แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัย ทางไซเบอร์แห่งชาติ

โดย

นาวาอากาศเอก ชนินทร เฉลิมทรัพย์
รองเสนาธิการวิทยาลัยเสนาธิการทหาร
สถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๐
ประจำปีการศึกษา พุทธศักราช ๒๕๖๐ – ๒๕๖๑

บทคัดย่อ

เรื่อง แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย นาวาอากาศเอก ชนินทร เฉลิมทรัพย์ **หลักสูตร** วปอ. **รุ่นที่** ๖๐

การวิจัยครั้งนี้ มีวัตถุประสงค์ เพื่อศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งการศึกษาค้นคว้า นโยบาย ยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ทั้งนี้เพื่อให้สามารถเสนอรูปแบบหรือแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ โดยมีขอบเขตในการศึกษา ได้แก่ เอกสาร ระเบียบ คำสั่ง นโยบาย ยุทธศาสตร์ การดำเนินงานของหน่วยงานที่รับผิดชอบทางด้านไซเบอร์ ภายใต้กระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยเป็นการดำเนินการวิจัยเชิงคุณภาพ ทำการศึกษาวิเคราะห์ การกำหนดนโยบายยุทธศาสตร์ และการบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ และสัมภาษณ์เชิงลึกกับกลุ่มผู้ทรงคุณวุฒิที่มีส่วนในการรับผิดชอบต่อการกำหนดนโยบาย ยุทธศาสตร์ และการดำเนินงานการรักษาความมั่นคงปลอดภัยไซเบอร์

ผลการวิจัย พบว่า การศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กรการบูรณาการการบริหารจัดการ และการรักษาความมั่นคงปลอดภัยไซเบอร์ จำเป็นต้องมีองค์กร ที่นำเทคนิคการบริหารจัดการมาใช้ ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้น การบูรณาการการบริหารจัดการ ต้องมีเจ้าภาพที่ชัดเจน โดยบริหารที่ทุกหน่วยงาน ทำงานแบบมุ่งเน้นผลงานตามยุทธศาสตร์ โดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุเป้าหมาย สำหรับภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามที่มีการเปลี่ยนแปลงไปจากเดิม มีรูปแบบการโจมตีที่หลากหลาย การวางแผนป้องกัน คือ การปรับกลยุทธ์ในการรับมือและใช้ระบบมาตรฐานทางไซเบอร์ (ISO/IEC27001 : 2013) หรือมาตรฐานที่จะถูกพัฒนาขึ้นต่อไป มาช่วยดำเนินการบริหารจัดการ แต่ปัจจัยในการดำเนินงานที่สำคัญที่สุดคือมนุษย์ การศึกษาแนวนโยบายและยุทธศาสตร์ ตลอดจนการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ พบว่า กระทรวงกลาโหมใช้แนวความคิดในการป้องกันทางไซเบอร์ เช่นเดียวกับการศึกษามั่นคงของประเทศ โดยเน้นการป้องกันเชิงรุก การผนึกกำลังป้องกันประเทศ และการร่วมมือด้านความมั่นคงทางไซเบอร์ โดยได้จัดตั้งส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSDC) เชิงรับและส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security incident Response Team : CSIRT) สำหรับกระทรวงดิจิทัลฯ ได้กำหนด กรอบแนวคิดและนโยบายในระดับชาติกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศ กำหนดแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard

Operating Procedure : SOP) รวมทั้งเสนอแนวความคิดในการจัดตั้ง Cyber Security Agency (CSA) หน้าที่เป็นหน่วยงานกลาง ในการประสานงานและเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์

ข้อเสนอแนะสำหรับแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ มีดังนี้ คือ การจัดการความรู้และบริหารความเสี่ยง(Knowledge Management & Risk) เพื่อให้ผู้นำองค์กร ผู้กำหนดนโยบายและผู้ปฏิบัติ ได้ตระหนักรู้และเก็บสะสมองค์ความรู้ และประสบการณ์ เพื่อเป็นประโยชน์ต่อไป มีการทำงานแบบเครือข่าย (Network) เชื่อมโยงตามประเด็นยุทธศาสตร์ร่วม (Common Agenda) ปฏิบัติงานตามมาตรฐานการปฏิบัติทางเทคโนโลยี และจัดตั้งศูนย์การศึกษาและการวิจัย พัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์

ABSTRACT

Title The Integrating of Nation's Cyber Security

Field Science and Technology

Name Group Captain Chanintorn Chalermsup **Course** NDC **Class** 60

The purpose of this research is to study the concepts of organizational competence, integration, management and cyber security. This includes policy, strategies and operations related to cyber security of the Ministry of Defense and the Ministry of Digital economy and society. In order to be able to offer a model or approach to integrating national cyber security The scope of the study includes documents, regulations, policies, operational strategies of the agencies responsible for cyberspace under the Ministry of Defense and the Ministry of Digital economy and society. This is a qualitative research by analytical studying Strategic Policy, Formulation management and cyber security and comparing to the foreign cyber security policies and operation. In-depth interviews with qualified panel members in charge of policymaking, strategy and implementation, cyber security.

The research found that the study of the theory of organizational competencies, the integration of management and cyber security need to establish an organization with management techniques used. Must have a structure and style that conform to the environment of the society. Integration of management must have a clear vision in order to the administration at all agencies focus on Strategy-oriented base by sharing common resources to achieve the goal. For cyber threats The condition and characteristics of the threat have changed. There are various types of attacks. Prevention planning is a strategy of coping and using standardized systems (ISO / IEC27001: 2013), or standards that will be further developed to help manage. But the most important operational factor is human. Policies and Strategic Studies as well as operating on cyber security, the Department of Defense used the concept of cyber defense as the country defense with emphasis on Active Defense, Force Synergy and Cooperation in cyber security It has established a Cyber Security Operation Center (CSDC) for defense and computer Security incident Response Team (CSIRT) to response the incident threat. For the Digital Ministry has set up a national framework and policy, setting out the Critical

Information Infrastructure (CII) of the country, setting out guidelines for responding to emergency situations, Standard Operating Procedure (SOP), as well as the idea of establishing a Cyber Security Agency (CSA) as a central agency to coordinate and respond to cyber security issues.

Recommendations for integrating cyber security are: 1)Knowledge Management & Risk for Policy makers and practitioners awareness, knowledge and experience, 2) Network operation that is linked to the Common Agenda, 3)Operating according to the standards of technology practice and 4)the establishment of a research and education center to develop cyber security

คำนำ

เทคโนโลยีสารสนเทศและการสื่อสาร ได้ถูกพัฒนาขึ้นมาอย่างรวดเร็ว และเข้ามามีผลอย่างมากกับวิถีชีวิตมนุษย์ ซึ่งประเทศไทยก็ไม่สามารถหลีกเลี่ยงได้ต้องเข้าไปเกี่ยวข้อง ทั้งทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ การปฏิบัติทางดิจิทัล (Digital revolution) ทำให้ประเทศต้องพึ่งพึงเทคโนโลยีดิจิทัล ทั้งในระบบการบริหารราชการแผ่นดินและการใช้บริการสาธารณะ ซึ่งถ้าหากมีการคุกคามและการก่อภัยโดยใช้ช่องทางทางดิจิทัล หรือโครงสร้างพื้นฐานทางดิจิทัล ที่เรียกว่า ภัยคุกคามทางไซเบอร์ย่อมก่อให้เกิดความเสียหายต่อสภาพเศรษฐกิจ การบริหารราชการ รวมทั้งด้านความมั่นคงของประเทศ

ประเทศไทยกำหนดให้มีหน่วยงานที่รับผิดชอบกิจกรรมทางไซเบอร์ คือ กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม ซึ่งโดยภารกิจหลัก คือ ดูแลการคุกคามทางไซเบอร์ต่อเศรษฐกิจและสังคมเป็นหลัก และกระทรวงกลาโหม ซึ่งรับผิดชอบดูแลเรื่องความมั่นคงของประเทศ แต่ถ้าถือว่าภัยคุกคามทางไซเบอร์ เป็นภัยในมิติใหม่ที่มีผลต่อความมั่นคงปลอดภัยของประเทศ จึงควรที่จะต้องมาพิจารณาการบูรณาการการทำงานในประเด็นดังกล่าวอย่างจริงจังเพื่อรับมือกับภัยคุกคามใหญ่ขึ้น

การศึกษาวิจัยครั้งนี้ ผู้วิจัยมีความสนใจที่จะศึกษาแนวทางการบูรณาการ การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ โดยมุ่งเน้นไปที่การบูรณาการ การทำงานของหน่วยงานภายใต้กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม และหน่วยงานภายใต้กระทรวงกลาโหมที่รับผิดชอบงานด้านความมั่นคงทางไซเบอร์ โดยศึกษาถึงแนวทางการบูรณาการการบริหารจัดการ ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อเป็นแนวทางปฏิบัติและเป็นจุดเริ่มต้นของการขยายผลไปสู่หน่วยงานอื่นทั้งภาครัฐ เอกชน และประชาชนทั่วไป เพื่อให้เกิดผนึกกำลังภายในจากการป้องกันภัยทางไซเบอร์ร่วมกัน

ผู้วิจัยหวังเป็นอย่างยิ่งว่า เอกสารวิจัยฉบับนี้จะเป็นประโยชน์ต่อผู้ที่เกี่ยวข้องและผู้ที่สนใจในการนำผลการวิจัยพร้อมทั้งข้อเสนอแนะไปใช้ประโยชน์ และพัฒนาแนวทางการบูรณาการการทำงานเพื่อความมั่นคงทางไซเบอร์ให้ขยายกว้างออกไป หรือการบูรณาการ การทำงานในประเด็นอื่น ๆ ที่สนใจต่อไป

นาวาอากาศเอก

(ชนินทร เฉลิมทรัพย์)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ ๖๐

ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

หน้า

ตารางที่

สารบัญแผนภาพ

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีสารสนเทศและการสื่อสาร ได้พัฒนาขึ้นในช่วงสองทศวรรษที่ผ่านมาอย่างก้าวกระโดดและปัจจุบันได้เข้ากับวิถีชีวิตของมนุษย์ในทุกมิติ ซึ่งประเทศไทยได้ก้าวเข้าสู่ยุคดิจิทัล ที่มีเศรษฐกิจ สังคมและชีวิตประจำวันของประชาชน ที่ขึ้นอยู่กับเทคโนโลยีดิจิทัลอย่างมาก

การปฏิวัติทางดิจิทัล (Digital revolution) ทำให้เกิดตัวแปรใหม่ที่ประเทศต้องพึ่งพิงเทคโนโลยีดิจิทัล ทั้งเศรษฐกิจและการบริหารราชการแผ่นดินของรัฐบาลและการให้บริหารสาธารณะที่จำเป็น ซึ่งปัจจุบันขึ้นอยู่กับความมั่นคงของโลกไซเบอร์และโครงสร้างพื้นฐานดิจิทัล อย่างไรก็ตาม การสูญเสียความไว้วางใจในระบบดิจิทัล จะเป็นภัยคุกคามต่อการพัฒนาเศรษฐกิจดิจิทัลของประเทศ

ฮาร์ดแวร์และซอฟต์แวร์ส่วนใหญ่ที่พัฒนาขึ้นเพื่ออำนวยความสะดวก ในสภาพแวดล้อมแบบดิจิทัลที่มีการเชื่อมต่อกันอย่างหนาแน่นยิ่งยวด (Hyperconnected) ได้ส่งผลกระทบต่อประสิทธิภาพ ต้นทุน และขีดความสามารถของอุตสาหกรรมและกากรใช้ชีวิตอย่างปกติของประชาชน แต่ไม่ได้มีการออกแบบที่มีความปลอดภัยมาตั้งแต่ต้นอย่างเหมาะสม จึงทำให้ผู้โจมตีไม่ว่าจะเป็นรัฐที่เป็นฝ่ายตรงข้าม องค์กร อาชญากรรม หรือผู้ก่อการร้าย และแม้แต่บุคคลทั่วไป ก็สามารถใช้ช่องว่างระหว่างความสะดวกและความปลอดภัยในการโจมตีได้ ดังนั้นการลดช่องว่างและความเสี่ยงทางไซเบอร์จึงควรได้รับการให้ความสำคัญเป็นอันดับแรก

การขยายตัวของอินเทอร์เน็ตที่เชื่อมโยงกับคอมพิวเตอร์และโทรศัพท์เคลื่อนที่มาสู่การใช้งานในระบบอัจฉริยะนั้น เป็นการขยายขอบเขตของการคุกคามทางไซเบอร์ ซึ่งระบบและเทคโนโลยีที่สำคัญกับชีวิตประจำวันของเรา เช่น ระบบการผลิตไฟฟ้า ระบบควบคุมการจราจรทางอากาศ ดาวเทียม เทคโนโลยีทางการแพทย์ โรงงานอุตสาหกรรมและระบบการขนส่ง ต่างมีการเชื่อมต่อกับอินเทอร์เน็ตที่อาจเสี่ยงต่อการถูกแทรกแซงและทำลายได้

ภัยคุกคามด้านไซเบอร์ที่เกิดจากช่องโหว่ที่มีและช่องว่างในขีดความสามารถและการป้องกันของประเทศ ทำให้รัฐบาลต้องเล็งเห็นถึงความสำคัญอย่างมากเพื่อให้สามารถตอบโต้ได้อย่างเท่าทันต่อภัยคุกคามทางไซเบอร์นี้ โดยจำเป็นที่จะต้องมี่แนวทางในการป้องกันอย่างรอบด้านเพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ (เศรษฐพงศ์ มะลิสุวรรณ, ๒๕๖๐ : ๓)

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศดังกล่าว ซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่

เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่าง ๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม

ดังนั้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ จึงเป็นเรื่องสำคัญสำหรับทุกหน่วยงาน เนื่องจากหน่วยงานเหล่านั้นต่างประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนงานตามภารกิจต่าง ๆของตน และเพื่อการบริการประชาชน การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ รวมทั้งการประสานงานกับหน่วยงานอื่นเพื่อกระจายข่าวสาร เพื่อปรับปรุงข้อมูล วิธีการ การป้องการ และลดผลกระทบจากอันตรายที่เกิดขึ้นจึงเป็นเรื่องจำเป็น

ผู้วิจัย จึงมีความสนใจในการศึกษา แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อหาทางพัฒนา และเสริมสร้างความมั่นคง โดยเฉพาะความมั่นคงทางทหารและความมั่นคงทางเศรษฐกิจ และเป็นแนวทางให้ส่วนราชการที่เกี่ยวข้องได้ดำเนินการไปในทิศทางเดียวกัน เพื่อตอบสนองต่อการคุกคามความมั่นคงปลอดภัยทางไซเบอร์ ได้รวดเร็วและทันท่วงที

วัตถุประสงค์ของการวิจัย

๑. ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ศึกษาแนวนโยบายการกำหนดยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. เสนอแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

ขอบเขตของการวิจัย

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยต้องการศึกษาแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ โดยมีขอบเขต ดังนี้

๑. ขอบเขตด้านประชากร ได้แก่ การสัมภาษณ์ผู้เกี่ยวข้อง ผู้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานที่เกี่ยวข้อง

๒. ขอบเขตด้านเนื้อหา ได้แก่ เอกสาร ระเบียบ คำสั่ง นโยบาย และแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

๓. ขอบเขตด้านพื้นที่ มุ่งเน้นเฉพาะการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างหน่วยงานที่เกี่ยวข้องภายใต้กระทรวงกลาโหม และกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์ การกำหนดนโยบายและการบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เปรียบเทียบกับแนวความคิดความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ และสัมภาษณ์เชิงลึกกับกลุ่มเป้าหมาย คือ ผู้ทรงคุณวุฒิ ในส่วนที่รับผิดชอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบกับการตรวจสอบเอกสารทางวิชาการที่เกี่ยวข้อง

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบแนวทางในการกำหนดนโยบาย ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมทั้งปัญหาและอุปสรรคในระดับปฏิบัติการฯ

๒. ได้แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

๓. สามารถนำแนวทางดังกล่าวไปขยายผลสู่หน่วยงานอื่นทั้งภาครัฐและเอกชน

คำจำกัดความ

ความมั่นคงปลอดภัยไซเบอร์	หมายถึง	มาตรการและการดำเนินการเพื่อปกป้อง ป้องกัน การส่งเสริม เพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐานระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหารความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ
ภัยคุกคามทางไซเบอร์ (cyber threats)	หมายถึง	ภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจตลอดจนความมั่นคงของประเทศด้วยการโจมตีทางไซเบอร์

		หลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) เป็นต้น
หน่วยงานของรัฐ	หมายถึง	ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น องค์กรอิสระ องค์การมหาชน รัฐวิสาหกิจ และหน่วยงานของรัฐที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในกรณีใดๆ
หน่วยงานเอกชน	หมายถึง	หน่วยงานที่จัดตั้งขึ้นจากการรวมตัวของบุคคล หรือคณะบุคคลเข้าด้วยกัน ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือที่ไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคลหรือไม่ก็ตาม

บทที่ ๒
แนวคิด ทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

การทำวิจัย เรื่อง แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ผู้ศึกษาได้ศึกษาจากเอกสาร แนวคิด ทฤษฎีและงานวิจัยต่างๆ ที่เกี่ยวข้องกับการบูรณาการการจัดองค์กรสมัยใหม่ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อนำมาเป็นกรอบแนวทางในการศึกษาค้นคว้า โดยใช้แนวคิด ทฤษฎีและงานวิจัยต่างๆ ที่เกี่ยวข้องดังกล่าวนำมาเป็นกรอบแนวทางในการศึกษาค้นคว้า ดังนี้

๑. แนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศองค์กรและองค์กรสมัยใหม่

๒. การจัดการความรู้และการบริหารความเสี่ยง

๓. การบูรณาการการบริหารจัดการ

๔. การรักษาความมั่นคงปลอดภัยทางไซเบอร์

๕. ยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

๖. งานวิจัยที่เกี่ยวข้อง

แนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศองค์กรและองค์กรสมัยใหม่

๑. สมรรถนะในองค์การ

๑.๑ ความหมายสมรรถนะ ผู้วิจัยได้ศึกษาการนิยามความหมายของสมรรถนะของนักวิชาการและผู้เชี่ยวชาญหลายท่านซึ่งสามารถสรุปได้ว่า สมรรถนะ หมายถึง ความรู้ ความสามารถ ทัศนคติ ที่จะปฏิบัติหน้าที่ให้ประสบความสำเร็จและเกิดประสิทธิภาพกับองค์กรอย่างสูงสุด

๑.๒ ประเภทของสมรรถนะ อาภรณ์ ภู่วิทยพันธุ์ (๒๕๕๒:๑๗-๑๘) กล่าวว่า สมรรถนะในองค์กรสามารถแบ่งออกเป็น ๓ ประเภทหลัก ได้แก่

๑.๒.๑ สมรรถนะหลัก (Core Competency) หมายถึง ความสามารถหลักที่คาดหวังให้พนักงานทุกคนทุกระดับองค์กรจะต้องมีองค์การบางแห่งเรียกสมรรถนะหลัก ซึ่งเป็นสิ่งที่ทำให้เป้าหมาย วิสัยทัศน์และภารกิจขององค์การประสบความสำเร็จ ทั้งนี้สมรรถนะหลักที่ถูกปฏิบัติเหมือนๆ กัน ในองค์กรจะนำไปสู่การสร้างนวัตกรรมองค์กร (Corporate Culture) ที่หลักปฏิบัติที่สืบทอดต่อไปยังพนักงานคนอื่นๆ ต่อไปได้ พบว่าสมรรถนะหลักที่กำหนดขึ้นในองค์กรนั้นไม่ควรมี

จำนวนมากนักประมาณ ๓-๕ ข้อ

๑.๒.๒ สมรรถนะทางการบริหาร (Managerial Competency) หมายถึง ความสามารถในการบริหารจัดการงานที่คาดหวังกับกลุ่มพนักงานแยกตามระดับตำแหน่งงาน ถ้าตำแหน่งงานเหมือนกันคาดหวังว่าจะมี สมรรถนะประเภทนี้เหมือนกัน เช่น ผู้จัดการฝ่าย ไม่ว่าจะเป็นฝ่ายใดๆ ก็ตามจะต้องมีสมรรถนะในเรื่อง วิสัยทัศน์เชิงกลยุทธ์ การวางแผนงาน การบริหารการเปลี่ยน แปลง การสร้างเครือข่ายที่เหมือนกัน พบว่าการกำหนดสมรรถนะทางการบริหารนั้น จะกำหนดขึ้นจากบทบาทหน้าที่และความรับผิดชอบหลักที่เหมือนกันตามระดับตำแหน่งงาน และจำนวนข้อของสมรรถนะทางการบริหารจะต้องมีจำนวนไม่มาก อยู่ระหว่าง ๓-๕ ข้อต่อระดับตำแหน่งงาน

๑.๒.๓ สมรรถนะตามหน้าที่ (Function Competency) หมายถึง ความสามารถในงานเฉพาะด้านที่แตกต่างกันไปในแต่ละหน่วยงาน พบว่าการกำหนดสมรรถนะตามหน้าที่ขึ้นอยู่กับลักษณะงานที่รับผิดชอบ (Job Description) โดยพิจารณาว่าในแต่ละตำแหน่งงานคาดหวังความรู้ ทักษะ และคุณลักษณะส่วนบุคคลในเรื่องใดบ้าง ซึ่งความสามารถเหล่านี้จะส่งผลการทำงานที่ผู้บังคับบัญชามอบหมายให้ประสบความสำเร็จ โดยสามารถวัดความสำเร็จของงานได้จากตัวชี้วัดผลงานหลัก (Key Performance Indicators) ดังนั้นจำนวนสมรรถนะตามหน้าที่จึงมีความแตกต่างกันไปแต่ละหน่วยงาน โดยปกติแล้วจะมีไม่มากเช่นเดียวกันอยู่ระหว่าง ๕-๗ ข้อ นอกจากนี้ยังพบว่าการจัดแบ่งสมรรถนะตามหน้าที่นั้นสามารถแบ่งได้อีก ๒ ประเภทย่อยได้แก่ ๑. Common Function Competency เป็นความสามารถในงานที่เป็นเรื่องทั่วๆ ไป ตำแหน่งงานอื่นในฝ่ายอื่นๆ และ ๒. Specific Function Competency เป็นความสามารถในงานทางเทคนิคเฉพาะด้านที่ต้องอาศัยความชำนาญและระยะเวลาในการเรียนรู้และฝึกฝน

๑.๓ องค์ประกอบที่สำคัญของสมรรถนะการเป็นผู้นำของผู้บริหารองค์กร

สมรรถนะทางการบริหาร (Managerial Competency : mc) หมายถึง สมรรถนะที่เป็นความสามารถทางการจัดการซึ่งสะท้อนให้เห็นถึงทักษะในการบริหารและจัดการงานต่างๆ กำหนดให้ต้องมีทั้งระดับผู้บริหารและระดับพนักงานปฏิบัติการ แต่จะแตกต่างกันตามบทบาทหน้าที่และความรับผิดชอบโดยแบ่งเป็นข้อย่อย ดังนี้

๑.๓.๑ วิสัยทัศน์เชิงกลยุทธ์ (Strategic Visioning) ความเข้าใจถึงวิสัยทัศน์พันธกิจของธนาคาร เพื่อกำหนดกลยุทธ์และยุทธศาสตร์การดำเนินงานของธนาคาร ตลอดจนการรวบรวมติดตามและวิเคราะห์กลยุทธ์การดำเนินงานต่างๆ

๑.๓.๒ การวางแผนงาน (Planning) ความรู้ความเข้าใจแนวคิดหลักการกระบวนการ วิธีการวางแผนและติดตามงานรวมทั้งการประมวลผลเพื่อประยุกต์ใช้ในการวางแผนและติดตามงานให้มีประสิทธิภาพและประเมินผลการปฏิบัติงานตามแผนที่กำหนดขึ้น

๑.๓.๓ ภาวะผู้นำ (Leadership) ความเหมาะสมของการวางตน แสดงออกถึงความเป็นผู้นำ มีความน่าเชื่อถือศรัทธา รับผิดชอบต่อผลงานที่เกิดขึ้นของตนเอง ทีมงาน หน่วยงาน รวมทั้งกระตุ้นจูงใจให้ผู้อื่นปฏิบัติตามโดยอยู่บนพื้นฐานของความถูกต้องตรวจสอบได้

๑.๓.๔ การแก้ไขปัญหาและตัดสินใจ (Problem Solving and Decision Making) ความสามารถในการวิเคราะห์สาเหตุ และผลกระทบของปัญหาพร้อมทั้งสามารถวิเคราะห์และค้นหา การแก้ไขปัญหาได้หลากหลายวิธี สามารถตัดสินใจแก้ไขปัญหาได้อย่างเหมาะสมกับสถานการณ์และเกิดประโยชน์สูงสุดแก่ธนาคาร

๑.๓.๕ บริหารการเปลี่ยนแปลง (Change Management) การวิเคราะห์และการคาดการณ์การเปลี่ยนแปลงที่เกิดภายองค์กรและหน่วยงานรวมทั้งการคิดหาเครื่องมือ และวิธีการใหม่ๆ มาใช้ในองค์กร

๒. แนวความคิดและทฤษฎีเกี่ยวกับบรรยากาศขององค์กร

๒.๑ ความหมายของบรรยากาศขององค์กร

ผู้วิจัยได้ศึกษาและสรุปความหมายของบรรยากาศองค์กรจากนักวิชาการด้านทรัพยากรมนุษย์หลายท่าน เพื่อนำมาใช้ประโยชน์ในการปรับปรุงและพัฒนาองค์กรให้เหมาะสมกับลักษณะการทำงานที่เป็นมาตรฐานซึ่งสรุปได้ว่า บรรยากาศองค์กร หมายถึง สภาพแวดล้อมในการทำงานที่เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอก ซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร

๒.๒ แนวคิดเกี่ยวกับบรรยากาศองค์กร

สเตียร์ส (Steers, ๑๙๗๗) ได้แบ่งองค์ประกอบของบรรยากาศองค์การไว้ ๖ ด้านดังนี้

๒.๒.๑ โครงสร้างการทำงาน (Task Structure) จากการสำรวจความรู้สึกนึกคิดของพนักงานในองค์กรเห็นว่าโครงสร้างในการทำงานเป็นอุปสรรคหรือบั่นทอนต่อจิตใจในการทำงานหรือไม่ตัวอย่างโครงสร้างในการทำงานที่เป็นอุปสรรค เช่น การรวบอำนาจในการบังคับบัญชา ระบบงบประมาณที่ค่อนข้างเข้มงวด กฎระเบียบที่ไม่ยืดหยุ่นและกรรมวิธีในการทำงานมีขั้นตอนที่ยุ่งยากซับซ้อน เป็นต้น

๒.๒.๒ ระบบรางวัลตอบแทน (Reward Systems) ต้องวิเคราะห์ว่าเป็นระบบที่มีความยุติธรรมและเพียงพอต่อมาตรฐานการครองชีพหรือไม่

๒.๒.๓ ความเป็นอิสระ (Autonomy) หมายถึง ความรู้สึกของพนักงานที่เห็นว่าเขามีอิสระและได้รับอนุญาตจากองค์กรให้สามารถแสดงออกซึ่งความคิดสร้างสรรค์งานใหม่ๆ

ขึ้นมา

๒.๒.๔ ความอบอุ่นและการสนับสนุน (Warmth and Support) หมายถึง ภาวะการเป็นผู้นำของหัวหน้าที่ให้ความอบอุ่นหรือการสนับสนุนต่อสมาชิกภายในองค์กรในการทำงานและความก้าวหน้ามากน้อยเพียงใด

๒.๒.๕ การยอมรับความขัดแย้ง (Tolerance of Conflict) หมายถึง การวิเคราะห์ดูว่าองค์การทำให้สมาชิกเกิดความรู้สึกว่าความคิดเห็นที่แตกต่างกันสามารถได้รับการยอมรับให้เกิดขึ้นได้หรือไม่

๒.๒.๖ ความรักในหมู่คณะ (Esprit) หมายถึง ความรู้สึกนึกคิดของพนักงานที่เห็นว่าสมาชิกภายในองค์กรมีความรักกันฉันเพื่อนในการทำงานร่วมกันหรือไม่

