แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์

โดย

พลเรือตรี อุดม ประตาทะยัง
รองเจ้ากรมข่าวทหาร
กองบัญชาการกองทัพไทย

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 60
ประจำปีการศึกษา พุทธศักราช 2560 - 2561

บทคัดย่อ

เรื่อง แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์
ลักษณะวิชา ยุทธศาสตร์
ผู้วิจัย พลเรือตรี อุดม ประตาทะยัง **หลักสูตร** วปอ.รุ่นที่ 60

การศึกษาเรื่อง แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ ในครั้งนี้จะศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษา แนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต ประกอบกับได้มีการนำแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องมาใช้เพื่อเป็นแนวทางในการศึกษา พร้อมเสนอแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ซึ่งพบว่าการมีหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อการป้องกันภัยคุกคามทางไซเบอร์ และประสานงานทั้งภายในและระหว่างประเทศในการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์มีความสำคัญ อีกทั้งต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐและเอกชนเพื่อยกระดับความพร้อมรับมือภัยคุกคามทางไซเบอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ ทั้งนี้ การร่างพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันนั้นอาจยังขาดองค์ประกอบที่สำคัญหลายประการ และถ้านำมาใช้เป็นเป็นกรอบในการบริหารยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะมีความสมบูรณ์เพียงพอที่จะนำไปใช้เป็นกลไกสำคัญในการขับเคลื่อนได้หรือไม่ ประกอบกับนโยบายของประเทศไทยในปัจจุบัน โดยรัฐบาลปัจจุบันมีนโยบายขับเคลื่อนประเทศไทยสู่ความมั่นคง มั่งคั่งและยั่งยืน และนำไปสู่ความเป็น Thailand 4.0 ปรับเปลี่ยนโครงสร้างเศรษฐกิจ ไปสู่ “Value–Based Economy” หรือ เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม หน่วยงานของรัฐจึงต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์เป็นอย่างมาก เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสามารถดำเนินการควบคู่ไปกับยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) ที่เข้มแข็งด้วย และจากการศึกษาข้อมูลพบว่าการดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ถึงแม้ว่าในปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์มากขึ้น แต่องค์กรต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและ บางครั้งมีความขัดแย้งกัน ประกอบกับการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ จากการศึกษาข้อมูลปัญหาการบูรณาการการดำเนินงานรักษาความปลอดภัยไซเบอร์มีปัจจัยต่างๆ ดังนี้ (1) ปัจจัยจากแนวความคิดของฝ่ายต่างๆ (2) ปัจจัยด้านการประสานงาน (3) ปัจจัยด้านงบประมาณ (4) ปัจจัยด้านข้อมูลระหว่างฐานข้อมูล ในการศึกษาต่อไปเพื่อแก้ไขปัญหา เห็นสมควรศึกษาเกี่ยวกับการพัฒนาการบูรณาการด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย เพื่อให้เห็นถึงแนวทางที่หน่วยงานต่างๆ สามารถบูรณาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ABSTRACT

Title Appropriate Approaches to Developing Cyber Security Strategies
Field Strategy
Name Rear Admiral Udom Pratathayang **Course** NDC Class 60

A proper study of the development of the national cyber security strategy will be the study of cyber security in the country. Develop cyber security, cyber attacks, the impact of cyber attacks on national security, and how to deal with cyber-security threats in the future. Theories and related research have been used as a guideline for the study. Offer Strategies for Developing Cyber Security Strategies There are cyber security agencies in the country. For protection against cyber threats. It is important to coordinate the exchange of cyber security information both locally and internationally. It also requires public-private partnerships to improve cyber threats. The Cyber Security Act today may still lack several key elements. And if it is used as a framework for managing cyber security strategies, is it enough or will it be a key driving force? In line with current Thai policy. The government has a policy to push Thailand into prosperity and prosperity and become Thailand. "Value for money" or innovation-driven economy. State agencies must be cautious about cybercrime threats. Accelerating the development of the digital industry is a right direction. However, there must be a strong cyber security strategy. The study also found that Thailand's cyber-security operations were different. Although the current cyber security risks are increasing But security organizations are fragmented and sometimes conflicting. In addition to the lack of security skills, Many organizations do not understand and can not handle the risk effectively. The study of the problems of integrating cybersecurity has the following elements: (1) the factors of the concept of the department; (2) the factors of coordination; (3) the factors of the budget; (4) the factors between the databases in the study. To fix It is recommended to study the development of cyber security in Thailand. To see how various agencies. Enables effective cyber security integration.

คำนำ

จากการที่ผู้วิจัยรับราชการในกรมข่าวทหาร ได้มีโอกาสปฏิบัติงานด้านการข่าวและด้านการต่างประเทศ ร่วมกับกองทัพมิตรประเทศที่มีความสัมพันธ์ด้านการทหารกับกองทัพไทย ทั้งกระทรวงการต่างประเทศ และหน่วยงานอื่นๆ ทั้งภาครัฐและเอกชน เห็นว่า ปัญหาความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ทุกประเทศจะต้องเรียนรู้ให้เกิดความเข้าใจ โดยเฉพาะอย่างยิ่งเข้าใจถึงความร้ายแรงของภัยคุกคามที่อาจเกิดขึ้นและกระทบต่องานด้านความมั่นคงของประเทศในอนาคต ประกอบกับนโยบายของประเทศไทยในปัจจุบัน มีนโยบายขับเคลื่อนประเทศไทยสู่ความเป็น Thailand 4.0 ปรับเปลี่ยนโครงสร้างเศรษฐกิจ ไปสู่ “Value–Based Economy” หน่วยงานของรัฐจึงต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์เป็นอย่างมาก เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสามารถดำเนินการควบคู่ไปกับยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็งด้วย การพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ จึงมีความสำคัญต่อความมั่นคงของชาติในอนาคตต่อไป

ผู้วิจัยหวังเป็นอย่างยิ่งว่า เอกสารวิจัยฉบับนี้จะเป็นประโยชน์ต่อการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เพื่อให้การปฏิบัติในการแก้ปัญหาดำเนินการอย่างเป็นระบบ สามารถรักษาไว้ซึ่งความมั่นคงของประเทศชาติในอนาคตต่อไป

พลเรือตรี

(อุดม ประตาทะยัง)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ.รุ่นที่ 60
ผู้วิจัย

สารบัญ

หน้า

สารบัญ

สารบัญตาราง

สารบัญแผนภาพ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ภายใต้การเปลี่ยนแปลงในศตวรรษที่ 21 เทคโนโลยีสารสนเทศทำให้เกิดการเปลี่ยนแปลงทางเศรษฐกิจและสังคมอย่างรวดเร็ว การเชื่อมโยงเครือข่ายออนไลน์กลายเป็นทั้งโอกาสและภัยคุกคามระดับชาติ กลุ่มอาชญากร กลุ่มก่อการร้าย กลุ่มแฮกเกอร์ และรัฐบาลต่างชาติ ต่างมุ่งหาประโยชน์จากโลกไซเบอร์ ซึ่งเป็นสภาวะของโลกเสมือนจริงที่ไม่มีเขตแดนกั้นระหว่างประเทศ ส่งผลให้เกิดภัยคุกคามในรูปแบบใหม่ที่เรียกว่า ภัยคุกคามทางไซเบอร์ โดยที่คนจำนวนมากยังไม่ตระหนักถึงความร้ายแรงของภัยคุกคามนี้

ริชาร์ด เอ. คลาร์ก (Richard A. Clarke) อดีตที่ปรึกษาประธานาธิบดีสหรัฐอเมริกาด้านความมั่นคง ได้สรุปปัญหาภัยคุกคามทางไซเบอร์แบ่งเป็น 4 ลักษณะ คือ Cybercrime เป็นปัญหาการก่ออาชญากรรมทางไซเบอร์, Hacktivism เป็นการแฮ็คข้อมูลลับไม่ว่าจะของภาครัฐหรือภาคเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะ, Espionage เป็นการจารกรรมข้อมูลเพื่อนำไปใช้ประโยชน์ และ War หรือ Cyberwar สงครามไซเบอร์ เป็นปฏิบัติการของรัฐหนึ่งต่อระบบคอมพิวเตอร์หรือเครือข่ายของอีกรัฐหนึ่ง โดยมีวัตถุประสงค์เพื่อก่อกวนหรือทำลายให้ระบบหยุดชะงักหรือไม่สามารถทำงานได้ตามปกติ (Disruption) ซึ่งบางประเทศได้กำหนดให้สงครามไซเบอร์บูรณาการเข้ามาเป็นส่วนหนึ่งของยุทธศาสตร์ทางทหาร โดยมีการทุ่มงบประมาณจำนวนมากเพื่อเพิ่มขีดความสามารถด้านสงครามไซเบอร์

ภัยคุกคามในรูปแบบดังกล่าว เป็นภัยคุกคามรูปแบบใหม่ (Non-traditional Threat) ที่ใช้พื้นที่ในโลกไซเบอร์ในการปฏิบัติการ มีการใช้เทคโนโลยีโจมตีเป้าหมายหลากหลายรูปแบบ ตั้งแต่ชนิดเบาที่สุดจนถึงรุนแรงที่สุด เช่น

1. การโจมตีเว็บไซต์ หรือ บล็อกเว็บไซต์
2. การโฆษณาชวนเชื่อด้วยการเผยแพร่ข้อมูลผ่านอินเทอร์เน็ต
3. การเจาะเครือข่ายคอมพิวเตอร์ของรัฐบาลเพื่อโจรกรรมข้อมูล
4. การทำลายเครือข่ายด้านการทหารเพื่อลดประสิทธิภาพการทำงานหรือทำให้ระบบไม่สามารถทำงานได้
5. การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้า ประปา การสื่อสาร การขนส่งและคมนาคม เป็นต้น

ช่วงสงครามอ่าวครั้งที่ 2 ระหว่างสหรัฐฯ และพันธมิตรกับอิรัก สิ่งที่สหรัฐฯ ปฏิบัติการเป็นอย่างแรก คือ ทำลายเครือข่ายคอมพิวเตอร์และอีเล็คโทรนิคของอิรักที่ใช้ควบคุมระบบการยิงของอาวุธ

พฤษภาคม 2550 ประเทศเอสโทเนีย ถูกโจมตีทางไซเบอร์อย่างหนัก ส่งผลให้เกิดความเสียหายทั้ง รัฐสภา กระทรวง ทบวง กรม ธนาคาร และสื่อสารมวลชนต่างๆ

กันยายน 2550 กระทรวงกลาโหมสหรัฐฯ ที่ทำการรัฐบาลของฝรั่งเศส เยอรมัน และอังกฤษ ถูกโจมตีทางไซเบอร์จนได้รับความเสียหายอย่างหนัก

ในปี 2552 ประธานาธิบดี บารัค โอบามา ประกาศว่า ระบบพื้นฐานดิจิตอลของสหรัฐอเมริกา เป็นสินทรัพย์ยุทธศาสตร์ของชาติ และในเดือน พฤษภาคม 2553 กระทรวงกลาโหมสหรัฐฯ ได้จัดตั้งกองบัญชาการไซเบอร์ (Cyber Command) เพื่อป้องกันเครือข่ายของกองทัพสหรัฐฯ และโจมตีระบบของประเทศอื่น โดยอยู่ในความรับผิดชอบของสภาความมั่นคงแห่งชาติ สงครามไซเบอร์ จึงถูกยกให้เป็นหนึ่งในสมรภูมิรบอับดับ 5 รองจาก สมรภูมิรบทางบก ทางทะเล ทางอากาศ และทางอวกาศ นายกรัฐมนตรีของอังกฤษ เดวิด คาเมรอน ในสมัยนั้นประกาศให้ หน่วยงานรักษาความปลอดภัยแห่งชาติ ยกระดับให้สงครามไซเบอร์ ขึ้นมาเป็นหนึ่งในภัยคุกคามที่สำคัญของสหราชอาณาจักร

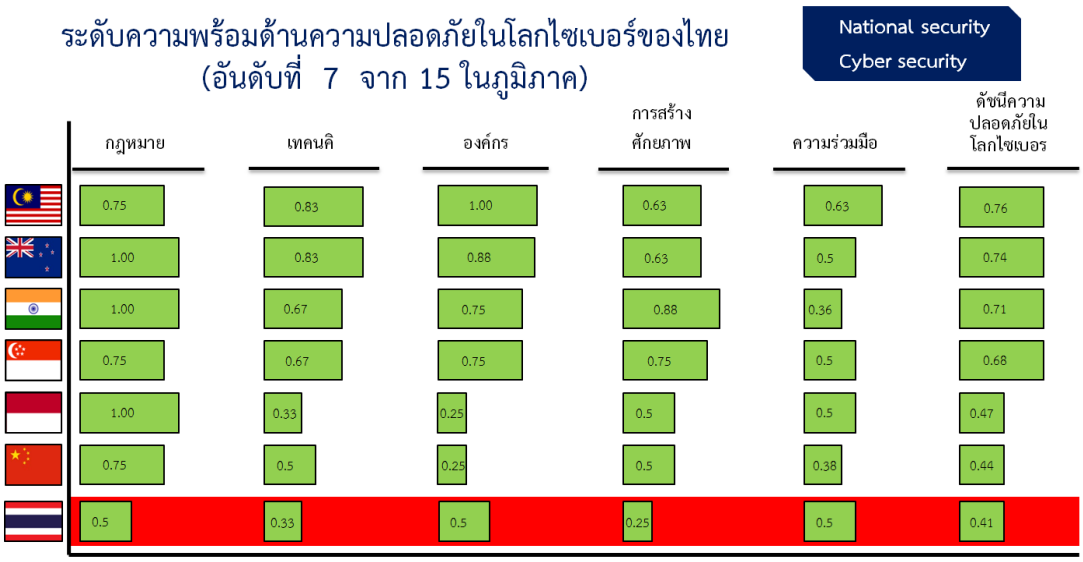
ปัจจุบันยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร (UK National Cyber Security Strategy 2016) จัดให้ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) มีความสำคัญเทียบเท่าภัยคุกคามก่อการร้าย ภัยคุกคามความมั่นคงทางทหาร และภัยคุกคามจากภัยธรรมชาติ ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร มุ่งป้องกันภัยคุกคามทางไซเบอร์เพื่อส่งเสริมการพัฒนาด้านเศรษฐกิจ ป้องกันภัยคุกคามความมั่นคงของชาติ และการดำเนินชีวิตของประชาชน มีแผนความร่วมมือระหว่างภาครัฐและเอกชนอย่างเป็นรูปธรรม

The Economist Magazine กล่าวว่า จีนมีแผนที่จะเป็นเจ้าแห่งสงครามสารสนเทศในกลางศตวรรษที่ 21 และยังมีประเทศอื่นที่มีแผนในลักษณะเดียวกัน เช่น รัสเซีย อิสราเอล เกาหลีเหนือ เป็นต้น นอกจากนั้นอิหร่านยังอ้างว่าจะพัฒนาขีดความสามารถของตนให้เป็นกองทัพไซเบอร์ที่ใหญ่ที่สุดเป็นอันดับ 2 ของโลก

ปัจจุบันประเทศไทยมีการปรับโครงสร้างตั้งศูนย์ไซเบอร์ทหาร มียุทธศาสตร์หลัก คือการตั้งรับดูแลระบบเครือข่ายให้เกิดความปลอดภัย แต่ก็ต้องแฝงด้วยปฏิบัติการเชิงรุก ทั้งนี้กองทัพไทยในฐานะหน่วยงานด้านความมั่นคง จึงวางยุทธศาสตร์สงครามไซเบอร์ ที่กำหนดให้เหล่าทัพ เพิ่มขีดความสามารถ 3 ด้าน คือ การป้องกัน การพัฒนา และร่วมกับหน่วยภายใน เพื่อใช้ประโยชน์ในการปฏิบัติการทางทหาร ในการผนึกกำลังป้องกันประเทศทุกรูปแบบ ทั้งการจารกรรม และการโจมตีฐานข้อมูล

อย่างไรก็ตาม การเติบโตและความสามารถในการเข้าถึงโครงข่ายอินเตอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างมาก ทำให้ความเสี่ยงจากภัยคุกคามทางไซเบอร์เพิ่มขึ้น และจะถูกยกระดับเป็นภัยคุกคามเชิงยุทธศาสตร์ของประเทศในอนาคต จากสถานการณ์ไซเบอร์ของประเทศไทยในปี 2558 ถูกจัดอันดับว่าเป็นประเทศที่ถูกโจมตีผ่านระบบไซเบอร์เป็นอันดับที่ 33 จาก 250 ประเทศทั่วโลก โดยเฉพาะสถานการณ์การถูกโจมตีเมื่อเดือน สิงหาคม 2558 นั้น เว็บไซต์ของหน่วยงานราชการ เช่น เว็บไซต์ของจังหวัดลำพูน และเว็บไซต์ของฝ่ายอำนวยการ 1 กองบัญชาการตำรวจนครบาล ถูกเจาะระบบเปลี่ยนหน้าโฮมเพจเป็นข้อความเรียกร้องสันติภาพชาวมุสลิม พร้อมระบุว่าเป็นฝีมือของแฮกเกอร์แอลจีเรีย ซึ่งปัญหานี้เกิดขึ้นมาในขณะที่ประเทศไทย ยังไม่มีมาตรการดูแลเรื่องความมั่นคงและปลอดภัยทางทางไซเบอร์ที่ชัดเจน และรัดกุม

แผนภาพที่ 1-1 : ระดับความพร้อมด้านความปลอดภัยในโลกไซเบอร์ของไทย



ที่มา : International Telecommunication Union Report April, 2015

จะเห็นได้ว่าความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ทุกประเทศจะต้องเรียนรู้ให้เกิดความเข้าใจ โดยเฉพาะอย่างยิ่งเข้าใจถึงความร้ายแรงของภัยคุกคามที่อาจเกิดขึ้นและกระทบต่องานด้านความมั่นคงของประเทศในอนาคต ประกอบกับนโยบายของประเทศไทยในปัจจุบัน โดยรัฐบาล พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี และหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) มีนโยบายขับเคลื่อนประเทศไทยสู่ความมั่นคง มั่งคั่ง และยั่งยืน และนำไปสู่ความเป็น Thailand 4.0 ปรับเปลี่ยนโครงสร้างเศรษฐกิจ ไปสู่ “Value–Based Economy” หรือ เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม หน่วยงานภาครัฐจึงต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์เป็นอย่างมาก เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสามารถดำเนินการควบคู่ไปกับยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) ที่เข้มแข็งด้วย การศึกษาแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ จึงมีความสำคัญต่อความมั่นคงของไทยในอนาคต ผู้วิจัยจึงมีความสนใจที่จะศึกษาวิจัย เรื่อง “แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์” เพื่อรักษาไว้ซึ่งความมั่นคงของประเทศชาติในอนาคตต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์
2. เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์
3. เพื่อศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา : จะศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษากำหนดแนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต พร้อมเสนอแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

2. ขอบเขตด้านประชากร : สัมภาษณ์เชิงลึกต่อผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานต่างๆ ดังนี้

2.1 ผู้เชี่ยวชาญจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวน 5 คน

2.2 ผู้เชี่ยวชาญจากกระทรวงกลาโหม จำนวน 5 คน

2.3 ผู้เชี่ยวชาญจากสภาความมั่นคงแห่งชาติ จำนวน 5 คน

2.4 ผู้เชี่ยวชาญจากกองบัญชาการกองทัพไทยและเหล่าทัพต่างๆ จำนวน 10 คน

3. ขอบเขตด้านเวลา : จะใช้เวลาในการศึกษาวิจัยในครั้งนี้ตั้งแต่ พฤศจิกายน 2560 – พฤษภาคม 2561

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ จะรวบรวมเรื่องเกี่ยวกับยุทธศาสตร์ความมั่นคงทางไซเบอร์จากเอกสารและข้อมูลที่เกี่ยวข้อง จากแหล่งข้อมูลประกอบด้วย ห้องสมุดวิทยาลัยป้องกันราชอาณาจักร ห้องสมุดกองทัพเรือ สภาความมั่นคงแห่งชาติ รวมถึงจากเว็บไซต์ที่เกี่ยวข้อง

1.2 ข้อมูลปฐมภูมิ รวบรวมจากการสัมภาษณ์ผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์ จำนวน 25 คน ตามขอบเขตด้านประชากรดังที่กล่าวแล้วข้างต้น

2. การวิเคราะห์ข้อมูล จะใช้การวิเคราะห์เนื้อหา (Content Analysis) เป็นหลัก โดยการนำข้อมูลที่รวบรวมได้ทั้งข้อมูลทุติยภูมิและข้อมูลปฐมภูมิ มาจัดระเบียบแล้วนำมาวิเคราะห์ร่วมกับแนวความคิด ทฤษฎี ที่เกี่ยวข้อง แล้วสังเคราะห์ออกมาเป็นแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบถึงการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยในปัจจุบัน

2. ทำให้ทราบผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์รวมถึงทราบปัญหาอุปสรรคที่เกิดในการดำเนินการต่อภัยคุกคามไซเบอร์

3. ทำให้ทราบแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์

คำจำกัดความ

ความมั่นคงทางไซเบอร์	หมายถึง	มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ
สงครามไซเบอร์	หมายถึง	ปฏิบัติการของรัฐหนึ่งต่อระบบคอมพิวเตอร์หรือเครือข่ายของอีกรัฐหนึ่ง โดยมีวัตถุประสงค์เพื่อทำลายหรือก่อกวน ให้ระบบหยุดชะงักหรือไม่สามารถทำงานได้ตามปกติ (Disruption) รวมถึงผู้กระทำที่ไม่ใช่รัฐ (Non - state actor) เช่น กลุ่มผู้ก่อการร้าย กลุ่มการเมือง กลุ่มหัวรุนแรง องค์กรอาชญากรรมข้ามชาติ เป็นต้น
เทคโนโลยีสารสนเทศ	หมายถึง	เทคโนโลยีสารสนเทศ การค้นคิดและพัฒนาความสามารถของคอมพิวเตอร์ ไมโครอิเล็กทรอนิกส์และการสื่อสารโทรคมนาคมที่ทำให้มนุษย์สามารถสร้าง เก็บและสื่อสารข้อมูลข่าวสาร (ข้อความ ตัวเลข เสียง ภาพ) ได้อย่างกว้างขวางสะดวกรวดเร็วมากยิ่งขึ้น และสามารถสื่อสารกันได้ทั่วทุกมุมโลกอย่างรวดเร็วชนิดที่ไม่เคยเกิดขึ้นมา ก่อนในประวัติศาสตร์ของมนุษยชาติ หรือหมายถึง กระบวนการต่างๆ และระบบงานที่ช่วยให้ได้สารสนเทศที่ต้องการ สารสนเทศคือ ข่าวสารที่ได้จากการนำข้อมูลดิบ (raw data) มาคำนวณทางสถิติ หรือประมวลผลอย่างใดอย่างหนึ่ง ซึ่งข่าวสารที่ได้ออกมานั้น จะอยู่ในรูปที่สามารถนำไปใช้ได้ทันที
อินเทอร์เน็ต	หมายถึง	เครือข่ายคอมพิวเตอร์ที่ใหญ่ที่สุด ผู้ที่เป็นสมาชิกอินเตอร์เน็ตสามารถใช้บริการด้านการสื่อสารข้อมูลข่าวสาร ได้อย่างหลากหลาย อาทิ จดหมายอิเล็กทรอนิกส์ (E – mail) การขนถ่ายแฟ้มข้อมูล (ทั้งข้อมูล ข่าวสาร โปรแกรมอื่นๆ) การค้นหาไฟล์และฐานข้อมูล (ด้านธุรกิจ การศึกษา การวิจัยฯลฯ)กลุ่มสนทนาและข่าวสารเพื่อแลกเปลี่ยนทัศนะการใช้โปรแกรมขนาดเครื่องคอมพิวเตอร์อื่นๆ

อาชญากรรมไซเบอร์	หมายถึง	ความผิดที่กระทำขึ้นต่อปัจเจกบุคคลหรือกลุ่มของปัจเจกบุคคล ด้วยเหตุจูงใจทางอาญา ที่เจตนาทำให้เหยื่อเสื่อมเสียชื่อเสียง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ โดยทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ อาทิ อินเทอร์เน็ต และโทรศัพท์เคลื่อนที่ อาชญากรรมเช่นนั้นอาจคุกคามความมั่นคงและสภาวะทางการคลังของรัฐ
ภาวะโลกเสมือนจริง	หมายถึง	การเปลี่ยนแปลงการติดต่อทางสังคมจากการพบเจอในโลกแห่งความจริงไปสู่การพบเจอในโลกเสมือนจริง ซึ่งภาวะโลกเสมือนจริงนี้ได้เปลี่ยนบทบาทและข้อจำกัดทางสถานที่และเวลา และทำให้คนสามารถทำในสิ่งที่ไม่สามารถทำหรือทำได้ยากโลกแห่งความเป็นจริงได้โดยง่าย โลกไซเบอร์มีความเป็นโลกเสมือนจริง เนื่องจากโลกไซเบอร์ทำให้ข้อจำกัดเรื่องของเวลาและสถานที่หายไป อย่างเช่น เรื่องของเวลาที่ใช้ในการเคลื่อนย้าย หรือดำเนินการใดๆ ที่ซึ่งปกติแล้ว ถูกจำกัดในโลกแห่งความเป็นจริง หรือเรื่องของสถานที่ หรือการที่สามารถกระทำการต่างๆ ได้ในสถานที่ต่างๆ กันในเวลาเดียวกัน เป็นต้น ด้วยสภาวะดังกล่าว ทำให้การโจมตีก่อการร้ายไซเบอร์สามารถดำเนินการในลักษณะที่การก่อการร้ายแบบดั้งเดิมไม่สามารถทำได้ในโลกแห่งความเป็นจริง
ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์	หมายถึง	กรอบการดำเนินการ เพื่อปกป้อง รับมือป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์ อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ
ไทยแลนด์ 4.0	หมายถึง	วิสัยทัศน์เชิงนโยบายการพัฒนาเศรษฐกิจของประเทศไทย หรือ โมเดลพัฒนาเศรษฐกิจของรัฐบาล ภายใต้การนำของพลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) ที่เข้ามาบริหารประเทศบนวิสัยทัศน์ที่ ว่า “มั่นคง มั่งคั่ง และยั่งยืน” ที่มีภารกิจสำคัญในการขับเคลื่อนปฏิรูปประเทศด้านต่าง ๆ เพื่อปรับแก้ จัดระบบ ปรับทิศทาง และสร้างหนทางพัฒนาประเทศให้เจริญ สามารถรับมือกับโอกาสและภัยคุกคามแบบใหม่ๆ ที่เปลี่ยนแปลงอย่างเร็วรุนแรงในศตวรรษที่ 21 ได้

บทที่ 2
การทบทวนวรรณกรรมที่เกี่ยวข้อง

การศึกษา เรื่อง แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ ได้มีการนำแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องมาใช้เพื่อเป็นแนวทางในการศึกษา ดังนี้

1. แนวความคิดเรื่องยุทธศาสตร์
2. แนวความคิดเรื่องความมั่นคงปลอดภัยทางไซเบอร์
3. แนวความคิดเรื่องผลประโยชน์แห่งชาติ
4. แนวความคิดเรื่องความมั่นคงแห่งชาติ
5. National Cyber Security Strategy ของประเทศต่างๆ
6. กรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย
7. งานวิจัยที่เกี่ยวข้อง
8. กรอบแนวคิดการวิจัย
9. สรุป

แนวความคิดเรื่องยุทธศาสตร์

ยุทธศาสตร์มีความสำคัญอย่างยิ่งต่อการปฏิบัติงานของภาครัฐ มีผลกระทบต่อทั้งภาครัฐ ภาคเอกชน และภาคประชาชน เพราะเป็นการกำหนดแนวทางในการใช้กำลังอำนาจแห่งชาติทุกสาขา เพื่อให้บรรลุวัตถุประสงค์แห่งชาติที่กำหนดในอันที่จะตอบสนองผลประโยชน์แห่งชาติและบรรลุความมุ่งประสงค์แห่งชาติ ยุทธศาสตร์ชาติที่จะกำหนดจึงต้องได้รับการพิจารณาอย่างละเอียดรอบคอบ มีความชัดเจน มีความเป็นไปได้ในทางปฏิบัติ และมีความเหมาะสมกับกรอบเวลา เพื่อให้ได้ผลการปฏิบัติตามนโยบายฯ ที่เป็นรูปธรรม ตามระยะเวลา ตอบสนองวัตถุประสงค์แห่งชาติและผลประโยชน์แห่งชาติและความมุ่งประสงค์แห่งชาติอย่างแท้จริง

ยุทธศาสตร์เป็นกระบวนการคำนวณความสัมพันธ์ระหว่าง เป้าหมาย (Ends) วิธีการ (Ways) ทรัพยากร (Means) ซึ่งก็คือ เป้าหมาย (Ends) ที่กำหนดทรัพยากร (Means) ที่มีอยู่เพื่อนำไปใช้ในการให้บรรลุต่อเป้าหมาย โดยใช้ วิธีการ (Ways) ก็คือ แนวความคิดหรือวิธีการที่กำหนดขึ้นมาสำหรับการประยุกต์ใช้ร่วมกับทรัพยากรเพื่อการบรรลุเป้าหมาย

สำหรับแนวความคิดเรื่องยุทธศาสตร์ประกอบไปด้วย ความหมายของยุทธศาสตร์ ทฤษฎีเกี่ยวกับยุทธศาสตร์ การแบ่งประเภทยุทธศาสตร์ สภาพแวดล้อมเชิงยุทธศาสตร์ เป้าหมาย (Ends) วิธีการ (Ways) ทรัพยากร (Means) การทดสอบยุทธศาสตร์ (FAS Test) และการประเมินและจัดการกับความเสี่ยง (Risk Assessment and Management)

1. ความหมายของยุทธศาสตร์

ยุทธศาสตร์ (Strategy) เป็นคำที่ถูกอธิบายหรือกล่าวถึงบ่อยครั้ง และมีความหมายที่แตกต่างกันไปตามความเข้าใจของแต่ละบุคคล ทำให้เกิดความสับมาตั้งแต่อดีตจนถึงปัจจุบัน ความหมายของยุทธศาสตร์มีวิวัฒนาการมาจากแนวความคิดทางการทหารที่ถูกใช้ในสถานการณ์สงคราม เป็นแนวความคิดของผู้นำกองทัพที่ใช้กำลังทหารในการรบ เพื่อต่อสู้เพื่อเอาชนะข้าศึก กล่าวคือ ยุทธศาสตร์เป็นศิลปะของผู้นำกองทัพ โดยยุทธศาสตร์ตามบริบทการทหารในอดีตนั้น เป็นการเคลื่อนทัพเข้าสู่สนามรบและยุทธวิธี เป็นการนำกำลังทหารเข้าต่อสู้ในสนามรบ

อย่างไรก็ตามความหมายยุทธศาสตร์ได้ถูกนิยามออกมาอย่างหลากหลาย ฉะนั้นในปัจจุบันยุทธศาสตร์จึงไม่ได้มีความหมายเฉพาะเรื่องการใช้เพียงกำลังอำนาจทางทหารเท่านั้น แต่ยังหมายถึงการใช้กำลังอำนาจทางด้านการเมือง กำลังอำนาจทางด้านเศรษฐกิจ กำลังอำนาจทางด้านสังคมและจิตวิทยา และอาจรวมถึงการใช้กำลังอำนาจด้านอื่น ๆ เท่าที่บุคคลในยุคสมัยต่าง ๆ คิดค้นได้ เช่น กำลังอำนาจทางวิทยาศาสตร์และเทคโนโลยี กำลังอำนาจด้านพลังงาน กำลังอำนาจด้านทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น ดังนั้น บทบาทของยุทธศาสตร์ในปัจจุบันจึงไม่ได้จำกัดการใช้ในสถานการณ์สงครามเท่านั้น แต่ยังสามารถใช้ได้ในยามสงบสุขด้วย

ความหมายของยุทธศาสตร์ได้ถูกนักวิชาการด้านยุทธศาสตร์นิยามทางยุทธศาสตร์ไว้อย่างหลากหลาย ทั้งกลุ่มนักวิชาการทางด้านการทหาร และกลุ่มนักวิชาการที่เป็นพลเรือนทั้งสองกลุ่มให้ความหมายของยุทธศาสตร์ในบริบทของตน โดยมีตัวอย่างความหมายของยุทธศาสตร์ ดังนี้

Carl von Clausewitz กล่าวถึงความหมายของยุทธศาสตร์ในมุมมองเฉพาะด้านการทหารและเป็นมุมมองในระดับยุทธการ หรือยุทธบริเวณ หรือการทัพ ไว้ว่า “ยุทธศาสตร์ คือ การใช้การสู้รบตามความมุ่งประสงค์ของสงคราม นักยุทธศาสตร์จึงต้องกำหนดจุดมุ่งหมายสำหรับการปฏิบัติทั้งปวงในสงคราม เพื่อให้บรรลุความมุ่งประสงค์นั้น กล่าวได้อีกนัยหนึ่งคือ นักยุทธศาสตร์ต้องทำแผนสำหรับการสงคราม และเป้าหมายของสงครามจะกำหนดชุดของการปฏิบัติเพื่อให้บรรลุเป้าหมายนั้น นั่นคือ การกำหนดรูปแบบของการทัพและภายในการทัพนั้น ต้องกำหนดวิธีรบในแต่ละขั้น เพื่อให้ได้รับชัยชนะ” (Bartholomees, 2006, p.79)

Antoine-Henri Jomini นักทฤษฎีทางการทหารแห่งประเทศสวิตเซอร์แลนด์ ในยุคศตวรรษที่ 19กล่าวถึงความหมายของยุทธศาสตร์ในมุมมองเฉพาะด้านการทหารไว้ว่า “ยุทธศาสตร์ คือ ศิลปะการทำสงครามบนแผนที่และทำความเข้าใจในเรื่องยุทธบริเวณ ขณะที่มหายุทธวิธีคือ ศิลปะการวางกำลังในสนามรบให้สอดคล้องกับเหตุการณ์และการนำกำลังเข้าปฏิบัติ รวมถึงเป็นศิลปะในการต่อสู้ที่แตกต่างจากการวางแผนบนแผนที่ ซึ่งการปฏิบัติการนั้น อาจจะขยายระยะได้ 10-12 ไมล์ จากพื้นที่การรบ การส่งกำลังบำรุง จะช่วยนำทัพไปยังพื้นที่การรบ และมหายุทธวิธีจะตัดสินใจในลักษณะของการปฏิบัติการและการวางกำลัง” (Bartholomees, 2006, p.79)

B. H. Liddell Hart นักประวัติศาสตร์และนักวิชาการทางทหารชาวอังกฤษ กล่าวไว้ว่า “ยุทธศาสตร์ คือ ศิลปะของการกระจายและการประยุกต์ทรัพยากรทางทหาร เพื่อให้บรรลุเป้าหมายของนโยบาย ยุทธศาสตร์ จะสำเร็จได้ต้องมีการคำนวณและมีการเชื่อมโยงระหว่างเป้าหมายและทรัพยากร เป้าหมายจะต้องได้สัดส่วนกับทรัพยากรที่มี และทรัพยากรนั้นจะใช้เพื่อการบรรลุเป้าหมายไปถึงเป้าหมายขั้นสุดท้าย ไม่ว่าจะด้วยวิธีใด เพื่อให้บรรลุความมุ่งประสงค์ที่ปรารถนา และการใช้ทรัพยากรที่มากเกินไปหรือน้อยเกินไปอาจทำให้เกิดอันตราย” (Bartholomees, 2006, p.80)

Gerry Johnson and Kevan Scholes อธิบายความหมายของยุทธศาสตร์ไว้ว่า “ยุทธศาสตร์เป็นกรอบและทิศทางระยะยาวขององค์กร โดยมีการจัดสรรทรัพยากรท่ามกลางสภาวะแวดล้อมที่ท้าทาย เพื่อให้เกิดประโยชน์กับองค์กร รวมถึงมีความสอดคล้องกับความต้องการทางการตลาด และความคาดหวังของผู้มีส่วนได้ส่วนเสียขององค์กร” (Exploring Corporate Strategy, 2006)

