยพิบัติต่างๆ

๓.๒ ส่งเสริมและสนับสนุนการวิจัยพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ตอบสนองความต้องการของผู้ใช้ทั้งภาครัฐและภาคเอกชนอย่างแท้จริง และลดการพึ่งพาเทคโนโลยีจากต่างประเทศ

๓.๓ ส่งเสริมและพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งด้านปริมาณและคุณภาพเพื่อสร้างบุคลากรประกอบอาชีพด้านความมั่นคงปลอดภัยไซเบอร์ และเป็นคลังสมองที่สำคัญของประเทศ รวมทั้งส่งเสริมและพัฒนาความร่วมมือทางด้านการวิจัยระหว่างนักวิจัยของไทยและต่างประเทศ

๓.๔ สนับสนุนให้มีการพัฒนายกระดับหน่วยงานที่รับผิดชอบในปัจจุบันไปสู่การเป็นศูนย์แห่งความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์ในเขตภูมิภาคเอเชียตะวันออกเฉียงใต้

๓.๕ ศึกษารวบรวมปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันและอนาคตจากหน่วยงานต่างๆ ทั้งภาครัฐ และภาคเอกชน รวมทั้งศึกษาความเป็นไปได้ในการแก้ไขปัญหาเหล่านั้นในรูปแบบของการวิจัยและพัฒนา

๓.๖ จัดทำกรอบงบประมาณ ๕ ปี ของงานวิจัยและพัฒนาทั้งหมดที่อยู่ภายใต้แผนยุทธศาสตร์ฯ ดังกล่าว

๔. ยุทธศาสตร์/กลยุทธ์การวิจัย

ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย ๕ ยุทธศาสตร์ โดยคำนึงถึงความเหมาะสมและสอดคล้องกับความต้องการของกลุ่มผู้ใช้งาน (Cluster) ซึ่งเผชิญปัญหาและภัยคุกคามทางด้านความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกัน อีกทั้งเป็นการจัดกลุ่มยุทธศาสตร์ตามแนวทางที่สอดคล้องกับแผนแม่บทความมั่นคงปลอดภัยระบบสารสนเทศ (Information and Communications Technology Security : ICT Security) แห่งชาติ ฉบับที่ ๑ ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร อีกด้วย

ยุทธศาสตร์ที่ ๑ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานด้านความมั่นคง และภาคบริการประชาชน เช่น กองทัพ สำนักงานตำรวจแห่งชาติ ศาล กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) หน่วยงานให้บริการด้านสาธารณสุข หน่วยงานราชการ และหน่วยงานของรัฐอื่นๆ

ยุทธศาสตร์ที่ ๒ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานด้านการเงิน การธนาคาร และพาณิชย์อิเล็กทรอนิกส์ เช่น ธนาคาร บริษัทหลักทรัพย์ ประกันภัย ตลาดหลักทรัพย์ ผู้ให้บริการด้านบัตรเครดิต และหน่วยงานภาครัฐที่เกี่ยวข้องกับการกำกับตรวจสอบสถาบันการเงิน เป็นต้น

ยุทธศาสตร์ที่ ๓ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านสาธารณูปโภคพื้นฐาน เช่น การไฟฟ้า การประปา หน่วยงานด้านพลังงาน หน่วยงานด้านการคมนาคม/ขนส่ง และธุรกิจด้านสายการบิน เป็นต้น

ยุทธศาสตร์ที่ ๔ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านการสื่อสารและโทรคมนาคม เช่น บริษัทที่ให้บริการอินเทอร์เน็ต (ISP) บริษัท ทีโอที จำกัด (มหาชน) บริษัท กสท โทรคมนาคม จำกัด (มหาชน) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ผู้ให้บริการโทรศัพท์มือถือ ดาวเทียม สถานีโทรทัศน์ เป็นต้น

ยุทธศาสตร์ที่ ๕ การวิจัยและพัฒนาการรักษาความมั่งคงปลอดภัยไซเบอร์สำหรับข้อมูลส่วนบุคคล เครือข่ายสังคมออนไลน์ และการป้องกันอาชญากรรมไซเบอร์ที่ส่งผลกระทบต่อบุคคล เศรษฐกิจ อุตสาหกรรม โดยรวม