๓. องค์กรสมัยใหม่ (Modern Organization)

ในปัจจุบันการพัฒนาองค์กรของไทยได้รับเอาแนวคิดการบริหารจากต่างประเทศมาใช้อย่างกว้างขวาง ทั้งนี้ก็เพื่อความอยู่รอดในกระแสการแข่งขันอันเชี่ยวกรากในระบบทุนนิยม (Capitalist) ดังนั้นสถานภาพที่องค์กรต้องการ คือ การสร้างความยั่งยืนให้กับองค์กร เครื่องมือทางด้านการบริหารที่จะมีส่วนช่วยให้องค์กรได้รับความสำเร็จอันยั่งยืนคือ องค์กรแห่งการเรียนรู้ (Learning Organization) ซึ่งได้รับการกล่าวถึงกันอย่างกว้างขวางทั้งในภาครัฐและเอกชน โดยภาครัฐได้กำหนดให้มีการตราไว้ในกฎหมายคือพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.๒๕๔๖ หมวด ๓ มาตรา ๑๑ “ส่วนราชการมีหน้าที่พัฒนาความรู้ในส่วนราชการเพื่อให้มีลักษณะเป็นองค์กรแห่งการเรียนรู้อย่างสม่ำเสมอ โดยต้องรับรู้ข้อมูลข่าวสารและสามารถประมวลผลความรู้ในด้านต่างๆ เพื่อนำมาประยุกต์ใช้ในการปฏิบัติราชการได้อย่างถูกต้องรวดเร็วและเหมาะสมกับสถานการณ์ รวมทั้งต้องส่งเสริมและพัฒนาความรู้ความสามารถสร้างวิสัยทัศน์ และปรับเปลี่ยนทัศนคติของข้าราชการในสังกัดให้เป็นบุคลากรที่มีประสิทธิภาพและมีการเรียนรู้ร่วมกัน” จากภาวะปัจจัยต่างๆ จึงทำให้เกิดความปรารถนาที่จะสร้างและพัฒนาองค์กรให้เป็นองค์การสมัยใหม่ บุคลากรสามารถเพิ่มพูนความรู้ความสามารถได้อย่างต่อเนื่องและสามารถสร้างผลงานได้ตามความปรารถนา อีกทั้งเป็นแหล่งสร้างความคิดทางปัญญา โดยการเรียนรู้ที่จะเรียนรู้ร่วมกัน ดังนั้นองค์กรสมัยใหม่ควรจะมีลักษณะสำคัญคือ ต้องเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง ๕ ระบบขององค์กรแห่งการเรียนรู้ ได้แก่ การเรียนรู้ (Learning) องค์กร (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology) ให้เป็นตัวขับเคลื่อนและพัฒนาองค์การ เพราะการเรียนรู้ประเภทนี้ไม่สามารถจะเกิดขึ้นและไม่สามารถคงอยู่ได้หากปราศจากความเข้าใจและการพัฒนาระบบย่อยที่สัมพันธ์กัน

การจัดการความรู้และการบริหารความเสี่ยง(Knowledge and Risk Management)

๑. การจัดการความรู้ (Knowledge Management)

๑.๑ Dave Snowden (๒๐๐๒) ได้กล่าวว่า การจัดการความรู้ หมายถึง การรวบรวมองค์ความรู้ที่อยู่กระจัดกระจายทั้งในตัวบุคคลหรือเอกสารมาพัฒนาให้เป็นระบบ เพื่อให้ทุกคนในองค์กรสามารถเข้าถึงความรู้และพัฒนาตนเองให้เป็นผู้รู้ นำความรู้ที่ได้ไปประยุกต์ใช้ในการปฏิบัติงานให้เกิดประสิทธิภาพอันจะส่งผลให้องค์กรมีความสามารถในเชิงแข่งขันสูงสุด (อ้างอิงจาก http://thaiocaladmin.go.th/work/km)

๑.๒ ชนิดของความรู้ (Types of knowledge) แบ่งเป็น ๓ ประเภท ประกอบด้วย ๑. ความรู้ที่อยู่ในตัวคน (tacit knowledge) หมายถึง ความรู้ ประสบการณ์ พรสวรรค์ต่างๆ ที่ผู้นั้นมีอย่างเชี่ยวชาญ ๒. ความรู้ที่ชัดแจ้ง (explicit knowledge) ได้แก่ ความรู้ที่ถ่ายทอดออกมาอยู่ในรูปของหนังสือ วารสาร สื่อโสตทัศนวัสดุ ๓. ความรู้ที่ชัดเจนแน่นอน (Implicit) เป็นความรู้ที่ชัดแจ้งและผ่านการถกเถียงและสรุปผลว่าเป็นความรู้ที่เหมาะสมกับวัตถุประสงค์ที่ต้องการมากที่สุด

๑.๓ กระบวนการจัดการความรู้ Demarest (๑๙๙๗) ได้อธิบายถึง กระบวนการในการจัดการความรู้ไว้ ๕ ขั้นตอนได้แก่ กระบวนการสร้างความรู้ (construction) กระบวนการรวบรวมความรู้ (embodiment) กระบวนการเผยแพร่ความรู้ (dissemination) กระบวนการใช้ความรู้หรือ นำความรู้ไปใช้ (use) และกระบวนการจัดการองค์ความรู้ (management)

๑.๔ การจัดการความรู้มีประโยชน์ คือ ช่วยประหยัดเวลาในการปฏิบัติงานและช่วยในการตัดสินใจเพื่อแก้ไขปัญหาได้ถูกต้องช่วยในการคิดผลิตสิ่งใหม่ๆ ช่วยพัฒนาทักษะของผู้ปฏิบัติงาน ส่งเสริมให้เกิดเครือข่ายและการปฏิบัติการณ์ของกลุ่มเพราะมีชุมชนนักปฏิบัติ ช่วยขับเคลื่อนกลยุทธ์ขององค์กร รับรู้ปัญหาขององค์กรได้อย่างรวดเร็ว ช่วยแพร่กระจายแนวปฏิบัติที่ดีระหว่างหน่วยงานในองค์กรช่วยสร้างคู่มือ/แนวปฏิบัติในการทำงานสำหรับหน่วยงานที่มีสาขามากจะช่วยให้สามารถปฏิบัติงานเหมือนกันหรืองานในหน้าที่เดี่ยวกันได้ไม่แตกต่างกัน ช่วยทำให้ผลผลิตและการบริการดีขึ้น ช่วยให้เกิดการแลกเปลี่ยนความคิดข้ามสายงานทำให้เกิดการพัฒนาและสร้างนวัตกรรมใหม่ๆ ช่วยเพิ่มความสามารถในการแข่งขันให้กับองค์กร ช่วยบันทึกความรู้ไว้ให้ให้กับองค์กร (กรณีคนลาออก เกษียณ) ช่วยลดช่องว่างทางความคิดระหว่างพนักงานเก่ากับพนักงานใหม่ ช่วยถ่ายโอนความรู้จากรุ่นไปสู่รุ่น และช่วยตอบสนองความต้องการของลูกค้าได้ตรงจุด

๒. การบริหารความเสี่ยง (Risk Management)

ความเสี่ยงมีความหมายในหลากหลายแง่มุม เช่น ความเสี่ยงคือโอกาสที่เกิดขึ้นแล้วธุรกิจจะเกิดความเสียหาย (Chance of Loss) ความเป็นไปได้ที่จะเกิดความเสียหายต่อธุรกิจ (Possibility of Loss) ความไม่แน่นอนของเหตุการณ์ที่จะเกิดขึ้น (Uncertainty of Event) และ การคลาดเคลื่อนของการคาดการณ์ (Dispersion of Actual Result)

๒.๑ องค์ประกอบการบริหารความเสี่ยง

๒.๑.๑ การระบุชี้ว่าองค์กรกำลังมีภัย เป็นการระบุชี้ว่าองค์กรมีภัยอะไรบ้างที่มาเผชิญอยู่และอยู่ในลักษณะใดหรือขอบเขตเป็นอย่างไร นับเป็นขั้นตอนแรกของการบริหารความเสี่ยง

๒.๑.๒ การประเมินผลกระทบของภัย เป็นการประเมินผลกระทบของภัยที่จะมีต่อองค์กรซึ่งอาจเรียกอีกอย่างหนึ่งว่า การประเมินความเสี่ยงที่องค์กรต้องเตรียมตัวเพื่อรับมือกับภัยแต่ละชนิดได้อย่างเหมาะสมมากที่สุด

๒.๑.๓ การจัดทำมาตรการตอบโต้ตอบความเสี่ยงจากภัย การจัดทำมาตรการตอบโต้ตอบความเสี่ยงเป็นมาตรการที่จัดเรียงลำดับความสำคัญแล้ว ในการประเมินผลกระทบของภัย มาตรการตอบโต้ที่นิยมใช้เพื่อการรับมือกับภัยแต่ละชนิด อาจจำแนกดังนี้

๒.๑.๓.๑ มาตรการขจัดหรือลดความรุนแรงของความอันตรายของภัยที่ต้องประสบ

๒.๑.๓.๒ มาตรการที่ป้องกันผู้รับภัยมิให้ต้องประสบภัยโดยตรง เช่น ภัยจากการที่ต้องปีนไปในที่สูงก็มีมาตรการป้องกันโดยต้องติดเข็มขัดนิรภัย กันการพลาดพลั้งตกลงมา ภัยจากไอระเหยหรือสารพิษก็ป้องกันโดยออกมาตรการให้สวมหน้ากากป้องกันไอพิษ เป็นต้น

๒.๑.๓.๓ มาตรการลดความรุนแรงของสถานการณ์ฉุกเฉินเช่น กรณีเกิดเพลิงไหม้ในอาคารได้มีการขจัดและลดความรุนแรง โดยออกแบบตัวอาคารให้มีผนังกันไฟกันเพลิงไหม้รุกลามไปยังบริเวณใกล้เคียงและมีการติดตั้งระบบสปริงเกอร์ ก็จะช่วยลดหรือหยุดความรุนแรงของอุบัติภัยลงได้

๒.๑.๓.๔ มาตรการกู้ภัยก็เป็นการลดความสูญเสียโดยตรง ลงได้มาก

๒.๑.๓.๕ มาตรการกลับคืนสภาพ เป็นการลดความเสียหายต่อเนื่องจากภัยและอุบัติภัยแต่ละครั้งลงได้

๒.๒ ขั้นตอนการบริหารความเสี่ยง ประกอบด้วย

๒.๒.๑ การกำหนดวัตถุประสงค์ (Objective Establishment)

๒.๒.๒ การระบุความเสี่ยง (Risk Identification)

๒.๒.๓ การประเมินความเสี่ยง (Risk Assessment)

๒.๒.๔ การสร้างแผนจัดการ(Risk Management Planning)

๒.๒.๕ การติดตามสอบทาน (Monitoring & Review)

๒.๓ การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management)

The Committee of Sponsoring Organization (COSO) เป็นหน่วยงานที่ได้เผยแพร่วิธีการและกรอบแนวคิดของการควบคุมภายในขององค์กร (Internal Control Framework) อย่างเป็นระบบเมื่อช่วงต้นทศวรรษของ ปี ค.ศ.๑๙๙๐ จนกระทั่งเป็นที่รู้จักและมีความนิยมอย่างแพร่หลาย การบริหารความเสี่ยงตามมาตรฐาน COSO ประกอบด้วยองค์ประกอบ ๘ ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน การบริหารความเสี่ยง ดังนี้

๒.๓.๑ สภาพแวดล้อมภายในองค์กร (Internal Environment) เป็นองค์ประกอบที่สำคัญในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการเช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศระเบียบเป็นต้น

๒.๓.๒ การกำหนดวัตถุประสงค์ (Objective Setting) องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม

๒.๓.๓ การบ่งชี้เหตุการณ์ (Event Identification) เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชีภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี

๒.๓.๔ การประเมินความเสี่ยง (Risk Assessment) เป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กร

๒.๓.๕ การตอบสนองความเสี่ยง (Risk Response) เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กร และประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่

จะเกิดผลกระทบให้ อยู่ในระดับที่องค์กรยอมรับได้

๒.๓.๖ กิจกรรมการควบคุม (Control Activities) การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลดความเสี่ยง และทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กรเพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

๒.๓.๗ สารสนเทศและการสื่อสาร (Information and Communication) องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพเพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาจัดทำการบริหารความเสี่ยงให้เป็นไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

๒.๓.๘ การติดตามประเมินผล (Monitoring) องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

๒.๔ การประเมินความเสี่ยงขององค์กร (Risk Assessment) การรักษาความปลอดภัยของระบบต่างๆ ในองค์กรจะเกี่ยวข้องกับการบริหารความเสี่ยง ถ้าไม่เข้าใจความเสี่ยงขององค์กรแล้วการใช้ทรัพยากรขององค์กรเพื่อการรักษาความปลอดภัยนั้นอาจมากเกินความจำเป็นหรือน้อยเกินไปก็ได้ กระบวนการบริหารความเสี่ยงตามมาตรฐาน ISO/IEC๒๗๐๐๑ ประกอบด้วย ๒ ส่วนหลักๆ คือ

๒.๔.๑ การประเมินความเสี่ยง (Risk Assessment) ขั้นตอนนี้จะเป็นขั้นการประเมินระดับของความเสี่ยงที่มีทั้งหมดต่อข้อมูลทรัพย์สินต่างๆ ขององค์กร โดยปกติระดับความเสี่ยงจะพิจารณาจาก ๒ ปัจจัยคือ

๒.๔.๑.๑ ความน่าจะเป็น โดยปกติคำนวณค่าโดยพิจารณาจากการวิเคราะห์ภัยคุกคามและช่องโหว่ที่มีต่อข้อมูล ร่วมกับวิธีการควบคุมและแก้ไขความเสี่ยงที่มีในปัจจุบัน

๒.๔.๑.๒ ความรุนแรง โดยปกติจะคำนวณค่าโดยการพิจารณาจากระดับความสำคัญของข้อมูลหรือทรัพย์สินนั้นๆที่มีต่อองค์กร

๒.๔.๒ การรักษาความเสี่ยง (Risk Treatment) แนวทางการควบคุมและแก้ไขความเสี่ยงมีอยู่ ๔ ทางคือ ๑. การลดความเสี่ยง คือ การพิจารณาหาวิธีในการควบคุมแก้ไขความเสี่ยงให้ลดลงมาอยู่ในระดับที่สามารถยอมรับได้ ๒. การยอมรับความเสี่ยง คือ การที่องค์กรพิจารณาแล้วว่าการดำเนินการแก้ไขและควบคุมความเสี่ยงนั้นไม่เหมาะสมไม่สามารถกระทำได้ในทางปฏิบัติหรือไม่คุ้มค่า ๓. การหลีกเลี่ยงความเสี่ยง คือ การหลีกเลี่ยงความเสี่ยงโดยการยกเลิกกระบวนการทำงาน มักกระทำเมือการแก้ไขด้วยวิธีอื่นนั้นไม่คุ้มกับผลที่จะได้รับ ๔. การย้ายโอนความเสี่ยง คือ

การถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย

สรุปการบริหารความเสี่ยงจะมีประโยชน์อย่างยิ่งต่อองค์กร สามารถลดความสูญเสียที่จะเกิดขึ้นได้ไม่มากก็น้อย ดังนั้นกระบวนการบริหารความเสี่ยงบุคลากรทั่วทั้งองค์กรต้องมีส่วนร่วมในการคิดวิเคราะห์และคาดการณ์ถึงเหตุการณ์หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการตามกรอบวิสัยทัศน์และพันธกิจขององค์กร

การบูรณาการบริหารจัดการ

การบูรณาการ (Integration) หมายถึง การประสานกลมกลืนกันของแผน กระบวนการ สารสนเทศ การจัดสรรทรัพยากร การปฏิบัติการ ผลลัพธ์ และการวิเคราะห์ เพื่อสนับสนุนเป้าประสงค์ที่สำคัญขององค์กร การบูรณาการที่มีประสิทธิผล เป็นมากกว่าความสอดคล้องไปในแนวทางเดียวกัน (Alignment) และจะสำเร็จได้ก็ต่อเมื่อการดำเนินการของแต่ละองค์ประกอบภายในระบบการจัดการผลการดำเนินการมีความเชื่อมโยงกันเป็นหนึ่งเดียวอย่างสมบูรณ์

ระบบบริหารจัดการ เป็นเรื่องสำคัญที่จะต้องบูรณาการวิธีการบริหาร ราชการ แนวใหม่ ดังจะเห็นได้จากเรื่องการมอบความรับผิดชอบของนายกรัฐมนตรีให้ แก่รองนายกรัฐมนตรี ๘ คน บทบาทของรองนายกรัฐมนตรีที่ผ่านมามิความรับผิดชอบดูแล การปฏิบัติราชการแทนนายกรัฐมนตรีในกระทรวงต่างๆ ตามที่ได้รับมอบหมาย ซึ่งบางครั้ง

กระทรวงที่ได้รับมอบหมายก็จะมีความเกี่ยวข้องกัน แต่บางครั้งกระทรวงที่ได้รับมอบหมาย ก็ไม่ได้มีความเกี่ยวข้องกัน

แต่มาในยุคปัจจุบัน รัฐบาลเห็นว่าเป็นเรื่องที่ต้องการความชำนาญการเฉพาะด้านที่แตกต่างกัน ซึ่งไม่ใช่บุคลากรของภาครัฐไม่มีความสามารถ แต่บางเรื่องความสามารถของ คนมีความแตกต่างกัน ต่างคนต่างเก่งไม่เหม่อนกัน จนบางครั้งไม่ประสานการทำงานกันใน ระดับกรมหรือระดับกระทรวง ความสามารถนั้นก็ไม่มีประโยชน์ โดยที่ทุกหน่วยงานต่างก็มีความตั้งใจที่จะร่วมมือกันดำเนินงาน แต่ลักษณะโครงสร้างการแบ่งส่วนราชการมีลักษณะ เป็นแบบแท่ง ต่างหน่วยต่างทำงาน ความร่วมมือกันจึงเป็นความร่วมมืออย่างไม่เป็นทางการ คือ เชิง Informal หรือเป็นลักษณะความร่วมมืออันเนื่องมาจากต้องช่วยกัน แต่ไม่มีความ ชัดเจนในระดับโครงสร้างจึงเห็นว่าการบูรณาการเชิงโครงสร้างอย่างเดียวไม่เพียงพอ ต้องมี การบูรณาการระบบการบริหารจัดการ ด้วย

การปฏิรูประบบราชการที่ผ่านมาได้ดำเนินการไปแล้วในขั้นตอนนี้ คือ การพัฒนา ระบบราชการที่ต้องปรับเปลี่ยนระบบการจัดการภาครัฐ ซึ่งในส่วนนี้เราจะต้องสร้างสมดุล (balance) ของการบริหารงานราชการ คือ การทำงานเชิงโครงการ ตามภารกิจหน้าที่ความ รับผิดชอบ (function) ก็ยังคงต้องดำเนินการต่อไป ในขณะที่ต้องมีความชำนาญเฉพาะด้าน (specialization) เพิ่มมากขึ้นที่

เรียกว่าการทำงานเชิงประเด็นยุทธศาสตร์หรือวาระแห่งชาติ (agenda) ซึ่งจะเป็นภารกิจที่มีความจำเป็นเฉพาะ และเมื่อจะดำเนินภารกิจนั้นให้บรรลุผลก็ ต้องมีการบริหารจัดการการทำงานร่วมกันชองหลาย ๆ ฝ่าย

ฉะนั้น ในรัฐบาลปัจจุบัน ถึงแม้จะมีการปฏิรูปในเชิงโครงสร้าง โดยแบ่งส่วนราชการทั้งหมด ๒๐ กระทรวงแล้วนั้น เห็นได้ว่า ถ้าพิจารณาในระดับบนชองระดับกระทรวงขึ้นไป นายกรัฐมนตรีจะปฏิบัติตนเหมือน CEO โดยที่มีผู้ช่วยลำดับรองลงมา คือ รองนายกรัฐมนตรี จะดูแลในส่วนชองประเด็นยุทธศาสตร์ (agenda) ในแต่ละด้าน

ลักษณะของการทำงานแบบ agenda งานจะสำเร็จได้จะต้องมีการทำงานข้ามกระทรวง ต้องใช้หลาย ๆ หน่วยงาน (function) ในการทำให้สำเร็จ อาจแก้ปัญหาในการทำงานใน รูปแบบของคณะกรรมการ แต่ประเด็นสำคัญที่เกิดขึ้น คือ ไม่มีเจ้าภาพที่ชัดเจน ฉะนั้น ใน อนาคตการทำงานแบบประเด็นยุทธศาสตร์ จะมีมากกว่างานที่เป็นในเชิงตามภารกิจ/หน้าที่ แต่ไม่ได้หมายความว่างานในเชิงภารกิจ/หน้าที่จะไม่มี แต่ลักษณะงานจะมีการผสมผสาน งานในเชิงที่เป็นประเด็นยุทธศาสตร์จะมากขึ้น ด้งนั้น จึงมีความจำเป็นจะต้องมีวิธีการ บริหารจัดการแนวใหม่ คือ การทำงานแบบบูรณาการ เพื่อให้มีเจ้าภาพที่ชัดเจนว่าประเด็น ยุทธศาสตร์ (agenda) นี้ใครจะเป็นเจ้าของ (owner) ใครเป็นผู้รับผิดชอบ และใครจะทำหน้าที่ประสานหน่วยงาน (function) ต่าง ๆ ให้เข้าด้วยกัน function ในที่นี้อาจจะหมายถึง มีหลายกระทรวง หรือหลายกรมที่ต้องทำงานร่วมกัน ซึ่งเป็นทั้งกรมที่อยู่ภายในกระทรวง เดียวกัน หรือระหว่างกระทรวง สุดท้ายที่จุดนี้ก็คือ “การทำงานแบบบูรณาการ”ฉะนั้น จึงมีความจำเป็นจะต้องมีการบริหารงานในเชิงบูรณาการเกิดขึ้น

การทำงานแบบ network

การทำงานแบบบูรณาการไม่ได้หมายความว่าทุกหน่วยงานต้องเป็น agenda หมด แต่ละหน่วยยังคงความเป็น function แต่มีการเชื่อมโยงการทำงานด้วยประเด็นยุทธศาสตร์ ที่ทำงานร่วมกัน (common agenda) โดยการทำงานร่วมกันนั้นจะเป็นไปในลักษณะของ เครือข่าย (network) ซึ่งในแต่ละกรม (Function) อาจมีหลายประเด็นยุทธศาสตร์ (agenda) ซ้อนทับกันอยู่ และในแต่ละประเด็นยุทธศาสตร์อาจมีการเชื่อมโยงกับกรมอื่น (Function อื่น) อยู่ด้วยเช่นกัน จึงทำให้เกิดการทำงานแบบเครือข่ายซ้อนเครือข่ายเพิ่มมากขึ้น ฉะนั้น การ ทำงานแบบประเด็นยุทธศาสตร์จึงต้องการบูรณาการ และในการบริหารเครือข่ายจึงจำเป็น ต้องใช้คนที่มีทัศนคติ (mindset) ที่ดีของการ'ทำงานแบบบูรณาการ

ในการทำงานแบบบูรณาการจะมีวัตถุประสงค์เป็นเป้าหมายหลักร่วมกัน โครงสร้าง การทำงานจะเป็นการทำงานแบบเครือข่ายหลายชั้นเชื่อมโยงกันอยู่ เรียก Network group ซึ่งในแต่ละกรุ๊ปจะมี ผู้มีส่วนใต้เสีย (stakeholder ที่เกี่ยวข้องแตกต่างกัน และแต่ละ stakeholder จะมีแต่ละ

หน่วยงาน (function) ที่ทำงานร่วมกันอยู่ และจะทำงาน (contribute) ในส่วนที่ตนเองเกี่ยวข้อง

ดังนั้น คนที่ทำงานแบบบูรณาการ จะต้องสามารถมองภาพแบบองค์รวม (Holistic) ได้ โดยจะต้องรู้

๑. ผู้มีส่วนได้เสีย (stakeholder ที่เกี่ยวข้องมีอะไรบ้าง เพราะแต่ละ stakeholder จะเชื่อมโยงกันแบบเครือข่าย

๒. function ของแต่ละ stakeholder มีอะไร

๓. แต่ละ function ได้ contribution อะไร

๔. สิ่งที่จะบูรณาการรวมกันให้ agenda สำเร็จนั้นคืออะไร

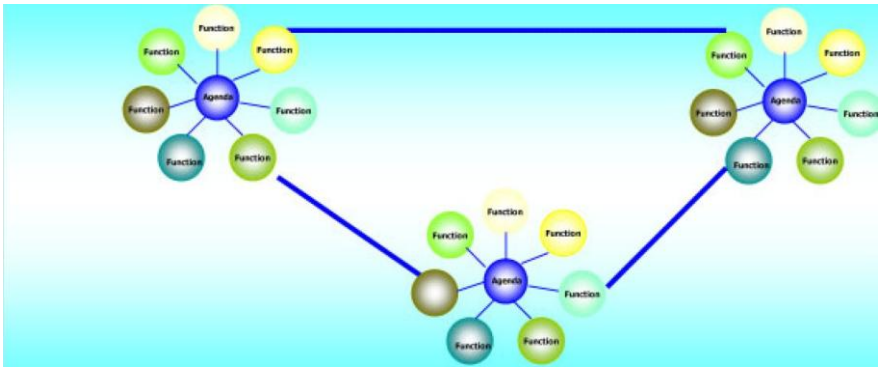
ฉะนั้นในแต่ละ agenda จะมีกลุ่มของ stakeholder (stakeholder group) ที่แตกต่างกัน และ stakeholder group จะเปลี่ยนไปตาม agenda เราเรียกลักษณะโครงสร้างแบบนี้ว่าโครงสร้างเครือข่ายแบบ dynamic network

เมื่อเกิดการทำงานแบบ agenda แล้ว โครงสร้างการทำงาน แบบ function ยังคงจำเป็นอยู่หรือไม่

การทำงานแบบโครงสร้าง (function) ยังจำเป็นตามสายการบังคับบัญชา แต่เวลาทำงานจริงทำงานแบบ network เป็น dynamic network

จากภาพจะสามารถอธิบายได้ว่า ทำไมการทำงานแบบ agenda จึงต้องเป็นการ ทำงานแบบ dynamic network และทำไมโครงสร้างแบบเดิมจึงยังคงอยู่

แผนภาพที่ ๒-๑ แสดงเปรียบเทียบโครงสร้างการทำงานแบบ Function



Agenda / Function	Agenda 1	Agenda 2	Agenda 3	Agenda 4	Agenda 5
Function 1	✓	✓			✓
Function 2		✓	✓		
Function 3	✓	✓		✓	
Function 4					✓

๑. ในการทำงานแต่ละ agenda จะต้องอาศัยหลาย ๆ function ทำงานร่วมกัน และ ในแต่ละ function จะมีความเกี่ยวข้องกับในหลาย agenda

๒. การทำงานที่มีการเชื่อมโยงกันทั้งหลาย agenda และหลาย function จึงทำให้เกิดการทำงานแบบ network และต้องเป็น dynamic network

๓. เพื่อให้บรรลุเป้าหมายในแต่ละ agenda จึงต้องมีการทำงานแบบบูรณาการ

๔. โครงสร้างแบบเดิมยังคงอยู่เพียงแต่ว่าแต่ละหน่วยงานมีระดับของการทำงานแบบ function และ agenda ที่แตกต่างกัน หน่วยงานระดับล่างจะมีการทำงานแบบ function ค่อนข้างสูง การทำงานแบบ agenda จะน้อย แต่หน่วยงานระดับบน การทำงานแบบ agenda จะค่อนข้างมาก และการทำงานแบบ function นั้นส่วนใหญ่เป็น function ของการทำหน้า ที่บูรณาการมากกว่า ซึ่งสามารถศึกษาได้จากกรณีศึกษาของผู้ว่าฯ CEO และทูตฯ CEO หรือ การทำงานแบบ agenda เช่น เรื่อง OTOP เรื่องยาเสพติด เป็นต้น

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union:

ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ว่าคือภาพรวมของเครื่องมือ (tools), นโยบาย (policies), แนวคิดการรักษาความปลอดภัย (security concepts), การรักษาความปลอดภัย (security safeguards), แนวทาง (guidelines), วิธีการบริหารความเสี่ยง (risk management approaches), การปฏิบัติ (actions), การอบรม (training), วิธีปฏิบัติที่เป็นเลิศ (best practices), การรับประกัน (assurance) และเทคโนโลยี (technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชัน, บริการ, ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ สำหรับประเทศไทย ยังไม่มีนิยามของคำว่าความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศ ได้ให้นิยามคำว่า ความมั่นคงปลอดภัย ไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กร ปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการก่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่างๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA ๓ ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของ ข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) (ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ สำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน)(สรอ.) ออนไลน์,๒๕๕๙)

๑. ความหมายของ Cyber

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” ไซเบอร์เนติกส์ (Cybernetics) เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์ หรือระบบกลไกที่ทำงานคล้ายคลึงกัน วิชานี้เปรียบเทียบความคล้ายคลึง และต่างกันระหว่างสิ่งมีชีวิตกับสิ่งไม่มีชีวิต และยึดหลักการพื้นฐานทางด้านการสื่อสารและการควบคุมที่สามารถอธิบายการทำงานของทั้งสิ่งมีชีวิตและสิ่งไม่มีชีวิตได้

๒. การรักษาความมั่นคงปลอดภัยของไซเบอร์ (Cyber Security)

Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ

ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรมและความผิดพลาดต่าง ๆ ซึ่งความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ การละเมิดการป้องกันข้อมูลส่วนตัว, การรบกวนการทำงานหรือการดำเนินธุรกรรม และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

๒.๑ มาตรการในการรักษาความปลอดภัยไซเบอร์

มาตรการในการรักษาความปลอดภัยไซเบอร์จึงมีระบบในการรักษาความปลอดภัยที่หลากหลาย ทำให้มาตรการรักษาความปลอดภัยที่ใช้ในห้วงไซเบอร์จึงสามารถนำไปประยุกต์ใช้ร่วมกับมาตรการรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ และระบบเทคโนโลยีสารสนเทศ เช่น เทคนิค Authentication ใช้ในการตรวจสอบและยืนยันตัวบุคคล หรืออุปกรณ์ปลายทางที่มีการติดต่อสื่อสารระหว่างกัน เทคนิค Automated theorem proving และเครื่องมือในการตรวจสอบอื่น ๆ สามารถทำให้กลไกที่ใช้งานระบบรักษาความปลอดภัยตามความต้องการที่ได้กำหนดไว้ เทคนิค Chain of Trust สามารถถูกใช้ในการทำให้ซอฟต์แวร์ที่ถูกใช้งานผ่านการตรวจสอบและยืนยันจากผู้ออกแบบระบบ เทคนิคการรหัส (Cryptographic) สามารถถูกใช้ในการป้องกันข้อมูลระหว่างการส่งข้อมูลระหว่างระบบ ลดโอกาสความเป็นไปได้ในการลักลอบเปิดเผยและแก้ไขข้อมูลระหว่างการรับ-ส่ง อุปกรณ์ Firewall สามารถป้องกันระบบจากการรุกรานแบบ online โดยการกำหนดการผ่านเข้าออกของ Data Package ผ่านเส้นทางการจราจรบนเครือข่ายที่กำหนดตามที่ผู้ดูแลระบบได้ออกแบบไว้ เป็นต้น

๒.๒ การปฏิบัติการในห้วงไซเบอร์ (Cyberspace Operations)

การดำเนินกลยุทธ์ภายใต้ขอบเขตในห้วงไซเบอร์ เป็นสิ่งนำมาซึ่งขีดความสามารถในการปฏิบัติการด้านต่าง ๆ ของ ทอ.สหรัฐ ได้แก่ การบัญชาการ การควบคุม การติดต่อสื่อสาร การปฏิบัติด้านคอมพิวเตอร์ การข่าวกรอง การเฝ้าตรวจ และการลาดตระเวน ปัจจุบันการทำงานของระบบการค้าระหว่างประเทศ อุตสาหกรรมพื้นฐาน และการป้องกันประเทศที่ทันสมัยขึ้นอยู่กับอิสรภาพของการใช้งานทรัพยากรภาคพื้น ภาคทะเล ภาคอากาศ ห้วงอวกาศ และห้วงไซเบอร์ โดยเฉพาะพลังอำนาจห้วงไซเบอร์มีอิทธิพลและส่งผลกระทบต่อกับการปฏิบัติในส่วนอื่น ๆ การควบคุมในห้วงไซเบอร์โดยรวมกับการปฏิบัติภารกิจ เป็นความต้องการพื้นฐานก่อนสิ่งอื่นใดของการปฏิบัติทุกภารกิจทางทหารที่มีประสิทธิภาพ ขณะที่เราชื่นชอบกำลังที่พร้อมด้วยขีดความสามารถด้านไซเบอร์ เรายังคงต้องตระหนักถึงขีดความสามารถและความพยายามที่ไม่สมมาตรในห้วงไซเบอร์ของศัตรูของเราเช่นกัน ดังนั้น เราต้องดำรงพันธะด้านการศึกษา การฝึกอบรม และการจัดหายุทโธปกรณ์ให้กับกำลังพล เพื่อความเหนือกว่าในการแข่งขันของห้วงไซเบอร์ต่อไป เมื่อพิจารณาแล้วการ

ปฏิบัติการไซเบอร์ไม่เพียงแต่ส่งผลกระทบด้านการทหารเท่านั้น หากสามารถนำไปใช้ในความมั่นคงด้านอื่น ๆ (ด้านเศรษฐกิจ ด้านสังคม และวัฒนธรรม) ดังนั้น ในภาคธุรกิจที่จะต้องคงความได้เปรียบคู่แข่งทางการค้า และรักษาฐานลูกค้าเดิม ตลอดจนขยายฐานการตลาดใหม่อยู่ตลอดเวลา จำเป็นจะต้องพึ่งพาการปฏิบัติการในห้วงไซเบอร์เช่นเดียวกันกับด้านการทหาร การสงครามไซเบอร์ หรือ Cyber Warfare (CW) เป็นการใช้กรอบของไซเบอร์เป็นเครื่องมือ เพื่อให้ได้มาซึ่งการครองความได้เปรียบในห้วงไซเบอร์ หรือ Cyberspace Superiority (ระดับขั้นในการควบคุมในห้วงไซเบอร์) โดยกำลังฝ่ายหนึ่งที่สามารถบังคับหรืออนุญาตให้การปฏิบัติการดำเนินการไปอย่างเชื่อมั่นและปลอดภัย โดยหน่วยกำลังที่ปฏิบัติบนพื้นที่ปฏิบัติการที่เกี่ยวข้อง การปฏิบัติการทางทหารที่ดำเนินการเพื่อขัดขวางการปฏิบัติงานระบบไซเบอร์และอาวุธของฝ่ายตรงข้าม รวมทั้ง เพื่อดำรงการปฏิบัติงานระบบไซเบอร์และอาวุธอย่างมีประสิทธิภาพของฝ่ายเราในการขัดกัน การปฏิบัติการดังกล่าวรวมถึง การโจมตีทางไซเบอร์ (Cyber Attack) การป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากการสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions) ดังนี้

๒.๓ การโจมตีทางไซเบอร์ (Cyber Attack)

การโจมตีทางไซเบอร์ คือ การกระทำใด ๆ ที่ใช้คอมพิวเตอร์ เครือข่าย หรือระบบ รวมทั้งอุปกรณ์ที่เกี่ยวข้อง ซึ่งตั้งใจเป็นภัยคุกคาม ขัดขวาง หรือทำลายระบบ ทรัพยากร และการทำงานของไซเบอร์ที่สำคัญของศัตรู ผลกระทบที่ต้องการของการโจมตีทางไซเบอร์ไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมาย ตัวอย่างเช่น การโจมตีต่อระบบคอมพิวเตอร์ที่ต้องการลิดรอน หรือทำลายโครงสร้างพื้นฐานสาธารณูปโภค หรือขีดความสามารถของระบบบัญชาการและควบคุม (C2) การโจมตีทางไซเบอร์อาจจะต้องใช้พาหะตัวกลางในการดำเนินการ รวมทั้ง อุปกรณ์ต่อเชื่อมต่าง ๆ (Peripheral Devices) เครื่องส่งสัญญาณอิเล็กทรอนิกส์ (Electronic Transmitters) การเข้ารหัส (Embedded Code) หรือเจ้าหน้าที่ปฏิบัติงาน (Operators) กิจกรรมหรือผลกระทบของการโจมตีอาจจะเกิดขึ้นอย่างกระจัดกระจายเป็นวงกว้าง หรือเป็นเฉพาะพื้นที่ที่เป็นเป้าหมาย

๒.๔ การป้องกันทางไซเบอร์ (Cyber Defense)

การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในห้วงไซเบอร์ของหน่วยงานที่เกี่ยวข้อง ในการดำรงขีดความสามารถด้านการตรวจจับ วิเคราะห์และลดภัยคุกคาม/จุดเสี่ยงต่าง ๆ และดำเนินกลยุทธ์ในการเอาชนะฝ่ายตรงข้าม เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ รวมถึงการปฏิบัติการเครือข่ายเชิงรุก (Proactive NetOps) การ

ดำเนินการดังนี้

๒.๔.๑ การป้องกันการโจมตีทางไซเบอร์ (Defensive Counter Cyber : DCC) เป็นมาตรการป้องกันต่าง ๆ ทั้งหมดที่ถูกออกแบบเพื่อตรวจจับ ระบุตัวตน สกัดกั้น และทำลาย หรือลดกิจกรรมอันตรายต่าง ๆ ที่พยายามเจาะ หรือโจมตีผ่านห้วงไซเบอร์

๒.๔.๒ มาตรการเชิงรับ (Defensive Countermeasures) เป็นมาตรการใน การใช้งานอุปกรณ์ และ/หรือเทคนิค ที่มีวัตถุประสงค์ต่อการทำให้การปฏิบัติของศัตรูด้อยประสิทธิภาพในเชิงการป้องกันระบบข้อมูลที่มีชั้นความลับ หรือระบบที่มีผลกระทบต่อการปฏิบัติการ

๒.๔.๓ การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ (Cyber Operational Preparation of Environment : C-OPE)

การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ (C-OPE) เป็นการทำงานภายในห้วงไซเบอร์ในการวางแผนและเตรียมการให้กับการปฏิบัติการทางทหารที่ตามมา โดยอาจรวมถึงการกำหนดระบุข้อมูล การกำหนดตั้งค่าระบบ/เครือข่าย หรือโครงสร้างการเชื่อมต่อทางกายภาพกับระบบหรือเครือข่ายที่เกี่ยวข้อง เพื่อตรวจสอบช่องโหว่/จุดอ่อนของระบบ รวมถึงการกระทำเพื่อเพิ่มความมั่นใจการเข้าถึง และ/หรือการควบคุมระบบ เครือข่าย หรือข้อมูลในระหว่างการต่อสู้กับภัยคุกคามต่าง ๆ ทั้งนี้การเตรียมสภาพแวดการปฏิบัติการทางไซเบอร์ (C-OPE) ครอบคลุมการเปิดเผยเครือข่ายคอมพิวเตอร์ (Computer Network Exploitation: CNE)

การดำเนินการด้านไซเบอร์เป็นการดำเนินการในระบบเครือข่ายที่ใช้งานอย่างกว้างขวาง ต้องมีการรักษาความปลอดภัยและการปฏิบัติการห้วงไซเบอร์ที่ถูกต้องเหมาะสม ซึ่งเป็นการป้องกันระบบและข้อมูลที่สำคัญภายในองค์กรเพื่อไม่ให้ตกเป็นผลประโยชน์ของฝ่ายที่ไม่หวังดี หากมีส่วนใดส่วนหนึ่งโดนล้วงข้อมูลหรือทำลายข้อมูล องค์กรจะศูนย์เสียความเป็นเอกภาพในการบริหารงานภายในทันที

๓. สงครามไซเบอร์ (Cyber Warfare)

๓.๑ ความหมายของสงครามไซเบอร์ สงครามไซเบอร์ (อังกฤษ: Cyber warfare) เป็นคำที่นิยามขึ้นมาโดยผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลที่ชื่อ ริชาร์ด เอ.คลาร์ก ในหนังสือที่ชื่อ Cyber War (พฤษภาคม ๒๐๑๐) โดยนิยามว่า “เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก" และวิลเลียม เจ.ลิน รองรัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐอเมริกา กล่าวว่า "โดยหลักการแล้วเพนตากอน ได้ยอมรับอย่างเป็นทางการแล้วว่า เป็นเหตุให้เกิดสงครามที่กลายเป็นเรื่องอันตรายต่อการปฏิบัติการทหาร ทั้งภาคพื้นดิน อากาศ ทะเล และทางอากาศ” อีกนัยหนึ่งสงครามไซเบอร์ (Cyber Warfare) หมายถึง การใช้คอมพิวเตอร์และอินเตอร์เน็ต ในการทำสงคราม เช่น การโจมตีเว็บ

หรือบล็อคเว็บ การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลด้านการเมืองผ่านอินเตอร์เน็ตการเจาะข้อมูลลับ โดยแฮกเกอร์ ที่นอกจากจะได้ข้อมูลความลับมาแล้ว ยังสามารถเปลี่ยนแปลงข้อมูลแล้วส่งกลับไปได้ ทำให้ข้อมูลมีการเปลี่ยนแปลง การทำลายอุปกรณ์ด้านการทหารที่ใช้คอมพิวเตอร์ควบคุมการทำงาน การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม ซึ่งระบบเหล่านี้มักควบคุมโดยระบบคอมพิวเตอร์ ซึ่งเป็นจุดอ่อนต่อการโจมตีมาก เป็นต้น

๓.๒ แนวคิดเกี่ยวกับการทำสงครามไซเบอร์ จุดกำเนิดแนวคิดของสงครามนี้ก่อตัวเป็นรูปร่างขึ้นจากนวนิยายชื่อนิวโรแมนเซอร์ (Neuromancer) ที่ชนะการประกวดจนถูกยกย่องเป็นวรรณกรรมประวัติศาสตร์ของแนวคิดใหม่จากผลงานเขียนของวิลเลียม กิ๊บสัน เป็นเรื่องราวของการนำเสนอ “ปัญญาประดิษฐ์”(Artificial Intelligence-AI) ในปี พ.ศ.๒๕๒๗ จนก่อให้เกิดแนวคิดต่อมาในการผลิตคอมพิวเตอร์โครงการที่ ๓ ของโลกเพื่อให้ทำหน้าที่ทางด้านนี้และนำไปสู่คำนิยามของคำว่า “ไซเบอร์” ที่ชัดเจนเป็นรูปธรรมว่าไม่ใช่เพียงแต่ในความหมายของทางคอมพิวเตอร์ที่มักตีความคำว่า “ไซเบอร์” โดยนำไปรวมกับคำว่า ไซเบอร์สเปซ (Cyberspace) มีความหมายว่าทุกแห่งทุกหนที่ไปได้ทั่ว ปัจจุบันไซเบอร์สเปซ จะหมายถึง การอยู่ในเครือข่ายอินเทอร์เน็ตที่อยู่ทุกแห่งทุกหนที่ระบบอินเทอร์เน็ตเชื่อมต่อไปถึง เมื่อได้นำคำว่าไซเบอร์เนติกส์ (Cybernetics) ที่บัญญัติขึ้นโดย นอร์เบิร์ต วีเนอร์ นักคณิตศาสตร์ที่มีชื่อเมื่อ ๔๘ ปีก่อนให้ความหมายว่า หมายถึง ระบบควบคุมการทำงานของเครื่องจักร หรือร่างกายที่สมบูรณ์ในตัวเอง และสามารถเรียนรู้ได้ภายในตัวของร่างกายด้วยระบบสื่อสารภายในหรือเชิงโทรจิตที่ติดกับตัวตน (mindset) จึงมีการพิจารณาลักษณะสงครามไซเบอร์นี้ลึกซึ่งเป็นสงครามความคิดที่ประยุกต์ใช้ระหว่างความคิดของความเป็นมนุษย์ที่มีตัวตนกับความเป็นเชิงมนุษย์หรือเลียนแบบมนุษย์ที่เรียกว่า “ไซเบอร์ก” (Cyborg) การดำเนินการสงครามไซเบอร์มีแนวทางในการดำเนินที่แตกต่างและหลากหลาย ซึ่งได้แก่

๓.๒.๑ การก่อการร้ายทางสารสนเทศ (Information Terrorism) : เป็นลักษณะของการก่อความรุนแรง ความเสียหาย หรือก่อความไม่สงบบนระบบเครือข่ายที่เชื่อมต่อกัน

๓.๒.๒ การโจมตีทางความหมาย (Semantic Attack) : เป็นการใช้เทคนิคและความสามารถในการเป็นแฮกเกอร์แอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้าม เพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน เช่น การใช้แฮกเกอร์เจาะระบบตรวจจับของฝ่ายตรงข้ามแล้วทำการแก้ไขโปรแกรมให้ทำงานผิดผลาด โดยตรวจจับเครื่องบินฝ่ายเราได้แล้วแสดงเป็นเครื่องบินฝ่ายเดียวกันกับเครื่องบินฝ่ายตรงข้าม ทำให้ฝ่ายตรงข้ามไม่สามารถตรวจจับเครื่องบินของฝ่ายเราได้

๓.๓ ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น ๔ ประเภท ดังนี้

๓.๓.๑ ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (application-based

threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคามที่เรียกว่า มัลแวร์ (malware) นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

๓.๓.๒ ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (web-based threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งานซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี

๓.๓.๓ ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้น ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่างๆ อาจได้รับผลกระทบโดยตรง

๓.๓.๔ ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย (targeted attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮกเกอร์ (hackers) ในประเทศต่างๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤติ สถาบันการเงิน และองค์กรอื่นๆ ของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

๓.๔ ผู้ก่อเหตุทางไซเบอร์ คือ กลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัยไซเบอร์สามารถแบ่งออกเป็น ๕ กลุ่ม (นงรัตน์ สายเพชร, ๒๕๕๖) คือ ๑. ประเทศที่มีความประสงค์ร้าย ๒. ผู้ก่อการร้าย ๓. สายลับภาคเอกชน/องค์กรอาชญากรรม ๔. แฮกเกอร์ (hackers) และ๕. แฮกทิวิส (hacktivists)

๓.๕ ชนิดของภัยคุกคามจากไซเบอร์ ภัยคุกคามไซเบอร์สามารถจำแนกออกเป็น ๒ กลุ่ม ได้แก่ การจำแนกตามประเภทของภัยคุกคาม และการจำแนกตามลักษณะ/ผลของภัยคุกคาม แต่ละกลุ่มมีรายละเอียดดังนี้

๓.๕.๑ การจำแนกภัยคุกคามตามประเภท หน่วยงาน The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามออกเป็น ๙ ประเภท (ไทยเซิร์ต, “การตรวจจับภัยคุกคามและอาชญากรรมไซเบอร์ในประเทศไทย”, ๒๕๕๖) ประกอบด้วย บอตเน็ต (Botnet) สแปม (Spam) โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) บรูตฟอร์ซ (Brute

Force) มัลแวร์ยูอาร์แอล (Malware URL) สแกนนิ่ง (Scanning) โอเพ่นพร๊อกซี่เซิร์ฟเวอร์ (Open Proxy Server) ฟิชชิ่ง(Phishing) สตอร์มเวิร์ม (Storm Worm) และดีดอส (DDoS)

๓.๕.๒ การจำแนกภัยคุกคามตามลักษณะ/ผลของภัยคุกคาม (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์ ผู้เขียนบทความเรื่องความเป็นมาของไทยเซิร์ตจากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที ในเอกสาร Cyber Security Articles ๒๐๑๒ ของไทยเซิร์ต ได้แสดงรายละเอียดของภัยคุกคามจำแนกตามลักษณะ/ผลของภัยคุกคามจำนวน ๘ ด้าน ประกอบด้วย เนื้อหาที่เป็นภัยคุกคาม (abusive content) การโจมตีสภาพความพร้อมใช้งานของระบบ (availability) การฉ้อฉลฉ้อโกงหรือหลอกลวง เพื่อผลประโยชน์ (fraud) ความพยายามรวบรวมข้อมูลของระบบ (information gathering) ความพยายามจะบุกรุกเข้าระบบ (intrusion attempts) การเจาะระบบได้สำเร็จ (intrusions) โค๊ดมุ่งร้าย (malicious code or malware) การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูล โดยไม่ได้รับอนุญาต(information security) และภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (others)

๓.๖ การรักษาความปลอดภัยไซเบอร์ (ปริญญา หอมเอนก.“Cyber security”. แผ่นภาพ,๒๕๕๗) ในปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนา และมีประยุกต์ใช้งานกันอย่างแพร่หลาย ข้อมูลสารสนเทศ การติดต่อสื่อสาร และการใช้งานคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ต่างๆ เป็นสิ่งที่มีความสำคัญ จำเป็นที่จะต้องได้รับการป้องกันจากภัยไซเบอร์เพื่อให้ข้อมูลสารสนเทศและเครือข่ายต่างๆ มีความปลอดภัย สามารถทำงานได้อย่างมีเสถียรภาพ ปราศจากภัยคุกคาม และลดระดับความรุนแรงที่อาจเกิดขึ้น ในการที่จะทำให้องค์กรสร้างความมั่นใจว่าการป้องกันและรักษาเป็นไปอย่างถูกต้องครบถ้วน ย่อมต้องมีมาตรฐานหรือแนวทางปฏิบัติที่มีประสิทธิภาพ ล่าสุดได้มีการกำหนดมาตรฐาน ISO/IEC ๒๗๐๐๑-๒๐๑๓ ซึ่งเกี่ยวกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศขึ้น โดยมีวัตถุประสงค์เพื่อบริหารจัดการกับความปลอดภัยไซเบอร์ ISO/IEC ๒๐๐๑-๒๐๑๓ เป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ เป็นมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่หลายองค์กรยึดถือร่วมกัน มีการนำไปใช้อย่างแพร่หลายทั่วโลก และได้มีการปรับปรุงอย่างต่อเนื่อง มาตรฐานนี้มีความเกี่ยวข้องกับข้อมูลโดยตรง เนื่องจากการรักษาความปลอดภัยของข้อมูลซึ่งถือเป็นส่วนสำคัญส่วนหนึ่งขององค์กร มาตรฐานนี้เป็นมาตรฐานที่พัฒนามาจากมาตรฐานในตระกูล ISO/IEC 27000 โดยองค์กรมาตรฐาน International Organization for Standardization (ISO) เป็นข้อกำหนดสำหรับการพัฒนาระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ระบบคุณภาพนี้กำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ ซึ่งเป็นมาตรฐานที่ยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความ

มั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก

หน่วยงานในประเทศไทยมีการนำมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์ (รุ่น ๒.๕) มาเป็นแม่แบบของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เช่นการจัดทำแผนแม่บท ICT Security แห่งชาติของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร การจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศโดย NECTEC รวมถึงหน่วยงานเอกชนอื่นๆ มีการนำมาตรฐานนี้มาใช้ในการจัดการระบบความปลอดภัยกันอย่างแพร่หลาย อย่างไรก็ตาม การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑-๒๐๑๓ ให้มีประสิทธิภาพนั้นควรอยู่บนพื้นฐานของการประเมินความเสี่ยง และจัดการความเสี่ยงในด้านต่างๆ ควบคู่กันไป ได้แก่ ๑. การรักษาความลับของข้อมูลต่างๆ ภายในหน่วยงาน (confidentiality) ซึ่งอาจกระทำได้หลากหลายวิธีด้วยกัน เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูลตามระดับความสำคัญของข้อมูล ๒. ความถูกต้องครบถ้วนของข้อมูล (integrity) เป็นการกำหนดมาตรการหรือแนวทางในการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูล เพื่อป้องกันความผิดพลาดหรือการเข้าแก้ไขโดยผู้ที่ไม่ได้รับอนุญาต และ ๓. ความพร้อมใช้ (availability) ผู้มีสิทธิ์ในการเข้าถึงข้อมูลในระบบต่างๆ ของหน่วยงานต้องสามารถเข้าใช้ข้อมูลได้ในกรอบเวลาที่ต้องการ

๓.๗ ตัวอย่างของภัยที่เกิดจากการทำสงครามไซเบอร์

๓.๗.๑ เมื่อวันที่ ๗-๙ กรกฎาคม ค.ศ.๒๐๑๐ สำนักข่าวรอยเตอร์รายงานว่าเครือข่ายคอมพิวเตอร์และเว็บไซต์หน่วยงานรัฐบาลเกาหลีใต้ถูกแฮ็กเกอร์ไม่ทราบสัญชาติ ส่งข้อมูลเข้าไปทำลายระบบเน็ตเวิร์ก จนเว็บไซต์ใช้งานไม่ได้นานกว่า ๔ ชั่วโมง เว็บไซต์เกาหลีใต้ที่ถูกโจมตีไม่ใช่เว็บไซต์ทั่วไป แต่เป็นเว็บไซต์ของกระทรวงกลาโหมเว็บไซต์ทำเนียบประธานาธิบดี รวมถึงบริษัทที่ให้บริการอินเทอร์เน็ตที่เรียกว่า “ไอเอสพี”ด้วย ศูนย์ต่อต้านการก่อการร้ายไซเบอร์ของเกาหลีใต้ หรือ “ซีทีอาร์ซี” (The Cyber Terror Response Centre) ซึ่งตั้งอยู่ในสำนักงานตำรวจแห่งชาติเกาหลีใต้เปิดเผยว่า สงครามไซเบอร์ครั้งนี้ไม่ได้เกิดขึ้นเฉพาะในเกาหลีใต้เท่านั้น แต่เครือข่ายเว็บไซต์ของรัฐบาลสหรัฐก็โดนด้วยเช่นกัน เบื้องต้นได้รับรายงานว่าเว็บไซต์สำคัญของสหรัฐกับเกาหลีใต้ไม่ต่ำกว่า ๒๕ แห่งโดนโจมตีเรียบร้อยแล้ว โดยเจ้าหน้าที่รายหนึ่งเปิดเผยว่า เป็นการโจมตีโดยใช้วิธี “ดีดีโอเอส0” (DD0S : Distributed Denial-of-Service) คือการใช้วิธีส่งข้อมูลจำนวนมหาศาลให้ไหลเข้าไปในเว็บไซต์ หรือเครือข่ายเน็ตเวิร์กของเป้าหมายที่ต้องการโจมตี เพื่อให้ระบบทำงานหนักขึ้นและช้าลงเรื่อยๆ จนในที่สุดต้องหยุดการทำงานลง และไม่สามารถใช้งานได้

๓.๗.๒ เมื่อวันที่ ๙ ธันวาคม ค.ศ.๒๐๑๐ สำนักข่าวต่างประเทศรายงานว่า

เว็บไซต์ของบริษัทวีซ่าและมาสเตอร์การ์ดผู้ให้บริการบัตรเครดิตรายใหญ่ได้ถูกกลุ่มแฮ็กเกอร์เข้าโจมตี โดยทางกลุ่มแฮ็กเกอร์ที่เรียกตัวเองว่ากลุ่มผู้ไม่เปิดเผยนาม (Anonymous group) ได้ประกาศว่าจะไล่ล่าบริษัทที่หยุดการให้บริการกับวิกิลีกส์ ไม่ว่าจะเป็น amazon.com และ paypal.com ซึ่งหยุดให้การเชื่อมต่อกับวิกิลีกส์ ส่งผลให้ไม่สามารถรับเงินบริจาคได้ บุคคลกลุ่มนี้เป็นกลุ่มที่สนับสนุน นายจูเลียน อัสซานจ์ ผู้ก่อตั้งเว็บวิกิลีกส์ เกิดความไม่พอใจในกรณีนายจูเลียน ชาวออสเตรเลียวัย ๓๙ ปี ถูกจับกุมตัวที่กรุงลอนดอน ประเทศอังกฤษ สำนักข่าวบีบีซีรายงานว่าพวกเขาได้รับการติดต่อจากบริษัทบริการชำระเงินแห่งหนึ่งซึ่งเชื่อมโยงกับมาสเตอร์การ์ด โดยกล่าวว่าลูกค้าของพวกเขามีปัญหาไม่สามารถใช้บริการได้อย่างสิ้นเชิง โดยเฉพาะในส่วนบริการพิสูจน์ยืนยันก่อนการชำระเงินออนไลน์ที่เรียกว่า Master card's Secure Code ก็มีปัญหาถูกรบกวน ด้านมาสเตอร์การ์ดกล่าวยอมรับว่ามีปัญหาด้านการให้บริการเกิดขึ้นจริงในระบบ Secure Code แต่ก็กล่าวเสริมด้วยว่า “ระบบปฏิบัติการหลักของเราไม่มีปัญหาและไม่มีความเสี่ยงใดกับข้อมูลบัญชีของผู้ถือบัตร” (www.thanonline.com) และข่าวล่าสุดเมื่อวันที่ ๑๐ ธันวาคม ค.ศ.๒๐๑๐ วิกิลีกส์ยังคงเดินหน้าทำสงครามในโลกไซเบอร์ต่อไปอีก โดยเปิดโปงข้อมูลทางการทูตสหรัฐว่า เกาหลีเหนือได้ส่งคนงาน ๓๐๐ คน เข้าไปช่วยพม่าสร้างโรงงานอาวุธนิวเคลียร์ มีคนเห็นรถบรรทุกขนเหล็กเป็นจำนวนมากเพื่อนำไปสร้างโรงงานนิวเคลียร์ดังกล่าว ดังนั้น จะเห็นว่าการทำสงครามไซเบอร์ในศตวรรษที่ ๒๑ เริ่มมีอุณหภูมิร้อนแรงขึ้นทุกขณะ อย่าพึงคิดว่ามันจบสิ้นลงแล้วแต่ทว่ามันกำลังเริ่มต้นขึ้น