วิทยาลัยกองทัพบกสหรัฐอเมริกา ได้ให้คำนิยามเกี่ยวกับยุทธศาสตร์ไว้ 2 ความหมาย คือ เกี่ยวกับศักยภาพในการดำเนินการยุทธศาสตร์ “ยุทธศาสตร์ คือ ความสัมพันธ์ของวัตถุประสงค์ หนทางปฏิบัติและทรัพยากร” และและอธิบายในทางความมั่นคงของชาติว่า “ศิลปะทางยุทธศาสตร์ คือ ความเชี่ยวชาญในการกำหนด เชื่อมต่อ และประยุกต์วัตถุประสงค์ หนทางปฏิบัติ ทรัพยากร เพื่อส่งเสริมและปกป้องผลประโยชน์แห่งชาติ” (วิทยาลัยกองทัพบกสหรัฐฯ, 2006)

พระราชบัญญัติ การจัดทำยุทธศาสตร์ชาติ พ.ศ. 2560 หมวดที่ 1 ระบุว่า “ยุทธศาสตร์ชาติ เป็นเป้าหมายในการพัฒนาประเทศอย่างยั่งยืน ตามหลักธรรมาภิบาลเพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกัน อันจะก่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว ตามระยะเวลาที่กำหนดไว้ในยุทธศาสตร์ชาติ” (พระราชบัญญัติ การจัดทำยุทธศาสตร์ชาติ พ.ศ. 2560)

จากความหมายของยุทธศาสตร์ที่กล่าวมาพบว่า จะเห็นได้ว่ามีความเกี่ยวข้องกับความมั่นคงและการทหาร แต่ในปัจจุบันมีการใช้คำว่ายุทธศาสตร์ในมุมองที่แตกต่างออกไปจากเดิมค่อนข้างมาก นักวิชาการภาคเอกชนมักจะใช้คำว่า “กลยุทธ์” แทนคำว่า “ยุทธศาสตร์” แต่ในภาษาอังกฤษจะใช้คำเดียวกัน คือ “Strategy”

จากความหมายของยุทธศาสตร์ดังกล่าวข้างต้นอาจสรุปได้ว่ายุทธศาสตร์ คือ แผนโยบายเพื่อนำทรัพยากร (Means) มาใช้ในการปฏิบัติงานให้บรรลุตามเป้าหมาย (Ends) ด้วยวิธีการ (Way) ที่กำหนดไว้ โดยใช้พื้นฐานความเป็นจริง มีกระบวนการที่มีเหตุผล มีวิธีการที่สมเหตุสมผล เพื่อบรรลุตามเป้าหมายครอบคลุมทั้ง ด้านความมั่นคงแห่งชาติ ด้านเศรษฐกิจ ด้านการทหาร ด้านสังคมจิตวิทยา และด้านอื่น ๆ นอกจากนั้นควรพิจารณาถึงความสัมพันธ์ระหว่างเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means) ร่วมกันในเรื่องของความเหมาะสม (Suitability) การยอมรับได้ (Acceptability) และความเป็นไปได้ (Feasibility) ผ่านการประเมินความเสี่ยงตลอดระยะเวลาดำเนินการ

2. สภาพแวดล้อมเชิงยุทธศาสตร์

ลักษณะสภาพแวดล้อมเชิงยุทธศาสตร์ 4 ลักษณะ คือ ความเปราะบาง (Volatile) ความไม่แน่นอน (Uncertain) ความซับซ้อน (Complex) และความคลุมเครือ (Ambiguous) โดยใช้คำย่อว่า “VUCA” ความเข้าใจเกี่ยวกับสภาพแวดล้อมเชิงยุทธศาสตร์ จะต้องเข้าใจถึงส่วนประกอบทั้งภายนอกและภายใน ซึ่งสภาพแวดล้อมเชิงยุทธศาสตร์ ได้แก่ สังคม วัฒนธรรม การเมือง จริยธรรม เศรษฐกิจ การส่งกำลังบำรุง องค์กร การบริหาร ข่าวสารสารสนเทศและความชาญฉลาด ทฤษฎีเชิงยุทธศาสตร์ หลักการ เทคโนโลยี การดำเนินงาน การบังคับบัญชา ภูมิศาสตร์ ความฝืด/โอกาส/ความไม่แน่นอน ศัตรู และเวลา สิ่งเหล่านี้จะต้องพิจารณาประวัติศาสตร์ที่เกิดขึ้นเป็นรายตัวแปร (วิทยาลัยกองทัพบกสหรัฐฯ, 2006)

อย่างไรก็ตาม ในการพิจารณาตัวแปรเหล่านี้จะต้องพิจารณาให้อยู่ในช่วงเวลาเดียวกัน (Yarger, 2006) ดังนั้น ยุทธศาสตร์เป็นเรื่องเกี่ยวกับอนาคต ซึ่งสถานการณ์อนาคตอาจจะเกิดผลลัพธ์ที่มาจากการดำเนินการทางยุทธศาสตร์ ในการจัดการยุทธศาสตร์อยู่บนความไม่แน่นอน ยุทธศาสตร์ถูกกำหนดมาจากความรู้และความเข้าใจในระบบที่เกี่ยวกับสภาพแวดล้อมเชิงยุทธศาสตร์ที่ข้อเท็จจริงและข้อสมมติฐาน การค้นหา การหาเหตุผล และการตั้งสมมติฐานภายในมิติของยุทธศาสตร์ ยุทธศาสตร์นั้นเกี่ยวข้องกับความคิดที่ยิ่งใหญ่และเหนือกาลเวลา ความคิดเชิงยุทธศาสตร์ไม่ใช่เรื่องที่เกี่ยวกับปรากฏการณ์ที่เพิ่มขึ้นหรือลดลงของความซับซ้อนของปัญหา แต่ยุทธศาสตร์ถูกกำหนดขึ้นเพื่อบรรลุผลตามความต้องการขั้นสุดท้ายของรัฐ (Desired End State) และอยู่ในสภาวะที่ชัดเจนในเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means)

3. เป้าหมาย (End)

การกำหนดยุทธศาสตร์ต้องมีการกำหนดเป้าหมาย (Ends) ที่เหมาะสมที่สุด บ่อยครั้งในการกำหนดเป้าหมาย (Ends) ถูกละเลยและใช้เวลาเพียงเล็กน้อยในการพิจารณาความเหมาะสมในบริบทของความต้องการของเชิงนโยบาย ผลประโยชน์แห่งชาติ และสิ่งแวดล้อม แต่แท้ที่จริงแล้วเป้าหมาย (Ends) เป็นสิ่งสำคัญของการกำหนดยุทธศาสตร์ และถ้าเป้าหมาย (Ends) ถูกกำหนดมาอย่างไม่เหมาะสมและไม่ชัดเจนแล้ว การดำเนินยุทธศาสตร์จะมีข้อบกพร่อง และไม่มีประสิทธิผล ถ้าเป้าหมาย (Ends) ไม่ถูกต้องจะทำให้การกำหนด วิธีการ (Ways) และทรัพยากร (Means)ตอบสนองไม่ตรง และไม่สามารถบรรลุวัตถุประสงค์สูงสุดในการปกป้องและเพิ่มพูนผลประโยชน์แห่งชาติที่แท้จริงได้ เป้าหมายของชาติ และเป้าหมาย (Ends) เชิงยุทธศาสตร์มาจากการพิจารณานโยบายของการปกป้องหรือการเพิ่มพูนผลประโยชน์แห่งชาติ ภายใต้บริบท ของสภาพแวดล้อมเชิงยุทธศาสตร์นโยบายเป็นแค่ข้อความแนะนำสำหรับเป้าหมายและการใช้พลังอำนาจแห่งชาติแต่กระบวนการกำหนดยุทธศาสตร์เป็นการขยายเหตุและผลในนโยบายให้ชัดเจนขึ้นในสังคมแบบประชาธิปไตยผู้เชี่ยวชาญทางทหารต้องสร้างความสัมพันธ์กับผู้นำพลเรือนในด้านอำนวยความสะดวก และการข่าวสารเป็นสิ่งที่จำเป็นที่สื่อให้เห็นถึงนโยบายและยุทธศาสตร์ ที่ชัดเจน ถ้านโยบายถูกทำให้เกิดความเข้าใจผิดจะทำให้ระดับของความเสี่ยงที่เกี่ยวข้องกับยุทธศาสตร์เพิ่มขึ้น (Yerger, 2006)

4. วิธีการ (Ways)

แนวคิดเชิงยุทธศาสตร์ หรือ วิธีการ (Ways) เป็นการอธิบายถึงหนทางปฏิบัติที่ทำให้เป้าหมาย (Ends)เกิดการบรรลุผลโดยการใช้เครื่องมือแห่งอำนาจ เครื่องมือแห่งอำนาจ คือการรวมตัวขององค์ประกอบแห่งอำนาจ หรือทรัพยากร (Means) ในการดำเนินการยุทธศาสตร์ วิธีการ (Ways)จะเชื่อมโยงทรัพยากรไปยังเป้าหมาย (Ends) โดยขึ้นอยู่กับว่า ใครทำอะไร ที่ไหน เมื่อไรทำไม ถึงทำ เพื่ออธิบายวิธีการที่ทำให้เป้าหมาย (Ends)จะสำเร็จผล วิธีการ (Ways)บ่อยครั้งจะเป็นศูนย์รวมของยุทธศาสตร์ บางครั้งแล้วเกิดความเข้าใจผิดคิดว่าวิธีการ (Ways) คือ ยุทธศาสตร์ แต่โดยความจริงแล้วยุทธศาสตร์ประกอบไปด้วยเป้าหมาย (Ends)วิธีการ (Ways) และทรัพยากร (Means) และจะเน้นเกี่ยวกับวิธีการนำส่วนประกอบดังกล่าวมาเชื่อมโยงให้เกิดความสมดุลร่วมกับสภาพแวดล้อมเชิงยุทธศาสตร์ เพื่อทำให้เกิดผลตามที่ต้องการ ยุทธศาสตร์ที่ดีจะต้องมีความสมบูรณ์โดยรวม

ทั้งความเหมาะสมในเป้าหมาย (Ends) ความเหมาะสมในวิธีการ (Ways) และได้รับการสนับสนุนจากทรัพยากร (Means)ที่จำเป็น ถ้ากำหนดเป้าหมาย (Ends) ที่ผิดแต่ได้รับการสนับสนุนวิธีการ (Ways)ที่ชาญฉลาดแล้วก็ตามแต่ก็ไม่อาจสามารถปกป้องหรือเพิ่มพูนผลประโยชน์แห่งชาติได้ (Yarger, 2006)

5. ทรัพยากร (Means)

การกำหนดทรัพยากร (Means) จะต้องกำหนดประเภทและระดับของทรัพยากรเท่าที่จำเป็นในการสนับสนุนวิธีการ (Ways)ของยุทธศาสตร์ ในยุทธศาสตร์นั้นทรัพยากร (Means) สามารถเป็นสิ่งที่มีตัวตนหรือไม่มีตัวตนก็ได้ เช่น สิ่งที่มีตัวตน ประกอบไปด้วย กำลังพล ประชาชน อุปกรณ์ เครื่องมือ เงิน และสิ่งอำนวยความสะดวกต่าง ๆ ส่วนสิ่งที่ไม่มีตัวตน ประกอบไปด้วย ความคิดที่จะทำบางสิ่งบางอย่าง ความกล้าหาญ หรือสติปัญญา และทรัพยากร (Means)เป็นองค์ประกอบของพลังอำนาจแห่งชาติที่ถูกใช้เพื่อปกป้องหรือเพิ่มพูนผลประโยชน์ชาติ (Yarger, 2006) แม้แต่ในการสงครามจะต้องบูรณาการใช้องค์ประกอบของพลังอำนาจแห่งชาติด้านการทูต (Diplomatic) ข้อมูลข่าวสาร (Information) การทหาร (Military) และเศรษฐกิจ (Economic) (DIME) การบูรณาการพลังอำนาจดังกล่าวอย่างได้ผลอาจจะป้องกันการเกิดสงครามได้ (Krenson, 2012)

อย่างไรก็ตาม พลังอำนาจของชาติ ยังสามารถประกอบด้วยการทูต ด้านการทูต (Diplomatic) ข้อมูลข่าวสาร (Information) การทหาร (Military) เศรษฐกิจ (Economic) การเงิน (Financial) การข่าวกรอง (Intelligence) และการบังคับใช้กฎหมาย (Law Enforcement) (DIMEFIL) และยังสามารถนำมาแสดงพลังอำนาจของชาติได้อีกรูปแบบหนึ่งที่ประกอบด้วย การทหาร (Military) ข่าวกรอง (Intelligence) การทูต (Diplomatic) ด้านกฎหมาย (Legal) ข้อมูลข่าวสาร (Information) การเงิน (Financial) และเศรษฐกิจ (Economic) (MIDLIFE)

ถึงแม้ว่าพลังอำนาจแห่งชาติจะถูกกำหนดเป็นรูปแบบที่หลากหลาย แต่การวิเคราะห์พลังอำนาจแห่งชาติให้สามารถนำไปใช้งานได้จริงในยามสงบที่ปราศจากสงครามและการก่อการร้ายจะใช้องค์ประกอบเพียง 4 ตัว คือ ด้านการทูต (Diplomatic) ข้อมูลข่าวสาร (Information) การทหาร (Military) และเศรษฐกิจ (Economic) (DIME) ส่วนการนำไปใช้งานจะสามารถทำให้ครอบคลุมตัวแปรอย่างตรงประเด็นหรือไม่ขึ้นอยู่กับนักยุทธศาสตร์ที่นำไปใช้งาน (Krenson, 2012)

ทรัพยากร (Means) ยังหมายถึงพลังอำนาจแห่งชาติ (National Power) อีกด้วย คำว่า “พลังอำนาจ” หรือ “กำลังอำนาจ” มีความหมายเหมือนกัน กล่าวคือมาจากรากศัพท์ภาษาอังกฤษคำเดียวกันว่า “Power” โดยทั่วไปมักจะนำมาใช้แยกกันเพื่อแสดงให้เห็นความแตกต่างของวัตถุประสงค์ สำหรับชาติหรือประเทศเป็นส่วนรวม จะใช้คำว่า “พลังอำนาจ” ส่วนคำว่า “กำลังอำนาจ” จะใช้ในเมื่อกล่าวถึงองค์ประกอบของพลังอำนาจอย่างใดอย่างหนึ่งโดยเฉพาะ (พจน์ พงศ์สุวรรณ, 2536) เช่น กำลังอำนาจทางการเมือง กำลังอำนาจทางทหาร กำลังอำนาจทางเศรษฐกิจ กำลังอำนาจทางสังคมจิตวิทยา กำลังอำนาจทางการข่าวสาร เป็นต้น

6. การประเมินและจัดการกับความเสี่ยง (Risk Assessment and Management)

นอกจากเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means) แล้วยังมีความเสี่ยง (Risk) ที่เกิดขึ้นในระหว่างการดำเนินการยุทธศาสตร์โดยความเสี่ยง คือ ความห่างระหว่างสิ่ง

ที่เป็นผลสำเร็จ วิธีการ (Ways) และทรัพยากร (Means) ที่ใช้เพื่อบรรลุเป้าหมาย (Ends) ความเสี่ยงเกิดขึ้นเนื่องจากทรัพยากร (Means)ไม่เพียงพอ หรือวิธีการ (Ways) ที่ไม่ฉลาดพอที่จะทำให้ประสบความสำเร็จได้ ในสภาพแวดล้อมการแข่งขันระหว่างประเทศจะมีความเสี่ยงบางอย่างที่นักยุทธศาสตร์ต้องพยายามลดลง โดยการพัฒนายุทธศาสตร์ให้เกิดความสมดุลของเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means)

ยุทธศาสตร์กับการจัดการความเสี่ยง การจัดการความเสี่ยงจะเกิดขึ้นก็ต่อเมื่อผลลัพธ์ของยุทธศาสตร์ไม่ได้เป็นไปตามเป้าหมาย (Ends) ที่กำหนดไว้ ถ้ากล่าวถึงยุทธศาสตร์ชาติ เป้าหมายทางยุทธศาสตร์ต้องคำนึงถึงผลประโยชน์แห่งชาติที่จะได้รับ เช่น การเจริญเติบโตทางเศรษฐกิจ ความมั่นคง มั่งคั่ง และยั่งยืน โดยที่กำลังอำนาจแห่งชาติ (National Power) คือ ทรัพยากรที่ใช้สนับสนุนให้บรรลุเป้าหมายทางยุทธศาสตร์ ดังนั้น กล่าวได้ว่า ยุทธศาสตร์ คือ การแสวงหาประโยชน์แห่งชาติผ่านการประยุกต์ใช้กำลังอำนาจแห่งชาติ โดยมีการกำหนดทิศทางหรือเงื่อนไขในอนาคต สำหรับการเผชิญหน้ากับฝ่ายตรงข้ามและการเผชิญกับความท้าทายต่าง ๆ ที่เหนือการควบคุม

แนวความคิดเรื่องความมั่นคงปลอดภัยทางไซเบอร์

การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้เกิดการพัฒนาทั้งทางเศรษฐกิจและสังคมอย่างก้าวกระโดด เนื่องจากปัจจุบันมีการพัฒนาแอพพลิเคชั่นและซอฟแวร์ที่มีประสิทธิภาพสูง ทำให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลได้สะดวก รวดเร็ว และประหยัดค่าใช้จ่ายได้มากขึ้น หากผู้ใช้งานนำข้อมูลไปใช้ในทางที่สร้างสรรค์ ก็สามารถใช้ให้เป็นประโยชน์ต่อการพัฒนาและยกระดับเศรษฐกิจ สังคม และสิ่งแวดล้อมในมิติต่างๆ ได้ ในทางกลับกัน เทคโนโลยีก็สามารถสร้างความเสียหายได้มากเช่นกัน หากผู้ประสงค์ร้ายได้พัฒนาเครื่องมืออันทันสมัยเพื่อโจมตีระบบ ขโมย ทำลาย บิดเบือนข้อมูล หรือหลอกลวง ก็จะส่งผลให้เกิดการแทรกแซงและทำลายความมั่นคงได้ในทุกระดับ ไม่ว่าจะเป็นในระดับบุคคล ระดับหน่วยงาน ระดับประเทศ และระดับโลก

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องคำนึงถึงการคุ้มครองความเป็นส่วนตัวและความสะดวกสบายในการเข้าถึงระบบของแต่ละบุคคลด้วยเช่นกัน การมุ่งเน้นรักษาความมั่นคงของชาติอาจเกิดการลุกล้ำความเป็นส่วนตัว ในขณะที่การมุ่งให้เกิดความสะดวกสบายในการเข้าถึงระบบอาจทำให้ความมั่นคงปลอดภัยทางไซเบอร์เกิดความหละหลวมเช่นกัน ดังนั้น หน่วยงานที่รับผิดชอบจำเป็นต้องรักษาสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองความเป็นส่วนตัว และการอำนวยความสะดวกในการเข้าถึงระบบให้เหมาะสม เพราะเป็นกลไกสำคัญในการสร้างความไว้วางใจ และการส่งเสริมเกิดการใช้เทคโนโลยีดิจิทัลในการทำงานทุกภาคส่วน

1. ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ว่า ภาพรวมของเครื่องมือ (tools), นโยบาย (policies), แนวคิดการรักษาความปลอดภัย (security concepts), การรักษาความปลอดภัย (security safeguards), แนวทาง (guidelines), วิธีการบริหารความเสี่ยง (risk management approaches), การปฏิบัติ (actions), การอบรม (training), วิธี

ปฏิบัติที่เป็นเลิศ (best practices), การรับประกัน (assurance) และเทคโนโลยี (technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชั่น, บริการ, ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ (Definition of cybersecurity : ITU)

Richard A. Clarke อดีตที่ปรึกษาประธานาธิบดีสหรัฐอเมริกาด้านความมั่นคง ได้สรุปปัญหาภัยคุกคามทางไซเบอร์แบ่งเป็น 4 ลักษณะ (C.H.E.W.) ดังนี้

C คือ Cybercrime เป็นปัญหาการก่ออาชญากรรมทางไซเบอร์โดยมีวัตถุประสงค์ทางการเงิน เช่นการแฮ็คบัญชีธนาคารหรือธุรกรรมออนไลน์ต่างๆ ทำให้คนส่วนหนึ่งไม่ยอมทำธุรกรรมออนไลน์ และคิดว่าตนเองก็จะไม่ได้รับผลกระทบ แต่ในมุมมองของผู้เชี่ยวชาญ อาชญากรรมเหล่านี้เพิ่มต้นทุนต่อระบบ และระบบก็จะผลักต้นทุนนั้นให้ผู้บริโภคทุกคนไม่ว่าจะออฟไลน์หรือออนไลน์แบกรับในที่สุด ปัญหานี้จึงกระทบทุกคนอย่างหลีกเลี่ยงไม่ได้

H คือ Hacktivism เป็นการแฮ็คข้อมูลลับไม่ว่าจะของทางการหรือเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะ เพื่อเปิดโปงเรื่องบางอย่างหรือสร้างความอับอายแก่เจ้าของข้อมูล รวมถึงการแฮ็คเว็บเพจแล้วเผยแพร่ข้อความของตนลงไปในเว็บเหล่านั้นเพื่อประกาศจุดยืนหรืออุดมการณ์ต่างๆ แม้เราจะป้องกันตัวเองดีเพียงใด แต่หากเป็นการสื่อสารกับปลายทาง เช่น อีเมล เมื่อปลายทางถูกแฮ็คข้อมูลของเราก็รั่วไหลอยู่ดี

E คือ Espionage เป็นการจารกรรมข้อมูลเพื่อนำไปใช้ประโยชน์ต่อ เช่น การเจาะข้อมูลนวัตกรรมต่างๆ การเจาะข้อมูลทางการทหาร ซึ่งในอดีตใครที่พยายามขโมยเอกสารที่มีชั้นความลับของหน่วยงานต่างๆ เท่ากับต้องบุกรุกเข้าไปในหน่วยงาน แต่ในยุคดิจิตัล แฮ็คเกอร์อาจซ่อนตัวอยู่มุมใดมุมหนึ่งของโลก แล้วเชื่อมต่อทางออนไลน์ ต้นทุนการจารกรรมจึงต่ำมาก และความเสี่ยงในการถูกจับตัวได้ก็ลดลงมาก

W คือ War **หรือ** Cyberwar ซึ่งเกิดขึ้นแล้ว เช่น การทำลายฐานผลิตอาวุธนิวเคลียร์โดยไม่ต้องส่งกำลังพลหรือใช้อาวุธกายภาพแม้แต่น้อย แต่เป็นการส่งคำสั่งเข้าไปให้เครื่องยนต์ทำลายตนเอง หรือแม้แต่การที่บางประเทศโจมตีทางไซเบอร์เพื่อให้ระบบสื่อสารและแหล่งพลังงานของปฏิปักษ์ล่ม แล้วใช้กำลังพลบุกยึดครองดินแดนจริงได้อย่างง่ายดาย

การรักษาความปลอดภัยของไซเบอร์ (Cyber Security) ตามพจนานุกรม Cyberspace Operations Lexicon ของ กระทรวงกลาโหมสหรัฐฯ กำหนดให้ Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ), ความปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรมท อุบัติเหตุ และความผิดพลาดต่างๆ ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้ถือผลประโยชน์ร่วม (Stakeholder), ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า, การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น, การรบกวนการทำงานหรือการดำเนินธุรกรรม, ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

บทนิยามศัพท์ในร่างกฎหมายไซเบอร์ของไทย ได้นิยามคำว่า“ความมั่นคงปลอดภัยไซเบอร์” ว่าหมายถึง “มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ” (ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของ ไซเบอร์ (Cyber) คือ คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” ไซเบอร์เนติกส์ (Cybernetics) เป็นวิชาการเกี่ยวกับระบบควบคุม เช่น ระบบประสาทของสิ่งมีชีวิต เพื่อนำไปใช้พัฒนาระบบอิเล็กทรอนิกส์ หรือระบบกลไกที่ทำงานคล้ายคลึงกัน วิชานี้เปรียบเทียบความคล้ายคลึง และต่างกันระหว่างสิ่งมีชีวิตกับสิ่งไม่มีชีวิต และยึดหลักการพื้นฐานทางด้านการสื่อสารและการควบคุมที่สามารอธิบายการทำงานของทั้งสิ่งมีชีวิตและสิ่งไม่มีชีวิตได้ ชื่อของวิชานี้มาจากคำภาษากรีก หมายความว่า นำ หรือ ปกครอง

ห้วงไซเบอร์ (Cyberspace) เป็นขอบเขตที่กำหนดโดยการใช้อุปกรณ์อิเล็กทรอนิกส์และแถบคลื่นแม่เหล็กไฟฟ้าในการจัดเก็บ แก้ไขเปลี่ยนแปลง และแลกเปลี่ยนข้อมูล ผ่านทางระบบเครือข่ายและโครงสร้างสาธารณูปโภคทางกายภาพที่เกี่ยวข้อง

จากนิยามศัพท์ “ความมั่นคงปลอดภัยไซเบอร์” ข้างต้น จะเห็นได้ว่าร่างกฎหมายไซเบอร์ของไทยมิได้มุ่งเฉพาะความมั่นคงปลอดภัยของระบบและข้อมูลอันกระทบต่อความมั่นคงทางเศรษฐกิจแต่เพียงอย่างเดียว แต่หมายความรวมถึงความมั่นคงทางการทหารและความสงบเรียบร้อยภายในประเทศด้วย

2. สงครามไซเบอร์ (Cyber Warfare)

สงครามในรูปแบบใหม่ของทหาร ซึ่งได้รับการยอมรับเป็นสมรภูมิรบที่ 5 นอกเหนือจาก ทางบก ทางน้ำ ทางอากาศ และทางอวกาศ กองทัพในหลายประเทศมีการก่อตั้งและพัฒนาหน่วยงานด้านไซเบอร์ และมีแนวโน้มการเพิ่มขีดความสามารถอย่างต่อเนื่อง

สภาพแวดล้อมทางยุทธศาสตร์ของสงครามไซเบอร์แตกต่างจากยุทธศาสตร์แบบดั้งเดิม กล่าวคือ มีการเปลี่ยนแปลงสภาพแวดล้อมที่จากแบบดั้งเดิมจะมองทางภูมิศาสตร์เป็นหลักเปลี่ยนแปลงมาเป็นการมองโครงสร้างพื้นฐานด้านคอมพิวเตอร์และระบบเครือข่าย นอกจากนั้นข้าศึกก็ยังมาในรูปแบบใหม่ และการรับมือมีความยากกว่าการต่อสู้ในสงครามรูปแบบเดิม ไม่ว่าจะเป็นเรื่องของระยะทางหรือสภาพแวดล้อมที่เปลี่ยนแปลงไป เพราะในสภาพแวดล้อมทางไซเบอร์นั้นไม่มีการกำหนดเขตแดน ดังนั้นแนวคิดทางภูมิศาสตร์แบบดั้งเดิมจึงแตกต่างไปจากบริบทของ Cyberspace อย่างไรก็ตาม Cyberspace อาจสร้างโอกาสให้เกิดพันธมิตรด้วยวิธีการใหม่ ๆ ได้เช่นกัน

การโจมตีทางไซเบอร์ (Cyber Attack) ไม่สามารถสร้างความได้เปรียบทางยุทธศาสตร์ในการครอบครองดินแดนโดยกองกำลังภาคพื้นดินได้ แต่สามารถโจมตีเป้าหมายและความสามารถของศัตรูที่สำคัญได้ เช่น ระบบป้องกันทางอากาศ ยุทโธปกรณ์ทางทหาร ระบบสั่งการ

และระบบควบคุมโครงสร้างพื้นฐานทางพลเรือน (ระบบไฟฟ้า ระบบการเงิน ระบบการขนส่ง และระบบการสื่อสาร) เป็นต้น (Cyber Warfare: Concepts and Strategic Trends, 2012, p.25)

การสงครามไซเบอร์ หรือ Cyber Warfare (CW) คือการขัดกันของกำลังที่ใช้กรอบของไซเบอร์เป็นเครื่องมือ เพื่อให้ได้มาซึ่ง การครองความได้เปรียบในห้วงไซเบอร์ หรือ Cyberspace Superiority (ระดับขั้นในการควบคุมในห้วง ไซเบอร์ โดยกำลังฝ่ายหนึ่งที่สามารถบังคับหรืออนุญาตให้การปฏิบัติการดำเนินการไปอย่างเชื่อมั่นและปลอดภัย โดยหน่วยกำลังที่ปฏิบัติบนพื้นที่ปฏิบัติการที่เกี่ยวข้อง (ได้แก่ ภาคพื้นดิน, ภาคทะเล, ภาคอากาศ และภาคอวกาศ) ปราศจากการขัดขวางของฝ่ายศัตรู) การปฏิบัติการทางทหารที่ดำเนินการเพื่อขัดขวางการปฏิบัติงานระบบไซเบอร์และอาวุธของฝ่ายตรงข้าม รวมทั้ง เพื่อดำรงการปฏิบัติงานระบบไซเบอร์และอาวุธอย่างมีประสิทธิภาพของฝ่ายเราในการขัดกัน การปฏิบัติการดังกล่าวรวมถึง การโจมตีทางไซเบอร์ (Cyber Attack), การป้องกันทางไซเบอร์ (Cyber Defense) และการแสวงหาประโยชน์จากการสภาพแวดล้อมทางไซเบอร์ (Cyber Operational Preparation of Environment หรือ Cyber Enabling Actions)

การโจมตีทางไซเบอร์ คือ การกระทำใด ๆ ที่ใช้คอมพิวเตอร์, เครือข่าย หรือระบบรวมทั้งอุปกรณ์ที่เกี่ยวข้อง ซึ่งตั้งใจเป็นภัยคุกคาม ขัดขวาง หรือทำลายระบบ, ทรัพยากร และการทำงานของไซเบอร์ที่สำคัญของศัตรู ผลกระทบที่ต้องการของการโจมตีทางไซเบอร์ไม่จำเป็นต้องจำกัดเพียงระบบคอมพิวเตอร์ และข้อมูลที่เป็นเป้าหมาย ตัวอย่างเช่น การโจมตีต่อระบบคอมพิวเตอร์ ที่ต้องการลิดรอน หรือทำลายโครงสร้างพื้นฐานสาธารณูปโภค หรือขีดความสามารถของระบบบัญชาการและควบคุม (C2) การโจมตีทางไซเบอร์อาจจะต้องใช้พาหะตัวกลางในการดำเนินการ รวมทั้ง อุปกรณ์ต่อเชื่อมต่าง ๆ (Peripheral Devices), เครื่องส่งสัญญาณอิเล็กทรอนิกส์ (Electronic Transmitters), การเข้ารหัส (Embedded Code), หรือ เจ้าหน้าที่ปฏิบัติงาน (Operators) กิจกรรมหรือผลกระทบของการโจมตีอาจจะเกิดขึ้นอย่างกระจัดกระจาย เป็นวงกว้าง หรือเป็นเฉพาะพื้นที่ที่เป็นเป้าหมาย

การโจมตีทางไซเบอร์ (Cyber Attack) ถูกใช้แทนที่คำว่า การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA) เนื่องจาก การโจมตีทางไซเบอร์นั้นเชื่อมโยงกับกระบวนทัศน์หรือหลักนิยมของการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations: CNO) ที่ใหญ่กว่า ซึ่งมีความแตกต่างกันจากวิธีการในความหมายของคำว่า การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CNA)

การโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack : CAN) คือประเภทหนึ่งของอำนาจการยิงที่ถูกใช้สำหรับวัตถุประสงค์การรุกซึ่งต้องปฏิบัติจากการใช้เครือข่ายคอมพิวเตอร์เพื่อที่จะรบกวน ลิดรอน ทำให้เสียหาย หรือทำลายข้อมูลที่อยู่ในระบบข้อมูลข่าวสารเป้าหมาย หรือ เครือข่ายคอมพิวเตอร์ หรือ ระบบ/เครือข่ายของอุปกรณ์ที่เกี่ยวข้อง ผลกระทบที่ต้องการอย่างยิ่งยวดอาจไม่ใช่ระบบที่เป็นเป้าหมายเพียงอย่างเดียว แต่อาจเป็นการปฏิบัติเพื่อสนับสนุนความพยายามที่สำคัญกว่านั้น เช่น การปฏิบัติการข้อมูลข่าวสาร หรือการต่อต้านการก่อการร้าย โดยใช้การเปลี่ยนแปลง (Altering) หรือการปลอมตัว (Spoofing) ต่อระบบการติดต่อสื่อสารต่าง ๆ หรือการลิดรอน (Denying) การเข้าถึงการติต่อสื่อสาร หรือช่องทางการส่งกำลังบำรุงของศัตรู” (กระทรวงกลาโหมสหรัฐฯ)

การโจมตีทางไซเบอร์จึงเป็นส่วนหนึ่งของสงครามสมัยใหม่ควบคู่ไปกับสงครามรูปแบบเดิม โดยมีการแบ่งบริบทของการการโจมตีทางไซเบอร์ ดังนี้

1. การสร้างความกดดันให้ศัตรูเปลี่ยนแปลงนโยบาย คือ ประเทศหนึ่งใช้การโจมตีทางไซเบอร์ต่ออีกประเทศหนึ่งซึ่งเป็นคู่ขัดแย้งกัน เพื่อกดดันให้ประเทศนั้นเปลี่ยนแปลงนโยบาย (เช่น รัสเซียโจมตีระบบไซเบอร์ของเอสโตเนีย เพราะรัสเซียไม่พอใจที่รัฐบาลเอสโตเนียเคลื่อนย้ายอนุสาวรีย์และหลุมศพทหารซึ่งสร้างไว้ในช่วงสหภาพโซเวียตยังปกครองเอสโตเนีย)

2. การเพิ่มความเสี่ยงด้านความปลอดภัยของอาวุธที่มีอานุภาพทำลายล้างสูง เช่น ระบบสั่งการอาวุธนิวเคลียร์ เป็นต้น

3. การพัฒนาขีดความสามารถในการโจมตีทางไซเบอร์และการป้องกันการโจมตีทางไซเบอร์ ให้เกิดความสมดุล

4. การตอบโต้การโจมตีทางไซเบอร์หรือประเทศที่เป็นต้นเหตุของการโจมตีทางไซเบอร์

แม้การโจมตีทางไซเบอร์อาจถือได้ว่าเป็นการทำของสงครามในรูปแบบหนึ่งซึ่งก่อให้เกิดความเสียหาย และยังไม่ได้ถูกควบคุมโดยกฎหมายระหว่างประเทศ แต่ในอีกด้านหนึ่งการสอดแนมทางไซเบอร์ ซึ่งไม่ทำลายระบบหรือข้อมูลให้เกิดความเสียหาย ก็ไม่ถือว่าเป็นการโจมตีทางไซเบอร์ (hereafter: Alexander, 2010)

อย่างไรก็ตาม การพัฒนาขีดความสามารถทางไซเบอร์ของประเทศต่าง ๆ อาจทำให้เกิดการเปลี่ยนสมดุลใหม่ของอำนาจระหว่างประเทศหรือองค์กรที่ไม่ใช่ของรัฐ เช่น กลุ่มผู้ก่อการร้าย กลุ่มชาติพันธุ์ หรือประเทศอนาธิปไตย ด้วยเหตุนี้ Cyberspace จึงสร้างสภาพแวดล้อมทางยุทธศาสตร์ใหม่ที่เป็นเอกลักษณ์ และกำลังจะขยายตัวอย่างต่อเนื่อง

แนวความคิดในการปฏิบัติด้านสงครามไซเบอร์ของกองทัพอากาศสหรัฐฯ มีอยู่ด้วยกัน 5 ประการ ได้แก่

1. Cyberspace Superiority คือ การครอง Cyberspace หรือการที่ต้องมีความสามารถในการปฏิบัติการบน Cyberspace เหนือกว่าฝ่ายตรงข้ามและต้องป้องกันไม่ให้ฝ่ายตรงข้ามสามารถปฏิบัติการต่าง ๆ บน Cyberspace ได้