๕. เป้าประสงค์ของยุทธศาสตร์/กลยุทธ์การวิจัย

๕.๑ มีแผนยุทธศาสตร์การวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีทิศทางที่ชัดเจนและครอบคลุมทุกประเด็นที่มีความสำคัญและมีความเร่งด่วนต่อการพัฒนาประเทศไทย

๕.๒ มีการปรับปรุงกฎหมายให้ทันสมัย และมีข้อเสนอแนะเชิงนโยบายในการพัฒนายกระดับองค์กร/หน่วยงานที่รับผิดชอบในปัจจุบันให้เป็นศูนย์ความเป็นเลิศทางด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ประเทศไทยเป็นศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์ของภูมิภาคเอเชียตะวันออกเฉียงใต้

๕.๓ เกิดการบูรณาการในการทำวิจัยและพัฒนาร่วมกันระหว่างภาครัฐและภาคเอกชน ทั้งในประเทศและต่างประเทศ เพื่อพัฒนาองค์ความรู้และนวัตกรรมใหม่อย่างจริงจังในการแก้ปัญหาทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันและอนาคต

๕.๔ หน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชน สามารถนำองค์ความรู้และนวัตกรรมที่ได้ไปใช้งานทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เกิดประโยชน์ได้จริง รวมทั้งลดการนำเข้าเทคโนโลยีทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีราคาแพงจากต่างประเทศในระยะยาว

๖. ผลผลิตและผลลัพธ์ ตัวชี้วัดและเป้าหมาย

๖.๑ ผลผลิต

๑) เชิงปริมาณ คือ รายงานการวิจัยการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาครัฐและภาคเอกชน

๒) เชิงคุณภาพ คือ สามารถใช้ผลการศึกษาวิจัยการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาครัฐ ภาคเอกชน และภาคประชาชน

๖.๒ ผลลัพธ์

องค์กร/หน่วยงานในภาครัฐ ภาคเอกชน และภาคการศึกษาระดับอุดมศึกษา มีการใช้องค์ความรู้และนวัตกรรมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

๖.๓ ตัวชี้วัด

จำนวนองค์กร/หน่วยงานในภาครัฐ ภาคเอกชน และภาคการศึกษาระดับอุดมศึกษา ที่นำผลการศึกษาวิจัยไปประยุกต์ใช้เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเป็นรูปธรรม

๖.๔ เป้าหมาย

ประเทศไทยใช้ฐานความรู้จากการวิจัยด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สร้างความสามารถในการแข่งขันของประเทศได้อย่างยั่งยืน

๗. หน่วยงานหลักและเครือข่ายที่สำคัญที่เกี่ยวข้อง

๗.๑ หน่วยงานหลัก

๑) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
๒) สำนักงานคณะกรรมการนโยบายวิทยาศาสตร์ เทคโนโลยีและนวัตกรรมแห่งชาติ
๓) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
๔) สำนักงานกองทุนสนับสนุนการวิจัย
๕) สำนักงานคณะกรรมการการอุดมศึกษา
๖) สำนักงานคณะกรรมการวิจัยแห่งชาติ

๗.๒ หน่วยงานเครือข่ายที่สำคัญ

สถาบันการศึกษารัฐ และเอกชน

๘. แผนงานวิจัยหลักและกรอบเวลา

ยุทธศาสตร์ที่ ๑ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานด้านความมั่นคง และภาคบริการประชาชน เช่น กองทัพ สำนักงานตำรวจแห่งชาติ ศาล กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) หน่วยงานให้บริการด้านสาธารณสุข หน่วยงานราชการ และหน่วยงานของรัฐอื่นๆ **กรอบเวลา ช่วงปีที่ ๑-๒**

ยุทธศาสตร์ที่ ๒ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านการเงิน การธนาคาร และพาณิชย์อิเล็กทรอนิกส์ เช่น ธนาคาร บริษัทหลักทรัพย์ ประกันภัย ตลาดหลักทรัพย์ ผู้ให้บริการด้านบัตรเครดิต และหน่วยงานภาครัฐที่เกี่ยวข้องกับการกำกับตรวจสอบสถาบันการเงิน เป็นต้น **กรอบเวลา ช่วงปีที่ ๒-๔**

ยุทธศาสตร์ที่ ๓ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านสาธารณูปโภคพื้นฐาน เช่น การไฟฟ้า การประปา หน่วยงานด้านพลังงาน หน่วยงานด้านการคมนาคม/ขนส่ง และธุรกิจด้านสายการบิน เป็นต้น **กรอบเวลา ช่วงปีที่ ๒-๔**