๓.๗.๓ เมื่อวันพุธที่ ๒๐ มีนาคม ๒๐๑๓ พนักงานของบริษัททั่วไปๆ ในกรุงโซล ได้เปิดเครื่องคอมพิวเตอร์ที่ทำงานเพื่อเช็คอีเมล์ (e-mail) แต่อีเมล์นั้นกลายเป็น“Malicious Software” ซึ่งก็คือ โปรแกรมคอมพิวเตอร์ (software) ที่ถูกสร้างขึ้นมาโดยมีจุดมุ่งหมายเพื่อที่จะทำลายหรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์....ไม่นานหลังจากนั้น คอมพิวเตอร์กว่า ๔๘,๐๐๐ เครื่องในสถาบันการเงินสามแห่งและสถานีโทรทัศน์สามสถานีต่างก็เกิดอาการทำงานผิดปกติไปตามๆ กันบนจอภาพของเครื่องคอมพิวเตอร์เหล่านี้มีข้อความแสดงที่หน้าจอเหมือนกันทุกเครื่องว่า “กรุณาติดตั้งระบบปฏิบัติการในฮาร์ดดิสก์ของท่าน” (Please install an operating system on your hard disk) และในเวลาเดียวกันเครื่อง ATM ของธนาคารสามแห่งที่ถูกโจมตีก็ไม่สามารถทำงานได้เพราะ malware (ภายหลังถูกตั้งชื่อว่า “DarkSeoul” หรือ“กรุงโซลที่มืดมิด”) ได้ลบข้อมูลในฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่มีปัญหาเหล่านั้นหายไปหมด

๓.๗.๔ วันที่ ๑๗ พฤษภาคม ปี ๒๐๐๗ ประเทศเอสโทเนีย ถูกโจมตีด้วยไซเบอร์อย่างหนักโดยเฉพาะรัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่างๆ จนข้อมูลเสียหายพังยับเยิน

๓.๗.๕ เมื่อต้นเดือนกันยายน ปี ๒๐๐๗ ตึกเพนทากอน กระทรวงกลาโหม

สหรัฐอเมริกา และที่ทำการรัฐบาลของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีด้วยคอมพิวเตอร์ซึ่งมีต้นกำเนิดจากประเทศจีน ได้รับความเสียหายอย่างหนัก แต่รัฐบาลจีนได้ปฏิเสธข้อกล่าวหา

๓.๗.๖ วันที่ ๑๔ ธันวาคม ปี ๒๐๐๗ เว็บไซต์ของคณะกรรมการการเลือกตั้งกลางประเทศเกียร์กีซ (Kyrgyz) ถูกโจมตีอย่างหนักระหว่างการเลือกตั้งจนทำให้การเลือกตั้งโกลาหล ซึ่งบนเว็บไซต์ระบุชัดเจนว่า เว็บไซต์นี้ถูกโจมตีโดยองค์กรดรีม (Dream) แห่งเอสโทเนีย

๒.๘ การสัมมนาเกี่ยวกับสงครามไซเบอร์

ในงาน Defence & Security ๒๐๑๓ ซึ่งจัดขึ้นที่อิมแพคเมืองทองธานี กระทรวงกลาโหมเป็นเจ้าภาพ ได้มีการถกกันในหัวข้อ “สงครามไซเบอร์ สิ่งที่ท้าทายความร่วมมือในอนาคตของชาติอาเซียน” Dr.Marwan Jamal หัวหน้าฝ่ายเทคโนโลยีของมหาวิทยาลัยแห่งชาติกลาโหม ไอคอลเลจ ประเทศสหรัฐอเมริกา ได้รับเชิญมาบรรยายในหัวข้อ “สงครามไซเบอร์ เป็นอย่างไร?”

ดร.มาร์วัน เปิดประเด็นว่า การทำสงครามไซเบอร์นั้นสามารถเอาชนะฝ่ายตรงข้ามได้โดยที่ไม่ต้องสู้รบกันแบบเผชิญหน้าเหมือนในอดีต จึงทำให้เวลานี้เกิดความวิตกกังวลและปั่นป่วนไปทั่วโลก ตัวอย่างเช่น การทำสงครามสมัยก่อน ถ้าข้าศึกต้องการจะโจมตีระบบสื่อสารของฝ่ายเราก็อาจใช้วิธีทำลายระบบสื่อสาร ด้วยการลักลอบเข้ามาตัดสายเคเบิลหรือนำระเบิดมาทิ้ง จนระบบสื่อสารของเราใช้การไม่ได้ แต่ทุกวันนี้ข้าศึกในยุคสงครามไซเบอร์ อาจไม่จำเป็นต้องทำเช่นนั้น แค่เพียงหาทางโจมตีระบบคอมพิวเตอร์ของศูนย์บัญชาการของฝ่ายเรา เพื่อให้เกิดความสูญเสียหรือใช้การไม่ได้ เท่านี้ระบบการติดต่อสื่อสารก็พังยับไม่เป็นท่าแล้ว...นี่คือตัวอย่างรูปแบบการรบสมัยใหม่ที่เรียกว่า “สงครามไซเบอร์” ในสงครามไซเบอร์ อาจมีชาติหนึ่งชาติใดแฝงตัวอยู่เบื้องหลัง การโจมตีกันด้วยช่องทางนี้เกิดขึ้นทั่วโลกนับล้านครั้งต่อเดือน ฝ่ายที่โจมตีไม่จำเป็นต้องใช้ต้นทุนสูง แค่เชี่ยวชาญในระบบคอมพิวเตอร์และอินเตอร์เน็ต สามารถเจาะผ่านระบบรักษาความปลอดภัย จนสามารถเข้าถึงข้อมูลในคอมพิวเตอร์ของอีกฝ่ายได้ เขายกตัวอย่าง ผู้โจมตีบางรายอาจเลือกใช้วิธีรบกวนเรดาร์หรือระบบเตือนภัยของอีกฝ่าย ขโมย ทำลาย หรือ ดัดแปลงแก้ไขข้อมูลเพื่อให้เกิดความสับสน เข้าใจผิด ทั้งนี้ขึ้นอยู่กับสถานการณ์ หนึ่งในวิธีที่นิยมใช้กันมาก คือ โจมตีไปที่เซิร์ฟเวอร์ (server) หรือระบบ ปฏิบัติการซึ่งทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งแก่เครื่องคอมพิวเตอร์ จนเซิร์ฟเวอร์ทำงานหนักมากจนเครื่องร้อนจัด ไหม้หรือต้องปิดตัวเอง ใครก็ตามที่เคยคิดว่า เรื่องทำนองนี้คงมีแต่ให้อ่านเล่นเอาสนุก ในนิยายเหนือจริงทางวิทยาศาสตร์ หรือหนังแนวโลกเหนือจินตนาการของฮอลลีวูด นาทีนี้ต้องรีบคิดใหม่ เดี๋ยวนี้ข้าศึกในโลกแห่งสงครามไซเบอร์ยังสามารถพัฒนาวิธีการโจมตีแบบแปลกๆ เช่น สามารถส่งผ่านคำสั่งระยะไกล เข้าไปเปิดสวิตช์ หรือทำให้การแก้ไขตัวเซ็นเซอร์ต่างๆ ภายในเครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรือแม้แต่เซ็นเซอร์ภายในรถยนต์ ถูก

ขัดขวางจนก่อปัญหา เช่น สั่งเปิดตัวเซ็นเซอร์ เพื่อให้ไปทำลายแบตเตอรี่ของอุปกรณ์เหล่านั้น เป็นต้น “บางทีเขาอาจใช้วิธีโจมตีดาวเทียมของฝ่ายตรงข้าม โดยผู้โจมตีจะส่งสัญญาณเข้าไปปิดสวิตช์การทำงานของดาวเทียม หรือไม่ก็อาจใช้วิธีแฮกฯ เข้าไป ทำให้ภาพการติดตามเครื่องบินต่างๆ ทางเรดาร์ ซึ่งเป็นระบบการป้องกันภัยทางอากาศถูกคุกคามโดยทำให้ภาพเครื่องบินลำจริงหายไปจากจอเรดาร์ แล้วใส่ภาพลำปลอมที่ถูกสร้างภาพขึ้นมาไปปรากฏบนจอเรดาร์แทน” ปัญหาก็คือ ถ้าเป็นเครื่องบินรบของฝ่ายตรงข้ามที่ลักลอบเข้ามาโจมตีแต่เรดาร์จับภาพไว้ไม่ได้ เพราะภาพจริงถูกทำให้หายไปจากจอ กลายเป็นภาพปลอมขึ้นมาแทนที่ กรณีเช่นนี้ย่อมทำให้เกิดการตัดสินใจผิดพลาดอย่างมหันต์ ทั้งนี้เพราะหากต้องไปเจอกับ “มัลแวร์” (Malware) หรือโปรแกรมคอมพิวเตอร์ทุกชนิดที่มีจุดประสงค์ร้ายต่อระบบคอมพิวเตอร์และเครือข่าย บุกรุกเข้าไปในอุปกรณ์คอมพิวเตอร์เหล่านั้น โดยที่ผู้ใช้ไม่รู้ตัว ย่อมสร้างความเสียหายให้กับระบบคอมพิวเตอร์และเครือข่ายนั้นๆ ยกตัวอย่าง สมมติว่า ฝ่ายจู่โจมส่งผ่านมัลแวร์เข้าไป แล้วระบบของคอมพิวเตอร์ หรือโทรศัพท์มือถือสามารถทำการอัพเดทตัวเองได้ หากเกิดขึ้นกับในทางการทหาร จะมีความเสี่ยงสูงมากเพราะรูปแบบการจู่โจมในสงครามไซเบอร์ ตามตัวอย่างข้างต้นล้วนก่อให้เกิดผลกระทบต่อศักยภาพในการสู้รบ ระบบควบคุม หรือการออกคำสั่ง หรือไม่ก็ทำให้ข้อมูลที่ส่งกลับเกิดความผิดพลาดอย่างมหันต์

ดร.มาร์วัน สรุปว่า ทางแก้หนึ่งที่ได้ผล ก็คือ นอกจากต้องมีการอัพเดทข้อมูลต่างๆ ของฝ่ายเราเป็นประจำ นานาชาติต้องมีมาตรการเตรียมความพร้อม เพื่อรับมือกับการโจมตีทางไซเบอร์ มียุทธศาสตร์ที่ครอบคลุมสงครามไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม ถ้ามีโอกาส สงครามไซเบอร์ จะลงเอยอย่างไร ณ วันนี้คงไม่มีใครตอบได้ ที่ทำได้อย่างเดียวก็คือ อยู่กับมันอย่างทันเกม หรือรู้เท่าทัน (ข่าว นสพ.ไทยรัฐ : วันที่ ๒ ม.ค. ๕๘. (ออนไลน์). เข้าถึงได้จาก: http://www.thairath.co.th/content/382273,2558)

ยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

การเพิ่มขึ้นของการใช้ การโจมตีทางไซเบอร์ เป็นเครื่องมือทางการเมือง สะท้อนให้เห็นถึงแนวโน้มที่อันตรายต่อระดับความสัมพันธ์ระหว่างประเทศ ระบบข้อมูลที่อ่อนแอจะเป็นสิ่งที่กระตุ้นให้ตัวแสดงในระดับรัฐ และตัวแสดงที่ไม่ใช่รัฐ ได้มีโอกาสการโจมตีต่อประเทศสหรัฐอเมริกา และผลประโยชน์ของชาติ ในระหว่างความขัดแย้ง กระทรวงกลาโหมต้องยอมรับว่า ประเทศฝ่ายตรงข้ามที่มีศักยภาพยังคงพยายามทำลายเป้าหมายในสหรัฐหรือโครงสร้างพื้นฐานวิกฤตและเครือข่ายทางทหาร เพื่อให้ตัวเองได้เปรียบทางยุทธศาสตร์ นอกเหนือจากการโจมตีดังกล่าวแล้ว ฝ่ายตรงข้ามยัง

พยายามทำลาย ระบบควบคุมทางอุตสาหกรรม (Industrial Control System :ICS) บนเครือข่ายสาธารณะเพื่อให้มีผลกระทบต่อความปลอดภัยหรือเข้าไปในเครือข่ายเพื่อบิดเบือนข้อมูลด้านสุขภาพเพื่อให้มีผลต่อความเป็นอยู่ของประชาชน การโจมตีทางไซเบอร์เพื่อทำให้ยุ่งเหยิง บิดเบือน หรือทำลาย ย่อมก่อให้เกิดความเสี่ยงที่สำคัญต่อระบบเศรษฐกิจ และความมั่นคงของชาติของสหรัฐฯ

เพื่อลดความเสี่ยงและปกป้องผลประโยชน์ของประเทศ ในสถานการณ์ปัจจุบันและอนาคต กระทรวงกลาโหม ได้กำหนดเป้าหมายทางยุทธศาสตร์ และวัตถุประสงค์เฉพาะสำหรับการดำเนินกิจกรรมและภารกิจทางไซเบอร์ ดังนี้

ประเด็นยุทธศาสตร์ที่ ๑ สร้างและบำรุงรักษา กำลังเตรียมพร้อมและขีดความสามารถในการปฏิบัติการทางไซเบอร์

เพื่อให้การปฏิบัติการเป็นไปอย่างมีประสิทธิภาพ กระทรวงกลาโหมมีความต้องการกำลังเจ้าหน้าที่ และบุคลากรพลเรือนซึ่งได้รับการฝึกตามมาตรฐาน มีความพร้อมและมีความสามารถทางเทคนิคเป็นอย่างดี โดยในปี ค.ศ.๒๐๑๓ กระทรวงกลาโหมได้จัดตั้งหน่วยปฏิบัติภารกิจทางไซเบอร์ (Cyber Mission Force :CMF) ขึ้น

ประเด็นยุทธศาสตร์ที่ ๒ ป้องกันเครือข่ายด้านข้อมูลข่าวสาร รักษาความลับของข้อมูลและลดความเสี่ยงในการปฏิบัติภารกิจของกระทรวงกลาโหม

เนื่องจากกระทรวงกลาโหม ไม่สามารถป้องกันการโจมตีทางไซเบอร์ต่อเครือข่ายที่กว้างขวางของประเทศได้ทั้งหมด กระทรวงฯ จึงต้องกำหนดขั้นตอนในการระบุความรุนแรง, กำหนดลำดับความสำคัญ และป้องกันในส่วนที่ข้อมูลและเครือข่ายที่สำคัญที่สุดก่อน

ประเด็นยุทธศาสตร์ที่ ๓ เตรียมพร้อมสำหรับป้องกันประเทศสหรัฐอเมริกาและผลประโยชน์ที่สำคัญยิ่งของสหรัฐฯ จากการโจมตีทางไซเบอร์

กระทรวงกลาโหม จะต้องทำงานร่วมกับหน่วยงานอื่นของภาครัฐ เอกชน และชาติพันธมิตร เพื่อป้องกัน และถ้าจำเป็นต้องเอาชนะการโจมตีทางไซเบอร์ ต่อผลประโยชน์ที่สำคัญยิ่งของประเทศ โดยการพัฒนาการ ขีดความสามารถทางด้านข่าวกรอง การแจ้งเตือน การปฏิบัติการเพื่อลดความเสียหายต่อการโจมตีทางไซเบอร์ที่มุ่งร้ายต่อผลประโยชน์ของชาติพร้อมกับการใช้มาตรการทางกฎหมายและทางนโยบายของประเทศ

ประเด็นยุทธศาสตร์ที่ ๔ สร้างและรักษาทางเลือกทางไซเบอร์ที่หลากหลายและวางแผนที่จะใช้ทางเลือกเหล่านั้น เพื่อควบคุมการขยายตัวของความขัดแย้งและเพื่อควบคุมสถานการณ์ของความขัดแย้งในทุกระดับ

ในระหว่างที่เกิดความตึงเครียดระหว่างประเทศสูงหรือมีการแสดงท่าทีเป็นปฏิปักษ์อย่างชัดเจน กระทรวงกลาโหมจะสามารถจัดเตรียมทางเลือกหลายๆ ทางเลือก เพื่อจัดการกับการขยายตัว

ของความขัดแย้ง นำเสนอต่อประธานาธิบดีเพื่อพิจารณา เมื่อได้รับคำสั่งฯ กระทรวงฯ สามารถใช้ปฏิบัติการทางไซเบอร์ เพื่อขัดขวางเครือข่ายในการควบคุมและสั่งการของข้าศึก โครงสร้างพื้นฐานที่สำคัญทางทหารและขีดความสามารถของอาวุธได้ทันที

ประเด็นยุทธศาสตร์ทหารที่ ๕ สร้างและรักษาความเป็นพันธมิตรที่เข้มแข็งและประเทศคู่เจรจาระหว่างประเทศ เพื่อร่วมกันป้องกันการคุกคามร่วมและเพื่อความมั่นคงและความมีเสถียรภาพระหว่างประเทศ

การปฏิบัติตามภารกิจทางด้านไซเบอร์ จำเป็นจะต้องได้รับความร่วมมือจากมิตรประเทศและประเทศคู่เจรจา เพื่อเสริมสร้างขีดความสามารถในด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกันทางไซเบอร์ โดยเฉพาะการปกป้องในพื้นที่ ที่เป็นผลประโยชน์ของสหรัฐ

งานวิจัยที่เกี่ยวข้อง

พลตรี สุชาติ ผ่องพุฒิ ได้วิจัยเรื่อง แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย ผลการวิจัยพบว่า ภัยคุกคามที่กองทัพไทยให้ความสำคัญมี ๔ รูปแบบ ขอบเขตการรองรับสงคราม ไซเบอร์ในมุมมองของกองทัพตามระดับภัยคุกคามแบ่งเป็น ๓ ระดับ กำหนดกรอบในการดำเนินการรองรับสงครามไซเบอร์ในอนาคตไว้ ๔ ด้าน แบ่งกรอบระยะเวลาออกเป็น ๓ ระยะ เสนอแนะให้ปรับภารกิจในภาพรวมของหน่วยในกองทัพเพื่อการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกเป็น ๒ รูปแบบคือ งานสนับสนุนการรบหลัก และงานในสายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ นำเสนอโครงสร้างหน่วยงานของกองทัพที่จะรองรับสงครามไซเบอร์อย่างเป็นรูปธรรมต่อไป

พลเรือตรี วิโรจน์ ธันวรักษ์กิจ ได้วิจัยเรื่อง แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย ผลการวิจัยพบว่า การดำเนินการในภาพรวมยังขาดการบูรณาการงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ บุคลากรมีจำนวนจำกัด เสนอแนะให้ สมช. เป็นหน่วยหลักรับผิดชอบการดำเนินการในภาพรวม เสนอแนะให้ตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ รวมทั้งการดำเนินการด้านอื่นๆ ควบคู่กันไป ผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต ผลักดันหน่วยงาน National CERT ให้เป็น ศูนย์ปฏิบัติการระดับประเทศ ผลักดันให้เป็นวาระแห่งชาติเร่งด่วน จะเป็นประโยชน์โดยตรงกับประเทศทำให้มีศักยภาพและขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

นาวาอากาศเอก รศ.ดร.ประสงค์ ปราณีตพลกรัง ได้วิจัยเรื่อง แผนยุทธศาสตร์

การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ ผลการวิจัยพบว่า สาเหตุหลักของการเกิดภัยคุกคามด้านไซเบอร์ของกองทัพอากาศเกิดจากปัจจัยภายใน อาทิ กำลังพลที่รู้เท่าไม่ถึงการณ์และขาดความตระหนักรู้ และสาเหตุรองคือระบบหรือเทคโนโลยีที่ใช้งานเช่น ช่องโหว่ในซอฟต์แวร์ ไวรัสหรือเวิร์ม ต่อมาเป็นสาเหตุจากปัจจัยภายนอกเช่นเกิดจากแฮกเกอร์ เกิดจากการก่ออาชญากรรมและเกิดจากการก่อการร้าย นอกจากนั้น ในงานวิจัยนี้ ยังได้ค้นพบ ๔ ยุทธศาสตร์ และ ๑๕ แผนงานวิจัยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดี งานวิจัยนี้ ยังได้ค้นพบ ดัชนีสภาพความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ สำหรับกองทัพอากาศ โดยอิง ITU & ABI Research และ ISO-๒๗๐๓๒ ประกอบกับการทำการสนทนากลุ่มกับผู้เชี่ยวชาญ ได้ดัชนีจำนวน ๗ ด้าน ผลของการวิจัย สามารถนำไปใช้เป็นแนวทางกำหนดยุทธศาสตร์ และนโยบายเชิงรุกของกองทัพอากาศด้านความมั่นคงปลอดภัยทางไซเบอร์ได้

นาวาอากาศโท จตุชัย แพงจันทร์ ได้วิจัยเรื่อง รูปแบบการปฏิบัติการสงครามไซเบอร์ และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง ผลการวิจัยพบว่า แนวทางมีความเหมาะสมที่จะนำไปใช้เพื่อพัฒนาบุคลากร การจัดองค์กร และการพัฒนาขีดความสามารถของระบบอาวุธยุทโธปกรณ์ ให้มีความพร้อมที่จะปฏิบัติการสงครามไซเบอร์ได้ทุกรูปแบบและสามารถรองรับเทคโนโลยีที่ใช้ระบบเครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพ โดยกำหนดให้มีการเตรียมบุคลากรให้เกิดความพร้อมอย่างเป็นขั้นตอน รวมถึงวงรอบในการฝึกเพื่อให้บุคลากรเกิดทักษะในการปฏิบัติงาน อีกทั้งได้ชี้ให้เห็นแนวทางการพัฒนาศักยภาพด้านสงครามไซเบอร์ที่จะทำให้กองทัพอากาศมีความสามารถในระดับ “Competent Capability” คือ มีความสามารถและความรู้เพียงพอที่จะปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ และมีความยั่งยืน บนพื้นฐานการพึ่งพาตนเอง

นาวาอากาศโท วัชรพงศ์ ธรรมรักษ์ ได้วิจัยเรื่อง ตัวแบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) สำหรับกองทัพอากาศ มีเนื้อหาโดยสรุปคือ จากการวิจัยพบว่า ระดับความพร้อมด้านบุคลากรของการรักษาความมั่นคงปลอดภัย เครือข่ายข้อมูลสารสนเทศต่างๆ มีค่าน้อยที่สุด และระดับความเสี่ยงด้านบุคลากรก็มีค่าสูงที่สุด ประกอบกับข้อมูลที่ได้รับพบว่าบุคลากรของกองทัพอากาศ ส่วนใหญ่ร้อยละ ๙๖ ไม่เคยเข้ารับการฝึกอบรมด้านการรักษาความมั่นคงปลอดภัยของเครือข่ายข้อมูลสารสนเทศเลย ดังนั้น การที่กองทัพอากาศจะพัฒนาไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) ได้อย่างมีประสิทธิภาพและสมบูรณ์แบบนั้น กองทัพอากาศควรให้ความสนใจในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยระดับสากล ISO27001 ผู้บังคับ บัญชาทุกระดับต้องให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

และที่สำคัญต้องสร้างความตระหนักให้บุคลากรในทุกหน่วยงาน ได้รับรู้ถึงกระบวนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ถูกต้องควรจัดให้มีการฝึกอบรมบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศ เพื่อให้มีความรู้ มีทักษะ มีความชำนาญและมีความสามารถในการรับมือกับเหตุการณ์ความเสี่ยง และภัยคุกคามด้านสารสนเทศต่างๆ ที่อาจจะเกิดขึ้นในอนาคตได้

สรุป

๑. สรุปแนวความคิด ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศขององค์กรและองค์กรสมัยใหม่

องค์กรเป็นกระบวนการ เมื่อมีการจัดองค์กรก็ต้องนำเทคนิคการบริหารจัดการมาใช้ การบริหารเป็นส่วนหนึ่งของการจัดการองค์กรที่เหมาะสมที่สุดคือ องค์กรที่มีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้นๆ ซึ่งรวมถึงสภาพภูมิศาสตร์ วัฒนธรรม ค่านิยม ความเชื่อ การสนับสนุน และความต้องการของสมาชิกในองค์กรนั้นด้วย องค์กรสมัยใหม่ต้องเป็นองค์การแห่งการเรียนรู้ (Learning Organization) ซึ่งจะต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง ๕ ระบบขององค์การแห่งการเรียนรู้อันได้แก่ การเรียนรู้ (Learning) องค์การ (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology) เนื่องจากการบริหารเป็นกระบวนการทำงานให้สำเร็จโดยใช้บุคคลอื่น พฤติกรรมของบุคคลในองค์การจึงมีความสำคัญต่อการเพิ่มผลผลิต และประสิทธิผลขององค์การ หากเข้าใจพฤติกรรมของมนุษย์ในองค์การอย่างถ่องแท้จะสามารถนำไปใช้ในการเพิ่มผลผลิตและความพึงพอใจของบุคลากร อันนำไปสู่การเพิ่มประสิทธิผลขององค์การในภาพรวม การบริหารจัดการเป็นสิ่งที่สำคัญต่อการปฏิบัติงาน ถ้าต้องการให้การบริหารจัดการและการปฏิบัติงานเกิดประสิทธิภาพสูงสุด สิ่งที่ทุกองค์การควรนำมาปรับใช้ในการบริหาร คือ การวางแผน (Planning) การจัดองค์การ (Organizing) การบังคับบัญชาสั่งการ (Commanding) การประสานงาน (Coordinating) และการควบคุม (Controlling)

ทฤษฎีการบริหารของ Henri Fayol การบริหารของ Dr.William Edwards Deming และกระบวนการบริหารของ Gulick L. and Urwick J. ต่างได้กล่าวถึง อำนาจหน้าที่และความรับผิดชอบของทุกส่วนที่เกี่ยวข้อง ให้ความสำคัญต่อเป้าหมายที่สำคัญขององค์การ คือ ความเป็นระเบียบ ความมั่นคง ความคิดริเริ่ม และความสามัคคี ผู้บริหารจะต้องมีคุณลักษณะพร้อมความสามารถทางร่างกาย จิตใจ ไหวพริบ การศึกษาหาความรู้ เทคนิคในการทำงานและประสบการณ์ต่างๆ ทฎษฎีที่เหมาะสมที่ควรนำมาใช้ในหน่วยงานของทหารคือ ทฤษฎีการบริหารของ Dr.William Edwards Deming คือ Plan-Do-Check-Action เนื่องจากเป็นกระบวนการที่สั้นกระทัดรัด มีการวางแผนและตรวจสอบตนเองทุกขั้นตอน ทำให้ผู้ปฏิบัติมีการวางแผน ป้องกันปัญหาที่ไม่ควรเกิด