2. Counter-Cyber เป็นการตอบโต้ฝ่ายตรงข้ามโดยใช้วิธีการปฏิบัติทางไซเบอร์ 2 รูปแบบ คือ

- Offensive Counter-Cyber (OCC) การปฏิบัติการตอบโต้ทางไซเบอร์เชิงรุก โดยวิธีการทำให้ระบบของฝ่ายตรงข้ามปฏิเสธการให้บริการ (Denail Of Service) การทำลายหรือลวงความสามารถของศัตรูในการที่จะปฏิบัติการทางไซเบอร์ เช่น สงครามอ่าวเปอร์เซีย ก่อนที่สหรัฐจะใช้กำลังทางทหาร ได้มีการปฏิบัติการทางไซเบอร์เพื่อโจมตีเครือข่ายของ AT&T ซึ่งเป็นศูนย์กลางการสื่อสารโทรคมนาคมของอิรัก ทำให้ไม่สามารถใช้การสื่อสารโทรคมนาคมได้

- Defensive Counter-Cyber (DCC) การป้องกันการตอบโต้ทางไซเบอร์จากฝ่ายตรงข้าม โดยใช้วิธีการตรวจสอบและสกัดกั้นทำลาย หรือลบล้างกองกำลังทางไซเบอร์ของฝ่ายตรงข้ามที่พยายามเจาะฐานข้อมูลหรือโจมตีทางไซเบอร์ เช่น การมีระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (Intrusion detection/Prevention System) หรือการใช้อุปกรณ์ควบคุมการเข้าถึงประเภทไฟล์วอลล์ (Firewall) โดยมีการตั้งกฎของไฟล์วอลล์เพื่อควบคุมและป้องกันการถูกโจมตีจากฝ่ายตรงข้ามผ่านทางระบบเครือข่าย

3. Cyberspace Control คือ ความสามารถในการควบคุมการปฏิบัติต่าง ๆ ทางไซเบอร์ เช่น

- การมีอำนาจในการอนุมัติการปฏิบัติการโต้ตอบทางไซเบอร์เชิงรุก
- ดำเนินการในการป้องกันทางไซเบอร์จากฝ่ายตรงข้าม
- การใช้ยุทธวิธี หรือยุทธศาสตร์ในการบูรณาการ การปฏิบัติการทางไซเบอร์ร่วมกับชาติต่าง ๆ เพื่อเป็นการลดความขัดแย้งที่อาจก่อให้เกิดสงครามไซเบอร์

4. Cross-Domain Operations คือ การใช้ปฏิบัติการทางไซเบอร์เพื่อให้บรรลุผลในพื้นที่การรบอื่น ๆ (กองทัพสหรัฐฯ แบ่งพื้นที่การรบออกเป็น 5 พื้นที่ คือ land sea air space Cyberspace (Air Command and Staff College : Air University : U.S.A.F., 2013) เช่น

- การใช้ปฏิบัติการทางไซเบอร์เพื่อทำให้เกิดการหยุดชะงักหรือทำลายการป้องกันทางกายภาพ (กล้องวงจรปิด CCTV, Sensor ตรวจจับการบุกรุก เป็นต้น)
- การสั่งห้ามหรือการควบคุมระบบ Command control (C2 link) ของฝ่ายตรงข้าม
- การใช้ปฏิบัติการทางไซเบอร์ที่ทำให้เกิดการหยุดให้บริการหรือการเข้าควบคุมระบบสาธารณูปโภค เช่น ไฟฟ้า ประปา นิวเคลียร์
- การทำให้เกิดการหยุดระบบตลาดการเงินหรือระบบเศรษฐกิจ

5. Operational Considerations สิ่งที่เป็นข้อพิจารณาในการใช้ปฏิบัติการทางไซเบอร์

- การตรวจสอบให้แน่ใจถึงการกระทำต่าง ๆ ในโลกไซเบอร์ ซึ่งทุกคนมีสิทธิเสรีภาพในการทำกิจกรรมต่าง ๆ แต่ต้องไม่เป็นการสร้างภัยคุกคามให้เกิดขึ้น
- ถ้าเราสามารถครอง หรือควบคุมทางไซเบอร์ได้ ฝ่ายตรงข้ามก็จะปฏิบัติการใด ๆ ทางไซเบอร์ได้ลำบากมากขึ้น
- การตอบโต้การใช้งานที่มีลักษณะเป็นภัยคุกคามทางไซเบอร์ของฝ่ายตรงข้าม
- การแทรกซึมหรือแฝงตัวเข้าถึงระบบต่าง ๆ ของฝ่ายตรงข้าม เช่น การฝัง botnet, Root kit หรือ Trojan horse ที่ช่วยให้สามารถใช้ในการปฏิบัติการทางไซเบอร์ได้

แนวความคิดเรื่องผลประโยชน์แห่งชาติ

1. ความหมายของผลประโยชน์แห่งชาติ

ผลประโยชน์แห่งชาติ (National Interests) หมายถึง เป้าหมายแห่งชาติ เป็นแนวความคิดที่ได้ไตร่ตรองอย่างรอบคอบที่สุด จากบรรดาองค์ประกอบต่าง ๆ ประมวลขึ้นเป็นความต้องการที่สำคัญที่สุดที่ชาติจะขาดเสียมิได้ ทั้งนี้ รวมถึงการคุ้มครองตนเอง ความเป็นเอกราชบูรณภาพแห่งชาติ ความมั่นคงทางทหาร เสถียรภาพทางเศรษฐกิจกับบรรดาความมั่งคั่งทั้งหลายที่จะพึงมี

ดังนั้น ผลประโยชน์แห่งชาติจึงมีความเกี่ยวข้องกับยุทธศาสตร์ชาติ และความมั่นคงแห่งชาติ ซึ่งประเทศชาติอันประกอบด้วย ดินแดน ประชากร รัฐบาล ความมีเอกราชอธิปไตย และการรับรองจากนานาชาติ จะต้องมีความมั่นคง มั่งคั่ง และยั่งยืน อันเป็นความมั่นคงแห่งชาติ แบบบูรณาการครอบคลุม ทุกด้านของกำลังอำนาจของชาติ ได้แก่ การเมืองภายในประเทศ การเมืองระหว่างประเทศ เศรษฐกิจ สังคมจิตวิทยา การทหาร วิทยาศาสตร์ เทคโนโลยี การพลังงาน

ทรัพยากรธรรมชาติและสิ่งแวดล้อม เทคโนโลยีสารสนเทศและการสื่อสารรวมทั้งการศึกษา หรืออีกนัยหนึ่ง พลังอำนาจแห่งชาติ (National Power)

Colins ได้ให้คำนิยามเกี่ยวกับผลประโยชน์ของชาติไว้ว่า “แนวความเกี่ยวกับผลประโยชน์ของชาตินั้น จะกำหนดขึ้นให้ชัดลงไปไม่ได้ง่ายนัก เพราะมีปัจจัยที่เกี่ยวข้องอยู่หลายสิ่งหลายอย่างด้วยกัน แต่โดยหลักทั่วไปอาจกล่าวได้ว่า ผลประโยชน์ของชาตินั้นเป็นสิ่งในคณะรัฐบาลที่กำลังบริหารประเทศ ในขณะนั้นกำหนดขึ้น โดยเห็นว่าผลประโยชน์เหล่านั้นสิ่งที่ผู้นำในคณะรัฐบาลที่กำลังบริหารประเทศ ในขณะนั้นกำหนดขึ้น โดยเห็นว่าผลประโยชน์เหล่านั้นมีความสำคัญต่อความอยู่รอด ความเป็นเอกราชบูรณภาพแห่งอาณาเขต ความมั่นคงปลอดภัย และสวัสดิภาพทางเศรษฐกิจ อย่างไรก็ตาม ผลประโยชน์ของชาติที่กำหนดขึ้นนั้น ก็จะต้องสอดคล้องกับความเห็นของประชาชนส่วนใหญ่ของประเทศด้วย ไม่เช่นนั้นแล้ว รัฐบาลก็จะไม่มีเสถียรภาพทางการเมือง เพราะขาดการสนับสนุนจากประชาชนส่วนใหญ่นั่นเอง” (Cited in USA WC, p.32)

นอกจากนี้ ข้อตกลงทั่วไปในเรื่องผลประโยชน์แห่งชาติของสหรัฐอเมริกาได้พิจารณาประเด็นสำคัญ 3 ประการ มาเป็นเกณฑ์กำหนดให้ผลประโยชน์แห่งชาติ คือ

1. ความมั่นคงทางกายภาพ (Physical Security) ซึ่งความมั่นคงทางกายภาพนี้เป็นการป้องกันการโจมตีอาณาเขตและประชาชนในชาติ เพื่อทำให้มั่นใจว่าจะเกิดความอยู่รอดในค่านิยมพื้นฐาน และความครบถ้วนของสถาบันอันเป็นสาธารณะ
2. การสนับสนุนค่านิยม (Promotion of Values)
3. ความมั่งคั่งทางเศรษฐกิจ (Economic Prosperity)

แต่ข้อตกลงดังกล่าวถูกนักปฏิบัติการเชิงยุทธศาสตร์และนักวิชาการบางกลุ่มตั้งข้อโต้แย้งว่าการดำรงอยู่ของโลกที่สมบูรณ์ คือ ผลประโยชน์แห่งชาติที่สำคัญเช่นกัน และการดำรงอยู่ของโลกที่สมบูรณ์ควรเป็นผลประโยชน์แห่งชาติที่มีมาตั้งแต่สมัยสงครามโลกครั้งที่ 2

อย่างไรก็ตาม ประเด็นสำคัญในข้อตกลงดังกล่าว สหรัฐอเมริกากำหนดให้เป็นเกณฑ์กำหนดให้ผลประโยชน์แห่งชาติ และถูกแปรเปลี่ยนไปเป็นมหายุทธศาสตร์ที่สำคัญของสหรัฐอเมริกา คือ

1. การปกป้องความมั่นคงของชนชาติอเมริกัน (Preserve American Security)
2. การเพิ่มพูนความมั่งคั่งทางเศรษฐกิจของชนชาติอเมริกัน (Bolster American Economic Prosperity)
3. การสนับสนุนของค่านิยมของชนชาติอเมริกัน (Promotion American Values)

และมหายุทธศาสตร์ถูกพิจารณากำหนดมาจากผลประโยชน์แห่งชาติ การบริหารทั้งหมดจะต้องเน้นเกี่ยวกับผลประโยชน์แห่งชาติ แต่ต้องขึ้นอยู่กับการประเมินความเสี่ยงและโอกาส ตลอดจนตัวแปรต่าง ๆ เช่น ความเชื่อส่วนบุคคล และสถานการณ์ที่ไม่ซ้ำกัน โดยด้านความมั่นคงนั้นสำหรับสหรัฐอเมริกาได้กำหนดให้สำคัญที่สุดในผลประโยชน์แห่งชาติ (Bartholomees, 2006)

2. ประเภทของผลประโยชน์แห่งชาติ

ผลประโยชน์แห่งชาติสามารถแบ่งประเภทได้เป็นลำดับชั้นของความสำคัญที่มีผลต่อความอยู่รอดของประเทศ ได้แก่

1. ผลประโยชน์แห่งชาติที่สำคัญยิ่งยวด (Vital National Interests) เป็นเงื่อนไขที่จำเป็นอย่างยิ่งยวดต่อการปกป้องรักษาและการเพิ่มพูนความอยู่รอดปลอดภัยและการอยู่ดีกินดีภายในประเทศที่มีความเสรีและปลอดภัย

2. ผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interest) สภาพเงื่อนไขซึ่งถ้าประนีประนอมแล้วอาจทำให้เกิดความเสียหายอย่างร้ายแรงแต่ไม่ทำให้ตกอยู่ในอันตรายอย่างร้ายแรงต่อรัฐบาลในการที่จะปกป้องและส่งเสริมความกินอยู่ที่ดีในการเป็นประเทศที่มีความเสรีภาพและมีความปลอดภัย

3. ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests) เป็นสภาพที่ว่าถ้าประนีประนอมแล้วจะเกิดผลทางลบอย่างมากตามมาในภายหลังต่อความสามารถของรัฐบาลในการที่จะปกป้องและเสริมสร้างความเป็นอยู่ที่ดีของประชาชนในฐานะที่เป็นประเทศอิสระและมีความปลอดภัย

4. ผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests) หรือผลประโยชน์แห่งชาติระดับรองนั้นไม่ใช่ว่าจะไม่มีความสำคัญแต่อย่างใด สิ่งเหล่านั้นล้วนแล้วแต่มีความสำคัญเป็นสภาพเงื่อนไขที่ต้องการเพียงแต่ว่ามีผลกระทบโดยตรงเพียงเล็กน้อยต่อความสามารถของรัฐบาลในอันที่จะปกป้องและเพิ่มพูนความกินอยู่ที่ดีของประชาชนในประเทศที่มีเสรีและมีความปลอดภัย

3. หลักการกำหนดผลประโยชน์แห่งชาติ

หลักการในการกำหนดผลประโยชน์แห่งชาติประกอบด้วยลักษณะสำคัญ 4 ประการ คือ

1. การอยู่รอดปลอดภัย (Survival)
2. การดำรงอยู่ของประชาชนในชาติ (Preservation of the people of the nation)
3. การอยู่ดีกินดี (Well-being)
4. การสร้างสรรค์สิ่งแวดล้อมระหว่างประเทศให้เกื้อกูลต่อผลประโยชน์ของชาติเหล่านี้ (Creation of an international environment favorable to theses interests) (USACGSC,1977)

อย่างไรก็ตาม ลักษณะของผลประโยชน์ของชาติ เป็นเรื่องที่ยอมรับกันโดยทั่วไปเพราะสามารถนำไปใช้ได้แทบทุกชาติในโลก โดยไม่เป็นการยุ่งยาก แต่ความยากลำบากอยู่ที่การนำไปใช้ปฏิบัติ สำหรับเรื่องความอยู่รอดของชาติถือเป็นผลประโยชน์ของชาติที่สำคัญอย่างยิ่ง แต่ความจริงแล้วยังไม่เคยมีปรากฏการณ์ทางประวัติศาสตร์ใด ๆ ที่จะชี้ให้เห็นว่าความอยู่รอดของชาตินั้นอยู่ตรงไหน จึงเป็นเรื่องยากสำหรับการกำหนดผลประโยชน์ของชาติขึ้นให้ชัดเจน และเนื่องจากการนิยามศัพท์ในเรื่องผลประโยชน์ของชาตินั้น มีลักษณะเป็นแนวความคิดทางอุดมการณ์ของบุคคล จึงมีบางคนที่ไม่ยอมรับอุดมการณ์ของผู้อื่น (พจน์ พงศ์สุวรรณ, 2536)

แนวความคิดเรื่องความมั่นคงแห่งชาติ

ความมั่นคงแห่งชาติในลักษณะของรูปธรรมประกอบด้วย ชาติ (Nation) ที่เน้นถึงคนที่มีวัฒนธรรมร่วมกัน มีเชื้อสายเดียวกัน มีความรู้สึกร่วมกัน และมีประวัติศาสตร์ร่วมกัน อยู่ในรัฐเดียวกัน

ภายใต้ประมุขของรัฐคนเดียวกัน รัฐ (State) คือ ชาติที่มีการจัดเป็นรูปองค์กรขึ้นเป็นประเทศ (Country) เป็นความหมายที่เน้นทางภูมิศาสตร์ หมายถึงการมีดินแดนอันเป็นที่รวมของชนชาติของรัฐ หรือเป็นที่รวมของสังคมขนาดใหญ่ สังคม (Society) เป็นความหมายที่เน้นถึงสภาพความเป็นอยู่ของกลุ่มคน ดังนั้น เมื่อกล่าวถึงความมั่นคงแห่งชาติ จึงอาจกล่าวได้ว่าเป็นความมั่นคงของสังคมก็ได้ ดังนั้น องค์ประกอบของชาติในส่วนที่เกี่ยวข้องกับความมั่นคงจึงประกอบด้วย ดินแดน ประชากร รัฐบาล ความมีเอกราชและการรับรองจากนานาชาติ

ประเทศไทยมีรูปแบบการปกครองที่สร้างขึ้นและประยุกต์เพิ่มเติมโดยได้รับอิทธิพลมาจาก ขอม อินเดีย และชาติตะวันตกที่เจริญแล้วในยุคนั้น ๆ ขณะระหว่างการเสริมสร้างการปกครองก็มีการรักษาความมั่นคงของประเทศควบคู่กันไป ก่อนปี 1994 การรักษาความมั่นคงของประเทศจะเน้นเพียงความมั่นคงแห่งชาติเป็นหลัก แต่หลังจากนั้นได้เกิดแนวความคิดใหม่เกี่ยวกับความมั่นคงเพิ่มเติมขึ้น มีการกล่าวถึงความมั่นคงของมนุษย์ (Human Security) โดยเสนอขึ้นเป็นวาระของโลก ในรายงานการพัฒนามนุษย์ 1994 ของแผนงานพัฒนาองค์การสหประชาชาติ (United Nations Development Program-UNDP) ซึ่งในรายงานฉบับนี้เป็นความพยายามในการขยายคำจำกัดความของคำว่า ความมั่นคง ซึ่งจากเดิมถือความมั่นคงของชาติเป็นหลักไปสู่ความมั่นคงทางการพัฒนาที่ถือประชาชนเป็นศูนย์กลาง (People Centered)

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช ทรงอธิบายความหมายของความมั่นคงแห่งชาติไว้อย่างชัดเจนในพิธีถวายสัตย์ปฏิญาณตนและสวนสนามของทหารรักษาพระองค์ เมื่อวันที่ 2 ธันวาคม 2544 ณ ลานพระบรมรูปทรงม้า ความว่า “...ประเทศชาตินั้นประกอบด้วยผืนแผ่นดินกับประชาชน และผืนแผ่นดินนั้น เป็นที่เกิด ที่อาศัย ที่อำนวยประโยชนสุข ความมั่นคง ร่มเย็นแกประชาชน ให้สามารถรวมกันอยู่เป็นปึกแผ่นเป็นชาติได้ ความมั่นคงปลอดภัยของประเทศจึงมิได้อยู่ที่การปกป้องรักษาผืนแผ่นดินไว้ด้วยแสนยานุภาพแต่เพียงอย่างเดียว หากจำเป็นที่ประชาชนจะต้องมีความวัฒนาผาสุก ปราศจากทุกข์ยากเข็ญด้วย...”

พลตรีหลวงวิจิตรวาทการ ให้ความหมายของความมั่นคงแห่งชาติไว้ว่า “ความมั่นคงแห่งชาติ คือ การทรงตัวอยู่อย่างแน่นหนาถาวร ดำรงเอกราช มีเสรีภาพแห่งชาติ มีความสงบสุขภายในประเทศ มีความแน่นอนในชีวิต และเศรษฐกิจของพลเมือง คาดหมายรายได้ของรัฐได้ถูกต้องใกล้เคียงกับความเป็นจริง ค่าของเงินตรามี เสถียรภาพ รัฐไม่ต้องประสบความยุ่งยากระส่ำระสาย ไม่เกิดการเปลี่ยนแปลงใด ๆ ได้ง่าย ประชาชนพลเมืองรู้สึกมีความปลอดภัย มีความหวังและความไว้วางใจในอนาคต และยังไว้วางใจต่อไปอีกว่า ถึงแม้ความผันผวนหรือเหตุร้ายอันใดจะเกิดขึ้นมา รัฐสามารถจะต่อสู้หรือป้องกันได้” นอกจากนั้นยังได้จำแนกความมั่นคง แห่งชาติออกเป็น 4 ด้านตามลักษณะของภารกิจที่ชาติจำเป็นต้องดำเนินการเพื่อบรรลุวัตถุประสงค์ของชาติ คือ ความมั่นคงแห่งชาติด้านการเมือง, ความมั่นคงแห่งชาติด้านเศรษฐกิจ, ความมั่นคงแห่งชาติด้านสังคมจิตวิทยา และความมั่นคงแห่งชาติด้านการทหาร (อุปถัมภ์ อินทามาระ, สารนิพนธ์รัฐประศาสนศาสตรมหาบัณฑิตสำหรับนักบริหาร มหาวิทยาลัยศรีปทุม, 2540, หน้า 42-43)

พลอากาศเอก สิทธิ เศวตศิลา ให้ความหมายของความมั่นคงแห่งชาติว่า “ความมั่นคงแห่งชาติหมายถึง การให้เอกราชของชาติ บูรณภาพของดินแดนและสวัสดิภาพของประชาชนอยู่ในความมั่นคงและปลอดภัย รวมตลอดถึง การให้ประเทศดำรงอยู่ในการปกครองระบอบประชาธิปไตย” (พจน์ พงศ์สุวรรณ์, พล.ต., หลักยุทธศาสตร์, หน้า 44)

พลเอก สายหยุด เกิดผล ให้ความหมายของความมั่นคงแห่งชาติไว้ว่า “ความมั่นคงแห่งชาติ หมายถึง ความรู้สึกของคนในชาติส่วนใหญ่ที่มีความรู้สึกว่าชาติของตนอยู่ในภาวะมั่นคง ทั้งนี้ด้วยความเชื่อมั่นและเข้าใจอย่างถูกต้องว่ากิจกรรมทั้งสี่ด้านของชาติ คือกิจกรรรมทางด้านการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยา มีประสิทธิภาพในตนเองสนับสนุนซึ่งกันและกัน ความขัดแย้งต่าง ๆ หากมีขึ้นก็จะสามารถประสานความเข้าใจและประสานการปฏิบัติได้ในระดับชาติ” (วิทยาลัยเสนาธิการทหาร, เอกสารแนะนำฝ่ายเสนาธิการร่วม ภาคที่ 2 ยุทธศาสตร์ชาติ , หน้า 2-30)

พลตรี ทวีป สัทธานน์ “ความมั่นคงแห่งชาติ หมายถึง ความปลอดภัยของรัฐ ซึ่งมีขอบเขตอย่างแคบประกอบด้วยปัจจัย 3 ประการ คือ เสถียรภาพทางการเมือง บูรณภาพแห่งอาณาเขต และเศรษฐกิจที่มั่นคง” (มหาวิทยาลัยสุโขทัยธรรมาธิราช, เอกสารการสอนชุดพัฒนศึกษา, 2535, หน้า 289)

โรงเรียนเสนาธิการทหารบกสหรัฐฯ ความมั่นคงแห่งชาติ หมายถึงการป้องกันชาติให้พ้นจากอันตรายทั้งปวง อันได้แก การรุกรานจากภายนอก การจารกรรม การลาดตระเวนของข้าศึก การก่อวินาศกรรม การบ่อนทำลาย การรบกวนและอิทธิพลอื่น ๆ ซึ่งจะเป็นอันตรายอย่างร้ายแรงแห่งชาติ (Ft. Leavenworth , USACGSC, STRATEGIC STUDIES : CURRENT US POLICY, POSTURES, AND ISSUES, 1980, p. 122)

พจนานุกรมคณะเสนาธิการร่วม เล่ม 1 กองทัพสหรัฐฯ "ความมั่นคงแห่งชาติ หมายรวมถึงทั้งการป้องกันประเทศของสหรัฐฯ และประเทศที่มีความสัมพันธ์กับสหรัฐฯ โดยเฉพาะภายใต้สถานการณ์ดังนี้

1. การได้เปรียบทางทหารหรือการป้องกันชาติอื่น ๆ หรือกลุ่มของชาติอื่น ๆ
2. ที่ตั้งที่เกื้อกูลแก่ต่างประเทศที่มีความสัมพันธ์กับสหรัฐฯ หรือ
3. การป้องกันการวางกำลังของข้าศึก ที่มีขีดความสามารถในการต้านทานสูงหรือ การทำลาย การปฏิบัติจากภายในหรือภายนอก, ทั้งเปิดเผยและปกปิด" (JCS Pub.I, DEPARTMENT OF DEFENSE DICTIONARY OF. MILITARY AND ASSOCIATED TERMS)

สุรชาติ บำรุงสุข ได้จำแนกปัญหาความมั่นคงในทศวรรษแรกของปี 2000 ไว้ 2 ลักษณะ คือ ปัญหาด้านการทหาร และปัญหาที่มิใช่ด้านการทหาร

1. ปัญหาด้านการทหาร แบ่งออกเป็น 4 ประเด็น คือ
   1.1 ปัญหาความขัดแย้งในเรื่องเส้นเขตแดน
   1.2 ปัญหาการเสริมสร้างแสนยานุภาพทางทหาร
   1.3 ปัญหาเศรษฐกิจทางทหาร
   1.4 ปัญหาความมั่นคงทางทหารระหว่างประเทศ
2. ปัญหาที่มิใช่ด้านการทหาร แบ่งออกเป็น 6 ประเด็น คือ
   2.1 ปัญหาสิ่งแวดล้อม
   2.2 ปัญหาการย้ายถิ่นของประชากร
   2.3 ปัญหาการขยายตัวของเทคโนโลยีสมัยใหม่
   2.4 ปัญหาการพัฒนาเศรษฐกิจ
   2.5 ปัญหาการแพร่กระจายของเชื้อโรค

2.6 ปัญหาด้านวัฒนธรรมและกลุ่มชาติพันธุ์

(สุรชาติ บำรุงสุข, ปัญหาความมั่นคง: ความเปลี่ยนแปลงในทศวรรษแรกของ ค.ศ.2000, เสนาธิปัตย์ ปีที่ 45 ฉบับที่ 3 เดือน ก.ย.-ธ.ค., หน้า 68-72)

ประจวบ ไชยสาส์น ได้กล่าวถึงแนวความคิดเรื่องความมั่นคงไว้ว่า “ความมั่นคง” มีความหมายครอบคลุมหลายมิติ และประเด็นในด้านต่างๆ ซึ่งปัจจุบันนิยมเรียกว่า “Comprehensive Security” อาทิ

1. ความมั่นคงทางทหาร หมายถึง ความพร้อมทางทหารเพื่อป้องกันการรุกราน
2. ความมั่นคงทางด้านการเมือง หมายถึง การมีระบบการเมืองที่มั่นคง มีการเปลี่ยนแปลงทางการเมืองอย่างเป็นระเบียบเรียบร้อย
3. ความมั่นคงทางเศรษฐกิจ หมายถึง การเจริญเติบโตทางเศรษฐกิจสูง มีอัตราการส่งออกสูง ประชาชนมีรายได้ต่อหัวสูง และ
4. ความมั่นคงทางสังคม หมายถึง คุณภาพชีวิตที่ดีของประชาชน โดยได้รับการศึกษาอย่างทั่วถึง มีระบบสาธารณะสุขที่ดี ปลอดโรคภัยไข้เจ็บ และมีความอยู่ดีกินดี เป็นต้น (ประจวบ ไชยสาส์น, กระทรวงการต่างประเทศกับการพัฒนานโยบายความมั่นคงแห่งชาติ, วารสารสราญรมย์ ฉบับระลึกครบรอบ ปีที่ 55, 2541, หน้า 143)

Richard Shuttz, Roy Godson and Ted Greenwood ได้กล่าวไว้ในหนังสือ Security for the 1990’s เกี่ยวกับแนวความคิดในเรื่องความมั่นคงว่าจะต้องเป็นไปในลักษณะของพหุภาคี ระบบความร่วมมือทางทหารที่มีลักษณะการรวมตัวกัน เป็นองค์กรพันธมิตรทางทหาร (Alliance) มีปัญหาใหญ่ 3 ประการ คือ

1. การจัดการเรื่องงบประมาณขององค์กร
2. ความเป็นผู้นำของประเทศเมื่อต้องเข้าสู่สงคราม
3. ปัญหาการเมืองภายในของประเทศสมาชิกขององค์กร

(Richard Shuttz, Roy Godson and Ted Greenwood,eds., Security for the 1990’s, 1993, p.251)

Stephen W. Walt ได้นำเสนอแนวความคิดความมั่นคงร่วม (Collective Security) เพื่อขจัดปัญหาดังกล่าวไว้ 3 รูปแบบ ดังนี้

1. Great Power Concert เป็นระบบที่ประเทศสมาชิกกำหนดข้อตกลงต่อต้านภัยคุกคามร่วมกัน เพื่อความมีเสถียรภาพ ตัวอย่างเช่น The Concert of Europe ช่วงหลังสงครามนโปเลียน ระบบนี้มีนักวิชาการบางคนเสนอว่า เป็นรูปแบบที่เหมาะสมในหลังยุคสงครามเย็น
2. Conflict Management by International Organization เป็นระบบที่องค์กรระหว่างประเทศ เช่น องค์การสหประชาชาติเข้าไปดำเนินการป้องปราม จัดให้มีการเจรจา กำหนดวาระการเจรจาในความขัดแย้งที่เกิดขึ้น อาจจะต้องจัดตั้งกองกำลังรักษาสันติภาพ ซึ่งหลังยุคสงครามเย็นกองกำลังรักษาสันติภาพ โดยองค์การสหประชาชาติได้มีบทบาทสำคัญในการยุติข้อขัดแย้งทั่วโลก
3. Limited Security Regimes เป็นกลไกของความร่วมมือระดับทวิภาคี หรือพหุภาคี เพื่อยุติหรือลดปัจจัยที่ก่อให้เกิดความไม่มั่นคง เช่น ข้อตกลงการควบคุมอาวุธ, มาตรการสร้างความมั่นใจ, “Hot line” ระหว่างประเทศมหาอำนาจ เป็นต้น (Richard Shuttz, Roy Godson and Ted Greenwood,eds., Security for the 1990’s, 1993, p.255-258)

National Cyber Security Strategy ของประเทศต่างๆ

1. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งสหภาพยุโรป (EU Cybersecurity Strategy)

นอกจากสหภาพยุโรปจะเป็นตลาดเดียวในด้านการค้า และสหภาพศุลกากร ปัจจุบันสหภาพยุโรปพยายามที่จะทำให้มีตลาดร่วมในด้านดิจิทัล (Digital Single Market) เพื่อเพิ่มศักยภาพของตลาดดิจิทัลภายในภูมิภาค สามารถแข่งขันกับประเทศคู่แข่งในภูมิภาคอื่น ๆ คณะกรรมาธิการยุโรปมองว่าการเป็นตลาดร่วมในด้านดิจิทัล เป็นหนึ่งในเป้าหมายที่สำคัญ เพราะสหภาพยุโรปจะสามารถทำให้รายได้ของสหภาพยุโรปเพิ่มขึ้นอีกถึง 250,000 ล้านยูโร ทำให้การจ้างงานเพิ่มขึ้นนับล้านตำแหน่ง รวมทั้งทำให้สังคมเกิดการแลกเปลี่ยนความรู้ต่อกัน ความมั่นใจและความมั่นคงปลอดภัยบนโลกไซเบอร์จึงกลายมาเป็นรากฐานที่สำคัญของการเป็นตลาดร่วมในด้านดิจิทัล ในปัจจุบันพลเมืองในสหภาพยุโรปต่างพึ่งพาอินเทอร์เน็ตสำหรับการรับบริการในด้านต่าง ๆ เช่น การรับบริการจากรัฐบาลอิเล็กทรอนิกส์ การรับบริการด้านสุขภาพ การซื้อสินค้าและบริการออนไลน์ และการติดต่อสื่อสารในเครือข่ายสังคมออนไลน์

อย่างไรก็ตาม โลกไซเบอร์มีอัตราความเสี่ยงเพิ่มขึ้นจากภัยคุกคามที่เกิดจากความล้มเหลวทางเทคนิค (Technical Failures) และการโจมตีทางไซเบอร์ (Cyber Attacks) ความล้มเหลวในการตอบโต้ต่อภัยคุกคามทางไซเบอร์เหล่านี้ อาจนำไปสู่การสูญเสียความเชื่อมั่นของผู้บริโภค ส่งผลให้ภาคธุรกิจเกิดความเสียหายคิดเป็นเงินมูลค่าจำนวนมหาศาล และกระทบต่อประสิทธิภาพของโครงการรัฐบาลอิเล็กทรอนิกส์ ตลอดจนกระทบต่อความมั่นคงของชาติ และเนื่องจากการโจมตีไซเบอร์ไม่อาจสกัดกันได้ด้วยพรมแดนของประเทศ วิธีการแก้ปัญหาของสหภาพยุโรปจึงต้องสร้าง “ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป” ขึ้น เพื่อสร้างความมั่นใจต่อภาคธุรกิจและประชาชนในสหภาพยุโรปว่าโลกไซเบอร์ในสหภาพยุโรปมีความมั่นคงปลอดภัย

สหภาพยุโรปกำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นโดยมีเป้าหมายเพื่อคุ้มครองสิทธิเสรีภาพ ตลอดจนรักษาความมั่นคงปลอดภัยอย่างสูงสุดสำหรับการติดต่อสื่อสารออนไลน์ ยุทธศาสตร์นี้จะช่วยสร้างความมั่นใจแก่ประชาคมแห่งสหภาพยุโรปและประชาคมโลกว่าสหภาพยุโรปมีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่แข็งแกร่ง มีประสิทธิภาพ และมีความปลอดภัยมากที่สุดแห่งหนึ่งของโลก

ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรปประกอบด้วย

1. การบรรลุความมั่นคงปลอดภัยไซเบอร์ โดยการเพิ่มขีดความสามารถ สร้างความพร้อม การบูรณาการความร่วมมือในการแลกเปลี่ยนข้อมูลและความตระหนักถึงภัยคุกคามทางไซเบอร์และความปลอดภัยของข้อมูลทั้งภาครัฐและเอกชน ทั้งระดับประเทศและระดับสหภาพ

2. การลดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยการเสริมสร้างทักษะ ความเชี่ยวชาญแก่เจ้าหน้าที่ ในการกำกับดูแล ตรวจสอบ และดำเนินการต่อผู้กระทำความผิด โดยมีการประสานงานระหว่างหน่วยงานบังคับใช้กฎหมายทั่วสหภาพยุโรปและการเสริมสร้างความร่วมมือกับหน่วยงานหรือบุคคลอื่น ๆ

3. การพัฒนานโยบายการป้องกันทางไซเบอร์ของสหภาพยุโรปและเพิ่มขีดความสามารถในการรักษาความปลอดภัยและนโยบายการป้องกันไซเบอร์ร่วมกัน

4. การสนับสนุนทรัพยากร ทั้งทางด้านอุตสาหกรรมและเทคโนโลยีที่จำเป็นในการเป็นตลาดร่วมในด้านดิจิทัล (Digital Single Market) ยุทธศาสตร์นี้จะช่วยกระตุ้นให้เกิดความมั่นคงปลอดภัยและความเชื่อมั่นแก่ภาคอุตสาหกรรมและตลาดเทคโนโลยีสารสนเทศและการสื่อสาร (Information Communication and Technology: ICT) ในสหภาพยุโรป ซึ่งท้ายสุดจะนำไปสู่การเจริญเติบโตและความสามารถในการแข่งขันทางเศรษฐกิจของสหภาพยุโรป ทั้งยังเป็นการเพิ่มงบประมาณในการวิจัยและพัฒนาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ให้กับภาครัฐและเอกชน

5. การเสริมสร้างนโยบายต่างประเทศของสหภาพยุโรปที่เกี่ยวกับโลกไซเบอร์ เพื่อส่งเสริมให้เกิดการกำหนดบรรทัดฐานสำหรับพฤติกรรมทางไซเบอร์ที่มีความรับผิดชอบ สนับสนุนการใช้กฎหมายระหว่างประเทศที่มีอยู่กับกิจกรรมบนโลกไซเบอร์ และเพื่อให้ความช่วยเหลือประเทศนอกกลุ่มสหภาพยุโรปในการสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์

2. แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป

สหภาพยุโรปมีการกำหนดกฎการรักษาความมั่นคงปลอดภัยของเครือข่ายและข้อมูลแห่งสหภาพยุโรป (EU Network and Information Security Directive) หรือที่รู้จักกันทั่วไปว่า “กฎการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป” ถูกเสนอโดยคณะกรรมาธิการยุโรป ในปี 2557 โดยมีจุดเป้าหมายในการสร้างความเชื่อมั่นต่อโลกว่าระบบไซเบอร์ในสหภาพยุโรปมีความมั่นคงปลอดภัย

การประชุมร่วมระหว่างสภายุโรป รัฐสภายุโรปและคณะกรรมาธิการยุโรป เมื่อวันที่ 13 มีนาคม 2557 ที่ประชุมเห็นว่าความเสี่ยงที่เกิดจากการโจมตีทางไซเบอร์ได้ทวีความรุนแรงมากขึ้นทั้งต่อหน่วยงานของภาครัฐและเอกชนทั่วสหภาพยุโรป จึงได้อนุมัติร่างกฎการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป โดยมีจุดมุ่งหมายที่จะนำมาบังคับใช้ควบคู่กับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป การดำเนินการภายใต้กฎการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป มีการดำเนินการที่สำคัญดังนี้