ยุทธศาสตร์ที ๔ การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานด้านการสื่อสารและโทรคมนาคม เช่น บริษัทที่ให้บริการอินเทอร์เน็ต (ISP) บริษัท ทีโอที จำกัด (มหาชน) บริษัท กสท โทรคมนาคม จำกัด (มหาชน) สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ผู้ให้บริการโทรศัพท์มือถือ ดาวเทียม สถานีโทรทัศน์ เป็นต้น **กรอบเวลา ช่วงปีที่ ๒-๔**

ยุทธศาสตร์ที่ ๕ การวิจัยและพัฒนาการรักษาความมั่งคงปลอดภัยไซเบอร์สำหรับข้อมูลส่วนบุคคล เครือข่ายสังคมออนไลน์ และการป้องกันอาชญากรรมไซเบอร์ที่ส่งผลกระทบต่อบุคคล เศรษฐกิจ อุตสาหกรรมโดยรวม **กรอบเวลา ช่วงปีที่ ๒-๔**

๙. ปัจจัยแห่งความสำเร็จของยุทธศาสตร์/กลยุทธ์การวิจัย

๙.๑ มีมาตรการที่จะพัฒนาองค์ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในด้านต่างๆ

๙.๒ ภาครัฐมีนโยบายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ต่อเนื่องในปัจจัยในแต่ละด้าน

๙.๓ ทุกหน่วยงานที่เกี่ยวข้องได้รับการจัดสรรงบประมาณเพื่อใช้ในการวิจัย พัฒนา สาธิต ส่งเสริม รณรงค์ เผยแพร่ และประชาสัมพันธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ภายใต้กรอบการดำเนินงานของแผน

๑๐. แนวทางการขับเคลื่อนยุทธศาสตร์การวิจัย

เพื่อขับเคลื่อนให้ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่กำหนดขึ้นมีการนำไปสู่การปฏิบัติอย่างมีประสิทธิภาพและบรรลุวิสัยทัศน์ พันธกิจ และเป้าประสงค์อย่างมีประสิทธิผล จึงมีแนวทางการขับเคลื่อนยุทธศาสตร์ ดังนี้

๑๐.๑ การจัดทำแผนปฏิบัติการ

ต้องมีการกำหนดแผนปฏิบัติการที่ชัดเจนและเป็นระบบ เพื่อกำหนดแนวทาง ขั้นตอน วิธีการ/กิจกรรม และเจ้าภาพผู้รับผิดชอบ เพื่อให้เกิดการแปลงกลยุทธ์และแผนงานวิจัยไปสู่การปฏิบัติเพื่อนำส่งผลผลิตและผลลัพธ์ตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิผล รวมทั้งมีการกำหนดกลไกของการทบทวนและปรับยุทธศาสตร์การวิจัยให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยเฉพาะในกรณีที่มีสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่างจากที่เคยศึกษาไว้ อันจะทำให้ยุทธศาสตร์การวิจัยมีความสอดคล้องกับสถานการณ์และสภาพแวดล้อม รวมทั้งสามารถปฏิบัติและนำส่งผลงานได้อย่างมีประสิทธิผล

๑๐.๒ การสื่อสารและการประสานงาน

การขับเคลื่อนยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ต้องเกี่ยวข้องกับภาคส่วน องค์กร และบุคคลจำนวนมาก และต่อเนื่องตามกรอบเวลาของยุทธศาสตร์ ดังนั้น เพื่อให้การขับเคลื่อนยุทธศาสตร์มีประสิทธิภาพและเกิดประสิทธิผลจำเป็นอย่างยิ่งที่จะต้องให้ความสำคัญและจัดให้มีกลไกการสื่อสารและการประสานงานอย่างเป็นระบบ ทั่วถึง และต่อเนื่อง โดยจัดตั้งศูนย์ประสานงาน (Focal Point) ในแต่ละภาคส่วนที่ชัดเจน และสนับสนุนให้มีการสื่อสารและประสานงานเป็นเครือข่ายของแต่ละภาคส่วน (Sector Networking) และข้ามภาคส่วน (Inter-Sector Networking) ซึ่งอาจใช้ประโยชน์จากเครือข่ายออนไลน์ที่พัฒนาเป็นระบบสังคมออนไลน์ (Social Networking) สำหรับการยกระดับความร่วมมือของนักวิจัยในสหวิทยาการ และอำนวยความสะดวกในการติดต่อสื่อสารและประสานงาน รวมทั้งการเผยแพร่ข้อมูล การโต้ตอบ รวมถึงการติดต่อขอข้อมูลการวิจัยระหว่างภาคส่วนได้