ช่วยลดความสับสนในการทำงาน ลดการใช้ทรัพยากรมากหรือน้อยเกินความพอดี ลดความสูญเสียในรูปแบบต่างๆ ทำให้การปฏิบัติงานมีความรัดกุมขึ้น และแก้ไขปัญหาได้อย่างรวดเร็วก่อนจะลุกลาม การตรวจสอบที่นำไปสู่การแก้ไขปรับปรุง ทำให้ปัญหาที่เกิดขึ้นแล้วไม่เกิดซ้ำ หรือลดความรุนแรงของปัญหา ถือเป็นการนำความผิดพลาดมาใช้ให้เกิดประโยชน์

การนำระบบสมรรถนะมาใช้ในการบริหารองค์กรนับว่ามีประโยชน์อย่างยิ่งในยุคปัจจุบัน เพราะเป็นการสร้างบุคลากรให้มีความรู้ ความสามารถ ทัศนคติ ที่จะปฏิบัติหน้าที่ให้ประสบความ สำเร็จและเกิดประสิทธิภาพกับองค์กรอย่างสูงสุด และผู้บริหารองค์กรจำเป็นต้องมีสมรรถนะด้านการบริหารอันประกอบด้วย การมีวิสัยทัศน์ การวางแผน ภาวะผู้นำ การแก้ปัญหาและการตัดสินใจ สุดท้ายต้องมีความสามารถในการบริหารความเปลี่ยนแปลงที่อาจเกิดขึ้นได้ทุกเวลาอีกด้วย

สภาพแวดล้อมในการทำงานเป็นสิ่งสำคัญที่จะทำให้บรรยากาศการทำงานภายในองค์มีประสิทธิภาพ เป็นการรับรู้ของบุคคลในองค์กร เชื่อมโยงกันระหว่างปัจจัยภายในและปัจจัยภายนอก ซึ่งแต่ละองค์กรจะมีความแตกต่างกันและเป็นสิ่งที่ส่งผลต่อพฤติกรรม ความรู้สึก ค่านิยม ในการทำงานของบุคคลในองค์กร ประกอบด้วย โครงสร้างการทำงานที่ดี มีระบบรางวัลตอบแทนที่เหมาะสม มีความเป็นอิสระในการทำงาน มีความอบอุ่นมีการสนับสนุนช่วยเหลือกันและกัน มีการยอมรับความขัดแย้ง ยอมรับฟังความคิดเห็นผู้อื่น และสุดท้ายต้องมีความรักในหมู่คณะด้วย

๒. สรุปการจัดการความรู้และการบริหารความเสี่ยง

เพื่อให้การพัฒนาคน พัฒนางาน พัฒนาองค์กรให้มีประสิทธิภาพ องค์กรจะต้องมีการจัดการความรู้ (Knowledge Management) เพื่อรวบรวมความรู้ที่เป็นประโยชน์กับองค์กรหรือบุคคลและนำความรู้นั้นมาจัดการความรู้อย่างเป็นระบบอาจใช้เทคโนโลยีสารสนเทศมาช่วยในการจัดการความรู้หรือไม่ก็ได้ สำหรับในภาครัฐ (public Sector) มีความต้องการองค์ความรู้ ทั้งองค์ความรู้ภายใน (Internal) และองค์ความรู้ภายนอกองค์กร (External) มาใช้เพื่อประกอบการตัดสินใจและเพื่อการปรับปรุงการให้บริการของหน่วยงานภาครัฐ กรอบการบริหารความเสี่ยงองค์กรนั้นสามารถสะท้อนให้เห็นถึงนโยบายการบริหารจัดการและการกำกับดูแลกิจการของแต่ละองค์กร โดยหากมีการบริหารความเสี่ยงอย่างมีประสิทธิภาพ จะส่งผลให้สามารถบรรลุวัตถุประสงค์องค์กรทั้งในเชิงประสิทธิภาพและประสิทธิผลของงาน ผลที่ได้จากการประเมินความเสี่ยง คือ ข้อแนะนำเกี่ยวกับวิธีป้องกันที่ดีที่สุด เพื่อปกป้องความลับ ความคงสภาพ และความพร้อมใช้งาน และยังคงสามารถทำงานและให้บริการได้ตามปกติ ดังนั้นทุกองค์กรควรจะจัดทำแผนบริหารความเสี่ยงเพื่อนำมาใช้ในการบริหารองค์กรให้มีประสิทธิภาพอีกทางหนึ่งด้วย

๓. สรุปแนวคิดเกี่ยวกับการบูรณาการองค์กร

การบริหารราชการแบบบูรณาการ” คือ การบริหารที่ทุกหน่วยงาน ทำงานแบบ

มุ่งเน้นผลงาน (Result) ตามยุทธศาสตร์เป็นหลัก เป็นการทำงานหลายหน่วยงาน โดยอาศัยความเชี่ยวชาญและความชำนาญการของแต่ละหน่วยงานที่แตกต่างกันเฉพาะด้าน ทำงานภายใต้เป้าหมายและวัตถุประสงค์หลักของยุทธศาสตร์เดียวกัน โดยร่วมกันคิด ร่วมกันทำงาน โดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุผลตามยุทธศาสตร์ มุ่งสู่ผลสำเร็จและ เป้าหมายของงานร่วมกัน เพื่อก่อให้เกิดความประหยัด เสริมสร้างประสิทธิผลและ ประสิทธิภาพชองการดำเนินงานเป็นหลัก ทั้งในลักษณะชองการทำงานข้ามกระทรวงกระทรวง เดียวกันแต่ต่างกรม หรือกรมเดียวกันแต่ต่างกอง รวมทั้งการมีส่วนร่วมของภาคเอกชน และภาคประชาชนที่เกี่ยวข้องมาร่วมในการทำงานกับภาครัฐในระบบเครือข่าย (Network)

๔. สรุปแนวคิดเกี่ยวกับสงครามสารสนเทศ และ สงครามไซเบอร์

แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ สำหรับปี ๒๐๑๖ โดย ISF ระบุทิศทางเชิงลบด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ข้อสรุปหลักๆ ทั้งหมด ๓ ประเด็น ได้แก่ ๑. ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป ๒. ความเชื่อมั่นในระบบหรือโซลูชั่นการรักษาความมั่นคงปลอดภัยในแนวทางที่ยอมรับโดยทั่วไปเสื่อมสลาย ต้องคิดหาแนวทางใหม่ ๓. ความล้มเหลวต่อการรักษาระดับการให้บริการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น องค์กรทั่วโลกต้องปรับกระบวนทัศน์ให้มีความสามารถในการปรับตัวเพื่อรองรับการเปลี่ยนแปลง และผลกระทบที่อาจจะเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่

ภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามมีการเปลี่ยนแปลงไปจากเดิมอย่างมาก ตลอดจนมีรูปแบบในการโจมตีเป้าหมายที่หลากหลาย มีรูปแบบมากมายในการปฏิบัติโดยไม่ต้องใช้กำลังพลมากมาย จนทำให้ผู้เชี่ยวชาญและผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามแทบไม่ทัน ดังนั้นแนวความคิดและแนวทางในการป้องกันระบบและทรัพย์สินขององค์กรให้ได้ประสิทธิผล (effectiveness) จำเป็นอย่างยิ่งที่จะต้องปรับความคิดและปรับกลยุทธ์ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป องค์กรต้องเตรียมตัวรับมือกับภัยคุกคามใหม่ๆ ที่มาทางไซเบอร์ โดยผ่านช่องทาง Social Network, Mobile Devices หรือ Cloud Services ต่างๆ ต้องมีการวางแผนป้องกันจากภัยจากสงครามไซเบอร์ ควรนำระบบมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ ซึ่งเป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศ เป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพ เป็นระบบที่อ้างอิงตัวแบบ PDCA (Plan, Do, Check, และ Act) ซึ่งเป็นโครงสร้างระบบบริหารที่เป็นสากลที่ใช้กันทั่วโลก นอกจากนั้นถ้าเราต้องการให้ระบบขององค์กรมั่นคงปลอดภัย เราควร “ลดเวลาในการตรวจจับลง” (decrease Detect time) และ “ลดเวลาในการตอบสนองลง” (decrease React time) ด้วยเช่นกัน ดังนั้นปัจจัยที่เราต้องนำมาพิจารณาไตร่ตรองอย่างรอบคอบในการวางแผนกลยุทธด้านความมั่นคงปลอดภัย (Security Strategy) ได้แก่ Protection (การป้องกัน) Detection (การตรวจจับ) Reaction (การตอบสนอง) และTime (เวลา) สำหรับการป้องกันอีกทางหนึ่งคือ ต้องมี

การอัพเดทข้อมูลต่างๆ ของฝ่ายเราเป็นประจำ นานาชาติต้องมีมาตรการเตรียมความพร้อม เพื่อรับมือกับการโจมตีทางไซเบอร์ มียุทธศาสตร์ที่ครอบคลุมสงครามไซเบอร์ แสวงหาความร่วมมือกับชาติอื่นๆ ในอาเซียนด้วยกัน หมั่นพัฒนาตัวเองจนถึงระดับที่เท่าเทียม หรือเหนือกว่าพวกแฮกเกอร์ทั้งหลายและควรดึงเอกชนเข้ามามีบทบาทพัฒนาร่วม

การแก้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศนั้น ควรมีมุมมอง ๓ ด้าน (PPT Concept) ได้แก่ People, Process and Technology การปรับกระบวนการโดยการปฏิบัติตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๑๓ เป็นการแก้ปัญหาที่ Process และ Technology แต่ปัจจัยสำคัญอยู่ที่ “มนุษย์” หรือ “People” ดังนั้นการเตรียมความพร้อมของผู้ใช้ระบบสารสนเทศทั่วไปและการให้ความรู้ด้านภัยสารสนเทศ จึงเป็นเรื่องจำเป็นที่องค์กรต้องทำเป็นประจำทุกปี เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารทั้งระดับกลางและระดับสูงได้ตระหนักรู้และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติ มีความพร้อมต่อการรับมือ “Incident” ต่างๆ ที่จะเกิดขึ้น นอกจากนี้กลไกกระบวนการและเทคนิคในการตรวจจับความผิดปกติในระบบแบบ Real-Time ก็มีความจำเป็นเช่นกัน เพราะฉะนั้นเราจึงต้องเตรียมพร้อมกับเหตุการณ์ที่ไม่พึงประสงค์อยู่ตลอดเวลา ก็จะช่วยให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของเรามีประสิทธิผลมากขึ้นโดยลำดับ สามารถทำให้องค์กรมี “Cyber Resilience” และ “Business Resilience” ในที่สุด

แนวโน้มในอนาคต ภัยคุกคามด้านไซเบอร์ (cyber threat) นับวันจะทวีความเข้มข้น และความรุนแรงมากยิ่งขึ้น ดังจะเห็นได้ว่า ที่ผ่านมามีเหตุการณ์การโจรกรรมทางไซเบอร์เกิดขึ้นบ่อย ครั้งและต่อเนื่อง และมีแนวโน้มที่จะรุนแรงขึ้นเรื่อยๆ องค์กรสำคัญในหลายประเทศได้ถูกผู้ก่อเหตุทางไซเบอร์เจาะระบบและโจรกรรมข้อมูล เพื่อนำไปใช้หาประโยชน์ในทางมิชอบ การโจมตีทางไซเบอร์มีการยกระดับถึงขั้นการทำสงครามทางไซเบอร์ ด้วยเหตุนี้หลายประเทศเริ่มให้ความสำคัญกับการรักษาความปลอดภัยไซเบอร์ มีการกำหนดมาตรฐานระบบบริหารความมั่งคนปลอดภัยทางสารสนเทศ รวมถึง มีการรวมกลุ่มความร่วมมือเพื่อจัดการกับภัยไซเบอร์อย่างจริงจัง

๕. สรุปยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

เพื่อลดความเสี่ยงและปกป้องผลประโยชน์ของประเทศ ในสถานการณ์ปัจจุบันและอนาคต กระทรวงกลาโหม ได้กำหนดเป้าหมายทางยุทธศาสตร์ โดยกำหนดประเด็นยุทธศาสตร์ไว้ดังนี้

ประเด็นยุทธศาสตร์ที่ ๑ สร้างและบำรุงรักษา กำลังเตรียมพร้อมและขีดความสามารถในการปฏิบัติการทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๒ ป้องกันเครือข่ายด้านข้อมูลข่าวสาร รักษาความลับของ

ข้อมูล และลดความเสี่ยงในการปฏิบัติภารกิจของกระทรวงกลาโหม

ประเด็นยุทธศาสตร์ที่ ๓ เตรียมพร้อมสำหรับป้องกันประเทศสหรัฐอเมริกาและผลประโยชน์ที่สำคัญยิ่งของสหรัฐฯ จากการโจมตีทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๔ สร้างและรักษาทางเลือกทางไซเบอร์ที่หลากหลายและวางแผนที่จะใช้ทางเลือกเหล่านั้น เพื่อควบคุมการขยายตัวของความขัดแย้งและเพื่อควบคุมสถานการณ์ของความขัดแย้งในทุกระดับ

ประเด็นยุทธศาสตร์ทหารที่ ๕ สร้างและรักษาความเป็นพันธมิตรที่เข้มแข็งและประเทศคู่เจรจาระหว่างประเทศ เพื่อร่วมกันป้องกันการคุกคามร่วมและเพื่อความมั่นคงและความมีเสถียรภาพระหว่างประเทศ

๖. สรุปงานวิจัยที่เกี่ยวข้อง

ภัยคุกคามด้านไซเบอร์ที่กองทัพไทยให้ความสำคัญมี ๔ รูปแบบ ขอบเขตการรองรับสงครามไซเบอร์ในมุมมองของกองทัพตามระดับภัยคุกคามแบ่งเป็น ๓ ระดับ กำหนดกรอบในการดำเนินการรองรับสงครามไซเบอร์ในอนาคตไว้ ๔ ด้าน แบ่งกรอบระยะเวลาออกเป็น ๓ ระยะ เสนอแนะให้ปรับภารกิจในภาพรวมของหน่วยในกองทัพเพื่อการปฏิบัติการสงครามไซเบอร์ โดยแยกการดำเนินการออกเป็น ๒ รูปแบบคือ งานสนับสนุนการรบหลัก และงานในสายเทคนิคหรือผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของกองทัพ นำเสนอโครงสร้างหน่วยงานของกองทัพที่จะรองรับสงครามไซเบอร์อย่างเป็นรูปธรรมต่อไป

แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย พบว่าการดำเนินการในภาพรวมยังขาดการบูรณาการงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ บุคลากรมีจำนวนจำกัด เสนอแนะให้ สมช. เป็นหน่วยหลักรับผิดชอบการดำเนินการในภาพรวม เสนอแนะให้ตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต ผลักดันหน่วยงาน National CERT ให้เป็นศูนย์ปฏิบัติการระดับประเทศ

บทที่ ๓
การดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของชาติ

ประเทศไทยมุ่งมั่นที่จะเดินหน้าสู่ยุคดิจิตอลด้วยการปรับใช้เทคโนโลยีที่ทันสมัยเพื่อพัฒนาศักยภาพทางด้านเศรษฐกิจของประเทศ ภายใต้โมเดล Thailand ๔.๐ ซึ่งมุ่งเน้นการสร้างสรรค์นวัตกรรมทางด้านเทคโนโลยีและการพัฒนาระบบดิจิตอลเพื่อปรับปรุงคุณภาพชีวิต กำลังการผลิตและประสิทธิภาพการทำงาน โดยมีการปรับใช้เทคโนโลยีดิจิตอลที่หลากหลาย เช่น Internet of Things (IOT), เทคโนโลยีคลาวด์ (Cloud), บิ๊กดาต้า (Big Data) และระบบวิเคราะห์ข้อมูลชั้นสูง (Analytics) ๑ แต่ต้องระมัดระวังในเรื่องภัยคุกคามด้านไซเบอร์ เนื่องจากปัจจุบันการเติบโตและความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชากรในประเทศไทยเพิ่มขึ้นอย่างก้าวกระโดด จึงทำให้ความเสี่ยงด้านภัยคุกคามไซเบอร์มีสูงขึ้นหลายเท่าตัวและจะเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศอย่างหลีกเลี่ยงไม่ได้ โดยภัยคุกคามรูปแบบใหม่นี้เป็นภัยคุกคามที่มีรูปแบบผสมซับซ้อน ทั้งในมิติของสังคม เศรษฐกิจ การเมือง และการทหาร ดังนั้นการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสมดุลกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ที่เข้มแข็ง

กระทรวงกลาโหม

กระทรวงกลาโหม ซึ่งมีภารกิจหลักด้านความมั่นคงของชาติ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๘ ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง ๔ ปี คือ พ.ศ.๒๕๕๘-๒๕๖๒ โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ ๓ ประเด็นดังนี้

๑. ประเด็นยุทธศาสตร์การป้องกันเชิงรุกสำหรับการปฏิบัติการในมิติของกองทัพไทย การใช้พลังอำนาจทางไซเบอร์กองทัพไทย เพื่อปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้าม ทั้งที่เป็นรัฐไม่ใช่รัฐและสนับสนุนโดยรัฐ ตลอดจนกลุ่มบุคคลหรือบุคคลใดๆที่อาจเป็นภัยคุกคามทางไซเบอร์และมีความมุ่งหมายในการลดทอน ขัดขวาง ระงับ ยับยั้งหรือรบกวน ความได้เปรียบในมิติไซเบอร์ของกองทัพไทย โดยจะมุ่งเน้นไปที่การปฏิบัติเชิงรุก ในลักษณะจำกัดและการตอบโต้อย่างรวดเร็วในกรณีถูกโจมตีทางไซเบอร์ ทั้งนี้เพื่อให้การสร้างความได้เปรียบกับฝ่ายตรงข้ามตั้งแต่สภาวะปกติและสร้างความตระหนักรู้ทางไซเบอร์ที่จะนำไปสู่การตัดสินใจคอร์ดระดับผู้บังคับบัญชาให้เท่าทันต่อสถานการณ์ต่างๆ

๒. ประเด็นยุทธศาสตร์การผนึกกำลังป้องกันประเทศสำหรับการปฏิบัติการในมิติไซ

เบอร์ของกองทัพไทย การสร้างความร่วมมือและบูรณาการขีดความสามารถในการปฏิบัติการในมิติไซเบอร์ของทุกภาคส่วนภายในประเทศเข้าด้วยกันอย่างเป็นระบบ ด้วยการมีแผนรองรับ ตั้งแต่สภาวะปกติ เพื่อแก้ไขข้อจำกัดของกองทัพไทยและชดเชยอำนาจกำลังรบของกองทัพไทยด้านการปฏิบัติในมิติไซเบอร์ที่มีอยู่อย่างจำกัด เพื่อให้สามารถปฏิบัติหน้าที่ในการป้องกันประเทศได้อย่างมีประสิทธิภาพหรือจะต้องมีการเตรียมการและต้องทำอย่างต่อเนื่อง ทั้งในยามปกติในยามสงคราม อีกทั้งยังรวมถึงการใช้พลังอำนาจทางไซเบอร์ของกองทัพไทย ในการสนับสนุนรัฐบาลในด้านการรักษาความมั่นคงภายในและการรักษาความสงบเรียบร้อยภายในประเทศในทุกมิติเพื่อให้เกิดความมีเสถียรภาพและความมั่นคงของประเทศโดยรวม

๓. ประเด็นยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย การใช้พลังอำนาจทางไซเบอร์กองทัพไทย ในการเสริมสร้างความร่วมมือกับประเทศเพื่อนบ้านประเทศสมาชิกอาเซียนและมิตรประเทศ ทั้งในระดับภูมิภาคและระดับโลก หรือมุ่งเน้นไปที่การสร้างความร่วมมือ เพื่อการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ การสร้างบรรยากาศความเป็นมิตร เพื่อลดเงื่อนไขที่จะนำไปสู่ความขัดแย้งและการควบคุมไม่ให้เกิดความขัดแย้งขยายวงกว้างจนไม่สามารถควบคุมได้หรือยุติความขัดแย้งได้อย่างสันติ เพื่อสนับสนุนรัฐบาลในการสร้างความร่วมมือระหว่างประเทศทั้งในระดับทวิภาคีและระดับพหุภาคี และได้จัดทำแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหมพ.ศ.๒๕๖๐-๒๕๖๔ ๘ รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหมที่ชัดเจน และมีการกำกับดูแลให้มีความสอดคล้อง ตามยุทธศาสตร์ไซเบอร์ป้องกันประเทศกระทรวงกลาโหม

ในระดับเหล่าทัพ กองบัญชาการกองทัพไทย ได้จัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ. ๒๕๕๘ ๑๐ เช่นเดียวกัน เพื่อให้กองทัพไทยมีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ ทั้งเชิงรับและเชิงรุกตั้งแต่สภาวะปกติ ตลอดจน สามารถบูรณาการและให้การสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ โดยได้กำหนดประเด็นยุทธศาสตร์ทหารสำหรับการปฏิบัติการทางทหารในมิติไซเบอร์เพื่อใช้เป็นกรอบแนวทางในการดำเนิน ให้สามารถบรรลุวัตถุประสงค์ทางการทหารที่ตั้งไว้แยกเป็น ๓ ประเด็นยุทธศาสตร์ได้แก่ยุทธศาสตร์การป้องกันเชิงรุกยุทธศาสตร์การผนึกกำลังป้องกันประเทศและยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคง ประเด็นยุทธศาสตร์ ได้แก่ ยุทธศาสตร์การป้องกันเชิงรุกยุทธศาสตร์การผนึกกำลังป้องกันประเทศและยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคง

กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ได้มีการจัดตั้งหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นที่เรียบร้อย โดยแบ่งการดำเนินการเป็น ๒ ส่วนคือส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) และส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) ซึ่งเป็นการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมในปัจจุบัน ดังนี้

ตารางที่ ๓-๑ การจัดหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจ

ระดับ	หน่วยงานไซเบอร์	CSOC (เชิงรับ)	CSIRT (เชิงรุก)
สำนักปลัดกระทรวงกลาโหม (สป.)	กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ทสอ.กห.)	กองเทคโนโลยีสารสนเทศ ทสอ.กห.	ศูนย์ไซเบอร์ ทสอ.กห.
กองบัญชาการกองทัพไทย (บก.ทท.)	ศูนย์ปฏิบัติการไซเบอร์ร่วม ทท.	กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร สส.ทหาร	กองสงครามเครือข่าย สปก.ยก.ทหาร
กองทัพบก	ศูนย์ไซเบอร์ ทบ.	กองปฏิบัติการไซเบอร์ (ศซบ.ทบ.)	กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศซบ.ทบ.
กองทัพเรือ	กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (สสท.ทร.)	กองสงครามไซเบอร์ สำนักปฏิบัติการ สสท.ทร.	กองสงครามไซเบอร์ สำนักปฏิบัติการ สสท.ทร.
กองทัพอากาศ	กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ททส.ทอ.)	ศูนย์คอมพิวเตอร์ กรมสื่อสารอิเล็กทรอนิกส์ ทหารอากาศ	กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม ททส.ทอ.

จากการศึกษาค้นคว้าข้อมูลจากหน่วยงานที่เกี่ยวข้อง รวมทั้งพิจารณามาตรฐานข้อกฎหมายงานวิจัยและเอกสารทางวิชาการต่างๆพบว่าการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมยังมีข้อจำกัดที่สำคัญ ดังนี้

การใช้มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กล่าวได้ว่าความมั่นคงปลอดภัยไซเบอร์ถือว่ามีความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับโดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำหนดเกณฑ์และแนวทางในการปฏิบัติ ซึ่งองค์กรสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของตนและอาจเพิ่มเติมหรือหรือยกเว้นการปฏิบัติในบางส่วนได้หากมีเหตุผลเพียงพอ

สำหรับมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DOD, มาตรฐาน ISO27001:2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST ๘๐๐ - ๑๔,มาตรฐาน COBIT, และมาตรฐาน IT BPM ๑๒ โดยมาตรฐาน U.S. DoD เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐอเมริกาที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์ เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรกคือกระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบพัฒนาผลิตหรือทดสอบสำหรับผู้ผลิตเทคโนโลยีหรือภาคเอกชนได้ปฏิบัติตามเพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้

มีการกำกับคุณภาพของคนโดยมีใบรับรอง IT Certificate ทางด้าน Cyber Security ทำให้ได้เจ้าหน้าที่ที่เหมาะสมเข้ามาทำงานด้านนี้ นอกจากนี้ยังให้ความสำคัญกับหลักการประกันความมั่นคงปลอดภัยสารสนเทศ (Informational Assurance : IA) โดยมีมาตรฐานในการประเมินและมี IT Audit team ในแนวทางในการดำเนินการพัฒนาการกำกับควบคุมทำให้การนำนโยบายด้านไซเบอร์มาสู่การปฏิบัติมีประสิทธิภาพมากยิ่งขึ้น

มาตรฐาน ISO ๒๗๐๐๑ : ๒๐๐๕ เป็นมาตรฐานที่มีแนวทางปฏิบัติที่ได้รับการยอมรับและนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรทั่วโลก ในขณะที่มาตรฐาน COBIT เป็นมาตรฐานที่มีจำนวนแนวทางปฏิบัติใกล้เคียงกับ ISO 27001 : 2005 ยกเว้นแนวทางในการป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อม จากภายในและภายนอกองค์กรและมาตรฐานที่มีแนวทางปฏิบัติน้อยที่สุดได้แก่ มาตรฐาน IT BMP เนื่องจากมาตรฐานนี้เป็นการกำหนดมาตรฐานขั้นต่ำที่องค์กรควรจะปฏิบัติ

แนวทางในการดำเนินการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมสู่มาตรฐานสากลนั้น จะต้องดำเนินการตามกฎหมาย คือ พระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓ ที่เกี่ยวข้องคือให้มีมาตรฐานการรักษาความมั่นคง

ปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

โดยตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศแบบปลอดภัย พ.ศ. ๒๕๕๕ ใกล้ออกประกาศกำหนดหลักเกณฑ์และรายละเอียดของมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ตามวิธีการแบบปลอดภัยในแต่ละระดับชั้นซึ่งมาตรฐานดังกล่าวจากครอบคลุมการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน

ไทยเซิร์ต (ThaiCert)

ศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์ (ไทยเซิร์ต) จัดตั้งขึ้นในปี พ. ศ. ๒๕๔๓ (ชื่อเดิม ศูนย์ประสานงานรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย) โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ภายใต้สังกัดของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ กระทรวงวิทยาศาสตร์และเทคโนโลยีมีภาระหน้าที่หลักเพื่อตอบสนองการจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขกับภัยคุกคามความมั่นคงปลอดภัยทางคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเตอร์เน็ต

ในฐานะที่เป็นสมาชิกองค์กรด้านการรักษาความปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/Forum of Incident Response and Security Team) ไทยเซิร์ต จึงมีบทบาทในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรเหล่านี้กับหน่วยงานในประเทศทั้งภาครัฐเอกชนมหาวิทยาลัยผู้ให้บริการอินเตอร์เน็ตหรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง

ในปัจจุบันภารกิจของ ISIS ถูกโอนย้ายมาสังกัดอยู่ภายใต้สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. แลกเปลี่ยนชื่อเป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย

ความเป็นมาของไทยเซิร์ต

ในเดือนกุมภาพันธ์ ๒๕๕๔ คณะรัฐมนตรีได้มีมติให้จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ คณะรัฐมนตรีได้มีมติให้จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การ

มหาชน) หรือ สพธอ. ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และได้มีการโอนภารกิจของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือไทยเศรษฐ์ จากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกระทรวงวิทยาศาสตร์และเทคโนโลยีมายัง สพธอ. เพื่อให้การดำเนินงานของ สพธอ. ด้านการสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์มีความเข้มแข็ง

ไทยเสิร์ต ได้เปิดให้บริการอย่างเต็มรูปแบบภายใต้ สพธอ. มาตั้งแต่วันที่ ๑ กรกฎาคม ๒๕๕๔ และได้ปรับเปลี่ยนชื่อทางการของไทยเซิร์ตเป็นศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand computer Emergency Response Team) โดยมีวิสัยทัศน์ให้สังคมออนไลน์มีความมั่นคงปลอดภัยความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ พันธกิจของไทยเซิร์ตมุ่งเน้นการประสานงานกับหน่วยงานในเครือข่ายและหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไขเหตุภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับแจ้งนอกจากนี้ไทยเซิร์ตยังมีพันธกิจเชิงรุกให้ความสำคัญกับการพัฒนาทรัพยากรบุคคลผู้ร่วมขีดความสามารถด้านการรักษาความมั่นคงปลอดภัย