1. ปรับปรุงประสิทธิภาพทางเทคนิคในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศสมาชิกแห่งสหภาพยุโรป โดยประเทศสมาชิกแต่ละประเทศจะต้องสร้างเครือข่ายข้อมูลรักษาความมั่นคงปลอดภัย (National Information Security: NIS) ของตน และแต่งตั้งเจ้าหน้าที่ผู้มีอำนาจ (National Competent Authority: NCA) เพื่อนำกฎการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรปมาใช้ในประเทศของตน นอกจากนี้ประเทศสมาชิกแต่ละประเทศต้องสร้างทีมตอบสนองเหตุฉุกเฉินทางคอมพิวเตอร์ของตน (Computer Emergency Response Team : CERT) เพื่อรับผิดชอบในการจัดการและลดปัญหาความเสี่ยงจากการรักษาความมั่นคงปลอดภัยไซเบอร์

2. เสริมสร้างความร่วมมือระหว่างประเทศสมาชิกในสหภาพยุโรป รวมถึงหน่วยงานภาครัฐและเอกชนเพื่อร่วมกันจัดการกับปัญหาความมั่นคงปลอดภัยไซเบอร์

3. กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยบนโลกไซเบอร์ขั้นต่ำสำหรับผู้ประกอบการภาคธุรกิจที่เกี่ยวกับโครงสร้างพื้นฐานที่สำคัญ เช่น พลังงาน สุขภาพ การขนส่ง บริการทางการเงิน ฯลฯ องกลุ่มประเทศสมาชิกสหภาพยุโรปทั้งหมด ตามมาตรฐานขั้นต่ำดังกล่าว

ผู้ประกอบการจะต้องกำหนดมาตรการในการบริหารจัดการความเสี่ยงด้านความปลอดภัยบนโลกไซเบอร์ และจะต้องรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยบนโลกไซเบอร์ที่มีผลกระทบต่อการให้บริการของตน

กฎรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรปนั้น ทำให้ประชาชนและผู้บริโภคเกิดความไว้วางใจในเทคโนโลยีที่ใช้ในชีวิตประจำวันมากขึ้น รัฐบาลและภาคธุรกิจจะสามารถใช้เครือข่ายโครงสร้างพื้นฐานที่จะให้บริการประชาชนทั้งในประเทศและนอกประเทศได้อย่างมั่นใจ มีความมั่นคงปลอดภัย เป็นการสร้างความเชื่อมั่นให้กับเศรษฐกิจของสหภาพยุโรป อีกทั้งการใช้วัฒนธรรมในการบริหารความเสี่ยงและระบบการรายงานเหตุการณ์ที่เกิดขึ้นทำให้เกิดความเท่าเทียมกันระหว่างองค์กรภาคธุรกิจที่ต้องการจะแข่งขันในตลาดดิจิทัลแห่งสหภาพยุโรป

3. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร (UK's National Cyber Security Strategy 2016 – 2021)

สหราชอาณาจักร หรือ อังกฤษ จัดให้ความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) มีความสำคัญเทียบเท่าภัยคุกคามก่อการร้ายสากล วิกฤติความมั่นคงทางทหารและภัยธรรมชาติ ยุทธศาสตร์ฉบับนี้มุ่งป้องกันภัยคุกคามทางไซเบอร์เพื่อส่งเสริมให้เศรษฐกิจเติบโต ปกป้องความมั่นคงของชาติและการดำเนินชีวิตทั่วไป มีแผนร่วมมือระหว่างภาครัฐกับเอกชนที่เป็นรูปธรรม และมุ่งให้อังกฤษเป็นหนึ่งในผู้นำโลกด้านการวิจัย การพัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ รัฐบาลอังกฤษกับมหาวิทยาลัยชั้นนำร่วมทำงานวิจัยด้านไซเบอร์ร่วมกันเพื่อให้ได้งานวิจัยด้านไซเบอร์ที่มีคุณภาพ

จากยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร (UK's National Cyber Security Strategy 2016 – 2021) อังกฤษมองว่าอนาคตของความมั่นคงและความเจริญรุ่งเรืองของอังกฤษขึ้นอยู่กับพื้นฐานของระบบดิจิทัล ความท้าทายของยุคนี้คือการสร้างสังคมดิจิทัลที่เฟื่องฟูและสามารถต่อกรกับภัยคุกคามทางไซเบอร์ได้ การเตรียมความพร้อมทั้งความรู้และความสามารถที่จำเป็นจะช่วยเพิ่มโอกาสและจัดการความเสี่ยงต่อปัญหาภัยคุกคามทางไซเบอร์ของประเทศได้

“เราอยู่กับความเสี่ยงบนอินเทอร์เน็ต มีความพยายามใช้ประโยชน์จากจุดอ่อนเพื่อโจมตีทางไซเบอร์ แม้ภัยคุกคามทางไซเบอร์นี้ไม่สามารถขจัดออกได้อย่างสมบูรณ์ แต่หากทำให้ความเสี่ยงต่าง ๆ ลดลง อาจทำให้สังคมยังคงประสบความสำเร็จและได้รับประโยชน์จากโอกาสอันมหาศาลที่จากเทคโนโลยีดิจิทัลได้” (UK's National Cyber Security Strategy 2016 – 2021, P 9)

ในปี 2011 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของอังกฤษได้รับการสนับสนุนจากโครงการความมั่นคงแห่งชาติของรัฐบาลด้วยงบประมาณกว่า 860 ล้านปอนด์ ทำให้การรักษาความปลอดภัยในโลกไซเบอร์ของอังกฤษมีประสิทธิภาพมากขึ้น

วิสัยทัศน์เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของอังกฤษในอนาคต ปี 2011 คือ “อังกฤษมีความปลอดภัยและรับมือต่อภัยคุกคามทางไซเบอร์ได้อย่างมั่นคง และสร้างความมั่นใจในโลกดิจิทัลได้” เพื่อให้บรรลุวิสัยทัศน์ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของอังกฤษได้กำหนดแนวทางการทำงานเพื่อให้บรรลุวัตถุประสงค์ดังต่อไปนี้

1. การป้องกัน (Defend) อังกฤษมีมาตรการในการป้องกันจากภัยคุกคามทางไซเบอร์ที่กำลังพัฒนาขึ้นเรื่อย ๆ สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ทำให้สามารถมั่นใจได้ว่าเครือข่ายข้อมูลและระบบในอังกฤษมีการป้องกันและความสามารถในการฟื้นตัวหากถูกโจมตีได้ ทั้งภาครัฐ ภาคธุรกิจ และพลเรือน มีความรู้ความสามารถในการป้องกันตนเอง

2. การยับยั้ง (Deter) อังกฤษสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทุกรูปแบบ นอกจากนั้นยังต้องสามารถตรวจจับ และขัดขวางการโจมตี รวมทั้งสามารถจัดการกับผู้กระทำความผิดได้

3. การพัฒนา (Develop) อังกฤษมีนวัตกรรมด้านอุตสาหกรรมการรักษาความปลอดภัยในโลกไซเบอร์ซึ่งได้รับการสนับสนุนโดยการวิจัยทางวิทยาศาสตร์ระดับโลก และมีโครงข่ายที่มีความสามารถของตนเองในการพัฒนาทักษะในการตอบสนองต่อความต้องการของชาติได้อย่างทั่วถึงทั้งภาครัฐ และภาคเอกชน ความทันสมัย การวิเคราะห์และความเชี่ยวชาญจะทำให้อังกฤษสามารถเอาชนะภัยคุกคามและความท้าทายในอนาคตได้

เพื่อสนับสนุนเป้าหมายเหล่านี้ อังกฤษได้ติดตามการดำเนินการระหว่างประเทศและใช้ความสามารถของประเทศสร้างความร่วมมือต่าง ๆ เพื่อกำหนดรูปแบบวิวัฒนาการของโลกไซเบอร์ในการส่งเสริมความสามารถด้านเศรษฐกิจและความมั่นคง และกระชับความสัมพันธ์ที่มีอยู่กับพันธมิตร เพื่อช่วยเพิ่มความมั่นคงปลอดภัยด้านไซเบอร์

นอกจากนี้ยังจะพัฒนาความสัมพันธ์กับพันธมิตรรายใหม่เพื่อสร้างระดับความปลอดภัยในโลกไซเบอร์และปกป้องผลประโยชน์ของอังกฤษในต่างประเทศ ทั้งในรูปแบบทวิภาคีและพหุภาคี รวมทั้งผ่านทางสหภาพยุโรป นาโต และสหประชาชาติ รวมทั้งส่งข้อความที่ชัดเจนเกี่ยวกับผลลัพธ์ที่จะเกิดขึ้นให้กับฝ่ายตรงข้ามที่ขู่ว่าจะทำลายอังกฤษหรือพันธมิตรของอังกฤษบนโลกไซเบอร์

เพื่อการบรรลุผลดังกล่าวตามแผน 5 ปี อังกฤษตั้งใจที่จะเข้าไปแทรกแซงและใช้เงินลงทุนเพื่อยกระดับมาตรฐานการรักษาความปลอดภัยในโลกไซเบอร์ทั่วประเทศ นอกจากนั้นรัฐบาลยังมีความร่วมมือกับ สกอตแลนด์ เวลส์ และไอร์แลนด์เหนือ ในการประสานการทำงานร่วมกับหน่วยงานภาครัฐและภาคเอกชน เพื่อให้มั่นใจว่าบุคคล ภาคธุรกิจ และองค์กรต่าง ๆ มีมาตรการที่จำเป็นในการรักษาความปลอดภัยทางไซเบอร์

“เราจะมีมาตรการในการแทรกแซง (เมื่อจำเป็นและอยู่ในขอบเขตอำนาจของเรา) เพื่อผลักดันให้เกิดการปรับปรุงเพื่อผลประโยชน์ของชาติ โดยเฉพาะอย่างยิ่งในเรื่องเกี่ยวกับความมั่นคงปลอดภัยบนโลกไซเบอร์ซึ่งเป็นหนึ่งโครงสร้างพื้นฐานที่สำคัญของประเทศของเรา” (UK's National Cyber Security Strategy 2016 – 2021, P 10)

รัฐบาลอังกฤษใช้วิธีการดึงขีดความสามารถของภาคอุตสาหกรรมเพื่อการพัฒนามาตรการป้องกันทางไซเบอร์ที่ใช้งานอยู่ เพื่อยกระดับความปลอดภัยบนโลกไซเบอร์ในเครือข่ายอังกฤษ มาตรการเหล่านี้ยังรวมถึงการลดการโจมตีที่เคยถูกตรวจพบมากที่สุด การกรองที่อยู่ IP ที่ไม่รู้จักหรือที่รู้จัก และบล็อกกิจกรรมทางไซเบอร์ที่เป็นอันตราย

รัฐบาลอังกฤษได้สร้าง ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งชาติ (National Cyber Security Center : NCSC) เพื่อกำกับดูแลงานด้านการรักษาความปลอดภัยในโลกไซเบอร์ของอังกฤษ แบ่งปันความรู้เกี่ยวกับจุดอ่อนของระบบ และมีบทบาทนำในประเด็นสำคัญด้านความปลอดภัยในโลกไซเบอร์แห่งชาติ

“เราจะมั่นใจได้ว่ากองทัพมีระบบป้องกันทางไซเบอร์ที่แข็งแกร่ง เพื่อรักษาความปลอดภัย ปกป้องเครือข่าย และแพลตฟอร์มต่าง ๆ ให้กองทัพสามารถปฏิบัติภารกิจได้อย่างเป็นอิสระ แม้จะมีภัยคุกคามจากโลกไซเบอร์ ศูนย์ปฏิบัติการรักษาความปลอดภัยไซเบอร์ของกองทัพ (Cyber Security Operations Centre : OCSC) จะทำงานใกล้ชิดกับ NCSC และเรามั่นใจว่ากองทัพสามารถช่วยในการรับมือจากการโจมตีทางไซเบอร์ในระดับชาติได้ เราจะมีวิธีตอบโต้ต่อการโจมตีทางไซเบอร์เช่นเดียวกับการตอบโต้การโจมตีในรูปแบบอื่น ๆ โดยใช้รูปแบบการตอบโต้ที่เหมาะสมที่สุด รวมถึงการใช้วิธีการโจมตีทางไซเบอร์” (UK's National Cyber Security Strategy 2016 – 2021, P 10)

รัฐบาลอังกฤษใช้อำนาจและอิทธิพลของรัฐบาล ในการลงทุนกับโครงการต่าง ๆ เพื่อแก้ไขปัญหาการขาดแคลนบุคลากรที่มีทักษะด้านความปลอดภัยบนโลกไซเบอร์ ตั้งแต่ระดับโรงเรียนจนถึงมหาวิทยาลัย มีการเปิดตัวศูนย์นวัตกรรมไซเบอร์ใหม่สองแห่งเพื่อขับเคลื่อนการพัฒนาทางไซเบอร์ที่ทันสมัย นอกจากนี้ยังจัดสรรสัดส่วนของกองทุนป้องกันและนวัตกรรมไซเบอร์มูลค่ากว่า 165 ล้านปอนด์ เพื่อสนับสนุนการจัดซื้อนวัตกรรมในด้านการป้องกันและการรักษาความปลอดภัย และวางแผนจะลงทุนอีกราว 1.9 พันล้านปอนด์ ในอีกห้าปีข้างหน้าเพื่อพัฒนาระบบการรักษาความปลอดภัยบนโลกไซเบอร์อังกฤษให้มีความมั่นคงและปลอดภัยมากยิ่งขึ้น

4. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของออสเตรเลีย (Australia's Cyber Security Strategy)

ออสเตรเลียมองว่าการรักษาความปลอดภัยทางไซเบอร์ที่แข็งแกร่งเป็นองค์ประกอบพื้นฐานของการเจริญเติบโตและความเจริญรุ่งเรืองของออสเตรเลียในเศรษฐกิจโลก และยังเป็นสิ่งสำคัญสำหรับการรักษาความปลอดภัยแห่งชาติ โดยต้องได้รับความร่วมมือที่ทั้งจากรัฐบาล ภาคเอกชน และภาคประชาชน

ออสเตรเลียต้องการที่จะพัฒนาและกระจายเศรษฐกิจของประเทศในการเข้าถึงตลาดใหม่และรูปแบบใหม่ของการสร้างความมั่งคั่ง เพื่อเปิดโอกาสใหม่สำหรับธุรกิจออนไลน์ที่จะทำให้การประกอบการและทำธุรกรรมต่างๆ มีความคล่องตัวมากยิ่งขึ้น การเชื่อมโยงเครือข่ายจึงเป็นสิ่งที่สำคัญในการสร้างโอกาสใหม่สำหรับนวัตกรรมและการเติบโตของออสเตรเลีย แต่ก็ทำให้เกิดความเสี่ยงที่ออสเตรเลียอาจตกเป็นเป้าหมายของอาชญากรรมและการถูกจารกรรมมากยิ่งขึ้น

ออสเตรเลียมองเห็นว่า หากองค์กรมีการเชื่อมต่อกับอินเทอร์เน็ตมีปริมาณและมูลค่าของข้อมูลในโลกออนไลน์เพิ่มสูงขึ้น จะกลายเป็นความเสี่ยงจากการพยายามขโมยและใช้ประโยชน์จากข้อมูลเพื่อทำลายความมั่นคง เศรษฐกิจ และความเป็นส่วนตัวของประชากรออสเตรเลีย และกลายเป็นภัยคุกคามถาวรในที่สุด ความสามารถในการรักษาความปลอดภัยใน Cyberspace ต้องมีการคาดการณ์และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่รวดเร็ว แต่ออสเตรเลียยังต้องเผชิญกับปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญด้านความปลอดภัยใน Cyberspace ซึ่งออสเตรเลียมองว่าเป็นสิ่งสำคัญที่ลงทุนเพื่อสร้างบุคลากรที่มีทักษะในการรักษาความปลอดภัยใน Cyberspace ซึ่งจะกลายเป็นสิ่งจำเป็นมากขึ้นสำหรับวิถีชีวิตและการทำงานใน Cyberspace ของออสเตรเลีย

รัฐบาลออสเตรเลีย ภาคธุรกิจ และชุมชน จึงมีความพยายามในการทำงานร่วมกันเพื่อสร้างความปลอดภัยและสามารถต่อกรกับภัยคุกคามความปลอดภัยใน Cyberspace ให้ได้มากที่สุด โครงสร้างพื้นฐานด้านดิจิตอลของออสเตรเลีย มีภาคเอกชนเป็นผู้ดูแล จึงต้องมีการประสานงาน

และรับผิดชอบร่วมกัน เพื่อปรับปรุงและสร้างการแก้ปัญหาร่วมกันในการป้องกันภัยคุกคามความปลอดภัยใน Cyberspace

ในยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของออสเตรเลีย (Australia's Cyber Security Strategy) ระบุว่า “การรักษาความปลอดภัยใน Cyberspace ของออสเตรเลียถูกสร้างขึ้นบนรากฐานที่มั่นคง ความคิดริเริ่มของรัฐบาลและการดำเนินการที่ผ่านมาทำเรามีความแข็งแกร่ง เช่น ศูนย์รักษาความปลอดภัยไซเบอร์ของออสเตรเลียได้ยกระดับความสามารถของรัฐบาลในการป้องกันภัยคุกคามความปลอดภัยใน Cyberspace , หลายธุรกิจขนาดใหญ่ของเราโดยเฉพาะอย่างยิ่งธนาคารและบริษัทโทรคมนาคมมีความสามารถในการรักษาความปลอดภัยใน Cyberspace ที่แข็งแกร่ง โดยเราจะใช้มาตรฐานนี้ในการสร้างและพัฒนาระบบการรักษาความปลอดภัยใน Cyberspace ต่อไปในอนาคต” (Australia's Cyber Security Strategy, 2016)

ออสเตรเลียจัดการกับความท้าทายเหล่านี้โดยการพยายามยกระดับการรักษาความปลอดภัยไซเบอร์เป็นปัญหาที่มีความสำคัญระดับชาติ โดยรัฐบาลออสเตรเลียจะมีบทบาทนำในความร่วมมือกับองค์กรต่างๆ เพื่อส่งเสริมการดำเนินการป้องกันความปลอดภัยใน Cyberspace

รัฐบาลออสเตรเลียมุ่งมั่นที่จะช่วยให้การสร้างสรรค์นวัตกรรม การเจริญเติบโต และความเจริญรุ่งเรืองให้กับชาวออสเตรเลีย การรักษาความปลอดภัยบนโลกไซเบอร์ที่แข็งแกร่งนี้ จะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อระบบเศรษฐกิจในศตวรรษที่ 21 ของออสเตรเลีย

ยุทธศาสตร์ดำเนินการรักษาความปลอดภัยบนโลกไซเบอร์ของออสเตรเลีย 2016-2020 กำหนดแนวทางการปฏิบัติออกเป็น 5 รูปแบบ คือ การประสานความร่วมมือด้าน Cyber, ระบบป้องกันทางไซเบอร์ที่แข็งแกร่ง, ความรับผิดชอบและอิทธิพลต่อโลก, การเจริญเติบโตและนวัตกรรม, A Cyber Smart Nation

1. การประสานความร่วมมือด้าน Cyber (A national cyber partnership)

เป็นการประสานความร่วมมือระหว่างรัฐบาลและภาคธุรกิจของออสเตรเลีย ผู้นำจะร่วมกันผลักดันให้การรักษาความปลอดภัยบนโลกไซเบอร์ของออสเตรเลียให้ได้รับการสนับสนุนลำดำเนินการได้อย่างมีประสิทธิภาพ มีการร่างระเบียบ และประชุมเชิงยุทธศาสตร์ผ่านการประชุมประจำปี โดยมีรัฐบาลเป็นเจ้าภาพ การประชุมจัดขึ้นเพื่อให้เกิดความคิดริเริ่มที่สำคัญในการส่งเสริมยุทธศาสตร์นี้และรับมือกับปัญหาด้านความปลอดภัยบนโลกไซเบอร์ที่เกิดขึ้นใหม่

ออสเตรเลียจะมีบทบาทนำในการปรับปรุงการกำกับดูแลการรักษาความปลอดภัยบนโลกไซเบอร์สำหรับหน่วยงานของรัฐบาลและเครือจักรภพ นอกจากนี้ศูนย์รักษาความปลอดภัยไซเบอร์ออสเตรเลียจะถูกย้ายไปยังสถานใหม่ เพื่อรองรับการขยายตัวของศูนย์และจะช่วยให้รัฐบาลและภาคเอกชนประสานการทำงานได้อย่างมีประสิทธิภาพมากขึ้นด้วย

นอกจากนี้ ออสเตรเลียจะสนับสนุนการวิจัยเพื่อให้เข้าใจภัยคุกคามจากโลกไซเบอร์ที่เป็นอันตรายต่อเศรษฐกิจของออสเตรเลีย เพื่อให้องค์กรต่าง ๆ มีข้อมูลสำหรับการลงทุนและการบริหารความเสี่ยงในการตัดสินใจของพวกเขาสำหรับการรักษาความปลอดภัยบนโลกไซเบอร์

2. ระบบป้องกันทางไซเบอร์ที่แข็งแกร่ง (Strong Cyber Defences)

เครือข่ายและระบบของออสเตรเลียมีแนวโน้มที่อาจจะถูกโจมตีมากขึ้น ออสเตรเลียต้องสามารถตรวจจับ ยับยั้ง และตอบสนองต่อภัยคุกคามด้านความปลอดภัยบนโลกไซ

เบอร์ให้ได้มากขึ้น รัฐบาลออสเตรเลียและภาคเอกชนจะทำงานร่วมกันเพื่อแบ่งปันข้อมูลเพิ่มเติมรวมจากแหล่งต่าง ๆ เกี่ยวกับภัยคุกคามและการตอบสนองผ่านศูนย์รักษาความปลอดภัยไซเบอร์ในเมืองต่าง ๆ และบนระบบภัยคุกคามไซเบอร์ออนไลน์ที่สามารถใช้งานได้ร่วมกัน

เพิ่มขีดความสามารถของทีมตอบสนองเหตุฉุกเฉินทางคอมพิวเตอร์ของประเทศออสเตรเลีย (Computer Emergency Response Team : CERT) ให้ทำงานสามารถทำงานร่วมกับภาคธุรกิจ โดยเฉพาะอย่างยิ่งองค์กรภาคธุรกิจที่สำคัญระดับประเทศ นอกจากนี้ยังปรับปรุงความสามารถของหน่วยตรวจจับสัญญาณเพื่อการตรวจหาช่องโหว่ด้านความปลอดภัยบนโลกไซเบอร์ สิ่งเหล่านี้จะช่วยสร้างความมั่นใจในการลงทุนให้กับภาคธุรกิจได้

รัฐบาลจะช่วยเพิ่มความสามารถในการแก้ไขปัญหาอาชญากรรมไซเบอร์ โดยการเพิ่มจำนวนของผู้เชี่ยวชาญดำเนินการตรวจจับภัยคุกคาม ใช้การวิเคราะห์ทางเทคนิคและการประเมินผลทางนิติวิทยาศาสตร์

ออสเตรเลียจะยกระดับประสิทธิภาพการรักษาความปลอดภัยบนโลกไซเบอร์ องค์กรทั้งในภาครัฐและเอกชนจำเป็นต้องทำความเข้าใจความเสี่ยงไซเบอร์และมีการป้องกันที่แข็งแกร่งบนโลกไซเบอร์ การรักษาความปลอดภัยบนโลกไซเบอร์โดยทั่วไปมักจะถูกมองว่าเป็นเพียงแค่ปัญหาด้านไอที แต่แท้ที่จริงแล้วมันเป็นศูนย์กลางของยุทธศาสตร์ด้านธุรกิจสำหรับองค์กรทั้งภาครัฐและเอกชน รัฐบาล ภาคธุรกิจ และหน่วยงานวิจัย จะร่วมกันออกแบบแนวทางการรักษาความปลอดภัยบนโลกไซเบอร์แห่งชาติ เพื่อส่งเสริมการปฏิบัติที่ทุกองค์กรสามารถใช้ร่วมกันได้ นอกจากนี้ยังจะช่วยให้องค์กรต่าง ๆ เข้าใจถึงจุดแข็งและจุดอ่อนของการรักษาความปลอดภัยบนโลกไซเบอร์ของพวกเขา

3. ความรับผิดชอบและอิทธิพลต่อโลก (Global Responsibility and Influence)

ออสเตรเลียจะทำงานร่วมกับพันธมิตรต่างประเทศเพื่อเป็นผู้นำด้านการใช้อินเทอร์เน็ตฟรีและมีความปลอดภัย เราจะทำงานร่วมกันเพื่อแก้ไขภัยคุกคามความปลอดภัยบนโลกไซเบอร์และเน้นโอกาสที่นำเสนอการใช้อินเทอร์เน็ตฟรีสำหรับเศรษฐกิจโลก ภารกิจนี้จะถูกดำเนินการผ่านการแต่งตั้งเอกอัครราชทูตไซเบอร์ ซึ่งจะประสานการดำเนินการระหว่างประเทศที่เป็นประโยชน์กับออสเตรเลีย และช่วยให้มั่นใจได้ว่าประเทศออสเตรเลียจะมีบทบาทสำคัญและมีอิทธิพลต่อประเด็นด้านไซเบอร์สากล

รัฐบาลออสเตรเลียสนับสนุนและปฏิบัติตามกฎหมายระหว่างประเทศหรือมาตรการที่ตกลงกันไว้สำหรับการปฏิบัติที่เหมาะสมที่เกี่ยวข้องกับ Cyberspace และสร้างความมั่นใจในทางปฏิบัติเพื่อลดความเสี่ยงจากความขัดแย้งใด ๆ

4. การเจริญเติบโตและนวัตกรรม (Growth and Innovation)

Cyberspace สร้างโอกาสอย่างมหาศาลให้กับองค์กรในออสเตรเลีย อินเทอร์เน็ตเป็นเครื่องมือสำคัญสำหรับธุรกิจทุกขนาด เป็นสถานที่มอบบริการและผลิตภัณฑ์ เป็นการเปิดช่องทางในการพัฒนาของเทคโนโลยีนวัตกรรมและโอกาสทางการค้ารูปแบบใหม่อย่างเท่าเทียมกัน ถือเป็นการเปลี่ยนแปลงกระแสในพื้นที่สาธารณะ สำหรับภาคธุรกิจ

การวิเคราะห์ข้อมูลในภูมิภาคเอเชียแปซิฟิก ธุรกิจที่ใช้เทคโนโลยีและอินเทอร์เน็ตสามารถสร้างกิจกรรมทางเศรษฐกิจได้ถึง 625 ล้านเหรียญสหรัฐต่อปี คิดเป็นร้อย 12 ต่อ GDP ที่คาดการณ์ไว้ในภูมิภาค

ความมุ่งมั่นของรัฐบาลออสเตรเลียในการรักษาความปลอดภัยบนโลกไซเบอร์จะช่วยให้การกระจายการลงทุนและพัฒนาตลาดใหม่ เกิดการวางรากฐานสำหรับอนาคตที่เจริญรุ่งเรือง เพื่อใช้ประโยชน์จากตลาดโลกที่เพิ่มขึ้น นอกจากนี้รัฐบาลยังจะสนับสนุนการขยายการรักษาความปลอดภัยภาคไซเบอร์ของออสเตรเลียเพื่อส่งเสริมความสามารถของตนในตลาดโลก ในประเทศที่แข็งแกร่งการรักษาความปลอดภัยบนโลกไซเบอร์จะส่งเสริมให้เกิดความไว้วางใจและความเชื่อมั่นในต่อภาคธุรกิจในการดำเนินกิจกรรมแบบออนไลน์

ด้วยการวิจัยและการพัฒนาด้านความปลอดภัยบนโลกไซเบอร์ที่มุ่งเน้นการตอบสนองความต้องการของภาคอุตสาหกรรม รัฐบาลออสเตรเลียจะสร้างการลงทุนและการจ้างงานและเพิ่มความปลอดภัยบนโลกไซเบอร์ของประเทศเพื่อทำให้ออสเตรเลียเป็นเป้าหมายที่น่าสนใจสำหรับการลงทุน

ออสเตรเลียพยายามจะทำให้ประเทศเป็นสถานที่สำหรับนวัตกรรมแห่งการรักษาความปลอดภัยบนโลกไซเบอร์ โดยจัดตั้งศูนย์พัฒนาการรักษาความปลอดภัยไซเบอร์ (Cyber Security Growth Centre) โดยใช้นวัตกรรมแห่งชาติและวิทยาศาสตร์ ในการสร้างเครือข่ายการวิจัยและนวัตกรรมระดับชาติ เพื่อกำหนดและจัดลำดับความสำคัญและความท้าทายด้านความปลอดภัยบนโลกไซเบอร์ซึ่งมีความสำคัญต่อผลสำเร็จของชาติ ทำให้ประเทศออสเตรเลียมีความสามารถในการเป็นผู้นำเพื่อสร้างโซลูชันการแข่งขันระดับโลก Cyber Security Growth Centre จะเชื่อมโยงกับไซเบอร์เทอร์มินัลในต่างประเทศ และเครือข่ายของบริษัทต่าง ๆ ทำให้เสริมสร้างความมั่นคงทางโลกไซเบอร์ของออสเตรเลีย ตลอดจนเพิ่มโอกาสทางธุรกิจและการสร้างงาน รวมถึงการเชื่อมต่อกับโครงการริเริ่มอื่น ๆ เช่น ศูนย์แบ่งปันภัยคุกคามร่วมกันบนโลกไซเบอร์ (Joint Cyber Threat Sharing Centres)

นอกจากนี้ยังมีการริเริ่มด้านวิทยาศาสตร์และนวัตกรรมแห่งชาติของรัฐบาลที่กำลังเพิ่มขีดความสามารถ โดยองค์กรวิทยาศาสตร์ดิจิทัลขององค์กรวิทยาศาสตร์และอุตสาหกรรมเครือจักรภพ (CSIRO : Data61) เพื่อขับเคลื่อนนวัตกรรมด้านความปลอดภัยบนโลกไซเบอร์ โดยมุ่งเน้นเฉพาะการสนับสนุนการเริ่มต้นระบบรักษาความปลอดภัยบนโลกไซเบอร์และการพัฒนาขีดความสามารถด้านเทคนิคภายใน ซึ่งจะรวมถึงโครงการทุนการศึกษาระดับปริญญาเอกเฉพาะด้านไซเบอร์ โครงการเหล่านี้ จะสนับสนุนธุรกิจการรักษาความปลอดภัยบนโลกไซเบอร์ที่จะเติบโตและประสบความสำเร็จ ในทำนองเดียวกันออสเตรเลียจะได้รับประโยชน์จากการป้องกันที่ดีขึ้น

5. A Cyber Smart Nation

การเสริมสร้างความสำเร็จของทั้ง 4 รูปแบบนี้ ในยุทธศาสตร์ความปลอดภัยทางไซเบอร์ คือ ความมุ่งมั่นของออสเตรเลียในการแก้ไขปัญหาการขาดแคลนผู้เชี่ยวชาญด้านความปลอดภัยบนโลกไซเบอร์ จากความคิดริเริ่มที่เกี่ยวกับวิทยาศาสตร์เทคโนโลยีวิศวกรรมและคณิตศาสตร์ (STEM) ที่มีอยู่ เราจะจัดการกับปัญหาสำคัญ ๆ นี้ในทุกระบบการศึกษาระดับเริ่มต้น ซึ่งเป็นความต้องการเร่งด่วนที่สุดในภาคอุดมศึกษา

รัฐบาล นักวิชาการ นักการวิจัย และภาคธุรกิจ จะร่วมออกแบบโมเดลและสร้างศูนย์การศึกษาด้านความปลอดภัยบนโลกไซเบอร์ในมหาวิทยาลัยเพื่อให้แน่ใจว่าผู้สำเร็จการศึกษามีทักษะและความชำนาญที่เหมาะสม ศูนย์ประสานงานต่าง ๆ จะเชื่อมโยงกับผู้คนทั่วโลก และเชื่อมโยง

กับโครงการริเริ่มอื่น ๆ เช่น ศูนย์แบ่งปันภัยคุกคามร่วมกันทางไซเบอร์ และ Cyber Security Growth Center

รัฐบาลรัฐออสเตรเลีย ภาคธุรกิจ และนักวิจัย จะทำงานร่วมกันเพื่อแก้ไขปัญหาด้านความปลอดภัยบนโลกไซเบอร์เพื่อให้เด็ก ๆ สามารถเรียนรู้ทักษะด้านความปลอดภัยไซเบอร์ในโรงเรียนที่ได้มากขึ้น และเพื่อให้แต่ละสายอาชีพสามารถพัฒนาทักษะด้านความปลอดภัยไซเบอร์ได้

รัฐบาลยังจะปรับปรุงการรับรู้และการรักษาความปลอดภัยบนโลกไซเบอร์ของชาติต่อไปเพื่อให้ชาวออสเตรเลียทุกคนเข้าใจถึงความเสี่ยงและประโยชน์ของอินเทอร์เน็ต รวมถึงวิธีการป้องกันตัวเองทางออนไลน์ด้วยการริเริ่มการรับรู้และการรณรงค์ด้านการศึกษาของภาครัฐและเอกชนอย่างต่อเนื่อง

แผนภาพที่ 2-1 : ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของออสเตรเลีย

ที่มา : Australia's Cyber Security Strategy 2016

โครงสร้าง บทบาทหน้าที่ และความรับผิดชอบ

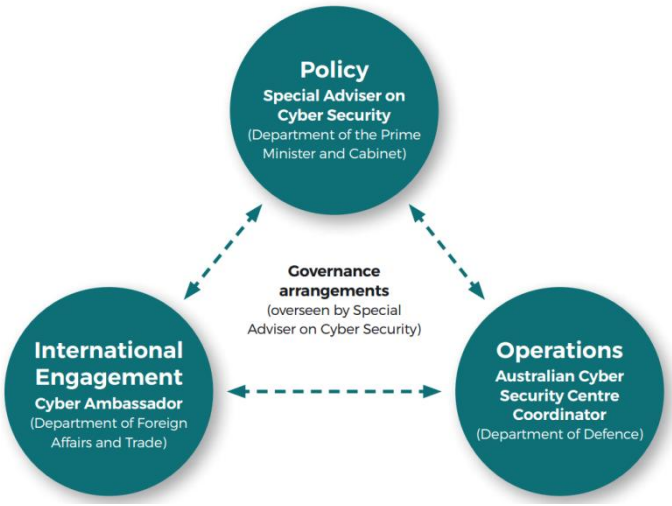
โครงสร้างหน่วยงานรักษาความปลอดภัยบนโลกไซเบอร์ของออสเตรเลีย แบ่งเป็น 3 เสาหลัก คือ ด้านนโยบาย (Policy) ด้านปฏิบัติการ (Operations) และด้านการดำเนินพันธกิจร่วมกับองค์กรนานาชาติ (International Engagement) โดยมีบทบาทหน้าที่และความรับผิดชอบ

1. ด้านนโยบาย (Policy) กำกับดูแลโดยที่ปรึกษาพิเศษด้านนโยบายรักษาความปลอดภัยไซเบอร์ สำนักนายกรัฐมนตรี มีบทบาทนำในปัจจุบันเกี่ยวกับนโยบายการรักษาความปลอดภัยบนโลกไซเบอร์และเป็นหลักในกำกับดูแลและการกำหนดนโยบายเกี่ยวกับยุทธศาสตร์ด้าน Cyber Security แบบบูรณาการ นอกจากนี้ยังมีหน้าที่จัดลำดับความสำคัญกิจกรรมของรัฐบาลเพื่อให้ตอบสนองต่อวัตถุประสงค์ของยุทธศาสตร์ไซเบอร์แห่งชาติ (National Cyber Security Strategy) บทบาทด้านนโยบายนี้จะถูกขับเคลื่อนกำกับดูแลโดยที่ปรึกษาพิเศษด้านนโยบายรักษาความปลอดภัยไซเบอร์ เพื่อนำไปสู่การพัฒนายุทธศาสตร์การรักษาความปลอดภัยบนโลกไซเบอร์ รวมถึงการปรับวัตถุประสงค์ของนโยบายให้มีความชัดเจน และจัดลำดับความสำคัญให้กับหน่วยงานต่าง ๆ เพื่อการดำเนินงานอย่างมีประสิทธิภาพ ร่วมกับภาคเอกชน ชุมชนการวิจัย และประเทศคู่ค้า