๑๐.๓ ความพร้อมด้านทรัพยากร

ความพร้อมด้านทรัพยากร ประกอบด้วย ความพร้อมด้านบุคลากร ด้านระบบงาน และความพร้อมด้านระบบฐานข้อมูลและสารสนเทศที่ใช้สำหรับการวิจัย บุคลากรที่สนับสนุนการวิจัยต้องมีความรู้และมีจำนวนเพียงพอในการประสานงาน ระบบงานต่างๆ จะต้องมีความคล่องตัวที่เอื้อให้นักวิจัยสามารถทำงานได้อย่างมีประสิทธิภาพ ระบบฐานข้อมูลการวิจัยในปัจจุบันยังมีลักษณะกระจัดกระจายและไม่ทันสมัย ซึ่งเป็นอุปสรรคอย่างมากต่อการวิจัยในอนาคต จึงจำเป็นต้องมีการพัฒนาระบบฐานข้อมูลและสารสนเทศการวิจัยที่เปิดโอกาสให้ทุกภาคส่วนสามารถเข้าถึงและมีส่วนร่วมในการพัฒนาระบบสารสนเทศและฐานข้อมูลดังกล่าวในขอบเขตที่กำหนด มีการเชื่อมโยงกับฐานข้อมูลการวิจัยขององค์การและภาคส่วนอื่นทั้งภายในและภายนอก

ประเทศ มีการประมวลผลปัญหาและถอดบทเรียนของการดำเนินงานในรูปแบบต่างๆ เพื่อจะนำไปพัฒนารูปแบบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อไป

๑๐.๔ วัฒนธรรมการวิจัย

สร้างเสริมวัฒนธรรมการวิจัย เช่น ควรส่งเสริมให้ภาครัฐ ภาคเอกชน ภาคประชาชน และองค์กรต่างๆ ได้มีโอกาสร่วมในการทำวิจัยในส่วนที่เกี่ยวข้องในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ตั้งแต่ขั้นตอนการเริ่มต้นการทำวิจัย โดยอาจร่วมแสดงความคิดเห็นต่อข้อเสนอการทำวิจัย และการร่วมวิจารณ์และเสนอแนะผลการวิจัย นอกจากนี้การเผยแพร่องค์ความรู้งานวิจัยไปสู่วงกว้างทั้งในประเทศและระดับสากล

๑๑. แนวทางในการติดตามและประเมินผล

การขับเคลื่อนให้ยุทธศาสตร์การวิจัยรายประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ บรรลุวิสัยทัศน์ พันธกิจ และเป้าประสงค์อย่างมีประสิทธิผล จำเป็นต้องมีการติดตามและประเมินผลที่ดีควบคู่ไปด้วย โดยใช้การบริหารจัดการระบบวิจัยซึ่งเป็นกลไกในการติดตามและประเมินผลที่เป็นระบบ ดังนี้

๑๑.๑ การประเมินก่อนดำเนินการวิจัย (Ex-Ante Evaluation) เพื่อวิเคราะห์กลั่นกรองข้อเสนอการวิจัยที่เหมาะสมและสอดคล้องตามยุทธศาสตร์การวิจัย

๑๑.๒ การติดตามผลระหว่างดำเนินการวิจัย (Ongoing Evaluation) เพื่อรับทราบปัญหา อุปสรรคในการดำเนินงานที่เกิดจากการนำยุทธศาสตร์การวิจัยดังกล่าวไปปฏิบัติ ว่าสามารถตอบโจทย์ความต้องการได้อย่างถูกต้องหรือไม่

๑๑.๓ การประเมินผลหลังดำเนินการวิจัย (Ex-Post Evaluation) ของงานวิจัยที่หน่วยงานดำเนินการวิจัยเสร็จสมบูรณ์แล้ว โดยเฉพาะการประเมินผลความคุ้มค่าของการวิจัย เพื่อประเมินผลผลิตและ/หรือผลลัพธ์ของการวิจัยโดยเปรียบเทียบกับวัตถุประสงค์ของโครงการวิจัย และเป้าประสงค์/ตัวชี้วัดของยุทธศาสตร์การวิจัย