เนื่องจากงานของไทยเซิร์ต มีลักษณะเป็นการประสานงานกับหน่วยงานต่างๆ ได้ที่สุดจึงมุ่งมั่นที่จะสร้างความร่วมมือกับหน่วยงานทุกประเภททั้งในและต่างประเทศในการแก้ไขภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารเช่นผู้ให้บริการทางอินเตอร์เน็ตและสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศสำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้เสริมสร้างความร่วมมือระหว่างประเทศผ่านเวที MIRST (Moral of incident Response and Security Teams) สำหรับ สำหรับความร่วมมือกับ ประเทศทั่วโลก และเวที APCERT (Asia Pacific Cert) สำหรับความร่วมมือกับประเทศในภาคพื้นเอเชียแปซิฟิก

ด้านการพัฒนาทรัพยากรบุคคลเลือกให้ความสำคัญกับการเผยแพร่ความรู้และข้อมูลข่าวสารเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อเป็นการสร้างภูมิคุ้มกันเบื้องต้นทางด้านไอที และจัดอบรมสัมมนาให้กับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์เฉพาะกลุ่มที่มีความต้องการข้อมูลข่าวสารเป็นการเฉพาะเช่นกลุ่มธุรกิจการเงินการธนาคารหรือกลุ่มสถาบันวิจัยและสถาบันการศึกษา นอกจากนี้ให้เกิดความเข้าใจและได้ลงมือปฏิบัติไทยเซิร์ต ยังจัดและร่วมในกิจกรรมซักซ้อมการรับมือภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารกับหน่วยงานทั้งในและต่างประเทศอีกด้วย

(ร่าง) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ – ๒๕๖๔

๑. ความนำ

ปัจจุบันอินเตอร์เน็ตเป็นส่วนสำคัญในการดำรงชีวิต ไม่ว่าจะในมิติต่างๆ ของการดำเนินการทางเศรษฐกิจและสังคม การรักษาความมั่นคงและการป้องกันประเทศ การสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญและจะทวีความสำคัญยิ่งขึ้นในอนาคต เนื่องจากความสามารถในการพัฒนาทางเทคโนโลยีที่รวดเร็วทั้งของประเทศชั้นนำด้านเทคโนโลยีเองและความสามารถในการพัฒนาและการเข้าถึงเทคโนโลยีของประเทศที่มีความก้าวหน้าทางเทคโนโลยีในระดับรองลงมา ซึ่งความก้าวหน้าทางเทคโนโลยีประเภทนี้ ตอบสนองต่อการใช้งานเครือข่ายเทคโนโลยีสารสนเทศของคนได้เป็นจำนวนมาก ทั้งกลุ่มที่เป็นผู้ใช้งานอินเตอร์เน็ตโดยตรงหรือผู้ที่ได้รับประโยชน์จากการใช้เครือข่ายเทคโนโลยีสารสนเทศในทางอ้อม เช่น การควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐานทั้งยังช่วยประหยัดเวลาและต้นทุนจากการรายงานของ ITU ปี ๒๕๕๘ พบว่าร้อยละ ๔๖ ของครัวเรือนทั่วโลกสามารถเข้าถึงอินเตอร์เน็ตได้

๒. การประเมินความพร้อมสภาพปัญหาและแนวโน้มของภัยคุกคามทางไซเบอร์

๒.๑ การประเมินความพร้อม

หากประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ๕ ด้านหลักๆด้วยกัน กล่าวคือความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ ความพร้อมด้านกลไกทางเทคโนโลยีเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ความพร้อมทางด้านบุคลากร ความพร้อมของระบบและเทคโนโลยี และความพร้อมด้านงานสืบสวน งานการข่าวการข่าวกรองทางไซเบอร์

๒ ๑.๑ ความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ

ประเทศไทยได้ให้ความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์มาอย่างต่อเนื่องโดยกฎหมายหลายฉบับได้กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เอาไว้แบ่งได้เป็น ๓ กลุ่ม คือ

๑) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ซึ่งได้กำหนดมาตรการสำคัญๆ ด้านความมั่นคงปลอดภัยเอาไว้เพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือเมื่อมีการใช้ระบบคอมพิวเตอร์หรือระบบอินเตอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งครอบคลุมทั้งในการพาณิชย์อิเล็กทรอนิกส์รวมไปจนถึงการให้บริการทางเรียก Sonic ของรัฐ หรือในงานรัฐบาลอิเล็กทรอนิกส์นั้นมีความมั่นคงปลอดภัย ตลอดจนกำหนดให้หน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure Protection) ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยและต่อมาก็ได้มีการตรากฎหมาย จัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ซึ่งได้กำหนดอำนาจหน้าที่สำคัญเพิ่มเติมอีกประการคือการยกระดับทักษะผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์รวมทั้งทำหน้าที่ดูแลศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)

๒) กฎหมายระดับอนุบัญญัติ หรือกฎหมายลูกที่กำหนดมาตรการในการกำกับดูแลของตลาดเงินโดยธนาคารแห่งประเทศไทย และของตลาดทุนโยสำนักงานคณะกรรมการในการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย รวมทั้งในการกำกับดูแลธุรกิจประกันโดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อให้บริการของผู้ให้บริการของผู้ประกอบการในภาคเศรษฐกิจที่มีการกำกับดูแลนั้นมีความนั้นมีความมั่นคงปลอดภัย

๓) กฎหมายว่าด้วยการกระทำซึ่งกำหนดฐานความผิดและบทลงโทษสำหรับการก่ออาชญากรรมทางคอมพิวเตอร์ ทั้งนี้โดยมีกองป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยี ภายใต้สำนักงานปลัดกระทรวงดิจิตอลเพื่อเศรษฐกิจและสังคม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติสำนักคดีเทคโนโลยีและสารสนเทศภาย ใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยีศูนย์เทคโนโลยีสารสนเทศภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน

๒.๑.๒ ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์

ปัจจุบันแม้ประเทศไทยจะให้ความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์มากขึ้นตามลำดับและได้มีการดำเนินงานของหน่วยปฏิบัติและหลายหน่วย เช่น การทำงานของศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ The computer Emergency Response Team หรือ ไทยเซิร์ต (ThaiSERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ที่ช่วยในการป้องกันและประสาทการทำงานด้านความมั่นคงปลอดภัยไซเบอร์และเริ่มมีการทำงานในรูปแบบ CERT ในองค์กรที่ทำหน้าที่กำกับดูแลองค์การภาคเอกชนบ้างแล้วก็ตามหรือมีการดำเนินงานของการป้องกันและปราบปรามการกระทำความผิด ทางเทคโนโลยีภายใต้สำนักงานปลัดกระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคมกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติสำนักคดีเทคโนโลยีและสารสนเทศ ภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยีศูนย์เทคโนโลยีสารสนเทศ ภายใต้สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ ธนาคารแห่งประเทศไทยแล้วก็ตามแต่รูปแบบการทำงานดังกล่าวก็เป็นการทำงานในเชิงป้องกันและตั้งรับ เมื่อมีภัยคุกคามทางไซเบอร์เท่านั้นจึงได้มีการจัดตั้งศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมหรือกองทัพไทยเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในเชิงรุกให้มากขึ้น

๒.๑.๓ ความพร้อมด้านบุคลากร ความพร้อมด้านบุคลากรถือเป็นสิ่งที่สำคัญอย่างยิ่งทั้งในด้านความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ทั้งระดับนโยบายและปฏิบัติและด้าน

ความรู้ความเชี่ยวชาญเฉพาะทาง ซึ่งจากการสำรวจพบว่ากว่าร้อยละ ๕๐ หน่วยงานรัฐและเอกชนยังไม่ได้ให้ความสัมพันธ์กับการจัดทำแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และร้อยละ ๗๙ ของหน่วยงานจะมีข้อจำกัดในการสร้างแรงจูงใจให้บุคลากรเสริมศักยภาพให้กับตนเอง เช่น การสอบใบประกาศนียบัตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะใบประกาศนียบัตรที่ได้รับการยอมรับในระดับสากลซึ่งประเทศไทยควรกำหนดทิศทางและให้ความสำคัญกับการส่งเสริมและสนับสนุนการพัฒนาบุคลากรที่มีความรู้ความเชี่ยวชาญในด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้นเพื่อเตรียมการรับมือกับภัยคุกคามที่อาจเกิดขึ้นในรูปแบบต่างๆได้อย่างครอบคลุมและมีประสิทธิภาพยิ่งขึ้น

๒.๑.๔ ความพร้อมของระบบและเทคโนโลยี ไทยยังขาดระบบการบริหารจัดการเครือข่ายเพื่อเสริมความมั่นคงของประเทศและยังต้องพึ่งพาต่างประเทศอย่างสูงในด้านนี้ ไทยจึงควรหันมาให้ความสำคัญกับการพัฒนาระบบและเทคโนโลยีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างจริงจัง เพื่อลดการพึ่งพาต่างชาติและเพื่อการรักษาผลประโยชน์ของชาติและความมั่นคงของชาติอย่างรอบคอบรัดกุมและได้มาตรฐานควบคู่ไปกับการเสริมสร้างระบบและเทคโนโลยีที่นำเข้ามาจากต่างประเทศ

๒.๑.๕ ความ ความพร้อมด้านงานสืบสวนงาน งานข่าวและข่าวกรองทางไซเบอร์ ปัจจุบันยังขาดการบูรณาการและการให้ความสำคัญกับการพัฒนาขีดความสามารถศักยภาพด้านงานข่าวกรองทางไซเบอร์ซึ่งมีส่วนสำคัญอย่างยิ่งในการทำความเข้าใจกับภัยคุกคามรูปแบบใหม่ๆ โดยเฉพาะภัยคุกคามทางไซเบอร์ท่านจะช่วยเสริมงานด้านการสืบสวนและงานข่าวโดยรวมอีกด้วย

๒.๒ โดยรวมแล้ว สถานการณ์ความพร้อมของประเทศเกี่ยวกับการรับมือและจัดการความเสี่ยงกับภาวะภัยคุกคามทางไซเบอร์ ยังมีข้อจำกัดในหลายด้านในขณะที่ความซับซ้อนของภัยคุกคามที่เกิดขึ้นมีความแปลกใหม่ตลอดเวลา ดูได้จากเหตุการณ์การค้นพบช่องโหว่ในระบบปฏิบัติการ Application หรือแม้แต่ซอฟแวร์ของอุปกรณ์ประเภทใด ไอโอที (internet of things) ที่เริ่มมีการใช้งานอย่างแพร่หลายในช่วงหลายปีที่ผ่านมาทำให้แฮกเกอร์สามารถลักลอบติดตั้งมัลแวร์ หรือโปรแกรมประสงค์ร้ายบนคอมพิวเตอร์ที่มีช่องโหว่และฝังรหัสอันตรายสามารถสร้างความเสียหายกับข้อมูลของเหยื่อเช่น WannaCry Ransomware ซึ่งเป็นมัลแวร์เรียกค่าไถ่ข้อมูลด้วยการเข้ารหัสลับซึ่งทำให้ผู้ใช้ไม่สามารถเปิดข้อมูลใช้งานได้และพบว่าแพร่กระจายได้ด้วยตัวเองผ่านการโจมตีช่องโหว่ของระบบปฏิบัติการ Windows ทำให้การระบาดเป็นไปอย่างรวดเร็วในวงกว้างกว่าเดิมหรือ Mirai Botnet ซึ่งเป็นมัลแวร์โจมตีอุปกรณ์ประเภทไอโอที ที่แฮกเกอร์สามารถสั่งการให้โจมตีระบบคอมพิวเตอร์ของผู้อื่นที่อยู่ในเครือข่ายคอมพิวเตอร์ในลักษณะ DDos (Distributed Denial of

Service) และทำให้บริการเครือข่ายอินเตอร์เน็ตและบริการที่ตกเป็นเป้าโจมตีขาดสภาพความพร้อมให้บริการ

นอกจากนี้ จากการายงานสถิติจากหลายแห่งได้ระบุว่า ไทยยังมีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น สถาบันนานาชาติได้จัดอันดับ ความสามารถในการแข่งขันของประเทศสมาชิกหรือ International institute for management Development (IMD) ได้มีรายงาน World Digital Competitiveness Rankings ประเมินจัดอันดับ ๖๓ เขตเศรษฐกิจ พบว่าอันดับความสามารถในการแข่งขันทั้งที่ต้องของไทยในปี ๒๕๕๙ อยู่ลำดับที่ ๔๑ จากอันดับที่ ๓๙ ในปี ๒๕๕๘ และในด้านความรู้อยู่ที่อันดับที่ ๔๔ จากเดิม ๔๒ แม้ว่าความพร้อมในอนาคตเลยรวมอยู่ที่อันดับ ๔๕ จากเดิมอันดับ ๔๘ แต่ยังหวังว่าจะมีจุดอ่อนในด้านไอที integration ที่อยู่อันดับ ๕๕ เนื้อว่านดาบจะดีขึ้นจากอันดับที่ ๕๗ ในปี ๒๕๕๘ ก็ตามแต่ด้าน- ก็ตามแต่ด้าน E-Government ไทยยังอยู่ในอันดับที่ ๕๕ และด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ที่อันดับที่ ๓๘

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ. ศ. ๒๕๖๐-๒๕๖๔

วัตถุประสงค์

๑. เพื่อสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนต่อการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

๒. เพื่อป้องกันโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

๓. เพื่อปกป้องผลประโยชน์และความมั่นคงของชาติจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

๔. เพื่อเสริมสร้างเศรษฐกิจดิจิตอล

๕. เพื่อบูรณาการและประสานความร่วมมือ รวมทั้งการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างหน่วยงาน

๖. เพื่อพัฒนาศักยภาพของหน่วยงานและเพิ่มขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๗. เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ

๘. เพื่อส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

๙. เพื่อส่งเสริมบทบาทของไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับ

ภูมิภาคและระดับนานาชาติ

เป้าหมาย

ภาคส่วนต่างๆเชื่อมั่นและไว้วางใจในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

โครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและประเทศโดยรวมมีความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์

ผลประโยชน์และความมั่นคงของชาติได้รับการปกป้องจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเทศเปลี่ยนผ่านสู่เศรษฐกิจที่ใช้เทคโนโลยีดิจิตอลได้อย่างราบรื่นและยั่งยืน

ทุกภาคส่วนมีความตระหนักถึงภัยคุกคามทางไซเบอร์และร่วมมือกันด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ประเทศไทยมีวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ

มีการบูรณาการและประสานความร่วมมือ รวมทั้งการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

งานด้านการป้องกันและปราบปรามอาชญากรรมมีความเข้มแข็ง การสืบสวนและงานข่าวมีคุณภาพและมั่นคงปลอดภัย

หน่วยงานมีความพร้อมสามารถตอบสนองการปฏิบัติการได้อย่างถูกต้องและรวดเร็ว

บุคลากรด้านความมั่นคงปลอดภัยไซเบอร์มีความเชี่ยวชาญ และมีศักยภาพในการปฏิบัติงาน

ไทยมีบทบาทในการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับนานาชาติและการลดความขัดแย้งทางไซเบอร์ระหว่างรัฐ

ประเด็นยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

แนวทางการดำเนินการ

๑.๑ ระดับนโยบายให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้การสนับสนุนการกำหนดนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒ พัฒนาโครงสร้างองค์กรในภาครัฐ เพื่อรองรับสังคมดิจิตอลและรับมือกับภัยคุกคามทางไซเบอร์ เพื่อเสริมสร้างความไว้วางใจแก่ภาคส่วนต่างๆที่ติดต่อประสานงานกับรัฐ

๑.๓ ส่งเสริมการใช้เทคโนโลยีดิจิทัลและอินเตอร์เน็ตเพื่อการบริการประชาชนของหน่วยงานรัฐและประชาสัมพันธ์เชิงรุกให้ประชาชนรับทราบ และมั่นใจการใช้บริการของหน่วยงานของรัฐ

๑.๔ ส่งเสริมให้ภาครัฐมีความโปร่งใสโดยใช้เทคโนโลยีและดำเนินกิจกรรมทางไซเบอร์โดยคำนึงถึงหลักการคุ้มครองสิทธิและเสรีภาพตลอดจนความเป็นส่วนตัวของผู้ใช้บริการออนไลน์ของภาครัฐ

๑.๕ สร้างความเชื่อมั่นและความไว้วางใจในภาคส่วนต่างๆ นอกเหนือจากภาครัฐ โดยเปิดโอกาสและจัดหาช่องทางให้ประชาชนเข้ามามีส่วนร่วมกับหน่วยงานของรัฐในการพัฒนาและปรับปรุงเทคโนโลยีและการดำเนินกิจกรรมทางไซเบอร์เพื่อให้ตรงตามความประสงค์ของผู้รับบริการ

๑.๖ ส่งเสริมให้ภาคเอกชนในธุรกิจสาขาต่างๆในทุกระดับดำเนินธุรกิจโดยใช้เทคโนโลยีดิจิทัลอินเตอร์เน็ตและไซเบอร์สเปซในวงกว้างและได้มาตรฐาน โดยประชาสัมพันธ์เชิงรุกและขอความร่วมมือจากภาคเอกชน

ประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

แนวทางการดำเนินการ

๒.๑ จัดทำกรอบนโยบาย/ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ. ศ. ๒๕๖๐ - ๒๕๖๔ สำหรับการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและทบทวนประเมินผลการดำเนินการตามนโยบายเพื่อการปรับปรุงนโยบายให้ทันกับสถานการณ์ที่เปลี่ยนไป

๒.๒ ให้มีการจัดตั้งหน่วยงานกลางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติเพื่อทำหน้าที่เป็นศูนย์กลางระดับนโยบายที่ขึ้นตรงต่อนายกรัฐมนตรี โดยเป็นศูนย์กลางด้านความมั่นคงปลอดภัยไซเบอร์และประสานการปฏิบัติทั้งในด้านการประสานงาน เฝ้าระวัง ตอบสนอง บริหารจัดการภัยคุกคามทางไซเบอร์ สร้างความตระหนัก ตลอดจนประสานความร่วมมือทั้งในและต่างประเทศและส่งเสริมการพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานต่างๆด้วยอาจพิจารณาจัดตั้งหน่วยปฏิบัติขึ้นมาสนับสนุนตามความเหมาะสม

๒.๓ จัดทำรายงานการเตรียมความพร้อมของหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของทั้งภาครัฐและเอกชน พร้อมจัดลำดับความสำคัญ เพื่อประกอบการจัดทำแผนปฏิบัติการและแผนเผชิญเหตุ

๒.๔ กำหนดบทบาทและหน้าที่ของหน่วยงานต่างๆของรัฐในด้านการปกป้องโครงสร้างพื้นฐานสำคัญที่การจัดการด้วยระบบสารสนเทศอย่างชัดเจน เพื่อการรับมือกับภัยคุกคามทางไซเบอร์ทั้งในยามปกติ ยามเกิดเหตุ การพื้นตัวและฟื้นฟูหลังเกิดเหตุ รวมทั้งการเยียวยาแก้ไขผลกระทบ รวมทั้งมีกลไกประสานความร่วมมือกับภาคเอกชนและผู้มีส่วนเกี่ยวข้องเพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศของไทยจากภัยคุกคามไซเบอร์

๒.๕ ส่งเสริมการจัดทำแผนการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศทั้งในภาครัฐและเอกชน โดยให้แต่ละองค์กรยึดถือหลักการปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดด้วยระบบสารสนเทศของหน่วยงานตนเองโดยอาศัยศักยภาพของหน่วยก่อน และในกรณีที่สถานการณ์ยกระดับหรือเป็นเหตุฉุกเฉินที่เกินความสามารถของหน่วย ก็สามารถประสานขอความสนับสนุนได้ทันต่อสถานการณ์

๒.๖ ส่งเสริมการจัดฝึกเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับประเทศ เพื่อเตรียมพร้อมการรับมือทางไซเบอร์ในรูปแบบต่างๆรวมทั้งในสภาวะวิกฤต

๒.๗ ร่างและปรับปรุงกฎหมายระเบียบปฏิบัติและข้อกำหนดเพื่อกำกับและวางกรอบการรักษาความมั่นคงปลอดภัยไซเบอร์โดยพิจารณากำหนดบทคุ้มครองและบทลงโทษที่เหมาะสม

๒.๘ พัฒนาศักยภาพของบุคลากรในภาครัฐผ่านการศึกษาฝึกอบรมในรูปแบบต่างๆ และส่งเสริมการถ่ายทอดความรู้ภายในภาครัฐหรือระหว่างภาครัฐกับเอกชนตลอดจนให้ความสำคัญกับการพัฒนาตำแหน่งงานในภาครัฐที่สนับสนุนการเติบโตของบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม เพื่อเป็นการรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้อยู่ในระบบราชการ

๒.๙ พัฒนาศักยภาพทางการวิจัยและพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนแสวงหาความร่วมมือกับเอกชนและต่างประเทศเพื่อสามารถเข้าถึงแหล่งเทคโนโลยี แหล่งเงินทุนและพัฒนาตลาดสำหรับอุตสาหกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์และนำไปสู่การลดการพึ่งพาจากต่างประเทศ

๒.๑๐ ส่งเสริมการมีส่วนร่วมของภาคเอกชนอย่างจริงจังในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในด้านการพัฒนาองค์ความรู้และเทคโนโลยีการพัฒนาบุคลากรการรักษาความมั่นคงปลอดภัย เพื่อยกระดับขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศแบบองค์รวม

๒.๑๑ พัฒนามาตรฐานและกระตุ้นให้มีกลไกลการตรวจสอบประเมินมาตรฐานความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ

๒.๑๒ ส่งเสริมให้มีการทำงานด้วยการปรับใช้มาตรการทางเทคนิคในลักษณะการทำงานแบบศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์หรือ CERT โดยเฉพาะอย่างยิ่งในกลุ่มโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อให้มีการประสานการทำงานรับมือกับภัยคุกคามทางไซเบอร์ในทางปฏิบัติให้มีความเข้มแข็งมากยิ่งขึ้น

ประเด็นยุทธศาสตร์ที่ ๓ ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

แนวทางการดำเนินการ

๓.๑ ศึกษา ติดตามและวิเคราะห์สถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องอย่างสม่ำเสมอ ทั้งภัยคุกคามในรูปแบบเดิมและรูปแบบใหม่ เพื่อทราบถึงแนวโน้มความเป็นไปได้ที่ผลประโยชน์และความมั่นคงของชาติได้รับผลกระทบและเพื่อหาทางป้องกันไม่ให้เกิดเหตุหรือลดความเสียหายให้น้อยลงมากที่สุด

๓.๒ หน่วยงานความมั่นคงที่เกี่ยวข้องพิจารณาจัดทำนโยบาย/ ยุทธศาสตร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์และบริหารจัดการการเก็บรักษาข้อมูลป้องกันการโจมตีหรือเจาะระบบ การใช้เครื่องมือทางไซเบอร์ในความขัดแย้งรวมทั้งประเมินสถานการณ์และทบทวนนโยบาย/ ยุทธศาสตร์ด้านไซเบอร์ให้ทันสมัย

๓.๓ กำหนดบทบาทให้กองทัพดูแลรับผิดชอบการป้องกันประเทศในมิติทางไซเบอร์และเป็นฝ่ายสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อได้รับการมอบหมายจากรัฐบาลโดยเฉพาะเมื่อเกิดสถานการณ์วิกฤตทางไซเบอร์ระดับชาติหรือสงครามไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๔ เสริมสร้างระบบเศรษฐกิจดิจิตอล

แนวทางการดำเนินการ

๔.๑ ส่งเสริมการพัฒนาขีดความสามารถหรือการดำเนินการที่สนับสนุนต่อการเปลี่ยนผ่านสู่ระบบเศรษฐกิจดิจิตอลอย่างสมดุลราบรื่น มีคุณภาพและนำไปสู่เศรษฐกิจดิจิทัลที่ยั่งยืน

๔.๒ สนับสนุนการมีส่วนร่วมของภาคเอกชนในการส่งเสริมเศรษฐกิจดิจิตอลกับภาครัฐทั้งในกลุ่มผู้ที่ใช้เทคโนโลยีดิจิทัลเพื่อดำเนินธุรกิจอยู่แล้วและส่งเสริมการใช้เทคโนโลยีดิจิทัลในวงกว้าง

๔.๓ พัฒนา ปรับปรุงยุทธศาสตร์ แผนหรือแผนงาน ตลอดจนกฎหมาย ระเบียบปฏิบัติที่เหมาะสมสอดคล้องและอำนวยต่อเศรษฐกิจดิจิทัลพร้อมทั้งมีการประเมินผลและทบทวนอย่างสม่ำเสมอ โดยเน้นการมีส่วนร่วมของภาคเอกชนในกระบวนการจัดทำยุทธศาสตร์ แผนหรือแผนงานดังกล่าว

ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางการดำเนินการ

๕.๑ ส่งเสริมการเผยแพร่ข้อมูลข่าวสารแก่ทุกภาคส่วนโดยทั่วถึงกัน ผ่านสื่อและกลไกต่างๆของภาครัฐ ภาคเอกชนและภาควิชาการ เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์และความสำคัญของการรักษาความมั่นคงปลอดภัยทางเบอร์ เพื่อการใช้เทคโนโลยีดิจิตอลและการดำเนินกิจกรรมทางใส่เบอร์อย่างปลอดภัยและเกิดประโยชน์และส่งเสริมความร่วมมือด้านการรักษาข้อความมั่นคงปลอดภัยไซเบอร์ในรูปแบบการรวมกลุ่มทั้งในระดับบุคคลและองค์กร

๕.๒ ส่งเสริมความร่วมมือกับสถาบันวิจัยและสถานศึกษาเช่น มหาวิทยาลัยและสถาบันคลังสมองในด้านการแลกเปลี่ยนความรู้ การวิจัยกันและ/หรือการนำเสนองานวิจัยตลอดจนการจัดทำคู่มือเผยแพร่ความรู้เกี่ยวข้องด้านไซเบอร์

๕.๓ ส่งเสริมและพัฒนาหลักสูตรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในการศึกษาตามระบบตั้งแต่ขั้นพื้นฐานทั้งสายสามัญและอาชีวะ โดยให้เนื้อหาของหลักสูตรมีความแตกต่างกันไปในแต่ละระดับการศึกษา

๕.๔ ส่งเสริมการให้ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แก่ประชาชนผู้ใช้อินเตอร์เน็ตทั่วไปผู้สูงอายุ เด็ก สตรีและเยาวชน ชุมชน ท้องถิ่น โดยร่วมมือกับสถานศึกษา องค์การบริหารส่วนท้องถิ่นหรือและหน่วยงานที่เกี่ยวข้องเพื่อเผยแพร่ความรู้และสร้างความตระหนักอย่างเป็นระบบและต่อเนื่อง

๕.๕ ส่งเสริมและประสานความร่วมมือระหว่างรัฐกับเอกชนและภาคประชาสังคมเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในลักษณะองค์รวมที่มีความเข้มแข็ง โดยจัดให้มีกลไกและช่องช่องทางการสื่อสารระหว่างกันเพื่อประโยชน์ในการทำความเข้าใจในแนวนโยบายจากรัฐสู่เอกชนและภาคประชาสังคมสู่การปฏิบัติ การมีส่วนร่วมของภาคเอกชนและภาคประชาสังคมในการสะท้อนปัญหา ประเมินผลการดำเนินนโยบายและการเสนอแนะนโยบายตลอดจนการสนับสนุนและการเป็นผู้ร่วมรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

แนวทางการดำเนินการ

๖.๑ ส่งเสริมค่านิยมอันดีงามของชาติบนโลกไซเบอร์ โดยส่งเสริมการใช้เทคโนโลยีสารสนเทศและการสื่อสารของประชาชนไปเพื่อการธำรงไว้ซึ่งชาติ ศาสนาและพระมหากษัตริย์