2. ด้านปฏิบัติการ (Operations) กำกับดูแลโดยศูนย์รักษาความปลอดภัยทางไซเบอร์ (Australian Cyber Security Centre : ACSC) กระทรวงกลาโหม เป็นหน่วยงานที่ได้รับความสำคัญในการรักษาความปลอดภัยบนโลกไซเบอร์ มีความเชี่ยวชาญและความสามารถในการรักษาความปลอดภัยบนโลกไซเบอร์ให้กับการดำเนินงานของรัฐบาล สามารถสนับสนุนองค์กรระดับปฏิบัติการได้อย่างทั่วถึง ACSC มีสามารถในการประสานการปฏิบัติกับภาคเอกชนได้อย่างคล่องตัว เพื่อสนับสนุนภาคเอกชนในการโต้ตอบกับภัยคุกคามทางไซเบอร์ สามารถในการบูรณาการร่วมกันระหว่างรัฐบาล ภาคเอกชน ชุมชนการวิจัย และประเทศคู่ค้า มีการรับสมัครบุคลากรใหม่ และจูงใจด้วยระบบสวัสดิการที่มีคุณภาพ เพื่อการดึงดูดพนักงานที่มีทักษะสูง นอกจากนั้นยังมีหน้าที่ประชาสัมพันธ์ภารกิจของ ACSC อีกด้วย

3. ด้านการดำเนินพันธกิจร่วมกับองค์กรนานาชาติ (International Engagement) กำกับดูแลโดยเอกอัครราชทูตไซเบอร์ กระทรวงการต่างประเทศและการค้า รัฐมนตรีว่าการกระทรวงการต่างประเทศของออสเตรเลีย จะแต่งตั้งเอกอัครราชทูตไซเบอร์ เพื่อความพยายามในการประสานความร่วมมือเกี่ยวกับ Cyberspace ระหว่างประเทศ เอกอัครราชทูตไซเบอร์จะมีบทบาทสำคัญในการประสานการทำงานอย่างใกล้ชิดกับที่ปรึกษาพิเศษด้านการรักษาความปลอดภัยไซเบอร์ ซึ่งจะสนับสนุนการรักษาความปลอดภัยอินเทอร์เน็ตบนพื้นฐานของเสรีภาพในการพูด การแสดงความคิดเห็น และความเป็นส่วนตัว ตามกฎหมายของออสเตรเลีย รวมถึงการสร้างความมั่นใจว่าออสเตรเลียสามารถสร้างขีดความสามารถบนโลกไซเบอร์ได้อย่างต่อเนื่อง เพื่อแสดงให้เห็นว่าทุกคนสามารถใช้อินเทอร์เน็ตได้อย่างปลอดภัยในภูมิภาคนี้

แผนภาพที่ 2-2 : โครงสร้าง บทบาทหน้าที่ และความรับผิดชอบ



ที่มา : Australia's Cyber Security Strategy 2016

4. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ (DOD Cyber Strategy - United States Department of Defense)

ประเทศสหรัฐอเมริกาใช้อินเทอร์เน็ตและระบบข้อมูลบนโลกไซเบอร์ในการให้บริการที่หลากหลาย ประเทศสหรัฐฯ องว่าการพึ่งพาเทคโนโลยีเหล่านี้ทำให้ประเทศเกิดเสี่ยงต่อภัยคุกคามทางไซเบอร์และเป็นอันตรายจากการโจมตีทางไซเบอร์เพื่อก่อกวนและทำลายเครือข่ายโครงสร้างพื้นฐานที่สำคัญของประเทศ อีกทั้งยังมีความพยายามจารกรรมข้อมูลเทคโนโลยีทางทหารเพื่อทำลายผลประโยชน์ทางเทคโนโลยีด้านการทหาร

การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในห้วงไซเบอร์ของหน่วยงานที่เกี่ยวข้อง ในการดำรงขีดความสามารถด้านการตรวจจับ, วิเคราะห์และลดภัยคุกคาม/จุดเสี่ยงต่าง ๆ, และดำเนินกลยุทธในการเอาชนะศัตรู เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ ประกอบด้วย

1. การปฏิบัติการเครือข่ายเชิงรุก (Proactive NetOps) : การปฏิบัติการเครือข่าย (NetOps) ถูกกำหนดโดย กห.สหรัฐในการปฏิบัติการ การจัดโครงสร้าง และขีดความสามารถทางเทคนิคสำหรับการปฏิบัติการ และการป้องกันโครงข่ายข้อมูลข่าวสารโลก (Global Information Grid: GIG) การปฏิบัติการเครือข่าย (NetOps) รวมถึงการบริหารจัดการองค์กร (Enterprise Management), การรับรองการทำงานหรือการป้องกันของเครือข่าย (Net Assurance หรือ Net Defense), และการบริหารข่าวสาร (Content Management) การปฏิบัติการเครือข่าย (NetOps) สามารถสนองตอบความต้องการของผู้บังคับบัญชาในการหยั่งรู้สถานการณ์ของ GIG เพื่อนำไปสู่การตัดสินตกลงใจในรูปแบบของการบัญชาการและควบคุม ทั้งนี้การหยั่งรู้สถานการณ์ของ GIG ทำได้โดยการบูรณาการทั้งทางเทคนิคและการปฏิบัติการของการบริหารจัดการองค์กร และการป้องกันและกิจกรรมตลอดทุกระดับการบังคับบัญชา (ยุทธศาสตร์, ยุทธการ และยุทธวิธี)

2. มาตรการเชิงรับ (Defensive Countermeasures) – เป็นมาตรการทางวิทยาศาสตร์เชิงรับในการใช้งานอุปกรณ์ และ/หรือเทคนิค ที่มีวัตถุประสงค์ต่อการทำให้การปฏิบัติของศัตรูด้อยประสิทธิภาพในเชิงการป้องกันระบบข้อมูลที่มีชั้นความลับ หรือระบบที่มีผลกระทบต่อการปฏิบัติการ มาตรการเชิงรับนี้รวมถึงการกระทำในการระบุแหล่งที่มาของกิจกรรมทางไซเบอร์ที่เป็นภัยคุกคาม, การป้องกันบริเวณจุดเชื่อมต่อ (เช่น ระบบป้องกันการบุกรุก (Intrusion Protection System: IPS), การป้องกันเชิงรุก (Pre-Emptive Blocks), การขึ้นบัญชีดำ (Blacklisting) เป็นต้น), การติดตามในเครือข่าย (เช่น การค้นหาคนภายใน ศัตรู หรือโปรแกรมประสงค์ร้ายต่าง ๆ เป็นต้น), การข่าวกรอง (รวมถึงการบังคับใช้กฎหมาย) ในการตรวจจับภัยคุกคาม

ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ มีวัตถุประสงค์เพื่อเป็นแนวทางในการพัฒนากองกำลังไซเบอร์ของกระทรวงกลาโหม และเสริมสร้างการป้องกันทางไซเบอร์ โดยมุ่งเน้นการสร้างขีดความสามารถและองค์กรทางไซเบอร์เพื่อปฏิบัติภารกิจด้านไซเบอร์ ปกป้องเครือข่ายระบบและข้อมูล ปกป้องประเทศและรักษาผลประโยชน์ของประเทศจากการโจมตีทางไซเบอร์ และทำให้เกิดการแบบบูรณาการเพื่อสนับสนุนการดำเนินงานทางทหารและแผนฉุกเฉินต่างๆ จึงกำหนดเป้าหมายทางยุทธศาสตร์ 5 ประการ และกำหนดวัตถุประสงค์เฉพาะสำหรับกระทรวงกลาโหมเพื่อให้บรรลุเป้าหมายในอีก 5 ปีถัดไป สิ่งที่ผลักดันให้กระทรวงกลาโหมพัฒนายุทธศาสตร์ไซเบอร์ใหม่มี 3 ประเด็นสำคัญคือ

1. ความรุนแรงและความซับซ้อนของภัยคุกคามทางไซเบอร์ที่มีต่อผลประโยชน์ของสหรัฐฯ รวมถึงเครือข่ายข้อมูลและระบบของกระทรวงกลาโหม กระทรวงกลาโหมสหรัฐฯ มีเครือข่ายที่ใหญ่ที่สุดในโลก จึงจำเป็นต้องมีมาตรการที่เด็ดขาดในการปกป้องเครือข่ายรักษาความปลอดภัยข้อมูลเพื่อลดความเสี่ยงในการปฏิบัติภารกิจของกระทรวงกลาโหม

2. ในปี 2012 ประธานาธิบดีโอบามาได้สั่งให้กระทรวงกลาโหม จัดระเบียบและวางแผนที่ปกป้องประเทศจากการโจมตีทางไซเบอร์อย่างมีนัยสำคัญและร่วมกับหน่วยงานรัฐบาลอื่นๆ ของสหรัฐฯ

3. การตอบสนองต่อภัยคุกคามนั้นในปี 2012 กระทรวงกลาโหม ได้เริ่มสร้าง Cyber Mission Force (CMF) เพื่อปฏิบัติภารกิจด้านไซเบอร์ของกระทรวง CMF จะมีเจ้าหน้าที่ฝ่ายสนับสนุนด้านการทหาร, พลเรือน และภาคเอกชนเกือบ 6,200 นาย เพื่อรองรับการดำเนินยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหม และเป็นแนวทางที่ชัดเจนในการพัฒนาของ CMF

นอกจากนั้น กระทรวงกลาโหมสหรัฐฯ ยังมีความพยายามในการสร้างการบูรณาการร่วมกับภาคเอกชนและองค์กรอื่นๆ เพื่อการสร้างสะพานเชื่อมสู่ภาคเอกชน สร้างพลังแห่งอนาคต กระทรวงกลาโหมใช้ความสามารถที่ดีที่สุด ความคิดที่ดีที่สุด และเทคโนโลยีที่ดีที่สุด ในการให้บริการสาธารณะ เพื่อให้บรรลุวัตถุประสงค์นี้ กระทรวงกลาโหมจะต้องสร้างสะพานที่แข็งแกร่งให้กับภาคเอกชนตลอดจนสถาบันการวิจัยที่ทำให้สหรัฐฯ เป็นประเทศที่เป็นนวัตกรรมใหม่ ภาคเอกชนและสถาบันวิจัยของสหรัฐฯ ออกแบบและสร้างเครือข่ายไซเบอร์และสามารถให้บริการด้านความปลอดภัยในโลกไซเบอร์รวมถึงการวิจัยและพัฒนาขีดความสามารถในระดับสูง อีกทั้งการยับยั้งเป็นส่วนสำคัญของยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหม ยุทธศาสตร์นี้อธิบายถึงการมีส่วนร่วมของกระทรวงกลาโหมในการกำหนดความสามารถระดับชาติที่กว้างขึ้นเพื่อยับยั้งศัตรูจากการโจมตีทางไซเบอร์

เป้าหมายทางยุทธศาสตร์และแนวทางในการดำเนินยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ ประกอบด้วย 5 ประเด็นสำคัญ ได้แก่

1. สร้างและคงไว้ซึ่งความพร้อมและความสามารถในการดำเนินงานบนโลกไซเบอร์ (CYBERSPACE OPERATIONS)
2. ป้องกันเครือข่ายข้อมูล และลดความเสี่ยงต่อภารกิจของกระทรวงกลาโหม
3. เตรียมพร้อมในการป้องกันประเทศสหรัฐฯ และสิ่งที่อยู่ในความสนใจของสหรัฐฯ จากการโจมตีทางไซเบอร์
4. สร้างตัวเลือกและเลือกใช้ตัวเลือกที่มีอยู่ และวางแผนที่จะใช้ตัวเลือกเหล่านี้เพื่อควบคุมความคลาดเคลื่อนที่เกิดขึ้นและเพื่อให้เกิดสภาวะแวดล้อมที่ได้เปรียบในทุกขั้นตอน เช่น ในสถานการณ์ความตึงเครียดที่เกิดจากการสู้รบหรือสถานการณ์คับขันอื่นๆ กระทรวงกลาโหมต้องเสนอแนวทางที่หลากหลายเพื่อให้ประธานาธิบดีมีตัวเลือกในการจัดการกับสถานการณ์ความขัดแย้ง นอกจากนั้นจะต้องพัฒนาขีดความสามารถในโลกไซเบอร์เพื่อให้บรรลุวัตถุประสงค์ด้านความปลอดภัยที่สำคัญด้วยความแม่นยำและเพื่อลดการสูญเสียชีวิตและการทำลายทรัพย์สิน
5. สร้าง รักษาความสัมพันธ์ระหว่างประเทศ และความร่วมมือระหว่างประเทศเพื่อลดความเสี่ยงด้านความมั่นคงระหว่างประเทศ เพราะภารกิจด้านไซเบอร์ของกระทรวงกลาโหมจำเป็นต้องมีการร่วมมือกันอย่างใกล้ชิดกับพันธมิตร ซึ่งกระทรวงกลาโหมพยายามที่จะสร้างและพัฒนาขีดความสามารถในการเป็นพันธมิตรด้านความปลอดภัยทางไซเบอร์

กรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย

ประเด็นสำคัญของกรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ที่นำมาพิจารณาร่วมกันในการสร้างความมั่นคงปลอดภัยไซเบอร์ของไทย คือ

1. ความมั่นคงปลอดภัยของระบบและข้อมูล
2. สิทธิเสรีภาพของประชาชน
3. ความมั่นคงของประเทศ
4. การร่วมมือกันของบุคคลที่เกี่ยวข้องกับโลกไซเบอร์

วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยในไซเบอร์ ได้แก่การสร้างความมั่นคงปลอดภัยในระบบ (network) และข้อมูล (data) การบรรลุวัตถุประสงค์ดังกล่าวต้องใช้ทั้งมาตรการทางเทคโนโลยีและ มาตรการทางกฎหมาย (statutory regulation) รวมถึงการบูรณาการร่วมกันของบุคคล 3 ฝ่าย ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาสังคม ด้วยเหตุที่การโจมตีทางไซเบอร์อาจถูกกระทำโดยผู้ไม่หวังดีที่มาจากทั้งภายในประเทศและภายนอกประเทศ ฉะนั้น ภาครัฐ ภาคเอกชน และภาคประชาสังคม ต้องมีการประสานความร่วมมือกันอย่างเป็นระบบเพื่อจัดการกับปัญหาการโจมตีทางไซเบอร์ทั้งจากภายในประเทศและนอกประเทศ

ในส่วนของ ร่าง พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ของไทยที่จะกล่าวถึงต่อไปนี้ เป็นฉบับที่คณะรัฐมนตรีเห็นชอบในหลักการ ซึ่งเป็นร่างฯ ฉบับแรก ที่เปิดเผยต่อสาธารณะในขณะนี้ ร่างพระราชบัญญัติฉบับนี้ ได้ให้เหตุผลในการยกร่างกฎหมายไว้ว่า เป็นการป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงบนไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือได้ทันสถานการณ์ และมีการดูแลรักษา

ความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง เพื่อให้เกิดทำงานรวมกันทั้งภาครัฐและเอกชนในการต่อสู้กับปัญหาการโจมตีไซเบอร์

บทนิยามศัพท์ในร่างพระราชบัญญัติฉบับนี้ ได้นิยามคำว่า“ความมั่นคงปลอดภัยไซเบอร์” ว่าหมายถึง “มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ” ซึ่งจะเห็นได้ว่าร่างกฎหมายไซเบอร์ของไทยมิได้มุ่งเฉพาะความมั่นคงปลอดภัยของระบบและข้อมูลอันกระทบต่อความมั่นคงทางเศรษฐกิจแต่เพียงอย่างเดียว แต่หมายความรวมถึงความมั่นคงทางการทหารและความสงบเรียบร้อยภายในประเทศด้วย

ร่างพระราชบัญญัติฉบับนี้ กำหนดให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อภาษาอังกฤษว่า “National Cybersecurity Committee” เรียกโดยย่อว่า “NCSC” มีอำนาจหน้าที่ที่สำคัญ ดังนี้

1. สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ

2. เมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงของประเทศ ให้ กปช. มีอำนาจสั่งการให้หน่วยงานของรัฐทุกแห่งดำเนินการอย่างหนึ่งอย่างใดเพื่อป้องกัน แก้ไขปัญหา หรือบรรเทาความเสียหายที่เกิดหรืออาจจะเกิดขึ้นได้ตามที่เห็นสมควร และอาจให้หน่วยงานของรัฐ หรือบุคคลใด รวมทั้งบุคคลซึ่งได้รับอันตรายหรืออาจได้รับอันตรายหรือความเสียหายดังกล่าว กระทำหรือร่วมกันกระทำการใด ๆ อันจะมีผลเป็นการควบคุม ระงับ หรือบรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นนั้นได้อย่างทันท่วงที

3. ในกรณีที่มีความจำเป็นเพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ กปช. อาจสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. ตามที่ กปช. ประกาศกำหนด

4. เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจดังต่อไปนี้

(1) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใด ๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้

(2) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

(3) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด

เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ การดำเนินการตาม (3) ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด

จากบทบัญญัติข้างต้นจะเห็นว่าคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) มีอำนาจสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชน เพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ โดยมีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธาน

งานวิจัยที่เกี่ยวข้อง

น.อ.หญิง จินดาสระสมบูรณ์ ร.น. (2557) ได้ศึกษาวิจัยเรื่อง ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย โดยมีวัตถุประสงค์เพื่อการศึกษาและวิเคราะห์หลักปฏิบัติการสงครามไซเบอร์ด้านการทหารและเสนอแนะแนวทางในการปฏิบัติการสงครามไซเบอร์ ซึ่งแม้ว่ากองบัญชาการกองทัพไทยจะมีการเตรียมความพร้อมเรื่องโครงสร้างองค์กรด้านปฏิบัติการสงครามไซเบอร์อยู่ในระดับหนึ่ง แต่ก็ยังขาดรูปแบบและแนวคิดการปฏิบัติการสงครามไซเบอร์ การกำหนดบทบาทและโครงสร้างของหน่วยงานที่รับผิดชอบอย่างชัดเจน และยังขาดการพัฒนาความพร้อมของกำลังพลต่อปฏิบัติการสงครามไซเบอร์ ซึ่งหากมีการบูรณาการและกำหนดนโยบาย รวมถึงแนวปฏิบัติไว้อย่างชัดเจน ก็จะเกิดประโยชน์อย่างสูงสุดต่อการคุ้มครองปกป้องข้อมูลข่าวสาร บุคคล องค์กร รวมถึงอธิปไตยของประเทศได้

พันเอก ชนกศ์ จรจำรัส ได้ศึกษาวิจัยเรื่อง การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม พบว่า กระทรวงกลาโหม ต้องดำเนินการตามประกาศคณะกรรมการ ธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคง ปลอดภัยของระบบ สารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 โดยใช้มาตรฐาน ISO 27001 : 2005 ซึ่งมีหลักการที่ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ เป็นมาตรฐานที่เหมาะสม ในสภาวะแวดล้อมทางธุรกิจ มากกว่า การนำมาใช้ในงานด้านการทหารหรืองานด้านความมั่นคง ที่ภารกิจต่าง ๆ ล้วนเกี่ยวข้องและมีความสำคัญต่ออธิปไตยของชาติ จึงกลายเป็นข้อจำกัดที่สำคัญ และส่งผลต่อกระบวนการจัดซื้อ จัดจ้าง ที่ใช้ในงานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ทั้งในส่วนฮาร์ดแวร์ และซอร์ฟแวร์ที่ต้องใช้งานเฉพาะเจาะจง ตามภารกิจหลักของเหล่าทัพที่ไม่เหมือนกัน และอาจถูกร้องเรียนว่าเกินกว่ามาตรฐานที่ใช้งาน และมีราคาสูงเกินกว่าเกณฑ์ราคากลาง และคุณลักษณะพื้นฐานครุภัณฑ์คอมพิวเตอร์ที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกำหนดไว้

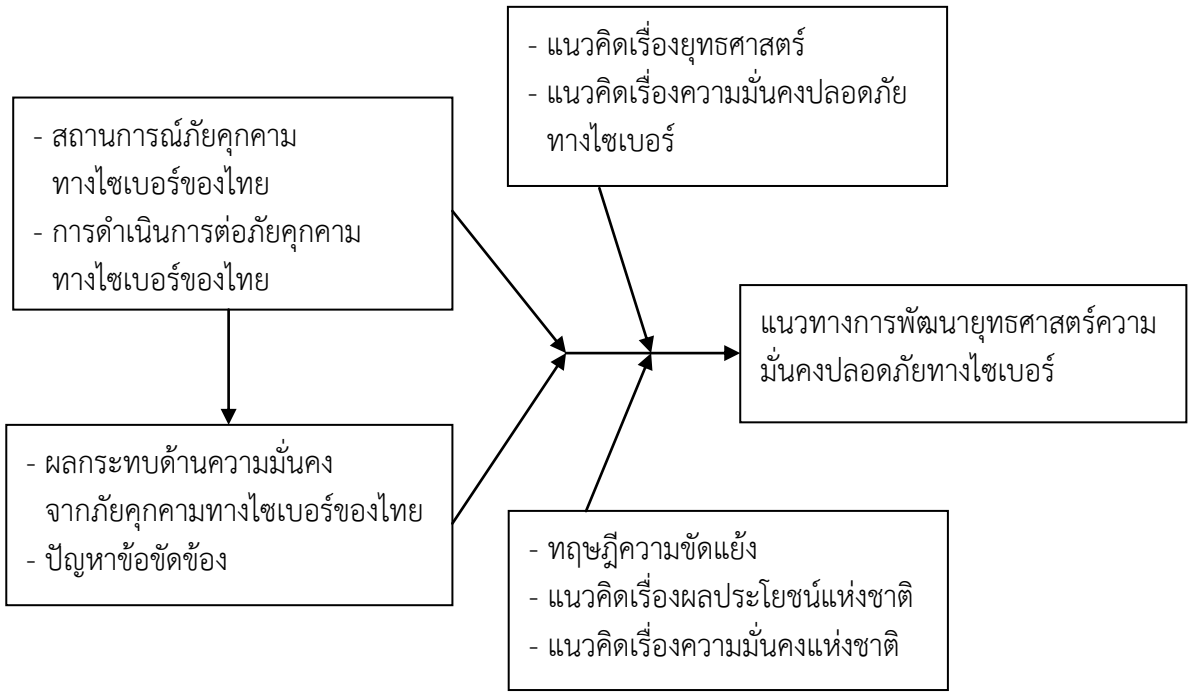
ดังนั้นกระทรวงกลาโหมจึงควรพัฒนามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมขึ้นมาใช้เอง โดยการปรับใช้ มาตรฐาน U.S. DoD ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของระบบคอมพิวเตอร์ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนา ผลิต หรือ ทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชนได้ปฏิบัติตาม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่กระทรวงกลาโหมกำหนด รวมทั้งการแก้ไข เพิ่มเติม ให้เหมาะสมกับบริบทของ กระทรวงกลาโหม แต่ทั้งนี้ต้องยังคงให้เป็นไปตามมาตรฐานสากล

นางสาวศิวลีย์ สิริโรจน์บริรักษา (2558) ได้ศึกษาเรื่อง การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม พบว่า สำหรับประเทศไทย

กรอบนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถูกกำหนดโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยได้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศไว้ใน พระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 รวมทั้ง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ 2553 โดยใช้มาตรฐาน ISO 27001: 2005 ซึ่งกระทรวงกลาโหมได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ

อย่างไรก็ตาม จากการทบทวนวรรณกรรม พบว่า มาตรฐาน ISO 27001: 2005 หรือมาตรฐาน NIST 800 มีหลักการที่ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ อาจมีความเหมาะสมในสภาวะแวดล้อมทางธุรกิจมากกว่า เพราะหน่วยงานด้านความมั่นคงที่ภารกิจต่าง ๆ ล้วนเกี่ยวข้องและมีความสำคัญต่ออธิปไตยของชาติ จำเป็นจะต้องมีระบบป้องกันความปลอดภัยไซเบอร์ที่เฉพาะเจาะจง กระทรวงกลาโหมจึงควรจะกำหนดมาตรฐานการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมสำหรับกระทรวงกลาโหมโดยเฉพาะ

กรอบแนวคิดการวิจัย



สรุป

จากข้อมูลข้างต้นจะเห็นได้ว่าการมีหน่วยงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อการป้องกันภัยคุกคามทางไซเบอร์ และประสานงานทั้งภายในและระหว่างประเทศในการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์มีความสำคัญ อีกทั้งต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐและเอกชนเพื่อยกระดับความพร้อมรับมือภัยคุกคามทางไซเบอร์ ที่มีผลกระทบต่อโครงสร้างพื้นฐานที่สำคัญของประเทศ ทั้งนี้ การร่าง พระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ในปัจจุบันนั้นอาจยังขาดองค์ประกอบที่สำคัญหลายประการ และถ้านำมาใช้เป็นเป็นกรอบในการบริหารยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะมีความสมบูรณ์เพียงพอที่จะนำไปใช้เป็นกลไกสำคัญในการขับเคลื่อนได้หรือไม่ ประกอบกับนโยบายของประเทศไทยในปัจจุบัน โดยรัฐบาล พล.อ. ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี และหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) มีนโยบายขับเคลื่อนประเทศไทยสู่ความมั่นคง มั่งคั่ง และยั่งยืน และนำไปสู่ความเป็น Thailand 4.0 ปรับเปลี่ยนโครงสร้างเศรษฐกิจ ไปสู่ “Value–Based Economy” หรือ เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม หน่วยงานของรัฐจึงต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์เป็นอย่างมาก เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสามารถดำเนินการควบคู่ไปกับยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) ที่เข้มแข็งด้วย

การวิจัยในครั้งนี้จะศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษาแนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต พร้อมเสนอแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

บทที่ 3
การดำเนินการเกี่ยวกับภัยคุกคามทางไซเบอร์

หน่วยงานหลักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมของประเทศไทย คือ กระทรวงดิจิตัลเพื่อเศรษฐกิจและสังคมหรือกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม ได้มีการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มาอย่างต่อเนื่อง แต่ทั้งนี้ต้องมีการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐ ภาคเอกชน ภาคประชาสังคม และสถาบันการศึกษาต่างๆ เพื่อเป็นการสร้างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้ครอบคลุมงานแต่ละสาขา รวมทั้งระบบโครงสร้างพื้นฐานของประเทศ

สำหรับงานความมั่นคงปลอดภัยทางไซเบอร์ในด้านความมั่นคงทางทหาร รวมถึงการทำสงครามไซเบอร์ มีกระทรวงกลาโหมเป็นหลัก เพราะเป็นเป้าหมายการโจมตีในระดับชาติ ทั้งระบบเทคโนโลยีทางทหาร อาวุธยุทโธปกรณ์ และระบบสื่อสารของกองทัพที่ใช้ในการป้องกันประเทศนั้น มีความซับซ้อนและแตกต่างจากระบบของพลเรือนทั่วไป จึงจำเป็นต้องมีการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์เช่นกัน

การศึกษาในบทที่ 3 ศึกษาการดำเนินการเกี่ยวกับภัยคุกคามทางไซเบอร์ของประเทศไทย เพื่อตอบวัตถุประสงค์ข้อที่ 1 การดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ และตอบวัตถุประสงค์ข้อที่ 2 เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ โดยมีลำดับการศึกษา ดังนี้

1. การดำเนินการต่อภัยคุกคามทางไซเบอร์ของประเทศไทยในปัจจุบัน
2. การดำเนินการของกองทัพไทยต่อภัยคุกคามทางไซเบอร์
3. สภาวการณ์เกี่ยวกับปัญหาและผลกระทบจากภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย
4. ปัญหาจากการดำเนินการต่อภัยคุกคามทางไซเบอร์ของประเทศไทย
5. สรุป

การดำเนินการต่อภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

ประเทศไทยดำเนินยุทธศาสตร์ Thailand 4.0 ที่เปลี่ยนเศรษฐกิจแบบเดิมไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม (Value–Based Economy) เพื่อก้าวข้ามกับดักประเทศรายได้ปานกลาง เมื่อบริบททางเศรษฐกิจเกิดการเปลี่ยนแปลง ทำให้ผู้ประกอบการโดยเฉพาะผู้ประกอบการในภาคอุตสาหกรรมการผลิตต้องปรับตัว เพื่อให้สามารถเติบโตท่ามกลางบริบทใหม่ทางเศรษฐกิจได้อย่างเข้มแข็ง การดำเนินยุทธศาสตร์ Thailand 4.0 บวกกับพลังของคนในชาติ จะทำให้เกิดการเปลี่ยนแปลงจาก ประเทศกำลังพัฒนา ไปสู่ ประเทศพัฒนาแล้ว แต่สิ่งที่ต้องตระหนักถึงคือเรื่องภัยคุกคามทางไซเบอร์ เพราะการเร่งการพัฒนาเศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม อุตสาหกรรมดิจิทัล

นั้นเป็นทิศทางที่ถูกต้อง แต่ต้องดำเนินการควบคู่ไปกับกับยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง สถานการณ์ปัจจุบันความเสี่ยงด้านภัยคุกคามไซเบอร์สูงขึ้นหลายเท่าตัว เป้าหมายการโจมตีส่วนใหญ่คือองค์กรทางเศรษฐกิจเป็นหลัก เช่น สถาบันการเงิน ตลาดหลักทรัพย์ โครงข่ายโทรคมนาคม ระบบขนส่งมวลชน ระบบสาธารณูปโภค เป็นต้น ภัยคุกคามทางไซเบอร์ (Cyber threats) จึงถือเป็นภัยคุกคามต่อผลประโยชน์ทางเศรษฐกิจ สังคมจิตวิทยา การเมืองภายในประเทศ การเมืองระหว่างประเทศ ตลอดจนความมั่นคงของชาติ การโจมตีทางไซเบอร์มีหลายรูปแบบ การโจมตีแต่ละครั้งสามารถสร้างความเสียหายอย่างมหาศาลทั้งต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ (Information systems and Computer network) ส่งผลต่อระบบเศรษฐกิจตลอดจนถึงความมั่นคงของชาติ

สำหรับดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของไทย เมื่อเปรียบเทียบกับต่างประเทศนั้น ในปี 2560 สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้ทำการสำรวจระดับความเอาจริงเอาจัง (Commitment) ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ 5 ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) พบว่า Global Cybersecurity Index (GCI) ของประเทศไทยอยู่ในอันดับที่ 22 จาก 194 ประเทศทั่วโลก ขณะเดียวกัน เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ 3 รองจากสิงคโปร์ และมาเลเซีย ซึ่งกระทรวงและหน่วยงานที่เกี่ยวข้องจะช่วยกันขับเคลื่อนให้ไทยติดอันดับ 1 ใน 20 อันดับแรกของประเทศที่มีความพร้อมต่อไป (การประชุมคณะกรรมการเตรียมการไซเบอร์แห่งชาติครั้งแรก ". (ออนไลน์)., 2561.)

กรอบความคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

การทำธุรกรรมทางอิเล็กทรอนิกส์มีการใช้งานอย่างแพร่หลาย และมีกฎหมายรองรับผลของการทำธุรกรรมทางอิเล็กทรอนิกส์มาตั้งแต่ปี 2544 (พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม พ.ศ. 2551) อย่างไรก็ตามการทำธุรกรรมทางอิเล็กทรอนิกส์มีความเสี่ยงจากภัยคุกคามทางไซเบอร์จากช่องโหว่ของระบบสารสนเทศ (Vulnerability) ซึ่งอาจถูกใช้เป็นช่องทางในการโจมตีทางไซเบอร์ได้ในหลายรูปแบบ ดั้งนั้นหน่วยงานภาครัฐ ภาคเอกชน และประชาชนต้องตระหนักถึงความรุนแรงของผลกระทบและความเสียหายที่อาจจะเกิดขึ้น และมีการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมเพื่อปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident)

กรอบความคิดด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของไทยใช้มาตรฐานสากล ISO/IEC 27001:2013 (Information Security Management System) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศซึ่งเป็นมาตรฐานที่ได้รับการยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพที่ใช้กันทั่วโลก โดยให้ความสำคัญกับการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสารสนเทศ (Integrity) และการรักษาสภาพพร้อมใช้งานของระบบ (Availability) ซึ่งเป็นปัจจัยพื้นฐานในการพิจารณาความมั่นคงปลอดภัยทางไซเบอร์ โดยอาศัย

การประเมินความเสี่ยง (Risk assessment) ที่ข้อมูลสารสนเทศอาจได้รับผลกระทบหรือเกิดความเสียหายจากภัยคุกคามทางไซเบอร์ เช่น ฐานข้อมูลรายชื่อผู้รับบริการของหน่วยงานซึ่งเป็นข้อมูลลับ มีความครบถ้วนสมบูรณ์ และอยู่ในสภาพพร้อมใช้งานตลอดเวลา ซึ่งภัยคุกคามต่อระบบสารสนเทศนั้นอาจมาจากทั้งทางอิเล็กทรอนิกส์ (Logical) และทางกายภาพ (Physical) ดังนั้นหน่วยงานจึงควรเตรียมการให้สามารถใช้ฐานข้อมูลรายชื่อผู้รับบริการได้แม้มีภัยคุกคามเกิดขึ้น เป็นต้น มาตรฐานนี้มีการนำไปใช้อย่างแพร่หลายทั่วโลก และมีการปรับปรุงอย่างต่อเนื่อง รวมทั้งกระทรวงกลาโหม ได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม) โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554

การรักษาความมั่นคงปลอดภัยไซเบอร์มีวัตถุประสงค์เพื่อการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ (Information systems & Computer network) เพื่อให้บรรลุวัตถุประสงค์ดังกล่าวต้องใช้ทั้งมาตรการทางเทคนิค (Technical measures) มาตรการทางกฎหมาย (Statutory Regulation) รวมถึงการกำกับดูแลตนเอง (Self-Regulation) และการกำกับดูแลร่วมกัน (Co-Regulation) จากทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคม ด้วยเหตุที่การโจมตีทางไซเบอร์อาจกระทำโดยผู้ไม่หวังดีที่มาจากทั้งภายในประเทศและภายนอกประเทศ ฉะนั้นหน่วยงานของรัฐ หน่วยงานภาคเอกชนและภาคประชาสังคม จะต้องมีการบูรณาการประสานความร่วมมือกันเพื่อจัดการกับปัญหาภัยคุกคามทางไซเบอร์ อย่างไรก็ตามการใช้มาตรการดังกล่าวต้องคำนึงถึงสิทธิเสรีภาพของประชาชนด้วย และถึงแม้หน่วยงานต่างๆ และภาคประชาชนจะมีความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์แล้ว แต่ภัยคุกคามทางไซเบอร์ก็ยังมีโอกาสที่จะก่อให้เกิดความเสี่ยงได้ตลอดเวลา ดังนั้น การกำหนดยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะทำให้หน่วยราชการ ภาคเอกชน และ ภาคประชาสังคม สามารถนำไปใช้เป็นมาตรฐานในการขับเคลื่อนความมั่นคงปลอดภัยไซเบอร์ในทุกระดับ และต้องทำให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกันในทุกภาคส่วน ข้อสำคัญคือมีศูนย์ปฏิบัติการส่วนกลางที่ทำให้เกิดการวิเคราะห์งานด้านการข่าวไซเบอร์ที่สามารถประมวลผลได้ทันที (Real Times) และสามารถเชื่อมโยง แลกเปลี่ยนข้อมูลข่าวสารด้านการข่าวกรองไซเบอร์ทั้งองค์กรภายในประเทศและระหว่างประเทศได้ ซึ่งความร่วมมือขององค์กรภายในประเทศและในระดับนานาชาติ จะสามารถช่วยในการติดตาม ค้นหาแหล่งที่มาของการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว ทันเวลา และสามารถคาดการณ์และแจ้งเตือนแนวโน้มการโจมตีได้อีกด้วย ซึ่งในปัจจุบันคือ ศูนย์ประสานการรักษาความมั่นคงระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สังกัดสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ไทยเซิร์ตให้ความสำคัญและสนับสนุนด้านพัฒนาศักยภาพบุคลากรให้พร้อมรับมือกับภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เช่น การพัฒนาขีดความสามารถของเจ้าหน้าที่ไอที หน่วยงานรัฐการส่งผู้แทนเข้าร่วมการประชุม สัมมนาในระดับนานาชาติในนามประเทศไทย การอาสาเป็นเจ้าภาพเพื่อพัฒนาบุคลากร ทั้งนี้ ไทยเซิร์ต ได้ส่งผู้แทนเข้าร่วมการประชุมทาง ด้านความมั่นคงปลอดภัยในกรอบความร่วม มือระหว่างประเทศ ซึ่งครอบคลุมทั้งในระดับ ปฏิบัติการ ผู้บริหารระดับกรม และรัฐมนตรี

ปัจจุบัน ประเทศไทยมีการตรวจพบภัยคุกคามทางไซเบอร์ในแต่ละปีเป็นจำนวนมาก ซึ่งรัฐบาลได้ตระหนักถึงความสำคัญดังกล่าว จึงมีนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์

ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยได้มีการจัดทำ ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และผ่านการเปิดรับฟังความคิดเห็นไปในระหว่างวันที่ 24 พฤษภาคม 2560 ถึงวันที่ 7 มิถุนายน 2560 โดยมีเหตุผลสำคัญ คือเพื่อให้ประเทศไทยสามารถปกป้อง ป้องกันหรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดให้มีหน่วยงานหลักเพื่อรับผิดชอบดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งต้องอาศัยความรวดเร็วตลอดจนการบูรณาการและการประสานการปฏิบัติร่วมกับทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนเพื่อป้องกันและรับมือได้ทันสถานการณ์ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง และกำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. (National Cybersecurity Committee : NCSC) โดยกำหนดให้ กปช. มีอำนาจหน้าที่ที่สำคัญ คือ วางยุทธศาสตร์การรักษาความมั่นคงปลอดภัยทางไซเบอร์อันเป็นหนึ่งในยุทธศาสตร์การพัฒนาดิจิทัลควบคู่ไปกับการเตรียมการประกาศใช้ร่างพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ และเตรียมการพัฒนาและการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดนโยบายและแผนระดับชาติ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเสนอคณะรัฐมนตรี กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ รวมถึงการบูรณาการ การพัฒนา และการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางไซเบอร์ ระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ (ร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.... (ออนไลน์)., 2561)

การตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อไม่ให้ส่งผลกระทบต่อความมั่นคงของประเทศ สามารถป้องกันสถานการณ์ด้านภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ซึ่งจะสร้างความเชื่อมั่นให้กับบุคคลที่เกี่ยวข้อง ทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคมได้อย่างมีประสิทธิภาพ โดยการจัดทำแผนแม่บทด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณากำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ เพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และวางกรอบการประสานความร่วมมือระหว่างหน่วยงานภาครัฐและหน่วยงานภาคเอกชน ซึ่งประกอบด้วย หน่วยงานประสานงานกลาง หน่วยงานเผชิญเหตุฉุกเฉิน และกรอบมาตรฐานการรักษาความปลอดภัยทางไซเบอร์ของหน่วยงานภาครัฐและเอกชน ตามหลักการบริหารความเสี่ยง มีการติดตาม ตรวจสอบ และประเมินผลการดำเนินการ เพื่อเสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมาย กฎ ระเบียบ และข้อบังคับที่เกี่ยวข้อง โดยคณะรัฐมนตรีได้มีมติเห็นชอบหลักการ ร่างระเบียบสำนักนายกรัฐมนตรี ว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อ 19 กันยายน 2560 ซึ่งมีนายกรัฐมนตรีหรือรองนายกรัฐมนตรีที่ได้รับมอบหมายเป็นประธาน

นโยบายด้านความมั่นคงปลอดภัยไซเบอร์

สภาความมั่นคงแห่งชาติ ได้กำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ไว้ โดยเน้นที่การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ 3 ประการ คือ (นโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2564, ส่วนที่ 2, :10)

1. ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยการบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กร และผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกันการโจมตีระบบสารสนเทศ การพัฒนาความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ การกู้คืนข้อมูล ระบบ/เครือข่าย และการพัฒนามาตรฐานด้านความปลอดภัยในทุกด้าน โดยมีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานรับผิดชอบหลัก และกระทรวงกลาโหม สำนักงานตำรวจแห่งชาติ และสำนักข่าวกรองแห่งชาติ เป็นหน่วยงานร่วม/องค์กรเครือข่าย

2. พัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์ ให้สามารถลดภัยคุกคามหรืออันตรายที่ส่งผลกระทบกับบุคคล ข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปของการทำธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูลสารสนเทศ การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิดตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ โดยมีสำนักงานตำรวจแห่งชาติเป็นหน่วยงานรับผิดชอบหลัก และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานร่วม/องค์กรเครือข่าย

3. พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยส่งเสริมการวิจัยพัฒนาและจดสิทธิบัตรเทคโนโลยีสารสนเทศที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลภาครัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบรัฐบาลอิเล็กทรอนิกส์ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) ตลอดจนการพัฒนาบุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญทางด้านระบบเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัย และการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการพัฒนาบุคลากรทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในเชิงปริมาณและคุณภาพอย่างต่อเนื่อง โดยมีกระทรวงวิทยาศาสตร์และเทคโนโลยีและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานรับผิดชอบหลัก และ กระทรวงศึกษาธิการ สำนักงานคณะกรรมการวิจัยแห่งชาติ สำนักงานกองทุนสนับสนุนการวิจัย และสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เป็นหน่วยงานร่วม/องค์กรเครือข่าย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้จัดตั้งศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Operation Center : CSOC) ตั้งแต่ปี 2554 เพื่อรองรับภารกิจในการดำเนินการติดตาม เฝ้าระวัง ตรวจสอบวิเคราะห์เว็บไซต์ และข้อมูลทางอินเทอร์เน็ตที่ไม่เหมาะสมหรือผิดกฎหมายต่างๆ รวมทั้งรวบรวมวิเคราะห์พยานหลักฐาน และป้องกันภัยคุกคามที่อาจเกิดขึ้นจากการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550 ตลอดจนการให้ความช่วยเหลือและให้ข้อแนะนำที่ถูกต้องแก่ประชาชน เพื่อให้สามารถใช้งาน

อินเทอร์เน็ตได้อย่างปลอดภัยและสร้างสรรค์ โดยมีเจ้าหน้าที่ปฏิบัติงานควบคุมดูแลตลอด 24 ชั่วโมง ถึงแม้ว่าประเทศไทยจะมีมาตรการทางกฎหมาย และมีหน่วยงานของรัฐกำกับดูแลภัยคุกคามด้านนี้มาแล้วหลายปี แต่แนวโน้มความรุนแรงและการขยายตัวของภัยคุกคามยังมีความต่อเนื่อง แพร่หลายไปกระทบความเชื่อมั่นด้านความมั่นคงของประเทศในด้านต่างๆ ดังนั้นรัฐบาลจึงได้แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC)

การบูรณาการและประสานความร่วมมือจากฝ่ายต่างๆ ทั้งภาครัฐ ภาคเอกชน และภาคประชาสังคมมีความสำคัญอย่างมากต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยแต่ละฝ่ายอาจมีบทบาทสำคัญดังนี้

1. หน่วยงานภาครัฐ ต้องกำหนดให้ภาคเอกชนโดยเฉพาะหน่วยที่ดำเนินกิจกรรมเกี่ยวข้องกับความมั่นคงของชาติ เช่น ธนาคาร สายการบิน ระบบโทรคมนาคม ระบบขนส่งมวลชน ระบบสาธารณูปโภคฯ เป็นต้น ให้สามารถการบริหารและจัดการความเสี่ยงได้หากเกิดสถานการณ์ และมีหน้าที่ในการประสานความร่วมมือกับหน่วยงานภาคเอกชนและภาคประชาสังคม

2. หน่วยงานภาคเอกชน ต้องสามารถบริหารและจัดการความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งสามารถให้บริการได้อย่างต่อเนื่องแม้จะเกิดสถานการณ์การโจมตีทางไซเบอร์ และต้องรายงานการโจมตีทางไซเบอร์ให้หน่วยงานของรัฐทราบทันทีเพื่อประโยชน์ในการป้องกันความเสียหาย

3. ภาคประชาสังคม รวมถึงประชาชน ต้องได้รับการคุ้มครองสิทธิเสรีภาพในโลกไซเบอร์ และมีหน้าที่เฝ้าระวังระบบและข้อมูลบนอินเทอร์เน็ตให้มีความมั่นคงปลอดภัย หากพบเว็บไซต์ที่มีเนื้อหาที่ไม่เหมาะสมหรือพบการโจมตีทางไซเบอร์ ควรแจ้งเหตุการณ์ต่อเจ้าหน้าที่เพื่อจัดการกับปัญหาดังกล่าวทันที

การคุ้มครองโครงสร้างพื้นฐาน

เทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ส่งผลกระทบให้เกิดเปลี่ยนแปลงในระบบเศรษฐกิจและสังคม เพราะสามารถอำนวยความสะดวกในการบริการให้ดีขึ้นโดยใช้ต้นทุนต่ำลง ทำให้เกิดตลาดสินค้าและบริการใหม่ๆ ส่งผลต่อการใช้ชีวิตประจำวันของมนุษย์ที่ต้องพึ่งพาโครงสร้างพื้นฐานทางสารสนเทศและเครือข่ายคอมพิวเตอร์เพื่อรับการให้บริการมากยิ่งขึ้น หน่วยงานทั้งภาครัฐและภาคเอกชนจำเป็นต้องปรับตัวให้ทันกับการเปลี่ยนแปลงและผลกระทบที่เกิดตามมาโดยเฉพาะอย่างยิ่งผลกระทบด้านความปลอดภัยของระบบโครงสร้างพื้นฐาน ทั้งนี้โครงสร้างพื้นฐานแต่ละกลุ่มมีความเสี่ยงและจุดอ่อนแตกต่างกัน

ประเทศที่มีหน่วยงานคุ้มครองโครงสร้างพื้นฐานอย่างเป็นระบบคือสหรัฐอเมริกา โดยในปี 2541 ประธานาธิบดีสหรัฐฯ ได้ออกคำสั่งว่าด้วยการคุ้มครองโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure Protection) ซึ่งเป็นนโยบายด้านการรักษาความปลอดภัยของโครงสร้างพื้นฐานด้านสารสนเทศของสหรัฐฯ สาระสำคัญของคำสั่งดังกล่าวก็คือให้หน่วยงานรัฐที่เกี่ยวข้องร่วมมือกับภาคเอกชนเพื่อหาแนวทางในการป้องกันและแก้ไขปัญหาความปลอดภัยของโครงสร้างพื้นฐานที่มีความสำคัญสูงต่อเศรษฐกิจ ความมั่นคงของประเทศ และเสี่ยงต่อการถูกโจมตีทั้งในรูปแบบเดิมและการโจมตีทางไซเบอร์ โดยโครงสร้างพื้นฐานวิกฤตแบ่งแยกออกเป็น 5 กลุ่ม (Critical infrastructure

protection in homeland security: defending a networked nation, Ted G. Lewis, 2006, p.14 - 16) ได้แก่

1. กลุ่มสารสนเทศและโทรคมนาคม ได้แก่ โครงข่ายโทรคมนาคมสาธารณะ โครงข่ายอินเทอร์เน็ต คอมพิวเตอร์ที่ใช้องค์กรต่างๆ รวมถึงคอมพิวเตอร์ประจำบ้าน

2. กลุ่มธนาคารและสถาบันการเงิน ได้แก่ ธนาคาร สถาบันการเงิน บริษัทเงินทุน ตลาดหลักทรัพย์

3. กลุ่มพลังงาน ได้แก่ หน่วยงานที่ผลิตและจ่ายพลังงานไฟฟ้า เชื้อเพลิง น้ำมัน ก๊าซธรรมชาติ

4. กลุ่มการขนส่งทางกายภาพ ได้แก่ โครงข่ายเส้นทางคมนาคม เช่นถนน ทางรถไฟ รถไฟฟ้า รถใต้ดิน เส้นทางการเดินเรือ การเดินอากาศ และสนามบิน

5. กลุ่มบริการที่จำเป็นต่อชีวิตประจำวัน ได้แก่ ระบบประปา ตำรวจ ดับเพลิง พยาบาล ฉุกเฉิน

ในส่วนของประเทศไทยมีการกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) โดยแบ่งหน่วยงานหรือเครือข่ายซึ่งจัดอยู่ในข่ายโครงสร้างพื้นฐานเป็น 6 กลุ่ม (รมว.ดิจิทัลฯ แถลงผลการประชุม คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2561 (ออนไลน์)., 2561) ดังนี้

1. กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ กำกับโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ กระทรวงกลาโหม

2. กลุ่มการเงิน กำกับโดย ธนาคารแห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

3. กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กำกับโดย คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

4. กลุ่มการขนส่งและโลจิสติกส์ กำกับโดย กระทรวงคมนาคม)

5. กลุ่มพลังงานและสาธารณูปโภค กำกับโดย กระทรวงพลังงาน และกระทรวงมหาดไทย

6. กลุ่มสาธารณสุข กำกับโดย กระทรวงสาธารณสุข

หลายกลุ่มงานได้มีการดำเนินงานไปมากแล้ว เช่น <u>กลุ่มการเงิน</u> ได้มีการตั้งหน่วยรับมือภัยคุกคาม (CERT) มีการซ้อมรับมือภัยคุกคามไซเบอร์ ซึ่งกระทรวงดีอีเข้าไป facilitate กลุ่มความมั่นคง <u>กลุ่มความมั่นคง</u> ได้มีการตั้งหน่วยรับผิดชอบงานด้านความมั่นคงปลอดภัยไซเบอร์ และได้ร่วมการฝึกรับมือภัยคุกคามไซเบอร์ <u>การซ้อมรับมือภัยคุกคาม</u> เป็นสิ่งจำเป็นโดยควรมีการจัดตารางกิจกรรมของแต่ละกลุ่มให้สอดรับกันเพื่อเป็นกำลังขับเคลื่อนอย่างมีเอกภาพ ทั้งนี้ในกลุ่มที่มีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์อยู่แล้ว

การทำงานร่วมกันระหว่างกลุ่มงาน แต่ละกลุ่มงานจำเป็นต้องมีการแลกเปลี่ยนข้อมูลความมั่นคงปลอดภัยไซเบอร์ มีการลงทุนใช้บริการรับข่าวสารข้อมูลภัยคุกคามไซเบอร์ที่นำมากระจายให้กลุ่มงานต่าง ๆ ได้รับรู้ด้วย ทั้งนี้การสร้างความไว้วางใจเป็นสิ่งจำเป็นอย่างยิ่ง โดยอาจดำเนินการอยู่ในรูปแบบ Platform กลาง และหรือมีเอกชนเข้าร่วมด้วย

ปัญหาและผลกระทบจากการบุกรุกหรือการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานเป็นประเด็นที่มีความสำคัญอย่างมาก เพราะหากข้อมูลในโครงสร้างพื้นฐานเหล่านี้ไม่มีการป้องกันหรือความสามารถในการป้องกันไม่เพียงพอต่อการโจมตี จะส่งผลกระทบโดยตรงต่อประเทศ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อระบบเศรษฐกิจและความมั่นคงของชาติ ฉะนั้นอาจกล่าวได้ว่าถึงเวลาที่ต้องดำเนินการทั้งด้านนโยบายและมาตรการที่เป็นรูปธรรมให้ชัดเจนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น

การดำเนินการของกองทัพไทยต่อภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์

ในส่วนกระทรวงกลาโหม ซึ่งมีภารกิจหลักด้านความมั่นคงของชาติ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี (พ.ศ.2558 – 2562) โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหม ซึ่งกระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ โดยอาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ตามมาตรฐาน ISO 27001: 2005 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ ของกระทรวงกลาโหม พ.ศ.2560 – 2564 มีสาระสำคัญคือ ครอบคลุมแผนงานหลัก 6 แผนงาน ได้แก่

1. แผนการจัดองค์กรด้านไซเบอร์ โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ดำเนินการจัดตั้งหน่วยงานด้านไซเบอร์/ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง

2. แผนการป้องกันระบบโครงสร้างพื้นฐาน โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ จัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของตนขึ้นมาเพื่อป้องกันโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูล และจัดตั้งทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านความปลอดภัยไซเบอร์ได้อย่างรวดเร็ว และทันเวลา

3. แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกัน สกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อ

ความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่างๆ รวมถึงการจัดให้มีการแข่งขันทักษะการปฏิบัติการไซเบอร์ (Cyber Contest)

4. แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตามความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวันจะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว

5. แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain)

6. แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน แต่สามารถนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ซึ่งมีพลังอำนาจที่ยิ่งใหญ่ได้

โดยดำเนินการจัดตั้งศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม เพื่อเชื่อมโยงกับ การตั้ง ศูนย์ไซเบอร์ของกองบัญชาการกองทัพไทย และเหล่าทัพ มีขอบเขตอำนาจหน้าที่ ในการประสานนโยบายไซเบอร์กับระดับชาติ รวมทั้งรับผิดชอบด้านนโยบายยุทธศาสตร์ และปฏิบัติงานด้านไซเบอร์ในระดับยุทธศาสตร์ของกระทรวงกลาโหมในภาพรวม รวมทั้งดำเนินการความร่วมมือด้านไซเบอร์กับหน่วยงาน ภาครัฐและภาคเอกชนที่เกี่ยวข้องทั้งในและต่างประเทศ ซึ่งในปัจจุบันได้มีการจัดตั้งหน่วยงานด้านไซเบอร์เพื่อรองรับภารกิจการรักษาความมั่นคงปลอดภัยไซเบอร์เรียบร้อยแล้ว โดยแบ่ง การดำเนินงานเป็น 2 ส่วนคือ ส่วนปฏิบัติกรด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) และส่วนสนับสนุนในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย (Computer Security Incident Response Team : CSIRT) ซึ่งเป็นการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมในปัจจุบัน

กระทรวงกลาโหมมีแนวคิดจะตั้ง MoDCERT เป็นหน่วยงานรับมือภัยคุกคามฝ่ายกลาโหม ซึ่งควรต้องผนึกกำลังกับ ThaiCERT ที่รับมือภัยคุกคามฝ่ายพลเรือน เมื่อพบภัยคุกคามต่อความมั่นคงของรัฐ สภาความมั่นคงฯและสภากลาโหมจะต้องเข้ามาดูแลเชิงนโยบายอย่างเต็มที่ โดยอาจอยู่ในลักษณะการทำพิมพ์เขียว (Blueprint) ของประเทศระหว่าง Cyber Security และ Cyber Defense

ในระดับเหล่าทัพ กองบัญชาการกองทัพไทย ได้จัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ. 2558 เพื่อให้กองทัพไทยมีขีดความสามารถและมีเสรีในการปฏิบัติการบนมิติไซเบอร์ ทั้งเชิงรับและเชิงรุก ทั้งในสภาวะปกติ ตลอดจนสามารถบูรณาการ และให้การสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ของประเทศไทยในภาพรวมได้อย่างมีประสิทธิภาพ โดยได้กำหนดประเด็นยุทธศาสตร์ทหารสำหรับการปฏิบัติการทางทหารในมิติไซเบอร์ เพื่อใช้เป็นกรอบแนวทางในการดำเนินการให้สามารถบรรลุวัตถุประสงค์ทางทหารที่ ตั้งไว้แยกเป็น 3 ประเด็น

ได้แก่ ยุทธศาสตร์การป้องกันเชิงรุก ยุทธศาสตร์การผนึกกำลังป้องกันประเทศ และยุทธศาสตร์การสร้างความร่วมมือด้านความมั่นคง

การดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพไทย การปฏิบัติการในมิติไซเบอร์ของกองทัพไทย ถือเป็นการปฏิบัติการทางทหารอย่างหนึ่งเพื่อรับมือกับ ภัยคุกคามรูปแบบใหม่ ซึ่งมีความสอดคล้องกับหน้าที่ของกองทัพไทยในการเตรียมกำลัง การป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทางทหาร โดยในระดับกระทรวงกลาโหมและกองบัญชาการกองทัพไทย มีหน่วยงานสำคัญที่มีบทบาทในการดำเนินภารกิจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่

1. กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร จัดตั้งขึ้นเมื่อพฤษภาคม 2556 โดยสภากลาโหมมีมติอนุมัติให้กองทัพไทยจัดตั้งหน่วยงานรับผิดชอบทางด้านไซเบอร์ โดยกองปฏิบัติการสงครามเครือข่ายฯ มีความรับผิดชอบหลักใน การจัดการและบูรณาการการปฏิบัติทางไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ ของกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็น องค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

2. กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร มีภารกิจในการดำเนินการตรวจสอบวิเคราะห์ป้องกันกู้คืนและประเมินผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำแนวทาง หลักการ ระเบียบ มาตรการ และแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมทั้งพิจารณาเสนอแนะการดำเนินการต่อภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศของของกองบัญชาการกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบ หนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

3. ศูนย์ไซเบอร์ทหาร จากข้อมูลข้างต้น จะเห็นได้ว่าปัจจุบันกองบัญชาการกองทัพไทยมีหน่วยงาน หลัก ที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ อยู่ 2 หน่วยงาน ซึ่งทั้ง 2 หน่วยงานมีภารกิจทางด้านไซเบอร์ ที่ต้องรับผิดชอบเหมือนกัน แต่มีสายการบังคับบัญชาที่แยกกันอยู่ เมื่อผู้บังคับบัญชาได้เล็งเห็นถึงความเชื่อมโยงระหว่าง 2 หน่วยงานนี้จึงมีนโยบายให้มีการแปรสภาพ 2 หน่วยงานดังกล่าวให้เป็น “ศูนย์ไซเบอร์ทหาร”ขึ้นตรง กับสำนักผู้บัญชาการทหารสูงสุด ซึ่งได้ทดลองปฏิบัติงาน ร่วมกันมาตั้งแต่ ตุลาคม 2559 และพร้อมปฏิบัติงานเมื่อ เมษายน 2560

แนวทางที่จะปฏิบัติกับภัยคุกคามทางไซเบอร์นั้นต้องมีการเฝ้าระวัง สืบค้น ติดตามสิ่งที่เป็นภัยต่อความมั่นคงของชาติอย่างต่อเนื่องและตลอดเวลา ทั้งจากภายในและภายนอกประเทศอย่างใกล้ชิด รวมถึงการปฏิบัติการเชิงรุกภายใต้กรอบกฎหมาย ในฐานะหน่วยงานด้านความมั่นคงของประเทศ จึงต้องมีการเตรียมความพร้อมโดยการผลิตและพัฒนาบุคลากร พัฒนาองค์ความรู้ให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว สร้างความตระหนักรู้ในเรื่องความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนพัฒนาความร่วมมือ ระหว่างหน่วยงานด้านความมั่นคงในการปฏิบัติงานร่วมกันเป็นประชาคมไซเบอร์ (Cyber Community)

สภาวการณ์เกี่ยวกับปัญหาและผลกระทบจากภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย

ในปัจจุบันสถานการณ์ความขัดแย้งในโลกค่อนข้างเป็นเรื่องน่าเป็นห่วง ตัวอย่างเช่น สำนักงานความมั่นคงแห่งชาติของสหรัฐฯ (NSA) เปิดเผยว่ามี 30 ถึง 40 ประเทศที่มีความสามารถในการบุกรุกข้อมูลส่วนตัวของผู้คนบนโลกไซเบอร์ได้ โดยมีรัฐบาลเป็นผู้สนับสนุนเพื่อต้องการใช้ข้อมูลไปทำบางอย่างที่เกี่ยวกับการก่อสงครามนั่นเอง ทำให้ต้องเพิ่มการระมัดระวังเป็นอย่างมากในเรื่องนี้ และรัฐบาลต้องเข้ามาช่วยป้องกันโดยออกกฎเกณฑ์และกำกับดูแลเรื่องนี้อย่างเข้มงวดและจริงจัง ซึ่งนี่เป็นเพียงภาพรวมที่ทำให้เราเห็นความตื่นตัวด้าน Cyber Security โดยมองในเชิงของกฎเกณฑ์บังคับใช้ ซึ่งถือเป็นเรื่องอีกหนึ่งที่หลายๆ ประเทศตื่นตัวและให้ความสำคัญ เพราะการมี Cyber Security ที่ไม่แข็งแรงเพียงพอนั้นเปรียบเสมือนเป็นการเปิดโอกาสให้เกิดอาชญากรรมทางไซเบอร์ได้ ซึ่งจะส่งผลกระทบไม่เพียงแต่ในประเทศเท่านั้นแต่รวมไปถึงระดับโลกด้วย ส่วนในระดับของผู้ใช้เอง ก็ต้องตื่นตัวที่จะติดตามข่าวสารด้านเทคโนโลยีอยู่เสมอ เช่น พวกข่าวเตือนภัย รวมถึงพยายามระมัดระวังรักษาข้อมูลส่วนตัวเพื่อไม่ให้ตกเป็นเหยื่อ

สภาที่ปรึกษาด้านเศรษฐกิจประจำทำเนียบประธานาธิบดีสหรัฐฯ (Council of Economic Advisers – CEA) เผยแพร่รายงานเมื่อ 17 กุมภาพันธ์ 2561 เกี่ยวกับผลกระทบทางเศรษฐกิจที่เกิดขึ้นเป็นวงกว้างที่สหรัฐฯ ได้รับจากภัยคุกคามทางไซเบอร์ พร้อมชี้ให้เห็นว่า สหรัฐฯ กำลังเผชิญภัยคุกคามด้านนี้มากขึ้นจากทุกทิศทาง เช่น ประเทศที่ไม่หวังดีกับสหรัฐฯ ภาคเอกชนต่างชาติ กลุ่มเคลื่อนไหวที่หวังผลประโยชน์ทางการเมือง และกลุ่มอาชญากรรมข้ามชาติ เป็นต้น ในรายงานดังกล่าวยังต้องการความร่วมมือจากทั้งภาครัฐและเอกชน ที่จะช่วยกันจำกัดความเคลื่อนไหวทางไซเบอร์ในทางที่ผิดกฎหมาย โดยมีเป้าหมายเพื่อเกื้อหนุนให้เกิดการเติบโตของเศรษฐกิจสหรัฐฯ (“สหรัฐฯ เผยแพร่รายงานผลกระทบที่สหรัฐฯได้รับจากภัยคุกคามทางไซเบอร์” (ออนไลน์)., 2018)

ในรายงานดังกล่าว ชี้ให้เห็นถึงกิจกรรมทางไซเบอร์ที่ส่งผลกระทบในเชิงลบต่อสหรัฐฯ โดยแบ่งผู้ก่อภัยคุกคามทางไซเบอร์ต่อสหรัฐฯ ออกเป็นกลุ่มได้ดังนี้

1. Nation-states ได้แก่ รัสเซีย จีน อิหร่าน และเกาหลีเหนือ ซึ่งเป็นกลุ่มที่มีความสามารถ มีเงินทุนสนับสนุน และมีเป้าหมายในการโจมตี ซึ่งขึ้นอยู่กับเวลาและเงินที่จะได้รับ การกระทำจะเกิดขึ้นจากแรงจูงใจทางการเมือง เศรษฐกิจ ทางเทคนิค หรือวาระทางทหาร กลุ่มนี้ส่วนใหญ่จะเกี่ยวข้องกับการจารกรรมทางอุตสาหกรรม และการล้วงความลับในระดับบุคคล รวมทั้งการทำลายทางธุรกิจด้วย

2. Corporate competitors โดยคู่แข่งในการดำเนินธุรกิจพยายามเจาะข้อมูลของฝ่ายตรงข้าม เช่น ด้านยุทธศาสตร์ การเงิน ข้อมูลลูกจ้าง ซึ่งส่วนใหญ่รัฐบาลต่างประเทศให้การสนับสนุนกลุ่มนี้

3. Hacktivists เป็นได้ทั้งคนเดียว หรือกลุ่มที่มีเป้าหมายทางการเมือง และต้องการสร้างชื่อเสียง หรือต้องการทำลายฝ่ายตรงข้ามด้วยเหตุผลทางอุดมการณ์

4. Organized criminal groups อาชญากรรมข้ามชาติต้องการหารายได้ โดยเป้าหมายคือทั้งภาครัฐและเอกชน

5. Opportunists คือ มือสมัครเล่นที่ต้องการสร้างชื่อเสียง โดยเป้าหมายมักเป็นบริษัทที่เก็บข้อมูลโดยใช้การเข้ารหัส หรือเทคนิคต่าง ๆ เพื่อปกป้องข้อมูล

6. Company insiders เป็นคนวงในของบริษัทที่ทั้งกำลังทำงานให้ และลาออกไปแล้ว แต่ต้องการแก้แค้น หรือแสวงประโยชน์ทางการเงิน

ซึ่งสามารถสรุปความเสียหายที่สหรัฐฯ ได้รับจากภัยทางไซเบอร์เมื่อปี 2560 CEA ประเมินไว้ประมาณ 57,000 – 109,000 ล้านดอลลาร์สหรัฐฯ หรือประมาณร้อยละ 0.31-0.58 ของ GDP ของสหรัฐฯ รวมทั้งยังส่งผลกระทบทางด้านจิตวิทยาที่เกิดจากการตื่นตระหนกและหวาดกลัว ความเสียหายที่ลุกลามไปยังภาคส่วนอื่น ๆ การต้องเพิ่มงบประมาณด้านการป้องกันภัยทางไซเบอร์ การชะลอตัวของการเติบโตทางเศรษฐกิจ และจะส่งผลเสียร้ายแรงที่สุดหากเกิดขึ้นต่อระบบโครงสร้างพื้นฐานที่สำคัญของสหรัฐฯ

อุปสรรคในการรับมือกับภัยคุกคามทางไซเบอร์มีหลายมิติ ในภาพรวมหน่วยงานของสหรัฐฯทั้งภาครัฐและเอกชนยังขาดข้อมูล ผู้เชี่ยวชาญ กฎหมาย และมาตรการที่จะรับมือกับภัยดังกล่าวให้ได้ทันท่วงที หรือสกัดกั้นก่อนที่จะเกิดขึ้น และที่ซับซ้อนกว่านั้นคือ บริษัท หรือหน่วยงานของรัฐฯ ปิดบังข้อมูลหรือรายละเอียดที่ได้รับจากภัยทางไซเบอร์ เพราะวิตกกังวลว่าจะส่งผลเสียหายต่อการดำเนินงานหากเปิดเผยข้อมูลดังกล่าว สหรัฐฯ ให้ความสำคัญกับปัญหานี้เป็นอย่างยิ่ง และประชาคมข่าวกรองของสหรัฐฯ เคยจัดอันดับให้ “Cyber Threat” เป็นภัยคุกคามอันดับหนึ่งต่อเนื่องถึง 3 ปี นอกจากนั้นยังมีหน่วยงานหลัก 2 หน่วยงานที่ดูแลเรื่อง ไซเบอร์ ได้แก่ สำนักงานความมั่นคงแห่งชาติ (National Security Agency–NSA) และ Cyber Command การที่ภัยทางไซเบอร์มีความซับซ้อน CEA จึงเตรียมการรับมือดังนี้ 1) ทั้งภาครัฐและเอกชนต้องตระหนักในภัยคุกคามทาง ไซเบอร์ที่จะส่งผลเสียต่อเศรษฐกิจร่วมกัน ทั้งต้องร่วมมือกันในการเสริมสร้างศักยภาพในการรับมือต่อภัยคุกคามทางไซเบอร์ 2) รัฐบาลรับฟังข้อเสนอจากภาคเอกชนที่จะร่วมมือกัน 3) รัฐบาลต้องเพิ่มการลงทุนในด้านการวิจัยทาง ไซเบอร์ 4) มีการบังคับใช้กฎหมาย หรือมาตรการที่เกี่ยวข้องกับทางไซเบอร์ได้อย่างมีประสิทธิภาพ 5) รัฐบาลต้องเพิ่มบทบาทในเวทีระหว่างประเทศด้วยการชี้ให้นานาประเทศหรือกรอบการเจรจาระหว่างประเทศ เช่น G-7 และ G-20 เห็นความสำคัญที่ต้องร่วมมือกันกำหนดมาตรการรับมือกับภัยคุกคามทางไซเบอร์

รายงานจาก McAfee Labs 2018 Threats Predictions Report สามารถสรุปประเด็นสำคัญได้ 5 ประการ (“McAfee Labs 2018 Threats Predictions Report” (ออนไลน์)., 2018) ดังนี้

1. Machine Learning ศึกใหญ่ระหว่างฝั่งโจมตีกับฝั่งป้องกันเทคนิค Machine Learning เริ่มถูกนำมาใช้เพื่อประมวลผลข้อมูลบนระบบเครือข่ายและอุปกรณ์ปลายทางเพื่อค้นหาช่องโหว่ พฤติกรรมต้องสงสัย หรือการโจมตีแบบ Zero-day อย่างไรก็ตาม ฝั่งแฮกเกอร์เองก็สามารถนำ Machine Learning มาใช้เพื่อสนับสนุนการโจมตีของตนเช่นเดียวกัน ไม่ว่าจะเป็นการเรียนรู้จากการป้องกันของอีกฝ่าย สร้างโมเดลในการขัดขวางการตรวจจับการโจมตี หรือเจาะช่องโหว่ใหม่ที่เพิ่งค้นพบให้เร็วกว่าที่แพตช์จะถูกอัปเดต เป็นต้น ก่อให้เกิดเป็นการปะทะกันระหว่างเทคนิค Machine Learning ของฝั่งโจมตีและฝั่งป้องกัน เพื่อให้มีชัยเหนือแฮกเกอร์ องค์กรควรเลือกใช้เทคนิค Machine Learning ที่มีประสิทธิภาพ และนำเทคนิคดังกล่าวมาผสานรวมกับกลยุทธ์การตอบสนองต่อภัย

คุกคาม เพื่อให้เข้าใจถึงรูปแบบการโจมตีของแฮกเกอร์และสามารถดำเนินการตัดสินใจเพื่อรับมือกับการโจมตีได้อย่างรวดเร็ว ถึงแม้ว่าจะไม่เคยประสบกับการโจมตีนั้นมาก่อนก็ตาม

2. เตรียมพบ Ransomware รูปแบบใหม่ ที่เทคโนโลยี เป้าหมาย และค่าไถ่ต่างไปจากเดิม การเรียกค่าไถ่จากแคมเปญ Ransomware แบบเดิมๆ จะเริ่มลดลง เนื่องจากโซลูชันสำหรับป้องกัน Ransomware มีให้เลือกมากขึ้น ผู้ใช้มีความตระหนัก และหลายองค์กรเริ่มวางกลยุทธ์สำหรับรับมือกับการโจมตี ส่งผลให้แฮกเกอร์เริ่มปรับเปลี่ยนเป้าหมายไปยังกลุ่มอื่น เช่น ผู้ใช้ทั่วไปที่มีฐานะและอุปกรณ์ Internet of Things แทน นอกจากนี้ เราจะเห็นรูปแบบหรือประเภทของ Ransomware น้อยลงกว่าเดิม เพราะอาชญากรไซเบอร์เริ่มหันไปใช้บริการ Ransomware as a Service มากขึ้น แทนที่จะพัฒนา Ransomware ใหม่ด้วยตนเอง อย่างไรก็ตาม Ransomware กลับมีเทคนิคในการโจมตีเพื่อเรียกค่าไถ่มากขึ้น แทนที่จะเข้ารหัสหรือบล็อกการเข้าไฟล์เพียงอย่างเดียว ยังมีการเพิ่มการทำลายข้อมูลและการขัดขวางธุรกิจเข้าไปด้วย เพื่อกดดันให้เหยื่อต้องจ่ายค่าไถ่แลกกับการไม่ต้องผจญกับวิกฤตทางธุรกิจ