๖.๒ ส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซด้วยความรับผิดชอบและมีจิตสำนึกต่อผู้อื่นและสังคมโดยรวม เคารพสิทธิเสรีภาพขั้นพื้นฐานบนโลกไซเบอร์และไม่ละเมิดกฎหมาย

ประเด็นยุทธศาสตร์ที่ ๗ ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

แนวทางการดำเนินการ

๗.๑ ยกระดับและกำหนดบทบาทของผู้บังคับใช้กฎหมายซึ่งได้แก่ เจ้าหน้าที่ตำรวจและเจ้าหน้าที่กรมสอบสวนคดีพิเศษและเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้องในการสืบสวนทางไซเบอร์เพื่อค้นหาตัวผู้กระทำความผิดมาลงโทษ

๗.๒ ส่งเสริมการพัฒนาขีดความสามารถบุคลากรด้านการสืบสวนและงานข่าว ตลอดจนส่งเสริมการใช้เทคโนโลยีที่ทันสมัยเข้ามาช่วยในงานสืบสวนและงานข่าว

๗.๓ ส่งเสริมการพัฒนางานข่าวทางไซเบอร์อย่างเป็นรูปธรรม เพื่อเพิ่มประสิทธิภาพการจัดการภัยคุกคามทางไซเบอร์ได้อย่างทันต่อสถานการณ์

๗.๔ ส่งเสริมความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ตลอดจนประสบการและแนวทางปฏิบัติที่ดีกับต่างประเทศทั้งในระดับทวิภาคีและกับองค์กรระหว่างประเทศที่เกี่ยวข้อง อาทิ

ตำรวจสากล เพื่อการพัฒนาขีดความสามารถในการป้องกันและปราบปรามอาชญากรรมของไทย โดยเฉพาะประโยชน์ในการสืบสวนและการข่าว

๗๕ ส่งเสริมและสนับสนุนการพัฒนาระเบียบและกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๘ ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาคและระดับนานาชาติ

แนวทางการดำเนินการ

๘.๑ สนับสนุนให้มีการใช้ไซเบอร์สเปซในทางสันติโดยไม่ใช้เทคโนโลยีสารสนเทศเพื่อการสร้างความขัดแย้ง ตลอดจนร่วมมือกับมิตรประเทศในการต่อต้านการใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการก่ออาชญากรรมข้ามชาติหรือการกระทำที่สร้างความเสียหาย

๘.๒ สนับสนุนการแลกเปลี่ยนองค์ความรู้ ข้อมูล แนวปฏิบัติที่ดีด้านไซเบอร์กับต่างประเทศทั้งในระดับทวิภาคีระดับภูมิภาคและระดับพหุภาคี

๘.๓ มีช่องทางการสื่อสารแลกเปลี่ยนข้อมูลและแนวทางปฏิบัติที่ชัดเจนในการร่วมมือกับต่างประเทศในการตอบสนองและรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

๘.๔ มีบทบาทการส่งเสริมการหารือเกี่ยวกับบรรทัดฐาน มาตรฐาน มาตรการสร้างความไว้วางใจหรือความเชื่อมั่นระหว่างประเทศในมิติไซเบอร์ รวมถึงการมีท่าทีร่วมกันในระดับภูมิภาคเพื่อให้บรรทัดฐานระหว่างประเทศเป็นที่ยอมรับและสะท้อนผลประโยชน์ของไทยและประเทศในภูมิภาค

ปัจจัยแห่งความสำเร็จ

๑ รัฐบาลให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและผลักดันให้เกิดผลเป็นรูปประธรรมอย่างจริงจัง

๒ หน่วยงานต่างๆนำแนวทางตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปปฏิบัติและจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานตัวเอง และปฏิบัติตามแผนฯอย่างจริงจัง

๓ ทุกภาคส่วนที่เกี่ยวข้อง ทั้งภาครัฐ เอกชนและภาคประชาชนให้ความร่วมมือและมีส่วนร่วมในการสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์

๔ จัดให้มีการทบทวนประเมินผลการดำเนินการตามยุทธศาสตร์ทุก ๒ ปี

บทที่ ๔
แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัย ทางไซเบอร์แห่งชาติ

ในการดำเนินการศึกษาวิจัยเรื่อง แนวทางการบูรณาการ การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาตินั้น มุ่งเน้นศึกษาถึงกำหนดนโยบาย การบริหารจัดการและยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของทั้งกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยใช้การวิจัยเชิงคุณภาพ (Quantitative Research) แบบวิจัยเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-Depth Interview) ต่อผู้ให้ข้อมูลสำคัญ โดยมีสาระสำคัญดังนี้

๑. การวิจัยเชิงเอกสาร

ผู้วิจัยได้ดำเนินกระบวนการศึกษาและวิเคราะห์ข้อมูลจากเอกสาร โดยการทบทวนแนวความคิด ทฤษฎี เอกสาร ตลอดจนงานวิจัยที่เกี่ยวข้องดังนี้

๑.๑ ทฤษฎีเกี่ยวกับสมรรถนะในองค์กร บรรยากาศองค์กร และองค์กรสมัยใหม่

๑.๒ การจัดการความรู้และการบริหารความเสี่ยง

๑.๓ การบูรณาการการบริหารจัดการ

๑.๔ การรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑.๕ ยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ

๑.๖ งานวิจัยที่เกี่ยวข้อง

๒. การสัมภาษณ์เชิงลึก

ผู้วิจัยได้ออกแบบโครงสร้างของข้อคำถามที่สามารถนำไปใช้ในการสัมภาษณ์แบบกึ่งโครงสร้างหรือการสัมภาษณ์แบบชี้นำ (Guide Interview) กล่าวคือ เป็นการสัมภาษณ์แบบไม่มีโครงสร้างหรือเป็นการสัมภาษณ์แบบปลายเปิด ซึ่งเป็นกระบวนการวิจัยฯ ที่มีความยืดหยุ่นและเปิดกว้างหรือมีการนำคำสำคัญ (Keywords) มาใช้ประกอบในการชี้นำคำสัมภาษณ์ โดยร่างข้อคำถามที่มีลักษณะปลายเปิด เพื่อให้ผู้ทรงคุณวุฒิได้ตอบข้อคำถามให้ได้ข้อมูลที่มีความหลากหลาย ในงานวิจัยครั้งนี้

การรวบรวมข้อมูลจากเอกสารด้านความมั่นคงปลอดภัยทางไซเบอร์

การรวบรวมข้อมูลจากเอกสารด้านความมั่นคงปลอดภัยทางไซเบอร์ สรุปได้ดังนี้

๑. กรอบแนวความคิดในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ต้องการให้ครอบคลุมในเรื่องความมั่นคงปลอดภัยของระบบและข้อมูล สิทธิเสรีภาพของประชาชน ความมั่นคง

ของประเทศ

๒. การบูรณาการและการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ เพื่อปกป้อง รับมือ ป้องกัน และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึงความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ รวมถึงที่อาจจะส่งผลกระทบต่อความมั่นคงทางทหาร หรือส่งผลต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม

๓. การพัฒนาและการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะอย่างยิ่งการจัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น โดยให้ครอบคลุมถึงมิติการรักษาความมั่นคงปลอดภัยทางการทหาร การรักษาความสงบเรียบร้อยภายในประเทศ โครงสร้างพื้นฐานสำคัญของประเทศ และรักษาความมั่นคงทางเศรษฐกิจ

๔. การปกป้องด้านโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructures) ของประเทศ ในเรื่องของระบบความปลอดภัยด้านสาธารณสุข พลังงาน เศรษฐกิจ ระบบการเตือนภัยต่างๆ และการละเมิดสิทธิส่วนบุคคลที่มีกรอบเนื้อหาที่ชัดเจน และมีระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย สามารถรับมือกับภัยที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิผล

๕. การประสานความร่วมมือระหว่างหน่วยงานของรัฐและหน่วยงานเอกชนในการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ และการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๖. การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยการสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน ตลอดจนการพัฒนาทางด้านไอทีที่มีประสิทธิภาพ

๗. การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ควรจะมีกฎหมายที่บังคับใช้ในด้านการจารกรรมไซเบอร์ที่ชัดเจน เหมาะสม และสามารถบังคับใช้ได้จริง

๘. การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

๙. การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ ตลอดจนการสร้างประชาคมข่าวสารเพื่อแลกเปลี่ยนความรู้ ความร่วมมือ และควรจัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศให้มีความชัดเจนยิ่งขึ้น

การรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึก

๑. พลตรี ปรัชญา เฉลิมรัตน์ (สัมภาษณ์, ๕ กรกฎาคม ๒๕๖๑) ผู้ชำนาญการสำนักงานปลัดกระทรวงกลาโหม โดยท่านกล่าวว่า “เห็นด้วยกับการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากโดยหน้าที่แล้วต้องเป็นเจ้าภาพหลักในการรับมือกับภัยคุกคามทางไซเบอร์ เนื่องจากมีความพร้อมมากกว่ากระทรวงหรือหน่วยงานอื่น แต่ต้องอยู่ภายใต้กรอบกฎหมายที่ชัดเจน ซึ่งในระดับนโยบายน่าจะอยู่ในร่างพระราชบัญญัติความมั่งคงปลอดภัยไซเบอร์ (ซึ่งยังไม่ผ่านการพิจารณาเป็นกฎหมาย) ที่จะมีการกำหนดหน่วยงานเพื่อกำกับดูแล กำหนดนโยบายและแผนการปฏิบัติอย่างชัดเจน นอกจากนี้ ในด้านการดำเนินงานของกระทรวงกลาโหมก็ยังไม่ชัดเจน เนื่องจากศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศ

และอวกาศกลาโหม มีหน้าที่วางแผน อำนวยการประสานงาน กำกับดูแลและดำเนินการเกี่ยวกับนโยบายและยุทธศาสตร์ด้านไซเบอร์ นำนโยบายด้านไซเบอร์ระดับรัฐบาลไปสู่การปฏิบัติสนับสนุนภารกิจด้านไซเบอร์เพื่อความมั่นคงของประเทศ กระทำได้ในลักษณะให้การสนับสนุนรัฐบาล และการป้องกันตัวเองตามขีดความสามารถ แต่ถ้าถือว่างานด้านไซเบอร์ เป็นอีกหนึ่งมิติหรือโดเมนของความมั่นคงทางทหาร กระทรวงกลาโหมก็ควรจะต้องมีบทบาทมากกว่านี้ เช่น การป้องกันเชิงรุก หรือสามารถปฏิบัติการเชิงรุกได้ สำหรับประเด็นการพัฒนาบุคลากร มีความสำคัญมาก ต้องมีระบบการพัฒนาและการฝึกอบรมที่ชัดเจน เพื่อให้ได้คนที่มีความสามารถโดยเฉพาะในเรื่องไซเบอร์”

๒. พลตรี อภิศักดิ์ สมบัติเจริญนนท์ ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ (สัมภาษณ์, ๔ กรกฎาคม ๒๕๖๑) โดยท่านได้กล่าวว่า “เห็นด้วยกับการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากเป็นหน่วยรับผิดชอบหลัก ตามการจัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย ในกลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ จึงควรเร่งดำเนินการให้เป็นรูปธรรม สำหรับกองบัญชาการกองทัพไทยได้จัดตั้งศูนย์ไซเบอร์ทหารขึ้น เพื่อเป็นหน่วยปฏิบัติหลัก ด้านความมั่นคงปลอดภัยทางไซเบอร์ และขยายขอบเขตของงานป้องกันทางไซเบอร์ให้กว้างขวางยิ่งขึ้น รองรับการทำงานต่อจากระดับกระทรวงกลาโหม นอกจากนี้ยังได้กล่าวถึงการทำงานร่วมกันต้องอยู่บนมาตรฐานเทคโนโลยีเดียวกันซึ่งหมายรวมถึง โครงสร้างพื้นฐาน (INFRASTRUCTURE) อุปกรณ์เครือข่ายคอมพิวเตอร์ (Hardware) และโปรแกรม, โปรแกรมประยุกต์ (SOFTWARE) เพื่อความสะดวกรวดเร็วและการรักษาความปลอดภัยตัวระบบ ในการเชื่อมโยงกับหน่วยงานอื่น ควรทำในลักษณะเป็นเครือข่าย (Network) หรือ Node การทำงานเพื่อการขยายตัวของการทำงานได้มากและเร็วขึ้นซึ่งเป็นเรื่องทางเทคนิคที่ต้องพัฒนาต่อไป ในส่วนการปฏิบัติการเชิงรุก ควรใช้การทำงานเป็นทีมของส่วนงานด้านไซเบอร์ภายในกระทรวงกลาโหม เช่น ทีมไซเบอร์ของ กห ไปสู่ทีมของ บก.ทท. และเหล่าทัพ ดำเนินการเช่น การรวบรวมข่าวกรองทางไซเบอร์”

๓. นาวาอากาศเอก เฉลิมชัย วงษ์เกตุ ผู้อำนวยการกองแผนไซเบอร์ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (สัมภาษณ์, ๒๙ มิถุนายน ๒๕๖๑) กล่าวว่า “เห็นด้วยกับการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากในระดับปฏิบัติมีการแลกเปลี่ยนข้อมูลในการทำงานป้องกันทางด้านไซเบอร์ เช่นการแจ้งเตือนเมื่อมีการบุกรุกหรือการเจาะระบบ (Hack) หรือการติดตั้งอุปกรณ์เพื่อบันทึก (Log) แล้วนำไปวิเคราะห์เพื่อหาทางแก้ไขโดย ศูนย์ประสานการรักษา ความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (THAICERT) แต่เข้าใจว่าในระดับนโยบาย และแผนปฏิบัติการยังคงรอความชัดเจนจากข้อกฎหมายที่เกี่ยวข้อง แต่อย่างไรก็ดี เนื่องจาก คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีมติกำหนดให้ โครงสร้างพื้นฐานสารสนเทศด้านกลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ รับผิดชอบโดย กระทรวงดิจิทัลฯและกระทรวงกลาโหม ดังนั้น หน่วยปฏิบัติจึงต้องดำเนินการเพื่อให้สอดคล้องแต่ปัจจุบันยังมีข้อขัดข้องเนื่องจากหน่วยปฏิบัติต้องได้รับการสนับสนุนในหลายๆ ด้าน ทั้งบุคลากร เทคโนโลยีที่แตกต่างกันและการซักซ้อมการปฏิบัติร่วมกับหน่วยงานข้ามกระทรวง เบื้องต้นได้เตรียมหน่วยเผชิญเหตุไว้ ๕ ทีม

เพื่อสนับสนุนการแก้ไขและป้องกันการโจมตีทางไซเบอร์ต่อกระทรวงกลาโหม แต่ยังมีขีดความสามารถค่อนข้างจำกัดเนื่องจากเหตุผลดังกล่าว”

๔. นาวาอากาศเอก สมศักดิ์ ขาวสุวรรณ์ รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (สัมภาษณ์, ๒๘ มิถุนายน ๒๕๖๑) กล่าวว่า “เห็นด้วยกับการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่าง กระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากเป็นส่วนหนึ่งในแนวทางที่รัฐบาลต้องผลักดัน เพื่อขยายเครือข่ายตามกรอบนโยบายและแผนระดับชาติ เพื่อปกป้องรับมือป้องกันและลดความเสี่ยงและให้เกิดความสอดคล้องไปในทิศทางเดียวกัน นอกจากนี้ยังได้ให้ความคิดเห็นในเรื่อง การปรับปรุงกฎหมายหลายฉบับทั้งที่ประกาศใช้แล้ว และยังไม่ประกาศ เนื่องจาก ยังมีบางส่วนที่ไม่สอดคล้องกัน ซึ่งทางกระทรวงในฐานะต้นเรื่องกำลังดำเนินการอยู่ สำหรับการดำเนินงานด้านรักษาความปลอดภัยทางไซเบอร์ในเชิงรุก อาจจะไม่สามารถระบุให้ชัดเจนในตัวบทกฎหมายได้ แต่อาจใช้อำนาจตามกฎหมายอื่น เช่น แต่งตั้งให้ ทีมตอบสนองด้านไซเบอร์เป็นผู้ช่วยเจ้าพนักงานในการปฏิบัติหน้าที่ ท่านได้กล่าวเสริมว่า ปัจจุบันเทคโนโลยีสารสนเทศและกิจกรรมทางไซเบอร์มีการเปลี่ยนแปลงที่รวดเร็วมาก การแก้ไขตามระบบราชการอาจจะล่าช้าเกินไป รัฐบาลจึงพยายามกำหนดให้เป็นคณะกรรมการดำเนินงานตามประเด็นยุทธศาสตร์ และหน่วยปฏิบัติที่อ่อนตัวเพื่อให้ตอบสนองได้เร็วขึ้น เรื่องโครงสร้างพื้นฐานสำคัญทางสารสนเทศบางส่วนรัฐบาลได้ดำเนินการไปบ้างแล้ว เช่นการสร้างโครงข่ายอินทราเน็ต(Intranet) เพื่อเป็นระบบเชื่อมต่อเฉพาะภายในส่วนราชการด้วยกัน แยกออกจากโครงข่ายสาธารณะ (Internet) ทั้งนี้เพื่อลดความเสี่ยงการรักษาความปลอดภัย และลดการรั่วไหลของข้อมูล รวมทั้งการพัฒนาต่อยอด เช่น การสร้างชานชาลาข้อมูลกลาง (Plat Form) เพื่อรองรับการแบ่งปันข้อมูล (Data) ของหน่วยราชการด้วยกัน”

๕. นายปราการ พันธุเสนา นักวิชาการคอมพิวเตอร์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (สัมภาษณ์, ๒ กรกฎาคม ๒๕๖๑) รับผิดชอบส่วนปฏิบัติการของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) หรือ สพธอ. ท่านได้กล่าวว่า “ เห็นด้วยกับการบูรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ระหว่างกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากจะเป็นจุดเริ่มต้นในการขยายความร่วมมือ และรองรับกับนโยบายและกฎหมายเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่จะเกิดขึ้น เนื่องจากปัจจุบัน ทาง สพธอ. มีการประสานการปฏิบัติกับหน่วยที่เกี่ยวข้องอยู่บ้างแล้ว เช่น การติดตั้งอุปกรณ์เพื่อเฝ้าติดตามและเก็บบันทึก (Log) ของการถูกโจมตีหรือรบกวนทางไซเบอร์ให้กับหน่วยงานต่างๆ เพื่อนำมาวิเคราะห์และแก้ไข เก็บสถิติ พร้อมทั้งแจ้งเตือนในกรณีที่มีความพยายามที่จะบุกรุก/เจาะ เข้าระบบ (Intrusion Attempts) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thai CERT) รวมทั้งเป็นจุดประสานงานหลักในการติดต่อแลกเปลี่ยนข้อมูลกับต่างประเทศ เพื่อเผยแพร่ข้อมูลที่เป็นประโยชน์แก่หน่วยงานอื่นๆ นอกจากนี้ ยังให้ความเห็นเพิ่มเติมว่า ต่อไปถ้ามีการจัดตั้งหน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Agency) ซึ่งจะมีลักษณะคล้ายกับสภาความมั่นคงแห่งชาติ แต่จำกัดอยู่เฉพาะการดำเนินงานทางด้านไซเบอร์ คือเป็นผู้เสนอแนะนโยบาย กำกับดูแล ประเมินผลภัยคุกคามทางด้านไซเบอร์ และเป็นเจ้าภาพหลักในการ

ปฏิบัติการเพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยอาจมีการจัดหรือแบ่งงาน หรือยุบรวมหน่วย เพื่อมาอยู่ภายใต้หน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งชาตินี้ สำหรับในด้านการพัฒนาบุคคลากรทางด้านความมั่นคงปลอดภัยทางไซเบอร์ สพธอ. จะเป็นเจ้าภาพหลักในการจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย ซึ่งได้รับการสนับสนุนจากประเทศญี่ปุ่นด้านงบประมาณและผู้เชี่ยวชาญ โดยจะเริ่มต้นจัดฝึกอบรมสำหรับข้าราชการและเจ้าหน้าที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของอาเซียนก่อนทุก ๒ เดือน โดยหลักสูตรที่ใช้มี ๓ หลักสูตร คือ ๑. หลักสูตรที่เน้นการรับมือกับภัยคุกคามทางไซเบอร์ ๒. หลักสูตรที่เกี่ยวข้องกับการตรวจพิสูจน์ พยานหลักฐานดิจิทัลจากการโจมตีทางไซเบอร์ และ ๓. หลักสูตรการวิเคราะห์มัลแวร์ประเภทต่างๆ”

สรุปผลการวิเคราะห์

๑. การศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการบริหารจัดการและการรักษาความมั่นคงปลอดภัยไซเบอร์ ผลการวิจัย สรุปได้ดังนี้

๑.๑ องค์กรต้องเป็นองค์กรที่นำเทคนิคการบริหารจัดการมาใช้ ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้นๆ ต้องเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ซึ่งจะต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบใหม่ทั้ง ๕ ระบบขององค์การแห่งการเรียนรู้อันได้แก่ การเรียนรู้ (Learning) องค์การ (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology)

๑.๒ การบูรณาการการบริหารจัดการ คือการบริหารงานที่ทุกหน่วยงาน ทำงานและมุ่งเน้นผลงาน (Result) ตามยุทธศาสตร์ หลักที่กำหนดขึ้น เป็นการทำงานหลายหน่วยงาน โดยอาศัยความเชี่ยวชาญและความชำนาญการของแต่ละหน่วยงาน ที่แตกต่างกัน โดยร่วมกันคิด ร่วมกันทำงานโดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุเป้าหมาย มั่งสู่ผลสำเร็จ

๑.๓ ภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามทีการเปลี่ยนแปลงไปจากเดิมอย่างมาก มีรูปแบบการโจมตีเป้าหมายที่หลากหลาย ดังนั้นแนวความคิดและแนวทางในการป้องกัน ให้เกิดประสิทธิผล จำเป็นอย่างยิ่งที่จะต้องปรับความคิดและปรับกลยุทธให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป การวางแผนป้องกันจากภัยของไซเบอร์ ควรนำระบบมาตรฐาน ISO/IEC๒๗๐๐๑ : ๒๐๑๓ ซึ่งเป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการ ความมั่นคงปลอดภัยสำหรับสารสนเทศมาเป็นแนวทาง นอกจากนี้แล้ว การแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ควรมีมุมมอง ๓ ด้าน (PPT) ได้แก่ People, Process and Technology การปรับกระบวนการโดยการปฏิบัติตามมาตรฐาน เป็นการแก้ปัญหาที่ Process และ Technology แต่ปัจจัยสำคัญที่สุดอยู่ที่มนุษย์ หรือ People

๒. การศึกษาแนวนโยบายการกำหนดยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษา

ความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๒.๑ กระทรวงกลาโหม ได้กำหนดกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง ๔ ปี คือ พ.ศ.๒๕๕๘-๒๕๖๒ โดยกำหนดประเด็นยุทธศาสตร์ ไว้ ๓ ประเด็น ดังนี้

๒.๑.๑ ประเด็นยุทธศาสตร์การป้องกันเชิงรุก โดยใช้พลังอำนาจทางไซเบอร์กองทัพไทย เพื่อปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้าม ทั้งที่เป็นรัฐ ไม่ใช่ รัฐ และสนับสนุนโดยรัฐ ตลอดจนกลุ่มบุคคลหรือบุคคลใดๆ ที่อาจเป็นภัยคุกคามทางไซเบอร์ โดยจะมุ่งเน้นไปที่ปฏิบัติการเชิงรุกในลักษณะจำกัดและการตอบโต้อย่างรวดเร็ว

๒.๑.๒ ประเด็นยุทธศาสตร์การผนึกกำลังป้องกันประเทศสำหรับการปฏิบัติการในมิติไซเบอร์ของทุกภาคส่วนในประเทศเข้าด้วยกันอย่างเป็นระบบ

๒.๑.๓ ประเด็นยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย โดยร่วมมือประเทศเพื่อนบ้าน ประเทศกลุ่มอาเซียนและมิตรประเทศ เพื่อการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

๒.๒ กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ได้มีการจัดตั้งหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นที่เรียบร้อยแล้วโดยแบ่งการดำเนินการเป็น ๒ ส่วน คือ ส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) เชิงรับ และส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security incident Response Team : CSIRT)

๒.๓ จากการศึกษาการดำเนินงาน พบว่า ยังคงมีปัญหาและข้อจำกัด ซึ่งส่งผลกระทบต่อการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๒.๓.๑ การจัดองค์กรด้านไซเบอร์ของกระทรวงกลาโหม อยู่ในระหว่างการปรับปรุง ส่งผลให้การประสานงานทั้งในด้านนโยบายและด้านการปฏิบัติเป็นไปอย่างจำกัด

๒.๓.๑ ยังมีข้อขัดข้องในการแลกเปลี่ยนข้อมูลการจัดการภัยคุกคามทางไซเบอร์ทั้งในระดับกระทรวงกลาโหม และการเชื่อมโยงระดับปกติ

๒.๓.๓ การผลิต รักษา และพัฒนาบุคลากรที่ปฏิบัติงานทางด้านไซเบอร์ยังไม่เป็นระบบและต่อเนื่อง

๒.๔ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ดำเนินการตามระเบียบสำนักนายกรัฐมนตรี ว้าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐ ได้กำหนดจัดประชุมคณะกรรมการฯ ครั้งที่ ๑/๒๕๖๑ โดยพัฒนา ๔ เรื่อง ดังนี้

๒.๔.๑ กรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อปกป้องหรือป้องกันและลดความเสี่ยง และความสอดคล้องไปในทิศทางเดียวกัน

๒.๔.๒ แนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Conical Information Infrastructure : CII) ของประเทศ และแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure :SOP)

๒.๔.๓ แนวทางการพัฒนาบุคคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ระยะเร่งด่วน

๒.๔.๔ แนวทางการจัดตั้ง Cyber security Agency (CSA) ทำหน้าที่หน่วยงานประสานงานกลาง และหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความมั่นคงปลอดภัยไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

๓. แนวทางในการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัยได้ศึกษาค้นคว้าแนวทางการบูรณาการบริหารจัดการของสำนักงานคณะกรรมการพัฒนาระบบราชการ นโยบาย แผนปฏิบัติการ และการดำเนินงาน การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตลอดจนความคิดเห็นจากการสัมภาษณ์ จึงขอเสนอแนวทางในการบูรณาการ ดังนี้

๓.๑ การจัดกาความรู้และการบริหารความเสี่ยง โดยต้องเป็นความริเริ่มของผู้นำองค์กรในการกำหนดนโยบาย หรือแนวทางปฏิบัติให้ชัดเจน มีเป้าหมายที่จัดให้มีมาตรการกำกับดูแลเพื่อให้หน่วยงานและบุคลากรได้ตระหนักรู้ถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์และบริหารความเสี่ยง เพื่อดำเนินการแก้ไขและฟื้นคืนสภาพ (Resilience) ให้เร็วที่สุด

๓.๒ การทำงานแบบเครือข่าย (Network) โดยการทำงานเชื่อมโยงตามประเด็นยุทธศาสตร์ร่วมกัน (Common agenda) โดยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นเจ้าภาพ

๓.๓ การร่วมกันกำหนดมาตรฐานแนวทางการปฏิบัติทั้งในด้านการทำงาน การเชื่อมโยงติดต่อประสาน รวมทั้งมาตรฐานในทางเทคโนโลยี โดยกำหนดเป็น ระเบียบปฏิบัติประจำ (SOP)

๓.๔ การศึกษาและการวิจัยพัฒนา ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อต่อยอดองค์ความรู้ พัฒนาบุคคล ซ้อมจับมือกับภัยคุกคาทางไซเบอร์ และปริเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ โดยประสานความร่วมมือกับศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคคลความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cyber security capacity Building Centre)

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

ความก้าวหน้าทางเทคโนโลยีสารสนเทศ ซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร และในขณะเดียวกันก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่ส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและหรือรุนแรงยิ่งขึ้น กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ จึงมีความจำเป็นที่ทุกภาคส่วน ทั้งภาคราชการและเอกชน ต้องตระหนักและร่วมมือกันในการป้องกันภัยคุกคามดังกล่าว การวิจัย เรื่อง การบูรณาการระหว่างกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากเป็นหน่วยงานหลักในการรับผิดชอบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ กลุ่มความมั่นคงและบริการภาครัฐ กับเป็นจุดเริ่มต้นในการขยายเครือข่ายความร่วมมือไปยังหน่วยงานอื่น ที่เกี่ยวข้องต่อไป โดยมีวัตถุประสงค์ดังนี้