3. แอปพลิเคชัน Serverless เริ่มแพร่หลาย สร้างช่องทางโจมตีใหม่แก่แฮกเกอร์แอปพลิเคชันประเภท Serverless เริ่มเป็นที่นิยมมากขึ้น เนื่องจากช่วยลดเวลาและค่าใช้จ่ายในการพัฒนาแอปพลิเคชัน อย่างไรก็ตามแอปพลิเคชัน Serverless ยังเปราะบางต่อการโจมตีที่อาศัยการทำ Privilege Escalation (การยกระดับสิทธิ์) และ Application Dependencies (การโจมตีแอปพลิเคชันที่เกี่ยวข้องเพื่อให้ส่งผลกระทบต่อแอปพลิเคชันหลัก) รวมไปถึงการโจมตีข้อมูลที่ส่งผ่านไปมาข้ามระบบเครือข่ายและการโจมตีแบบ Denial of Service เนื่องจากสถาปัตยกรรมแบบ Serverless มักมีปัญหาเรื่องการขยายระบบเพื่อป้องกันปัญหาดังกล่าว กระบวนการพัฒนาและวางระบบของแอปพลิเคชัน Serverless ควรมีการพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัย การรองรับการขยายระบบในอนาคต และการใช้ VPN หรือการเข้ารหัสข้อมูลในการปกป้องทราฟฟิกที่รับส่งบนระบบเครือข่าย

4. ข้อมูลจากครัวเรือนอัจฉริยะถูกแอบเก็บไปใช้ประโยชน์โดยไม่สนความเป็นส่วนบุคคล บ้านเรือนในปัจจุบันเริ่มนำเอาอุปกรณ์อัจฉริยะเข้ามาใช้งานเพิ่มขึ้นเรื่อยๆ ส่งผลให้ผู้ผลิตหรือผู้ให้บริการอุปกรณ์เหล่านี้เริ่มต้องการเก็บข้อมูลพฤติกรรมการใช้งานเพื่อนำไปใช้ประโยชน์ทางการตลาด ที่สำคัญคือลูกค้าส่วนใหญ่ไม่ให้ความสำคัญเกี่ยวกับข้อตกลงเรื่องความเป็นส่วนบุคคล ทำให้ผู้ผลิตเหล่านั้นแอบเปลี่ยนเงื่อนไขและข้อตกลงภายหลังเพื่อเก็บข้อมูลโดยไม่ผิดกฎหมาย หรือต่อให้ถูกจับได้ทางผู้ผลิตก็ได้คำนวณค่าปรับเข้าไปในการดำเนินธุรกิจเพื่อป้องกันการขาดทุนด้วยเช่นกัน

5. ข้อมูลออนไลน์ของผู้เยาว์จะถูกนำไปใช้อ้างถึงตัวตนในอนาคตโลกกำลังถูกขับเคลื่อนด้วยเทคโนโลยี มนุษย์ทุกเพศทุกวัยต่างหันมาใช้งานเทคโนโลยีเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งกลุ่ม Gen Z หรือกลุ่มวัยเด็กที่เรียกได้ว่าเติบโตมาพร้อมกับเทคโนโลยีอย่างแท้จริง ข้อมูลดิจิทัลต่างๆ ที่คนกลุ่มนี้สร้างขึ้นบนโลกออนไลน์จะถูกรวบรวมและถูกนำใช้อ้างอิงถึงตัวตนในอนาคต ซึ่งอาจส่งผลในแง่ร้ายได้ เช่น สถานศึกษาติดสิทธิ์ผู้เข้าสมัคร เนื่องจากพบโพสต์วิดีโอไม่เหมาะสมบน YouTube สมัยยังเป็นเด็ก เป็นต้น

ในปี 2560 มีรายงานว่าโรงพยาบาลในสหรัฐอเมริกาได้รับผลกระทบจากมัลแวร์เรียกค่าไถ่ Wanna Cry โดยอุปกรณ์ที่ถูกโจมตีในครั้งนี้ไม่ได้มีเฉพาะเครื่องคอมพิวเตอร์ที่ใช้งานทั่วไป แต่อุปกรณ์ทางการแพทย์ที่ใช้ควบคุมเครื่องฉาย X-ray สำหรับทำการสแกน MRI ได้รับความเสียหายด้วย จากรายงานพบว่า อุปกรณ์ทางการแพทย์หลายอย่างใช้ Windows XP ในการทำงาน และเจ้าหน้าที่

ไม่สามารถอัปเดตแพตช์เองได้เนื่องจากอาจเกิดผลกระทบกับฮาร์ดแวร์ที่ใช้งานร่วมกับตัวเครื่อง การอัปเดตต้องทำผ่านเฟิร์มแวร์ที่ได้รับการรับรองจากผู้ผลิตเท่านั้น นั่นทำให้เมื่อนำอุปกรณ์ที่มีช่องโหว่มาเชื่อมต่อเข้ากับระบบเครือข่ายของโรงพยาบาล (ที่อาจมีการติดมัลแวร์มาแล้ว ก่อนหน้านี้) ก็ทำให้อุปกรณ์ดังกล่าวติดมัลแวร์ที่สามารถแพร่กระจายผ่านเครือข่ายได้ทันที ผู้ผลิตอุปกรณ์ทางการแพทย์หลายยี่ห้อได้ออกแถลงการณ์และคำแนะนำเบื้องต้น โดยแจ้งว่าจะมีเฟิร์มแวร์อัปเดตออกมาแก้ไขปัญหาให้ในเร็วๆ นี้ หากสถานพยาบาลใดที่มีการใช้งานอุปกรณ์ทางการแพทย์ที่ควบคุมโดยระบบปฏิบัติการ Windows ควรสอบถามข้อมูลเพิ่มเติมจากผู้ผลิต นอกจากอุปกรณ์ทางการแพทย์แล้วยังมีรายงานว่าอุปกรณ์ที่ใช้ควบคุมระบบเครื่องจักร (Industrial Control System - ICS) มีความเสี่ยงที่จะติดมัลแวร์เรียกค่าไถ่ได้ด้วย เนื่องจากอุปกรณ์ที่ใช้ควบคุมการทำงานยังใช้ Windows เวอร์ชันเก่าที่มีข้อจำกัดในการอัปเดตเช่นเดียวกัน โดยทางผู้ผลิตอุปกรณ์หลายรายได้มีการออกแถลงการณ์ในเรื่องนี้แล้ว หน่วยงานที่มีการใช้งานอุปกรณ์ลักษณะดังกล่าวควรสอบถามข้อมูลเพิ่มเติมจากผู้ผลิต (Bleeping Computer (ออนไลน์). 2558)

เมื่อวันที่ 7 กันยายน 2560 บริษัท Equifax ซึ่งดูแลเรื่องข้อมูลเครดิตได้ประกาศว่าระบบของบริษัทถูกโจมตี ส่งผลให้ข้อมูลลูกค้าชาวอเมริกันกว่า 143 ล้านรายรั่วไหลสู่สาธารณะ โดยในเบื้องต้นทางบริษัทได้แจ้งว่าระบบถูกโจมตีผ่านช่องโหว่ของซอฟต์แวร์ Apache Struts (https://struts.apache.org) ซึ่งเป็นเฟรมเวิร์กสำหรับใช้พัฒนาซอฟต์แวร์ เหตุเกิดระหว่างช่วงเดือนพฤษภาคมถึงกรกฎาคมที่ผ่านมาจากการตรวจวิเคราะห์ข้อมูลในเวลาต่อมา ผู้เชี่ยวชาญพบว่าระบบของ Equifax ถูกเจาะผ่านช่องโหว่ CVE-2017-5638 ซึ่งเป็นช่องโหว่ระดับความรุนแรงสูงที่ส่งผลให้ผู้ประสงค์ร้ายสามารถส่งคำสั่งอันตรายเข้ามาประมวลผลที่เซิร์ฟเวอร์ได้ ช่องโหว่ดังกล่าว

มีการรายงานเมื่อวันที่ 8 มีนาคม 2560 และทางผู้พัฒนาซอฟต์แวร์ได้ออกอัปเดตแพตช์แก้ไขปัญหาดังกล่าวแล้ว แต่ทาง Equifax ไม่ได้มีการติดตั้งแพตช์ดังกล่าวเป็นเวลากว่า 9 สัปดาห์จนส่งผลให้ระบบถูกโจมตีและข้อมูลรั่วไหลได้ในที่สุดก่อนหน้านี้ในช่วงเดือนมีนาคม 2560 ภายหลังจากที่มีการเปิดเผยช่องโหว่ Apache Struts พบรายงานว่าเว็บไซต์จำนวนมากถูกโจมตีผ่านช่องโหว่ดังกล่าว โดยหนึ่งในหน่วยงานที่ได้รับผลกระทบคือกรมสรรพากรของประเทศแคนาดาซึ่งระบบถูกโจมตีจนต้องปิดให้บริการชั่วคราว (https://www.thaicert.or.th/newsbite/2017-03-15-02.html)

การอัปเดตแพตช์ซอฟต์แวร์เป็นสิ่งที่ควรทำอยู่เป็นประจำเนื่องจากหากมีช่องโหว่แค่เพียงหนึ่งจุดก็มีโอกาสที่ระบบจะถูกโจมตีจนเกิดความเสียหายได้ กรณีเหตุการณ์ Equifax นี้เป็นตัวอย่างที่ดีของผลกระทบที่เกิดขึ้นจากการที่ไม่ได้มีระบบบริหารจัดการแพตช์ที่ดีพอ

นักวิจัยจาก Kromtech Security Center รายงานว่า เซิร์ฟเวอร์ที่ติดตั้งและใช้งานซอฟต์แวร์ Elastic Search กว่า 4,000 เครื่องถูกใช้แพร่กระจายมัลแวร์สำหรับโจมตีเครื่อง POS (Point of Sale) โดยเป็นมัลแวร์สายพันธุ์ AlinaPOS และ JackPOS (POS เป็นเครื่องที่ใช้ในการชำระเงินเมื่อซื้อสินค้าหรือบริการ) เซิร์ฟเวอร์เกือบทั้งหมดที่ถูกโจมตี อยู่บน Amazon AWS (ElasticSearch เป็นซอฟต์แวร์ที่นิยมใช้ในระบบที่ต้องการประมวลผลข้อมูลและอำนวยความสะดวกในการค้นหา นักวิจัยพบเซิร์ฟเวอร์จำนวนมากบนอินเทอร์เน็ตที่ถูกตั้งค่าให้บุคคลทั่วไปสามารถเข้าถึงได้และมีรายงานว่าเครื่องเซิร์ฟเวอร์ดังกล่าวถูกโจมตีเพื่อใช้ในการแพร่กระจายมัลแวร์) นักวิจัยพบว่าสาเหตุที่ทำให้เครื่องจำนวนมากที่ถูกโจมตีเป็นเครื่องที่อยู่บน Amazon AWS เนื่องจากบริการ EC2 ของ Amazon อนุญาตให้ติดตั้ง ElasticSearch ได้เฉพาะเวอร์ชัน 1.5.2 และ 2.3.2 ซึ่งเป็นเวอร์ชัน

เก่า ปัจจุบันนักวิจัยได้แจ้งเตือนเจ้าของเซิร์ฟเวอร์ที่ได้รับผลกระทบแล้ว โดยเบื้องต้นแนะนำว่าควรตั้งค่าตามข้อแนะนำด้านความมั่นคงปลอดภัย นอกจากนี้ เมื่อช่วยต้นปี 2560 ที่ผ่านมาพบการโจมตีเซิร์ฟเวอร์ ElasticSearch เพื่อเข้ารหัสลับฐานข้อมูลเรียกค่าไถ่ ผู้ดูแลระบบควรระวังป้องกันก่อนตกเป็นเหยื่อ (“ElasticSearch” (ออนไลน์). 2560)

จากหนังสือ CYBER THREATS 2017 โดย ThaiCERT ระบุว่าเว็บไซต์ Malwarebytes ได้นำเสนอความเชื่อผิด ๆ เรื่อง Cyberbullying (CYBER THREATS 2017 (ออนไลน์)., 2018) ตัวอย่างเช่น

- ไม่ใช่เฉพาะผู้ที่ตกเป็นเหยื่อเท่านั้น ถึงจะได้รับผลกระทบจาก Cyberbullying จากข้อมูลการศึกษาพบว่าผู้ที่เป็นฝ่ายกลั่นแกล้งเองก็มีโอกาสที่จะได้รับผลกระทบจากการกระทำนั้นด้วย ไม่ว่าจะเป็นความกระวนกระวาย ความเครียด นอนไม่หลับ หรือผลกระทบด้านสุขภาพอื่น ๆ
- ไม่ใช่เฉพาะเด็กหรือวัยรุ่นเท่านั้นที่ประสบปัญหา Cyberbullying เพราะผู้ใหญ่ในสหรัฐฯ กว่า 40% ก็ประสบปัญหานี้เช่นกัน และไม่เฉพาะปัญหาครูกลั่นแกล้งนักเรียน แต่ยังพบกรณีนักเรียนกลั่นแกล้งครูด้วย
- การบอกให้คนที่ถูกกลั่นแกล้งนั้นสู้กลับ หรือบอกให้ยอมรับมันไปเพราะเป็นเรื่องธรรมดาที่ต้องเจอ นั้นไม่ใช่การแก้ปัญหาที่ถูกวิธี หลายครั้งผู้ที่ถูกกลั่นแกล้งนั้นเกิดบาดแผลทางจิตใจต้องได้รับการช่วยเหลือ

นอกจากนั้นยังมีกล่าวถึงข้อมูลที่น่าสนใจเกี่ยวกับ Dark Web ซึ่งหลายคนน่าจะเคยได้ยินผ่านสื่อกันมาบ้าง ตัวอย่างเช่น ข่าวการจับกุมเจ้าของเว็บไซต์ซื้อขายของผิดกฎหมาย ลักษณะการทำงานของ Dark Web สามารถอธิบายได้ ดังนี้

- Surface Web คือเว็บไซต์ที่เปิดให้เข้าถึงได้ด้วยวิธีปกติ (รู้จักกันในชื่อ World Wide Web) สามารถค้นหาเว็บไซต์เหล่านี้ได้ผ่าน Search engine
- Deep Web เป็นเว็บไซต์ที่ไม่ปรากฏในฐานข้อมูล Search engine และไม่เปิดให้บุคคลภายนอกเข้าถึงได้ด้วยวิธีปกติ เช่น เว็บที่ใช้งานเฉพาะเครือข่ายภายในองค์กร
- Dark Web เป็นเว็บไซต์ที่ตั้งใจซ่อนอำพรางการเข้าถึงปกปิดข้อมูลผู้อยู่เบื้องหลัง โดยส่วนใหญ่มีจุดประสงค์เพื่อใช้ในเชิงผิดกฎหมาย การเข้าถึง Dark Web จะต้องใช้ช่องทางพิเศษ เช่น เข้าผ่านเครือข่าย Tor หรือ I2P ซึ่งเป็นการเข้าถึงแบบไม่ระบุตัวตน (Anonymous) และตรวจสอบย้อนกลับเส้นทางได้ยาก เนื้อหาใน Dark Web โดยส่วนใหญ่มักเป็นเรื่องผิดกฎหมายหรืออาชญากรรม เช่น ซื้อขายยาเสพติด ขายอาวุธ ค้ามนุษย์ ซื้อขายมัลแวร์ หรือซื้อขายข้อมูลที่ถูกขโมยออกมา เป็นต้น

ถึงกระนั้น Dark Web บางส่วนไม่ได้เป็นเนื้อหาผิดกฎหมาย (หรืออาจเข้าข่ายผิดกฎหมายเฉพาะในบางประเทศ) เช่น การนำเสนอข่าวของผู้สื่อข่าวที่ทำงานอยู่ในประเทศที่ไม่อนุญาตให้เผยแพร่ข่าวสารบางอย่าง การรณรงค์ทางการเมือง การเปิดเผยข้อมูลอาชญากรรมโดยผู้เปิดเผยต้องการปกปิดตัวตน บริการแลกเปลี่ยนสกุลเงินดิจิทัล หรือการพูดคุยสนทนาในหัวข้อที่ไม่เปิดเผยต่อสาธารณะ เป็นต้น

อย่างไรก็ตาม การเข้าถึงเว็บไซต์ประเภทนี้ อาจมีผลกระทบด้านกฎหมาย และมีความเสี่ยงที่จะตกเป็นเหยื่อจากมัลแวร์ ควรพิจารณาอย่างรอบคอบก่อนเข้าถึงเว็บไซต์เหล่านี้ (http://thcert.co/gWagFt)

ภัยคุกคามบนโลกไซเบอร์กำลังส่งผลกระทบทั้งระดับบุคคล องค์กร และประเทศ ผู้อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ 3 ฝ่าย ได้แก่ รัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม นายไพรัตน์ เติมศักดิ์มิตรชัย ผู้เชี่ยวชาญด้านผลิตภัณฑ์ แคสเปอร์สกี้ แลป ประเทศไทย ผู้ให้บริการโซลูชั่นด้านไซเบอร์ซิเคียวริตี้ชั้นนำ กล่าวว่า สถานการณ์ภัยคุกคามในประเทศไทยมีความน่าเป็นห่วงอย่างมาก จากการสำรวจโดยแคสเปอร์สกี้ แลป พบว่าผู้ใช้ออนไลน์ไทยมากถึง 67% ไม่เชื่อว่าตนเองสามารถตกเป็นเหยื่อบนโลกไซเบอร์ได้ (ภัยไซเบอร์ป่วนไทย“ชาวเน็ต” 67% เสี่ยงเป็นเหยื่อ (ออนไลน์). เข้าถึงได้จาก : http://www.bangkokbiznews.com/news/detail/766588)

จากดัชนีชี้วัดความปลอดภัยไซเบอร์ “แคสเปอร์สกี้ ไซเบอร์ซิเคียวริตี้ อินเด็กซ์” ระบุว่า 3 ตัวชี้วัดหลักที่แสดงถึงภาพรวมของระดับขั้นความอันตรายของผู้ใช้งานอินเทอร์เน็ตพบว่า ในประเทศไทยมีจำนวนผู้บริโภคที่ “ไม่ตระหนัก” หรือ ไม่เชื่อว่าตนเองตกเป็นเป้าการโจมตีทางไซเบอร์ 67% มีผู้ใช้ที่ “ไม่ป้องกัน” หรือ ไม่ติดตั้งโซลูชั่นเพื่อความปลอดภัยบนคอมพิวเตอร์ แทบเล็ต หรือสมาร์ทโฟน 31%

นอกจากนี้ ผู้ที่ “ได้รับผลกระทบ” หรือ ตกเป็นเหยื่อภัยคุกคามทางไซเบอร์ มีอยู่ 46% สูงกว่าค่าเฉลี่ยทั่วโลก 29% เหตุที่เป็นเช่นนี้เนื่องจากคนทั่วไปยังไม่สนใจและคิดว่าเป็นเรื่องไกลตัว ไม่ชอบความยุ่งยาก ซับซ้อน อีกทางหนึ่งมีการใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ รวมถึงช่องโหว่ที่ไม่อัพเดทระบบปฏิบัติการคอมพิวเตอร์ให้เป็นปัจจุบัน

“วิถีชีวิตแบบดิจิทัลได้เพิ่มความเสี่ยง แต่ผู้ใช้งานหลายคนไม่คาดคิดว่าตนเองจะตกเป็นเหยื่อภัยคุกคามจึงไม่ได้ให้ความสำคัญต่อการติดตั้งโปรแกรมเพื่อป้องกันความปลอดภัยบนดีไวซ์ ทั้งไม่ระมัดระวังขณะอยู่บนโลกออนไลน์ จนกลายเป็นเหยื่อได้ง่ายๆ” หากเทียบกับประเทศในเอเชียตะวันออกเฉียงใต้ด้วยกัน นับว่าสถานการณ์ไทยไม่เลวร้ายมากนักโดยประเทศที่ได้รับผลกระทบมากที่สุดอันดับหนึ่งคือ เวียดนาม 59% ตามด้วยอินโดนีเซีย 58% ฟิลิปปินส์ 52% ไทย 46% และมาเลเซีย 42%

สำหรับสถานการณ์ภัยคุกคามที่พบในไทยอันดับต้นๆ ประกอบด้วย การติดไวรัสติดมัลแวร์ ถูกหลอกลวงให้เปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงิน ถูกเจาะระบบเข้าอุปกรณ์ส่วนตัว ถูกโจมตีโดยแรนซัมแวร์ มีปัญหาที่ข้อมูลส่วนบุคคลถูกเปิดเผยโดยบริษัทที่เข้าไปใช้บริการ ถูกแฮกระหว่างเชื่อมอินเทอร์เน็ต รวมถึงถูกขโมยบัญชีออนไลน์ โดยรวมภัยคุกคามที่เข้ามาโจมตีมากที่สุด 2 อันดับแรกยังคงเป็นมัลแวร์ และมัลแวร์เรียกค่าไถ่ หรือ แรนซัมแวร์ แนวโน้มครึ่งปีหลังจากนี้สถานการณ์น่าจะทวีความรุนแรงต่อเนื่อง แรนซัมแวร์สมัยใหม่พุ่งเป้าไปที่การเจาะระบบและเข้ายึดข้อมูลที่มีความสำคัญ แต่ทั้งนี้ความรุนแรงหรือผลกระทบที่เกิดขึ้นอาจต้องพิจารณาเป็นรายกรณีไป “นับเป็นสงครามไซเบอร์ที่แรงจูงใจหลักๆ มักเป็นเรื่องเงิน หรือต้องการโจรกรรมข้อมูลเพื่อเรียกร้องค่าไถ่จากองค์กรธุรกิจ”

ปัจจุบัน ในระดับโลกแคสเปอร์สกี้สามารถตรวจจับมัลแวร์ได้วันละกว่า 3.1 แสนตัว ข้อมูลระบุว่า ค่าใช้จ่ายที่คนไทยต้องจ่ายเพื่อแก้ปัญหามัลแวร์ในแต่ละกรณีที่เกิดขึ้นเฉลี่ยอยู่ที่ 49 ดอลลาร์ นับว่ายังน้อยกว่าเฉลี่ยทั่วโลกที่จ่ายประมาณ 92 ดอลลาร์ ด้านความเสียหายต้องสูญเสียเงินเฉลี่ย 293 ดอลลาร์ เฉลี่ยทั่วโลก 482 ดอลลาร์

ด้านอุปกรณ์ที่ภายในครัวเรือนมีการใช้งานมากที่สุดคือ สมาร์ทโฟน แทบเล็ต โน้ตบุ๊ค และเดสก์ท็อปตามลำดับ ซึ่งแม้ยอดผู้ใช้สมาร์ทโฟนที่เติบโตอย่างก้าวกระโดดและเป็นดีไวซ์ที่เข้าถึง

ผู้บริโภคมากที่สุด แต่อุปกรณ์ที่เป็นเป้าหมายหลัก ยังคงเป็นพีซีทั้งโน้ตบุ๊คและเดสก์ท็อป เนื่องจากสามารถหวังกับผลได้มากกว่า

ส่วนพฤติกรรมการใช้งาน 10 อันดับแรก พบว่าผู้ใช้อินเทอร์เน็ตชาวไทยนิยมชมภาพยนตร์และวีดิโอออนไลน์มากถึง 97% ค่าเฉลี่ยทั่วโลก 88% ใช้อีเมล 96% ทั่วโลก 95% ตามมาด้วยเข้าใช้โซเชียลมีเดีย 94% ทั่วโลก 81% ดาวน์โหลดซอฟต์แวร์หรือแอพพลิเคชั่น 91% ทั่วโลก 75% ชอปปิงออนไลน์เฉลี่ยเท่ากับโดยทั่วโลก 90%

นอกจากนี้ นิยมอ่านข่าวสาร 89% ส่วนทั่วโลก 84% อัพโหลดหรือแชร์คอนเทนท์ 87% ทั่วโลกแค่ 62% เล่นเกมออนไลน์ 84% ทั่วโลก 52% ออนไลน์แบงกิ้ง 82% ทั่วโลก 77% ใช้โปรแกรมแชทหรือวีดิโอคอลล์ 81% ทั่วโลกใช้ 66% ตามลำดับ

แคสเปอร์สกี้ แลป ประเทศไทยประเมินว่า การลงทุนด้านไซเบอร์ซิเคียวริตี้ในประเทศไทยค่อยๆ ขยายตัวมากขึ้นตามลำดับ เพราะข่าวการโจมตีจากแรนซัมแวร์ ความตระหนักรู้ที่เพิ่มมากขึ้น อีกทางหนึ่งการเปลี่ยนผ่านดิจิทัลและการไปสู่อุตสาหกรรม 4.0 ส่งผลให้ธุรกิจองค์กรหันมาโฟกัสการลงทุนด้านซิเคียวริตี้เพื่อเตรียมความพร้อมรับมือภัยไซเบอร์ที่อาจเข้ามาคุกคามได้โดยไม่คาดคิดมาก่อน

สำหรับการแข่งขันระหว่างผู้ให้บริการซอฟต์แวร์โซลูชั่นด้านซิเคียวริตี้นั้น มีความรุนแรงมาต่อเนื่อง จากนี้จะแข่งกันทั้งด้านเทคโนโลยีและราคา แต่ละรายจะมีจุดโฟกัสที่ต่างกันไปและจำต้องทำตลาดรายเซ็กเมนท์ โดยกลุ่มที่คาดว่าจะตื่นตัวสูงมากคือ การเงินการธนาคาร และอุตสาหกรรมการผลิต

ผลสำรวจ “แคสเปอร์สกี้ ไซเบอร์ซิเคียวริตี้ อินเด็กซ์” เป็นความคิดเห็นผู้ใช้งานอินเทอร์เน็ตทั่วโลก สำรวจตามกลุ่มอายุและเพศของแต่ละประเทศ รวมมีผู้ตอบแบบสอบถามจำนวน 17,377 คน จาก 28 ประเทศทั่วโลก เฉพาะประเทศไทยเข้าร่วมตอบคำถามจำนวน 511 คน ผลสำรวจแสดงให้เห็นแนวโน้มเชิงบวก เนื่องจากมีจำนวนผู้ใช้ที่ตระหนักเรื่องความปลอดภัยสูงขึ้น ขณะเดียวกันมีความพร้อมในการปกป้องตนจากภัยไซเบอร์มากขึ้นตามลำดับ

ประเทศไทยมีหลายหน่วยงานที่ถูกจัดตั้งขึ้นเพื่อเข้ามามีบทบาทสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ศูนย์ไซเบอร์กองบัญชาการองทัพไทย ศูนย์ไซเบอร์กองทัพบก เป็นต้น

โดยแต่ละหน่วยงานมีบทบาทและหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งติดตามข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านทางไซเบอร์ ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ เพื่อให้การปฏิบัติการด้านความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเป็นไปด้วยความเรียบร้อย

ภัยคุกคามความมั่นคงทางไซเบอร์ สามารถแบ่งเป็นรูปแบบของภัยคุกคามได้ 9 ลักษณะ ดังนี้

1. เนื้อหาที่เป็นภัย (Abusive Content) ได้แก่ ภัยคุกคามที่เกิดจากการใช้หรือการเผยแพร่ข้อมูลที่เป็นเท็จ หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือ หรือเผยแพร่ข้อมูลที่ไม่ถูกต้อง

ตามกฎหมาย เช่น ลามกอนาจาร รวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลนั้น ๆ (Spam)

2. โปรแกรมไม่พึงประสงค์ (Malicious Code) ได้แก่ ภัยคุกคามที่เกี่ยวข้องกับโปรแกรมหรือชุดคำสั่งที่ถูกพัฒนาขึ้นด้วยความประสงค์ร้ายที่เรียกว่า Malware เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ เช่น Virus, Worm, Trojan หรือ Spyware อาจอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์จากนั้นจึงติดตั้งตัวเองหรือเริ่มทำงานได้ หรืออาจแพร่เข้ามายังเครื่องของผู้ใช้และเริ่มทำงานโดยอัตโนมัติ ซึ่งอาจมาจากหน้าเว็บไซต์ที่มีโค้ดอันตรายที่เผยแพร่ Malware (Malware URL) แก่ผู้เข้าชมเว็บไซต์

3. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) เป็นรูปแบบของภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ประสงค์ร้าย ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบ เป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่ายและการล่อลวงหรือใช้เลขคนต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

4. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) ได้แก่ ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญหรือเปลี่ยนแปลงแก้ไขข้อมูล รวมทั้งสามารถเผยแพร่ข้อมูลที่รั่วไหลได้

5. ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) เป็นภัยคุกคามที่เกิดจากความพยายามเจาะเข้าระบบผ่านทางจุดอ่อนหรือช่องโหว่สาธารณะ หรือผ่านจุดอ่อนหรือช่องโหว่ที่ยังไม่เคยถูกตรวจพบมาก่อน เพื่อเข้าควบคุมหรือเข้าถึงข้อมูลของระบบ รวมถึงความพยายามเจาะระบบผ่านช่องทางการล็อคอินด้วยวิธีการสุ่มบัญชีชื่อผู้ใช้งานและรหัสผ่าน หรือวิธีการทดสอบรหัสผ่านลูกค้า

6. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) เป็นภัยคุกคามที่เกิดจากการเจาะระบบได้สำเร็จ ทำให้ผู้ไม่ประสงค์ดีสามารถควบคุมระบบและกระทำการต่าง ๆ เช่น การปรับเปลี่ยนหน้าเว็บไซต์เพื่อทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ หรือเข้าถึงและเปลี่ยนแปลงข้อมูลสำคัญในระบบได้

7. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) เป็นภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองการให้บริการ จนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ สาเหตุอาจเกิดจากการโจมตีที่บริการของระบบโดยตรงหรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบก็ได้

8. ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) งานที่เกิดจากการฉ้อฉล ฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ เช่น การสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกขโมยรหัสผ่านสำหรับล็อกอินจากผู้ใช้ เป็นต้น

9. ลักษณะอื่นๆ นอกเหนือจากที่กล่าวมาข้างต้น ซึ่งมักจะมาในรูปแบบใหม่ หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามลักษณะอื่นๆ ในข้อนี้มีจำนวนมากขึ้น ก็จะมีการปรับปรุงการจัดแบ่งลักษณะของภัยคุกคามใหม่อีกครั้ง

จากข้อมูลสถิติพบว่าในปี 2558 มีการแจ้งเกี่ยวกับภัยคุกคามทางไซเบอร์กว่า 2 ล้าน IP ไม่ซ้ำกัน และยังสามารถแบ่งสถิติเป็นตามการโจมตีออกเป็น 2 ประเภท คือ องค์กรในประเทศถูกใช้เป็นฐานในการโจมตี และ องค์กรในประเทศตกเป็นเหยื่อในการโจมตี ตามแผนภาพที่ 3-1

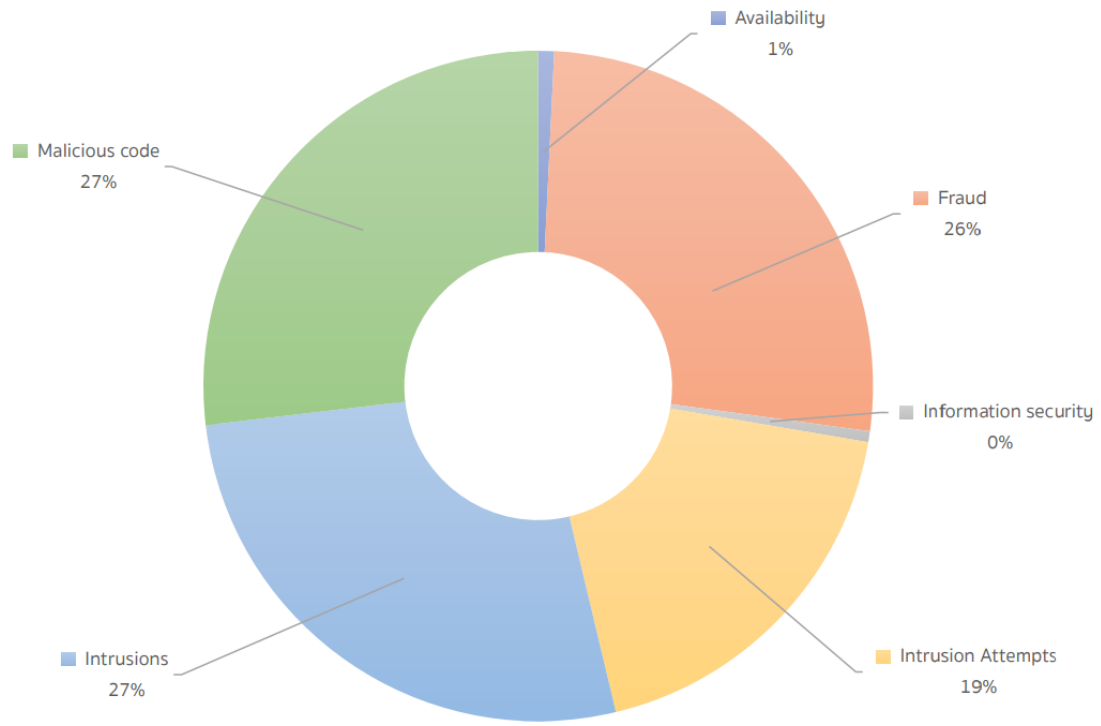
แผนภาพที่ 3-1 : จำนวนหมายเลข IP ที่ได้รับแจ้งตามภัยคุกคาม

ประเภทภัยคุกคาม		จำนวนไอพีที่ได้รับแจ้งตามประเภทภัยคุกคาม		
		จำนวนรวม	องค์กรในประเทศไทย ถูกใช้เป็นฐานในการโจมตี	องค์กรในประเทศไทย ตกเป็นเหยื่อในการโจมตี
1. Abusive Content		8	0	8
2. Malicious Code	Malware	2,093,979	1,110,867	903,112
	Malware URL	907	907	0
3. Information Gathering	Scanning	31	31	0
4. Information Security	Data Leakage	81	0	81
5. Intrusion Attempts	Brute Force	570	570	0
6. Intrusion	Web Defacement	430	0	430
7. Availability	Open DNS Resolver	46,463	46,463	0
	DDoS	5	0	5
8. Fraud	Web Phishing	540	520	20
9. Others	Open Proxy Server	5,418	5,418	0

ที่มา : Annual Report 2015

ในปี 2559 ภัยคุกคามประเภท Malicious code และ Intrusions ได้รับ แจ้งมากที่สุด โดยมีสัดส่วนเท่ากัน รองลงมาคือภัยคุกคามประเภท Fraud และ Intrusion attempts ตามลำดับ ในขณะที่ภัยคุกคามประเภท Availability และ Information security ขยับตัวสูงขึ้นในช่วงเดือนธันวาคม ซึ่งสอดคล้องกับการเพิ่มขึ้นของภัยคุกคามประเภท Intrusions ในช่วงเวลาเดียวกัน จากการวิเคราะห์พบว่าสาเหตุเกิดจากการพยายามโจมตีระบบเว็บไซต์ หน่วยงานภาครัฐด้วยจุดประสงค์ทางการเมือง ตามแผนภาพที่ 3-2