๑. ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ศึกษาแนวนโยบายการกำหนดยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

๓. เสนอแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

จากผลการวิจัยพบว่า แนวคิดทฤษฎีที่ได้ทำการศึกษาเป็นแนวคิดตามหลักวิชาการและมีแนวทางในการดำเนินงานที่สามารถนำมาปรับใช้กับงานวิจัยได้ สำหรับการดำเนินงานตามแนวนโยบาย ยุทธศาสตร์แผนปฏิบัติงานของทั้ง ๒ กระทรวง โดยแต่ละกระทรวงมีหน่วยงานที่รับผิดชอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยตรง มีทั้งส่วนที่ควบคุมนโยบาย การบริหารการติดต่อประสานและหน่วยที่เป็นหน่วยปฏิบัติ ซึ่งในปัจจุบันมีการดำเนินงานติดต่อประสานงานในระดับหน่วยปฏิบัติและงานทางด้านเทคนิค แต่ยังขาดการบูรณาการการบริหารงานที่ชัดเจนในระดับหน่วยควบคุมการปฏิบัติและในระดับนโยบาย เพื่อเป็นการเริ่มต้นในการบูรณาการการทำงานในระดับปฏิบัติการ จึงขอเสนอแนวทางการบูรณาการ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อการพัฒนา ดังนี้

๑. การจัดการความรู้และการบริหารความเสี่ยง เพื่อส่งเสริมให้บุคลากรทั้งองค์กรได้ตระหนักรู้ถึงภัยทางไซเบอร์ และการบริหารความเสี่ยงเพื่อป้องกันรับมือ ลดความเสี่ยงและดำเนินงานให้สอดคล้องไปในทิศทางเดียวกัน

๒. การดำเนินงานแบบเครือข่าย (Network) โดยการทำงานตามประเด็นยุทธศาสตร์ร่วมกัน (Common agenda) ซึ่งกำหนดขึ้นโดยหน่วยงานที่รับผิดชอบตามแผนงาน

๓. การร่วมกันกำหนดมาตราทั้งมาตรฐานการดำเนินงาน มาตรฐานในการเชื่อมต่อประสานงาน รวมทั้งมาตรฐานทางเทคโนโลยี

๔. ส่งเสริมการศึกษาและการวิจัยพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์

ข้อเสนอแนะ

๑. ข้อเสนอแนะเชิงนโยบาย

๑.๑ รัฐบาล ควรเร่งประกาศใช้พระราชบัญญัติ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และปรับปรุงแก้ไขกฎหมายที่ออกมาก่อน เช่น พระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และแก้ไขเพิ่มเติม พ.ศ.๒๕๖๐ เพื่อให้เกิดความสอดคล้องและทันสมัย

๑.๒ เร่งรัดการดำเนินการด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อเป็นพื้นฐานในการดำเนินงานที่เป็นมาตรฐานของภาครัฐและการจัดสร้างชานชาลาข้อมูล (Platform) เพื่อเป็นพื้นฐานในการแลกเปลี่ยนและแบ่งปันข้อมูลระหว่างหน่วยงานและเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒. ข้อเสนอแนะระดับปฏิบัติการ

๒.๑ การดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในลักษณะการป้องกันเชิงรุก (Active defense) และการปฏิบัติการเชิงรุก (Offense) เช่น การข่าวกรองทางไซเบอร์ ควรมีหน่วยงานที่ชัดเจนในการดำเนินงานในที่นี้ควรเป็นกระทรวงกลาโหม แต่ควรมีกฎหมายรองรับเนื่องจากปัจจุบันอาจจะเสี่ยงต่อการผิดกฎหมายทั้งในประเทศและระหว่างประเทศ

๒.๒ ควรมีกรอบการดำเนินงานเพ่อความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) โดยอาจใช้กรอบการดำเนินงานของสถาบันมาตรฐานแลชะเทคโนโลยีแห่งสหรัฐอเมริกา (The National Institute of Standards and Technology : NIST) สามารถนำมาปรับใช้ให้เข้ากับวัฒนธรรมองค์กรและนโยบายของประเทศได้ โดยกรอบการดำเนินงานนี้เป็นกระบวนการแบบวนซ้ำพัฒนาแบบค่อยเป็นค่อยไป เพื่อรับมือกับรูปแบบที่เปลี่ยนแปลงไปของภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

๒.๓ การคาดการณ์ การถูกโจมตี โครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ โดยการจำลองสถานการณ์ (Simulation) เป็นสิ่งจำเป็นสำหรับหน่วยงานที่มีหน้าที่ป้องกัน โดยจะต้องมีการดำเนินงาน เช่นเดียวกับแผนการรับมือกับภัยพิบัติแห่งชาติ มีผู้รับผิดชอบในแต่ละ ระดับความรุนแรงของสถานการณ์ เพื่อบริหารงานในการแก้ปัญหา

๒.๔ การขยายขอบเขตของการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นสิ่งจำเป็น โดยเฉพาะหน่วยงานในระดับปฏิบัติการ ทั้งภาครัฐ รัฐวิสาหกิจ และหน่วยงาน

ภาคเอกชนที่สำคัญ เพื่อขยายฐานในการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศให้ครอบคลุมทั้ง ๖ กลุ่ม

๓. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

๓.๑ การวิจัยเพื่อการประเมินผลการบูรณาการและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เพื่อการพัฒนาและการยกระดับขีดความสามารถของไทย ตามห้วงระยะเวลาที่เหมาะสม เช่น ๖ เดือน ๑ ปี และ ๒ ปี เป็นต้น

๓.๒ การวิจัยเปรียบเทียบ ด้านการพัฒนาบุคคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างการฝึกและผลิตบุคลากรขึ้นเอง ของหน่วยงานที่รับผิดขอบกับการจ้างบุคลากรจากภายนอก (Out sourcing) เพื่อพัฒนาทางด้านกระบวนการศึกษาและประสิทธิภาพในการปฏิบัติงาน

บรรณานุกรม

ภาษาไทย

วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

จตุชัย แพงจันทร์, นาวาอากาศโท. “รูปแบบการปฏิบัติการสงครามไซเบอร์ และแนวทางการพัฒนาศักยภาพความพร้อมในการปฏิบัติการสงครามไซเบอร์ ภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, ๒๕๕๕.

ชนกศ์ จรจำรัส, พันเอก. “การพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหม” เอกสารวิจัย, วิทยาลัยการทัพบก,๒๕๕๙๘.

ณรงค์เวตย์ เรืองจวง, นาวาอากาศเอก. “แนวทางการพัฒนาขีดความสามารถ บุคลากรด้านไซเบอร์ของกองทัพอากาศ”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๙.

ประสงค์ ปราณีตพลกรัง, นาวาอากาศเอก ดร. “แผนยุทธศาสตร์การวิจัยและพัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศ” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ อากาศ สถาบันวิชาการทหารอากาศชั้นสูง กองบัญชาการฝึกศึกษาทหารอากาศ, ๒๕๕๗.

วัชรพงศ์ ธรรมรักษ์, นาวาอากาศโท. “ตัวแบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรองรับการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) สำหรับกองทัพอากาศ” เอกสารวิจัย, โรงเรียนเสนาธิการทหารอากาศ, ๒๕๕๔.

วิโรจน์ ธันวรักษ์กิจ,พลเรือตรี. “แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย” เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๖.

สุชาติ ผ่องพุฒิ ,พลตรี. “แนวทางการรองรับสงครามไซเบอร์ของกองทัพไทย” เอกสารวิจัย,;ll วิทยาลัยป้องกันราชอาณาจักร, ๒๕๕๖.

วารสาร และหนังสือพิมพ์

คณะกรรมการพัฒนาระบบราชการ, สำนักงาน. “การบูรณาการการบริหารราชการ”, เอกสารดาวน์โหลด, มกราคม ๒๕๖๐.

รัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “ความมั่นคงปลอดภัยทางไซเบอร์”, เอกสารเผยแพร่. ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์, ๑๐ กันยายน ๒๕๕๙.

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, “แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์” เอกสารศึกษาเฉพาะกรณี พ.ศ.๒๕๖๐.

สัมภาษณ์

เฉลิมชัย วงษ์เกตุ, นาวาอากาศเอก, ผู้อำนวยการกองแผนไซเบอร์ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศ และอวกาศกลาโหม, สัมภาษณ์, ๒๙ มิถุนายน ๒๕๖๑.

ปรัชญา เฉลิมรัตน์, พลตรี, ผู้ชำนาญการสำนักงานปลัดกระทรวงกลาโหม, สัมภาษณ์, ๕ กรกฎาคม ๒๕๖๑.

ปราการ พันธุเสนา, นักวิชาการคอมพิวเตอร์ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สัมภาษณ์, ๒ กรกฎาคม ๒๕๖๑.

สมศักดิ์ ขาวสุวรรณ์, นาวาอากาศเอก, รองปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, สัมภาษณ์, ๒๘ มิถุนายน ๒๕๖๑.

อดิศักดิ์ สมบัติเจริญนนท์, พลตรี, ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, สัมภาษณ์, ๔ กรกฎาคม ๒๕๖๑.

ฐานข้อมูลอิเล็กทรอนิกส์

“การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ : ความท้าทายของกองทัพบก”. (ออนไลน์). เข้าถึงได้จาก http://rittee1834.blogspot.com/2014/08/cyber-challenge-of-army.html,2557.

“คู่มือ Cyber Security สำหรับประชาชน”. (ออนไลน์). เข้าถึงได้จาก http://www.nbtc.go.th/News/รวมบทความ-(1)/คู่มือ-Cyber-Security-สำหรับประชาชน.aspx.

“แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”, (ออนไลน์). เข้าถึงได้จาก http://rtna.ac.th/download/cyber/nationalcybersecurity.pdf.

“แนวโน้มภัยคุกคามความมั่นคงปลอดภัยสารสนเทศ”. (ออนไลน์). เข้าถึงได้จาก https://www.acisonline.net/?p=5040&kabg=th}2559.

“ภัยคุกคาม แนวโน้ม และการสร้างความเชื่อมั่นด้าน Cyber Security”. (ออนไลน์). เข้าถึงได้จาก http:--www.techtalkthai.com/cdic-2 0 1 6 –cyber-security-threats-and-trends-,2559.

“มาตรฐาน ISO/IEC 27001 : 2013”. (ออนไลน์). เข้าถึงได้จาก http://www.rtna.ac.th/Download/247001-2013.pdf, 2556.

“ศัพท์น่ารู้ในโลกไซเบอร์”. (ออนไลน์). เข้าถึงได้จาก https://krujayja.wordpress.com/Blog-d-d/class-room-คำศัพท์น่ารู้ในโลกไซเบอร์.

“หลักการและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์”. (ออนไลน์). เข้าถึง

ได้จาก http://www.dmsc.moph.go.th/itc/usefiles/files/law_lecture%20(2),odf.

ระเบียบ

“ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐”, ราชกิจจานุเบกษา, เล่มที่ ๑๓๔ ตอนพิเศษ ๒๕๙ ง, ๒๐ ตุลาคม ๒๕๖๐, หน้า ๑-๗.

เอกสารไม่ตีพิมพ์

กลาโหม, กระทรวง. “แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐-๒๕๖๔.

ดิจิทัลเพื่อเศรษฐกิจและสังคม, กระทรวง. “ร่างยุทธศาสตร์การรักำษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.๒๕๖๐-๒๕๖๔, ๒๐ ธันวาคม ๒๕๖๐.

ภาษาต่างประเทศ

Department of Defense USA, “The Department of Defense Cyber Strategy”. : Washington. DC, April 2015, P 1-33.

Ministry of Science, Technology and Innovation, Malaysia. “ the National Cyber Security Policy”. Malaysia 2017, P 1-7.

ประวัติย่อผู้วิจัย

ชื่อ นาวาอากาศเอก ชนินทร เฉลิมทรัพย์

วัน เดือน ปีเกิด ๑๐ มกราคม ๒๕๐๕

การศึกษา ปริญญาตรี วิศวกรรมอากาศยาน โรงเรียนนายเรืออากาศ พ.ศ.๒๕๒๙
ปริญญาโท การบริหารจัดการทรัพยากรเพื่อความมั่นคง มหาวิทยาลัยบูรพา พ.ศ.๒๕๒๙

ประวัติการทำงาน

นายทหารยุทธการ ฝูงบิน ๒๐๑ กองบิน ๒
หัวหน้าแผนกปกครอง โรงเรียนนายทหารชั้นผู้บังคับหมวด กรมยุทธศึกษาทหารอากาศ
หัวหน้าแผนกปฏิบัติการ กองจำลองยุทธ วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ
ผู้ช่วยผู้อำนวยการกองจำลองยุทธ วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ
รองผู้อำนวยการกองจำลองยุทธ วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ
ผู้อำนวยการกองจำลองยุทธ วิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

ตำแหน่งปัจจุบัน รองเสนาธิการวิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ
ผู้วิจัย นาวาอากาศเอก ชนินทร เฉลิมทรัพย์ **หลักสูตร** วปอ. **รุ่นที่** 60
ตำแหน่ง รองเสนาธิการวิทยาลัยเสนาธิการทหาร สถาบันวิชาการป้องกันประเทศ

ความเป็นมาและความสำคัญของปัญหา

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศ ซึ่งถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสาร จึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้น สร้างความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่าง ๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม

ดังนั้น การรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ จึงเป็นเรื่องสำคัญสำหรับทุกหน่วยงาน เนื่องจากหน่วยงานเหล่านั้นต่างประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนงานตามภารกิจต่าง ๆของตน และเพื่อการบริการประชาชน การบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ รวมทั้งการประสานงานกับหน่วยงานอื่นเพื่อกระจายข่าวสาร เพื่อปรับปรุงข้อมูล วิธีการ การป้องการ และลดผลกระทบจากอันตรายที่เกิดขึ้นจึงเป็นเรื่องจำเป็น

ผู้วิจัย จึงมีความสนใจในการศึกษา แนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ เพื่อหาทางพัฒนา และเสริมสร้างความมั่นคง โดยเฉพาะความมั่นคงทางทหารและความมั่นคงทางเศรษฐกิจ และเป็นแนวทางให้ส่วนราชการที่เกี่ยวข้องได้ดำเนินการไปในทิศทางเดียวกัน เพื่อตอบสนองต่อการคุกคามความมั่นคงปลอดภัยทางไซเบอร์ ได้รวดเร็วและทันท่วงที

วัตถุประสงค์ของการวิจัย

1. ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการ และ การรักษาความมั่นคงปลอดภัยไซเบอร์

2. ศึกษาแนวนโยบายการกำหนดยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความ

มั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

3. เสนอแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

ขอบเขตของการวิจัย

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยต้องการศึกษาแนวทางการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ โดยมีขอบเขต ดังนี้

1. ขอบเขตด้านประชากร ได้แก่ การสัมภาษณ์ผู้ทรงคุณวุฒิที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานที่เกี่ยวข้อง

2. ขอบเขตด้านเนื้อหา ได้แก่ เอกสาร ระเบียบ คำสั่ง นโยบาย และแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

3. ขอบเขตด้านพื้นที่ มุ่งเน้นเฉพาะการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างหน่วยงานที่เกี่ยวข้องภายใต้กระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาวิเคราะห์ การกำหนดนโยบาย ยุทธศาสตร์และการบริหารจัดการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เปรียบเทียบกับแนวความคิดความมั่นคงปลอดภัยไซเบอร์ของต่างประเทศ และสัมภาษณ์เชิงลึกกับกลุ่มเป้าหมาย คือ ผู้ทรงคุณวุฒิ ในส่วนที่รับผิดชอบการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบกับการตรวจสอบเอกสารทางวิชาการที่เกี่ยวข้อง

ผลการวิจัย

ผู้วิจัยได้สรุปผลการวิจัยตามวัตถุประสงค์ 3 ข้อ ดังนี้

1. การศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการบริหารจัดการและการรักษาความมั่นคงปลอดภัยไซเบอร์ สรุปได้ดังนี้

1.1 องค์กรต้องเป็นองค์กรที่นำเทคนิคการบริหารจัดการมาใช้ ต้องมีโครงสร้างและรูปแบบที่สอดคล้องกับสภาพแวดล้อมของสังคมนั้นๆ ต้องเป็นองค์กรแห่งการเรียนรู้ (Learning Organization) ซึ่งจะต้องอาศัยความเข้าใจและความมุ่งมั่นในการทำระบบย่อยทั้ง 5 ระบบและองค์การแห่งการเรียนรู้อันได้แก่ การเรียนรู้ (Learning) องค์การ (Organization) คน (People) ความรู้ (Knowledge) และเทคโนโลยี (Technology)

1.2 การบูรณาการการบริหารจัดการ คือการบริหารงานที่ทุกหน่วยงาน ทำงานแบบมุ่งเน้นผลงาน (Result) ตามยุทธศาสตร์ หลักที่กำหนดขึ้น เป็นการทำงานของหลายหน่วยงานโดยอาศัยความเชี่ยวชาญและความชำนาญการของแต่ละหน่วยงาน ที่แตกต่างกัน โดยร่วมกันคิดร่วมกันทำงาน โดยใช้ทรัพยากรร่วมกัน เพื่อให้บรรลุเป้าหมาย มั่งสู่ผลสำเร็จ

1.3 ภัยคุกคามด้านไซเบอร์ โดยสภาพและลักษณะของภัยคุกคามที่มีการเปลี่ยนแปลงไปจากเดิมอย่างมาก มีรูปแบบการโจมตีเป้าหมายที่หลากหลาย ดังนั้นแนวความคิดและแนวทางในการป้องกัน ให้เกิดประสิทธิผล จำเป็นอย่างยิ่งที่จะต้องปรับความคิดและปรับกลยุทธให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป การวางแผนป้องกันจากภัยของไซเบอร์ ควรนำระบบมาตรฐาน ISO/IEC27001 : 2013 ซึ่งเป็นมาตรฐานที่มุ่งเน้นด้านการบริหารจัดการ ความมั่นคงปลอดภัยสำหรับสารสนเทศมาเป็นแนวทาง นอกจากนี้แล้ว การแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ ควรมีมุมมอง 3 ด้าน (PPT) ได้แก่ People, Process and Technology การปรับกระบวนการโดยการปฏิบัติตามมาตรฐาน เป็นการแก้ปัญหาที่ Process และ Technology แต่ปัจจัยสำคัญที่สุดอยู่ที่ มนุษย์ หรือ People

2. การศึกษาแนวนโยบายการกำหนดยุทธศาสตร์และการดำเนินงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

2.1 กระทรวงกลาโหม ได้กำหนดกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี คือ พ.ศ.2558-2562 โดยกำหนดประเด็นยุทธศาสตร์ ไว้ 3 ประเด็น ดังนี้

2.1.1 ประเด็นยุทธศาสตร์การป้องกันเชิงรุก โดยใช้พลังอำนาจทางไซเบอร์กองทัพไทย เพื่อปฏิบัติการในมิติไซเบอร์ต่อฝ่ายตรงข้าม ทั้งที่เป็นรัฐ ไม่ใช่ รัฐ และสนับสนุนโดยรัฐ ตลอดจนกลุ่มบุคคลหรือบุคคลใดๆ ที่อาจเป็นภัยคุกคามทางไซเบอร์ โดยจะมุ่งเน้นไปที่ปฏิบัติการเชิงรุกในลักษณะจำกัดและการตอบโต้อย่างรวดเร็ว

2.1.2 ประเด็นยุทธศาสตร์การผนึกกำลังป้องกันประเทศสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย โดยการสร้างความร่วมมือและบูรณาการขีดความสามารถในมิติไซเบอร์ของทุกภาคส่วนเข้าด้วยกันอย่างเป็นระบบ

2.1.3 ประเด็นยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคงสำหรับการปฏิบัติการในมิติไซเบอร์ของกองทัพไทย โดยร่วมมือประเทศเพื่อนบ้าน ประเทศสมาชิกกลุ่มอาเซียน และมิตรประเทศ เพื่อการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

2.2 กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ได้มีการจัดตั้งหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นที่เรียบร้อยแล้ว โดยแบ่งการดำเนินการเป็น 2 ส่วน คือ ส่วนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) เชิงรับ และส่วนสนับสนุนในการตอบสนองต่ออุบัติการณ์ด้านความมั่นคงปลอดภัย (Computer Security incident Response Team : CSIRT)

2.3 จากการศึกษาการดำเนินงาน พบว่า ยังคงมีปัญหาและข้อขัดข้อง ซึ่งส่งผลกระทบต่อการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

2.3.1 การจัดองค์กรด้านไซเบอร์ของกระทรวงกลาโหม อยู่ในระหว่างการปรับปรุง ส่งผลให้การประสานงานทั้งในด้านนโยบายและด้านการปฏิบัติเป็นไปอย่างจำกัด

2.3.2 ยังมีข้อขัดข้องในการแลกเปลี่ยนข้อมูลการจัดการภัยคุกคามทางไซเบอร์ทั้งในระดับกระทรวงกลาโหม และการเชื่อมโยงระดับชาติ

2.3.3 การผลิต รักษา และพัฒนาบุคลากรที่ปฏิบัติงานทางด้านไซเบอร์ยังไม่เป็นระบบและต่อเนื่อง

2.4 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ดำเนินการตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วย คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ.2560 ได้กำหนดจัดประชุมคณะกรรมการฯ ครั้งที่ 1/2561 โดยพัฒนา 4 เรื่อง ดังนี้

2.4.1 กรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยง และความสอดคล้องไปในทิศทางเดียวกัน

2.4.2 แนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ของประเทศ และแนวทางปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure :SOP)

2.4.3 แนวทางการพัฒนาบุคคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ระยะเร่งด่วน

2.4.4. แนวทางการจัดตั้ง Cyber security Agency (CSA) ทำหน้าที่หน่วยงานประสานงานกลาง และหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความมั่นคงปลอดภัยไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

จากการศึกษา พบว่า การดำเนินงานอยู่ในขั้นเตรียมการ ทั้งในระดับนโยบายและแผนปฏิบัติการ เพื่อเตรียมความพร้อมในการปกป้อง ป้องกันและรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ ยังขาดรายละเอียดอีกมากทั้งในด้านโครงสร้างหน่วย อำนาจหน้าที่ในการดำเนินงาน กฎหมายที่รองรับการทำงาน เป็นต้น

3. แนวทางในการบูรณาการการรักษาความมั่นคงปลอดภัยไซเบอร์

ผู้วิจัยได้ศึกษาค้นคว้าแนวทางการบูรณาการบริหารจัดการของสำนักงานคณะกรรมการพัฒนาระบบราชการ นโยบาย แผนปฏิบัติการ และการดำเนินงาน การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหม และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตลอดจนความคิดเห็นจากการสัมภาษณ์ จึงขอเสนอแนวทางในการบูรณาการ ดังนี้

3.1 การจัดกาความรู้และการบริหารความเสี่ยง โดยต้องเป็นความริเริ่มของผู้นำองค์กรในการกำหนดนโยบาย หรือแนวทางปฏิบัติให้ชัดเจน มีเป้าหมายที่จัดให้มีมาตรการกำกับดูแล เพื่อให้หน่วยงานและบุคลากรได้ตระหนักรู้ถึงความสำคัญของการรักษาความปลอดภัยทางไซเบอร์ และบริหารความเสี่ยง เพื่อดำเนินการแก้ไขและฟื้นคืนสภาพ (Resilience) ให้เร็วที่สุด

3.2 การทำงานแบบเครือข่าย (Network) โดยการทำงานเชื่อมโยงตามประเด็นยุทธศาสตร์ร่วมกัน (Common agenda) โดยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นเจ้าภาพ

3.3 การร่วมกันกำหนดมาตรฐานแนวทางการปฏิบัติทั้งในด้านการทำงาน การเชื่อมโยงติดต่อประสาน รวมทั้งมาตรฐานในทางเทคโนโลยี โดยกำหนดเป็น ระเบียบปฏิบัติประจำ (SOP)

3.4 การศึกษาและการวิจัยพัฒนา ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อต่อยอดองค์ความรู้ พัฒนาบุคคล ซ้อมจับมือกับภัยคุกคาทางไซเบอร์ และปริเมินความพร้อมด้านความมั่นคง

ปลอดภัยไซเบอร์ โดยประสานความร่วมมือกับศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคคลความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cyber security capacity Building Centre)

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

1. รัฐบาล ควรเร่งประกาศใช้พระราชบัญญัติ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... และปรับปรุงแก้ไขกฎหมายที่ออกมาก่อน เช่น พระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และแก้ไขเพิ่มเติม พ.ศ.2560 เพื่อให้เกิดความสอดคล้องและทันสมัย

2. เร่งรัดการดำเนินการด้านโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เพื่อเป็นพื้นฐานในการดำเนินงานที่เป็นมาตรฐานของภาครัฐและการจัดสร้างชานชาลาข้อมูล (Platform) เพื่อเป็นพื้นฐานในการแลกเปลี่ยนและแบ่งปันข้อมูลระหว่างหน่วยงานและเพื่อรักษาความมั่นคงปลอดภัยทางไซเบอร์

ข้อเสนอแนะระดับปฏิบัติการ

1. การดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในลักษณะการป้องกันเชิงรุก (Active defense) และการปฏิบัติการเชิงรุก (Offense) เช่น การข่าวกรองทางไซเบอร์ ควรมีหน่วยงานที่ชัดเจนในการดำเนินงานในที่นี้ควรเป็นกระทรวงกลาโหม แต่ควรมีกฎหมายรองรับเนื่องจากปัจจุบันอาจจะเสี่ยงต่อการผิดกฎหมายทั้งในประเทศและระหว่างประเทศ

2. ควรมีกรอบการดำเนินงานเพื่อความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) โดยอาจใช้กรอบการดำเนินงานของสถาบันมาตรฐานแลชะเทคโนโลยีแห่งสหรัฐอเมริกา (The National Institute of Standards and Technology : NIST) สามารถนำมาปรับใช้ให้เข้ากับวัฒนธรรมองค์กรและนโยบายของประเทศได้ โดยกรอบการดำเนินงานนี้เป็นกระบวนการแบบวนซ้ำพัฒนาแบบค่อยเป็นค่อยไป เพื่อรับมือกับรูปแบบที่เปลี่ยนแปลงไปของภัยคุกคามความมั่นคงปลอดภัยไซเบอร์

3. การคาดการณ์ การถูกโจมตี โครงสร้างพื้นฐานที่สำคัญทางสารสนเทศ โดยการจำลองสถานการณ์ (Simulation) เป็นสิ่งจำเป็นสำหรับหน่วยงานที่มีหน้าที่ป้องกัน โดยจะต้องมีการดำเนินงาน เช่นเดียวกับแผนการรับมือกับภัยพิบัติแห่งชาติ มีผู้รับผิดชอบในแต่ละระดับความรุนแรงของสถานการณ์ เพื่อบริหารงานในการแก้ปัญหา

4. การขยายขอบเขตของการบูรณาการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นสิ่งจำเป็น โดยเฉพาะหน่วยงานในระดับปฏิบัติการ ทั้งภาครัฐ รัฐวิสาหกิจ และหน่วยงานภาคเอกชนที่สำคัญ เพื่อขยายฐานในการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศให้ครอบคลุมทั้ง 6 กลุ่ม

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. การวิจัยเพื่อการประเมินผลการบูรณาการและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เพื่อการพัฒนาและการยกระดับขีดความสามารถของประเทศ ตามห้วงระยะเวลาที่

เหมาะสม เช่น 6 เดือน 1 ปี และ 2 ปี เป็นต้น

2. การวิจัยเปรียบเทียบด้านการพัฒนาบุคคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างการฝึกและผลิตบุคลากรขึ้นเองโดยหน่วยงานที่รับผิดขอบกับการจ้างบุคลากรเชี่ยวชาญจากภายนอก (Out sourcing) ทั้งนี้เพื่อให้เกิดการพัฒนาทางด้านกระบวนการศึกษาและประสิทธิภาพในการปฏิบัติงาน