แผนภาพที่ 3-2 : สถิติภัยคุกคามแบ่งตามลักษณะการโจมตี

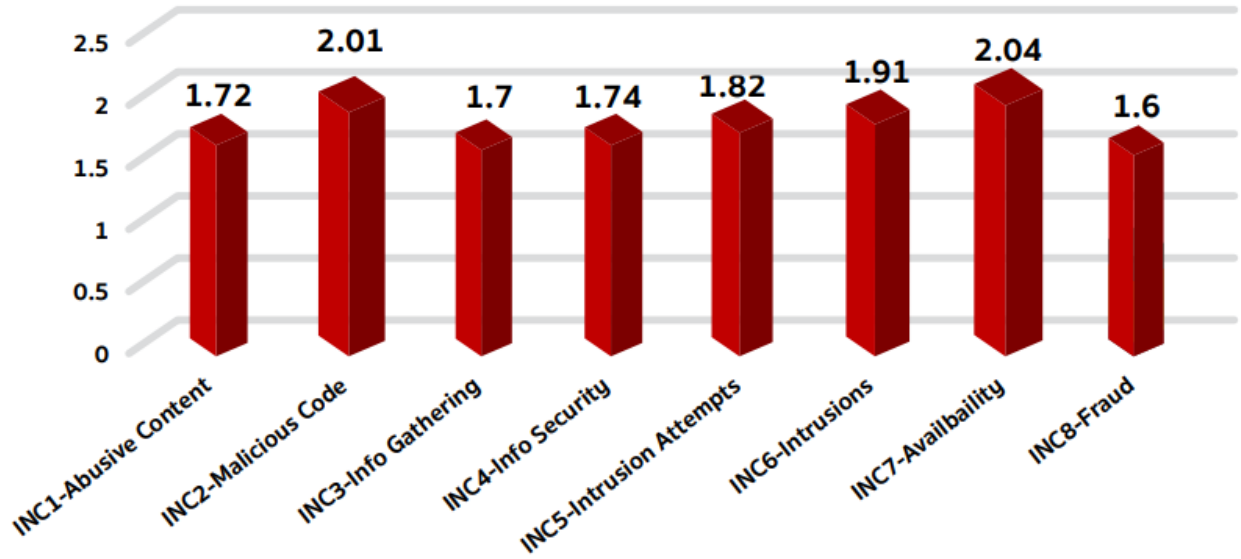


ที่มา : Annual Report 2016

นอกจากนั้น มีข้อมูลระบุว่าหน่วยงานภาครัฐที่เคยประสบเหตุภัยคุกคามไซเบอร์ คิดเป็นสัดส่วนสูงถึงประมาณร้อยละ 90 เหตุภัยคุกคามไซเบอร์ที่สร้างความเสียหายหรือผลกระทบต่อหน่วยงานมากที่สุด 3 อันดับแรก พิจารณาเปรียบเทียบจากค่าเฉลี่ยของระดับผลกระทบโดยรวมของหน่วยงาน ทั้งหมด ได้แก่ เหตุจากการถูกโจมตีความพร้อมใช้งานของระบบ (Availability) เหตุจากการถูกโปรแกรมไม่ พึงประสงค์ (Malicious Code) และเหตุจากการถูกบุกรุกหรือเจาะระบบ (Intrusions) และพบว่า เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อหน่วยงานอิสระ คือ Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ) หน่วยงานของศาล คือ Intrusions (การบุกรุกหรือถูกเจาะระบบ) กระทรวง คือ Malicious Code (โปรแกรมไม่พึงประสงค์) สำนักนายกรัฐมนตรี คือ Abusive Content (เนื้อหาที่เป็นภัย) องค์กรประกอบวิชาชีพ องค์การมหาชน รัฐวิสาหกิจ และมหาวิทยาลัยของรัฐ คือ Availability (ความพร้อมใช้งานของระบบ)

อย่างไรก็ตามในภาพรวมระดับความเสียหายหรือผลกระทบที่หน่วยงานได้รับจากภัยคุกคามทั้งหมดโดยรวมยังอยู่ในมีระดับต่ำถึงต่ำมาก

แผนภาพที่ 3-3 : ระดับความเสียหาย หรือผลกระทบจากเหตุภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐ



หมายเหตุ: จากการคำนวณคะแนนค่าเฉลี่ยรวมของผลกระทบจากเหตุภัยคุกคามแต่ละประเภทของหน่วยงานทั้งหมด ในระดับคะแนน ตั้งแต่ 1-5 โดยที่ 1 หมายถึง ได้รับผลกระทบน้อยที่สุด และ 5 หมายถึง ได้รับผลกระทบมากที่สุด

ที่มา : Cybersecurity Survey 2016

ตารางที่ 3-1 : เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดของหน่วยงานภาครัฐ

หน่วยงานภาครัฐ	**เหตุภัยคุกคามที่สร้างความเสียหายสูงสุด**
หน่วยงานอิสระ	Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ)
หน่วยงานของศาล	Intrusions (การบุกรุกหรือถูกเจาะระบบ)
กระทรวง	Malicious Code (โปรแกรมไม่พึงประสงค์)
สำนักนายกรัฐมนตรี	Abusive Content (เนื้อหาที่เป็นภัย)
องค์กรประกอบวิชาชีพ / องค์การมหาชน / รัฐวิสาหกิจ / มหาวิทยาลัยของรัฐ	Availability (ความพร้อมใช้งานของระบบ)

ที่มา : Cybersecurity Survey 2016

ในส่วนของภาคเอกชน พบว่าเหตุภัยคุกคามที่สร้างความเสียหายสูงสุดต่อ ธุรกิจการเงิน (Bank) คือ Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) ธุรกิจหลักทรัพย์ คือ Intrusions (การบุกรุกหรือเจาะ ระบบ) และ Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์) ธุรกิจชำระเงินและ

ประกันภัย คือ Availability (ความพร้อมใช้งานของระบบ) ธุรกิจพลังงาน คือ Abusive Content (เนื้อหาที่เป็นภัย) โรงพยาบาล เทคโนโลยี สารสนเทศและการสื่อสาร และขนส่งและโลจิสติกส์ คือ Malicious Code (โปรแกรมไม่พึงประสงค์)

ตารางที่ 3-2 : เหตุภัยคุกคามที่สร้างความเสียหายสูงสุดของภาคเอกชน

ภาคเอกชน	เหตุภัยคุกคามที่สร้างความเสียหายสูงสุด
ธุรกิจการเงิน (Bank)	Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์)
ธุรกิจหลักทรัพย์	Intrusions (การบุกรุกหรือเจาะ ระบบ) / Fraud (การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์)
ธุรกิจชำระเงินและประกันภัย	Availability (ความพร้อมใช้งานของระบบ)
ธุรกิจพลังงาน	Abusive Content (เนื้อหาที่เป็นภัย)
โรงพยาบาล / เทคโนโลยี สารสนเทศและการสื่อสาร /การขนส่งและโลจิสติกส์	Malicious Code (โปรแกรมไม่พึงประสงค์)

ที่มา : Cybersecurity Survey 2016

ปัญหาจากการดำเนินการต่อภัยคุกคามทางไซเบอร์ของประเทศไทย

จากการศึกษาเกี่ยวกับการดำเนินการต่อภัยคุกคามทางไซเบอร์ รวมถึงสภาวการณ์เกี่ยวกับปัญหาและผลกระทบจากภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย ประกอบกับการ สัมภาษณ์เชิงลึกต่อผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานต่างๆ พบว่าการความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยยังมีปัญหาในการดำเนินการด้านต่างๆ ซึ่งผู้วิจัยสามารถสรุปแบ่งเป็น 4 ประเด็น ดังนี้

1. การบูรณาการการดำเนินงานรักษาความปลอดภัยไซเบอร์

จากการศึกษาข้อมูลพบว่าการดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ถึงแม้ว่าในปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์มากขึ้นแต่องค์กรต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและบางครั้งมีความขัดแย้งกัน ประกอบกับการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ จากการศึกษาข้อมูลปัญหาการบูรณาการการดำเนินงานรักษาความปลอดภัยไซเบอร์มีปัจจัยต่างๆ อาจพอสรุปได้ดังนี้

1.1 ปัจจัยจากแนวความคิดของฝ่ายต่างๆ ปัญหาเรื่องการบูรณาการเริ่มต้นจากวิธีคิดของฝ่ายต่างๆ ซึ่งมักยึดติดกับตำแหน่ง กลุ่มและองค์กรที่สังกัด ประกอบกับระบบการศึกษาและการกล่อมเกลาทางสังคม เช่น “รู้สิ่งไรไม่สู้รู้วิชา รู้รักษาตัวรอดเป็นยอดดี” จึงทำให้บุคลากรในสาขาต่างๆ ของประเทศไทยใช้วิชาความรู้ที่มีความเชี่ยวชาญเฉพาะด้านที่ตนมีเพื่อการเอาตัวรอดปลอดภัยไว้ก่อนเป็นหลักในการดำรงชีวิต กลายเป็นวิธีคิดกระแสหลักที่ครอบงำจิตสำนึกของผู้คนส่วนใหญ่ในสังคม ในขณะที่ความคิดเชิงระบบแบบองค์รวมกลายเป็นสิ่งถูกละเลย เมื่อแต่ละคน แต่ละองค์กร ต่างพยายามรักษาตัวรอดด้วยการแย่งชิงทรัพยากรให้ได้มากที่สุด การบูรณาการเพื่อแก้ปัญหาต่างๆ ก็ยากที่จะเกิดขึ้นได้ เพราะเมื่อไรก็ตามที่ปัญหานั้นแก้ไขได้สำเร็จ ต่างฝ่ายต่างก็พยายามช่วงชิงเอาไปเป็นผลงานของตนเอง เพื่อนำความสำเร็จเป็นฐานในการขอเลื่อนตำแหน่ง เพิ่มอำนาจ ขยายทรัพยากรและงบประมาณต่อไป ผู้บริหารส่วนมากมีความปรารถนาอย่างจริงใจในการแก้ไขปัญหาของประเทศและเชื่อมการบูรณาการของภาคส่วนต่างๆ เป็นเงื่อนไขสำคัญในการปฏิบัติเพื่อแก้ไขปัญหาเหล่านั้น แต่ทำไมการบูรณาการทั้งในแง่ของการวิเคราะห์ปัญหาและการนำยุทธศาสตร์ไปสู่การปฏิบัติจึงเกิดขึ้นได้ค่อนข้างยาก มีเพียงบางเรื่องและบางหน่วยงานเท่านั้นที่พอจะเห็นร่องรอยของการบูรณาการอยู่บ้าง แต่ส่วนใหญ่แล้วการคิดวิเคราะห์และการปฏิบัติมีแนวโน้มเป็นไปในทิศทางแบบต่างคนต่างทำมากกว่า ประเด็นดังกล่าวจึงทำให้สังคมไทยมีโอกาสน้อยมากที่จะเกิดการเกิดบูรณาการ การกำหนดแนวทางแก้ปัญหา และขับเคลื่อนยุทธศาสตร์ไปสู่การปฏิบัติอย่างเป็นระบบ

ในส่วนของหน่วยงานและองค์กรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีการให้ความสำคัญกับความมั่นคงทางไซเบอร์ที่แตกต่างกัน มีการจัดองค์กรที่แตกต่างกันออกไปตามภารกิจและการให้ความสำคัญกับเรื่องความมั่นคงลอดภัยทางไซเบอร์ไปคนละทิศละทาง โดยหน่วยงานระดับนโยบายอย่างเช่น คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) ให้ความสำคัญและกำลังดำเนินการบรรจุเนื้อหาเกี่ยวกับความมั่งคงปลอดภัยทางไซเบอร์ไว้ในนโยบายและแผนแม่บทที่กำลังดำเนินการอยู่ ส่วนกระทรวงเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งเป็นหน่วยงานของรัฐบาลที่รับผิดชอบโดยตรงมีความพยายามแสวงหาความร่วมมือระหว่างกระทรวงที่เกี่ยวข้อง กระทรวงกลาโหมมุ่งเน้นการ ติดตาม และป้องปรามสื่อที่มีการละเมิดต่อสถาบันพระมหากษัตริย์ สำหรับภาคเอกชนบางรายกลับมองปัญหาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องในระดับรองลงไป สิ่งเหล่านี้ได้ก่อให้เกิดปัญหาการบูรณาการระหว่างองค์กรและหน่วยงาน ซึ่งเป็นประเด็นสำคัญ อีกทั้งประเทศไทยยังไม่มีการจัดองค์กรกลางประสานงานเรื่องความมั่นคงทางไซเบอร์โดยเฉพาะ มีแต่ความร่วมมือกับหน่วยงานความมั่นคงในลักษณะการจัดการเฉพาะกิจในรูปแบบของคณะกรรมการต่างๆ เท่านั้น ซึ่งทำให้เกิดผลอย่างเป็นรูปธรรมได้ยาก ส่วนหน่วยที่บังคับใช้กฎหมาย คือ สำนักงานตำรวจแห่งชาติ มีบทบาทหน้าที่ในการดำเนินคดีเกี่ยวกับภัยคุกคามความมั่นคงของชาติโดยตรง มีกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ รับผิดชอบ แต่ก็ยังไม่มีการประสานกับเหล่าทัพอย่างเป็นรูปธรรม สำหรับในระดับบริษัทเอกชนรายใหญ่ที่เป็น Gateway ของการสื่อสารผ่านระบบอินเทอร์เน็ตคือ TOT และ CAT Telecom ก็ไม่มีการจัดองค์กรเพื่อประสานงานโดยตรงกับกองทัพ เพราะยึดถือลูกค้าและผลกำไรเชิงธุรกิจมากกว่าความมั่นคงของชาติ

การวางแนวความคิดแบบองค์รวมและการรักษาสังคมส่วนรวมให้รอดนั้น ถือเป็นเสาหลักที่จะทำให้เกิดการบูรณาการในการปฏิบัติงาน หากสามารถวางแนวคิดแบบนี้ให้เติบโตและขยาย

ออกไปโดยเริ่มจากหน่วยงานภาครัฐไปสู่ภาคเอกชนและภาควิชาการได้ โอกาสที่จะเกิดการคิดและทำงานแบบบูรณาการในสังคมไทยก็จะขยายออกไปมากยิ่งขึ้น ยิ่งการทำงานแบบบูรณาการขยายออกไปมากเท่าไร โอกาสที่จะทำให้สังคมมีสมรรถนะในการแก้ปัญหาต่างๆ ก็มีสูงขึ้นตามไปด้วย และจะนำไปสู่ความเข้มแข็งของประเทศต่อไป

1.2 ปัจจัยด้านการประสานงาน เนื่องจากยังไม่มีหน่วยงานกลางด้านไซเบอร์ของประเทศ ซึ่งเป็นประเด็นปัญหาในระดับประเทศ จึงเกิดปัญหาเรื่องการประสานงานและการบูรณาการด้านการข่าวระหว่างกลุ่มโครงสร้างพื้นฐานทางไซเบอร์ที่สำคัญของประเทศ (Critical Information Infrastructure : CII) หากประเทศไม่มีหน่วยงานกลางในการบูรณาการให้เกิดการทำงานร่วมกัน การดำเนินยุทธศาสตร์ของภาครัฐต่อภัยคุกคามทางไซเบอร์ก็จะไม่มีทิศทางที่ชัดเจน กระบวนการที่ไม่มีหน่วยงานกลางด้านไซเบอร์ระดับประเทศทำให้สถานการณ์ด้านไซเบอร์ของประเทศไม่ค่อยพัฒนาและไม่เกิดการบูรณาการมาเท่าที่ควรมา 5 – 6 ปีแล้ว เพื่อให้เกิดการบูรณาการประเทศต้องมีต้องมีหน่วยงานกลางด้านไซเบอร์ Cyber Security Agency (CSA) ซึ่งปัจจุบันมีแผนตั้งไว้แล้ว โดยให้ Cyber Security Agency (CSA) สังกัดกระทรวงเศรษฐกิจดิจิทัล แต่ต้องรอพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ผ่านสภานิติบัญญัติแห่งชาติก่อน ปัจจุบันพระราชบัญญัติฯ ฉบับนี้ยังไม่ผ่านจึงให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เป็นผู้ดำเนินการในฐานะเป็นหน่วยงานกลางชั่วคราวทำหน้าที่เป็น Cyber Security Agency (CSA) ไปก่อน

1.3 ปัจจัยด้านงบประมาณ การใช้งบประมาณด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ไม่คุ้มค่า เพราะหน่วยงานของประเทศไทยยังมีการปฏิบัติในลักษณะต่างคนต่างทำ การต่อต้านภัยคุกคามความมั่นคงทางไซเบอร์นั้นต้องใช้งบประมาณในการลงทุนด้านเทคโนโลยีจำนวนมาก ซึ่งการที่ยังมีการปฏิบัติในลักษณะต่างคนต่างทำนั้นเป็นการใช้งบประมาณแบบไม่คุ้มค่า ด้วยสาเหตุที่หน่วยงานต่างๆ จัดตั้งงบประมาณซื้อคอมพิวเตอร์และระบบต่างๆ เอง แต่ไม่มีหน่วยงานใดเข้ามาดูแลและตรวจสอบเรื่องระบบการรักษาความปลอดภัยทางไซเบอร์ สิ่งที่กระทรวงเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคมดำเนินการอยู่ คือ สำนักงานรัฐบาลอิเล็กทรอนิกส์ ซึ่งสามารถกำหนดการทำงานในลักษณะเข้ามารวมศูนย์ได้ แต่ปัญหาคือทุกหน่วยงานต้องการจัดซื้อคอมพิวเตอร์และระบบต่างๆ เอง

ปัจจุบันหน่วยราชการหลายแห่งให้เอกชนเข้ามาเป็นผู้ติดตั้งทั้งที่เป็นหน่วยงานด้านความมั่นคง จึงเกิดปัญหาในเรื่องของความปลอดภัยและไว้วางใจ สำนักงานรัฐบาลอิเล็กทรอนิกส์ได้ให้ความสำคัญและตระหนักถึงปัญหาเรื่องการพึ่งพาภาคเอกชน แต่ฝ่ายปฏิบัติเห็นว่าแม้จะอยู่กับสำนักงานรัฐบาลอิเล็กทรอนิกส์ ถ้าไม่ได้มาตรฐานก็สามารถถูกโจมตีได้ ดังนั้น สำนักงานรัฐบาลอิเล็กทรอนิกส์จึงมีการจัดทำมาตรฐานขึ้นเพื่อป้องกันข้อมูลไม่ให้หลุดออกไปหรือถูกโจมตีทางระบบได้ นอกจากนั้นยังมีแอนตี้ไวรัสหรือไฟร์วอลล์ที่ได้ตั้งมาตรฐานไว้แล้ว อย่างไรก็ตามยังมีหน่วยงานภาครัฐเข้ามาใช้บริการไม่มาก เนื่องจากบางหน่วยงานต่างๆ ยังกังวลอีกว่า การที่หน่วยงานกลางนำ Server มาติดตั้งและสามารถ Monitor ข้อมูลนั้นจะทำให้ข้อมูลรั่วไหลได้

ถ้าประเทศไทยต้องการใช้งบประมาณในการลงทุนด้านระบบไซเบอร์ภาครัฐให้เกิดความคุ้มค่า จะต้องพยายามทำเรื่องการรวมศูนย์ข้อมูล และต้องมีกติกาและมาตรฐานที่ชัดเจนมาควบคุม ยกตัวอย่างประเทศสหรัฐฯ ที่มีหน่วยงานกลาง เป็นผู้ควบคุมกำกับดูแลทั้งหมด

1.4 ปัจจัยด้านข้อมูลระหว่างฐานข้อมูล ทั้งภายในหน่วยงาน และระหว่างหน่วยงานภาครัฐ มีหลายสาเหตุ เช่น การใช้รหัสอ้างอิงที่แตกต่างกัน รูปแบบและชนิดของข้อมูลต่างกัน หรือการอ้างอิงมาตรฐานต่างกัน ซึ่งปัญหานี้ สำนักงานรัฐบาลอิเล็กทรอนิกส์กำลังดำเนินการแก้ปัญหา สำนักงานรัฐบาลอิเล็กทรอนิกส์จะเน้นที่งานภาครัฐ ฉะนั้น เครือข่ายจะเป็นเครือข่ายอินทราเน็ตที่เป็นเครือข่ายปิดในภาครัฐเท่านั้น สำหรับหน่วยงานภาครัฐที่ได้เข้าไปติดต่อเพื่อนำอุปกรณ์สำหรับตรวจสอบภัยคุกคามไปติดตั้งแล้ว ได้แก่ กรมป้องกันและบรรเทาสาธารณภัย สำนักงานตำรวจแห่งชาติ สำนักงบประมาณ และกรมศุลกากร

ปัญหาการบูรณาการการดำเนินงานรักษาความปลอดภัยไซเบอร์ขาดนั้น สามารถศึกษาจากยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จากประเทศต่างๆ เพื่อนำมารับปรุงการดำเนินการได้ ยกตัวอย่างเช่น สหภาพยุโรปที่พยายามจะทำให้มีตลาดร่วมในด้านดิจิทัล (Digital Single Market) เพื่อเพิ่มศักยภาพของตลาดดิจิทัลภายในภูมิภาค สามารถแข่งขันกับประเทศคู่แข่งในภูมิภาคอื่นๆ คณะกรรมาธิการยุโรปมองว่าการเป็นตลาดร่วมในด้านดิจิทัล ความมั่นใจและความมั่นคงปลอดภัยบนโลกไซเบอร์จึงกลายมาเป็นรากฐานที่สำคัญของการเป็นตลาดร่วมในด้านดิจิทัล ซึ่งมีความคล้ายกับยุทธศาสตร์ไทยแลนด์ 4.0 ของรัฐบาลไทย สหภาพยุโรปได้กำหนดยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งสหภาพยุโรป โดยให้ความสำคัญกับการบรรลุความมั่นคงปลอดภัยไซเบอร์โดยการเพิ่มขีดความสามารถ สร้างความพร้อม การบูรณาการความร่วมมือในการแลกเปลี่ยนข้อมูลและความตระหนักถึงภัยคุกคามทางไซเบอร์และความปลอดภัยของข้อมูลทั้งภาครัฐและเอกชน ทั้งระดับประเทศและระดับสหภาพยุโรปเป็นอันดับแรก

ในส่วนของโครงสร้างหน่วยงานรักษาความปลอดภัยบนโลกไซเบอร์ของออสเตรเลีย แบ่งเป็น 3 เสาหลัก คือ ด้านนโยบาย (Policy) ด้านปฏิบัติการ (Operations) และด้านการดำเนินพันธกิจร่วมกับองค์กรนานาชาติ (International Engagement) โดยให้ความสำคัญกับการบูรณาการในทุกด้าน ได้แก่

1. ด้านนโยบาย (Policy) กำกับดูแลโดยที่ปรึกษาพิเศษด้านนโยบายรักษาความปลอดภัยไซเบอร์ สำนักนายกรัฐมนตรี มีบทบาทนำในปัจจุบันเกี่ยวกับนโยบายการรักษาความปลอดภัยบนโลกไซเบอร์และเป็นหลักในกำกับดูแลและการกำหนดนโยบายเกี่ยวกับยุทธศาสตร์ด้าน Cyber Security แบบบูรณาการ เพื่อให้เกิดการดำเนินงานอย่างมีประสิทธิภาพ ร่วมกับภาคเอกชน ชุมชนการวิจัย และประเทศคู่ค้า

2. ด้านปฏิบัติการ (Operations) กำกับดูแลโดยศูนย์รักษาความปลอดภัยทางไซเบอร์ (Australian Cyber Security Centre : ACSC) กระทรวงกลาโหม เป็นหน่วยงานที่ได้รับความสำคัญในการรักษาความปลอดภัยบนโลกไซเบอร์ มีความเชี่ยวชาญและความสามารถในการรักษาความปลอดภัยบนโลกไซเบอร์ให้กับการดำเนินงานของรัฐบาล สามารถสนับสนุนองค์กรระดับปฏิบัติการได้อย่างทั่วถึง ACSC มีสามารถในการประสานการปฏิบัติกับภาคเอกชนได้อย่างคล่องตัว เพื่อสนับสนุนภาคเอกชนในการโต้ตอบกับภัยคุกคามทางไซเบอร์ โดยสามารถบูรณาการร่วมกันระหว่างรัฐบาล ภาคเอกชน ชุมชนการวิจัย และประเทศคู่ค้า

3. ด้านการดำเนินพันธกิจร่วมกับองค์กรนานาชาติ (International Engagement) กำกับดูแลโดยเอกอัครราชทูตไซเบอร์ กระทรวงการต่างประเทศและการค้า รัฐมนตรีว่าการกระทรวงการต่างประเทศของออสเตรเลีย จะแต่งตั้งเอกอัครราชทูตไซเบอร์ เพื่อความ

พยายามในการประสานความร่วมมือเกี่ยวกับ Cyberspace ระหว่างประเทศ เอกอัครราชทูตไซเบอร์จะมีบทบาทสำคัญในการประสานการทำงานอย่างใกล้ชิดกับที่ปรึกษาพิเศษด้านการรักษาความปลอดภัยไซเบอร์ เพื่อให้เกิดการบูรณาการด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างประเทศ

สำหรับประเทศไทยมีการระบุเรื่องการบูรณาการการด้านความมั่นคงปลอดภัยทางไซเบอร์ไว้ใน มาตรา 5 (1) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และผู้บริหารพยายามกำหนดแนวทางการดำเนินงานที่ชัดเจนเพื่อให้เกิดการบูรณาการร่วมกันระหว่างหน่วยงานภาครัฐ ภาคเอกชน ฯลฯ แต่กระนั้น ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่ได้ถูกประกาศใช้ การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยจึงยังมีลักษณะต่างฝ่ายต่างทำ ตลาดเทคโนโลยีต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและขัดแย้งกัน และการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ

นอกจากนั้น เพื่อให้การบูรณาการยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์สามารถดำเนินการร่วมกันได้อย่างมีประสิทธิภาพ ภาครัฐจะต้องพิจารณาถึงบทบาทของผู้มีส่วนได้เสียและกำหนดกรอบการดำเนินงานร่วมกัน ซึ่งต้องมีแนวทางและวิธีปฏิบัติในการส่งเสริมความมั่นคงของชาติที่มีมาตรฐาน โดยกรอบการดำเนินงานจะต้องมีการสร้างแนวทางเพื่อทำความเข้าใจถึงภัยคุกคาม และมีแนวทางสำหรับการลดความเสี่ยง จากภัยคุกคามทางไซเบอร์โดยเฉพาะ เพื่อเป็นการช่วยให้ทุกภาคส่วนสามารถจัดลำดับความสำคัญ และดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญได้รวดเร็วและมีประสิทธิภาพมากขึ้น รัฐต้องเป็นผู้นำในการกำหนดเป้าหมายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สร้างโครงการหรือโปรแกรมสำหรับปกป้องโครงสร้างสารสนเทศพื้นฐานสำคัญของชาติอย่างเป็นระบบ เพื่อปกป้องภัยคุกคาม และมอบหมายหน้าที่รับผิดชอบต่อผู้ที่มีหน้าที่และผู้มีส่วนได้ส่วนเสีย เพื่อสร้างให้เกิดความร่วมมือ และสามารถประสานการปฏิบัติงาน รวมทั้งต้องมีการวิเคราะห์ความเสี่ยงและให้ข้อมูลด้านความเสี่ยงมาตรการป้องกัน และการรับมืออย่างมีประสิทธิภาพ

กรอบการดำเนินงานจะเป็นแนวทางให้องค์กรภาครัฐและภาคเอกชน สามารถทำความเข้าใจ ในการปฏิบัติงานและการลงทุนด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีความสอดคล้องกับความต้องการในองค์กรแต่ละองค์กรและประสานสอดคล้องกับมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของชาติ แม้กรอบการดำเนินงานอาจมีแนวปฏิบัติด้านการรักษาความปลอดภัยที่ไม่ได้เหมาะสมกับองค์กรทุกองค์กร แต่ถือเป็นจุดเริ่มต้นที่ดีในการบูรณาการการดำเนินงานรักษาความปลอดภัยไซเบอร์สำหรับทุกองค์กร

2. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศใช้

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์ โดยให้อำนาจพิเศษแก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. มีอำนาจสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความ

มั่นคงปลอดภัยไซเบอร์ในทิศทางเดียวกัน และในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง กปช. มีอำนาจอนุมัติให้เจ้าหน้าที่เข้าถึงการติดต่อสื่อสารทุกรูปแบบของประชาชน เช่น ไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด หรือดำเนินการตามมาตรการที่เหมาะสม เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และระงับยับยั้งความเสียหายที่จะเกิดขึ้น โดยไม่ต้องขอคำสั่งศาล

คณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านการสื่อสารมวลชน สภาขับเคลื่อนการปฏิรูปประเทศ (สปท.) เสนอปรับ (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (รายงานของคณะกรรมาธิการขับเคลื่อนการปฏิรูปประเทศด้านการสื่อสารมวลชน เรื่อง ผลการศึกษาและข้อสังเกตร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคง ปลอดภัยไซเบอร์, การประชุมสภาขับเคลื่อนการปฏิรูปประเทศ ครั้งที่ 60/2559, 28 พ.ย.59) ตามแนวทางและยุทธศาสตร์ของเหล่าทัพ กำหนดมาตรการตอบโต้เชิงรุก ให้หน่วยงานความมั่นคงทางทหารและตำรวจร่วมเป็นคณะกรรมการทั้งระดับนโยบายและปฏิบัติการ โดยหนึ่งในประเด็นที่เสนอคือการปรับสัดส่วนสัดส่วนคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้นายกรัฐมนตรีเป็นประธาน มีรัฐมนตรีกลาโหมและรัฐมนตรีดิจิทัลเป็นรองประธาน 2 คน และเพิ่มกรรมการอีกรวม 10 ตำแหน่ง และให้ พลเอก ประยุทธ์ จันทร์โอชา แต่งตั้งเพื่อปฏิบัติหน้าที่ไปพลางก่อน ในระหว่างที่กฎหมายยังไม่แล้วเสร็จ โดยในรายงานซึ่งประมวลจากความคิดเห็นจากกระทรวงดิจิทัล กระทรวงกลาโหม เหล่าทัพ ตำรวจ สภาความมั่นคงแห่งชาติ และสำนักข่าวกรอง เสนอให้แก้ไขใน 4 แนวทาง ดังนี้

1. กำหนดกรอบแนวคิดในการยกร่างกฎหมายให้ชัดเจน สอดคล้องกับแนวทางและยุทธศาสตร์ของหน่วยงานความมั่นคง โดยเฉพาะเหล่าทัพ กำหนดให้เห็นถึงมาตรการป้องกัน มาตรการตอบโต้เชิงรุก และมาตรการพัฒนาขีดความสามารถ

2. กำหนดผู้รับผิดชอบหลักในการกำกับดูแล ทั้งในภาวะปกติและภาวะฉุกเฉิน

3. แก้ไขรายละเอียดของ ร่าง พระราชบัญญัติฯ ตามที่หน่วยงานความมั่นคงทางทหารและฝ่ายตำรวจเสนอแนะ (เช่น เพิ่มบทกำหนดโทษผู้ไม่ให้ความร่วมมือ)

4. ให้หน่วยงานความมั่นคงทางทหารและฝ่ายตำรวจ ร่วมเป็นคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับนโยบายและระดับปฏิบัติการ

ประเด็นปัญหาการบูรณาการส่วนหนึ่งมาจากการที่ปัจจุบัน ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ อยู่ในขั้นตอนการพิจารณายังไม่ได้มีการประกาศใช้ ดังนั้นการปฏิบัติภารกิจเชิงรุกทั้งภายในและภายนอกประเทศ จึงยังไม่มีข้อกฎหมายรองรับการดำเนินการในปัจจุบันซึ่งยังเป็นข้อจำกัดที่สำคัญ แต่ทั้งนี้ ฝ่ายความมั่นคงของไทยยังมองปัญหาภัยคุกคามความมั่นคงทางไซเบอร์ โดยเน้นไปที่ “เนื้อหา” เป็นหลัก ซึ่งไม่ใช่ปัญหาทาง “เทคนิค” เช่น การโจมตีระบบ เป็นต้น ข้อเสนอส่วนใหญ่ของฝ่ายความมั่นคงจึงมุ่งเน้นการเพิ่มอำนาจเจ้าหน้าที่ให้ดักฟังและสอดแนมข้อมูล วางมาตรการระบุตัวตน ฯลฯ เพื่อติดตามตัวผู้กระทำผิดมาดำเนินคดี ซึ่งปัญหาทั้งด้านเนื้อหาและเทคนิคควรให้ความสำคัญเท่าๆ กัน และควรเน้นการยกระดับขีดความสามารถในการรักษาความปลอดภัยของระบบ การประสานงานระหว่างรัฐกับเอกชน และการยกระดับศักยภาพของบุคลากร ซึ่งมีความจำเป็นต่อการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ เพราะปัจจุบันได้มีการนำระบบเครือข่ายไปใช้ในระบบโครงสร้างพื้นฐานที่สำคัญต่างๆ ของประเทศ เช่น ระบบโทรคมนาคม ระบบขนส่ง

มวลชน ระบบโรงผลิตไฟฟ้า เป็นต้น ซึ่งถือว่าเป็นอันตรายอย่างยิ่งต่อความมั่นคง ในกรณีที่มีผู้ประสงค์ร้ายลอบเข้าโจมตีระบบผ่านเครือข่ายคอมพิวเตอร์ ดังนั้นเพื่อป้องกันมิให้เกิดผลกระทบต่อความมั่นคงทางด้านต่างๆ ของประเทศ

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศนั้นต้องมีนั้นคือ (1) ยุทธศาสตร์ (2) กฎหมายรองรับ เพื่อให้ยุทธศาสตร์บังคับใช้ได้ ปัจจุบันยุทธศาสตร์มีแล้ว แต่พระราชบัญญัติฯ ยังไม่ผ่าน (3) หากพระราชบัญญัติฯ ผ่านแล้วต้องตั้งหน่วยงานกลางด้านไซเบอร์ (4) จัดทำนโยบาย เพื่อให้ทราบถึงบทบาทหน้าที่ต้องมีแผนรับมือด้านไซเบอร์ และ (5) สิ่งที่สำคัญอย่างมาก คือ ต้องมีแผนรับมือด้านไซเบอร์ของประเทศ ซึ่งในปัจจุบันมีเพียง ยุทธศาสตร์ด้านไซเบอร์เท่านั้น อีก 4 ส่วนยังไม่ได้ดำเนินการ มีการประชุมคณะกรรมการความมั่นคงปลอดภัยไซเบอร์ ครั้งแรกเมื่อปี 56 หลังจากนั้นผ่านมา 5 ปี ยังไม่มีการดำเนินการต่อ มีการประชุมคณะกรรมการเตรียมการ แต่ก็ยังไม่เกิดขั้นตอนที่ชัดเจน ยังไม่มีผู้รับผิดชอบ กระทรวงเศรษฐกิจดิจิทัลมอบให้ สพธอ. ดำเนินการเป็นการชั่วคราวเพื่อรอ พระราชบัญญัติฯ ไซเบอร์ ผ่านสภาก่อน

เนื่องจากส่วนราชการต้องอาศัยอำนาจตามกฎหมายในการดำเนินการ หากไม่มีกฎหมายรองรับผู้ปฏิบัติจะมีความผิด ดังนั้นในการดำเนินการอย่างเปิดเผย กระทรวงกลาโหมจึงต้องดำเนินการร่วมกับหน่วยงานที่มีกฎหมายรองรับ แนวความคิดของกระทรวงกลาโหมจะมอบหมายให้กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหมทำงานเฉพาะทางเปิด โดยมุ่งการสร้างความเข้าใจที่ถูกต้องให้กับทุกภาคส่วน สร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ ความสำเร็จอยู่ที่ความร่วมมือของหน่วยงานภาครัฐและภาคเอกชนอย่างจริงจัง ซึ่งหากมีกฎหมายรองรับ มีนโยบายแผนแม่บทเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะสามารถทำให้การดำเนินการเป็นไปในทิศทางที่ดีขึ้น

3. การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์

เครื่องมือที่สำคัญที่สุดในการรักษาความปลอดภัยทางไซเบอร์คือทรัพยากรมนุษย์ เป็นหนึ่งในอุปสรรคสำคัญของวงการความมั่นคงปลอดภัยไซเบอร์ เพราะจำนวนผู้เชี่ยวชาญในด้านนี้ยังมีไม่เพียงพอกับความต้องการในตลาดแรงงานทั่วโลก จากข้อมูลของเว็บไซต์ Indeed.com ในปี 2559 ซึ่งเป็นเว็บไซต์สำหรับประกาศหางาน พบว่าประเทศที่มีความต้องการบุคลากรด้านไซเบอร์มากที่สุดคือประเทศอิสราเอล รองลงมาคือประเทศไอร์แลนด์ สหราชอาณาจักร และสหรัฐฯ ส่วนหลายประเทศในแถบเอเชียแปซิฟิก เช่น ญี่ปุ่น มาเลเซีย และสิงค์โปร์ ได้เริ่มตระหนักถึงความสำคัญของปัญหาการขาดแคลนบุคลากรและเริ่มมีโครงการสนับสนุนการพัฒนาบุคลากรด้วยมาตรการต่างๆ ทั้งการพยายามเพิ่มหลักสูตรการศึกษา และการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญ ปัจจุบันประเทศไทยมีหลายหน่วยงานที่มีความพยายามผลักดันการพัฒนาในด้านนี้ เช่น เริ่มมีการเปิดสอนวิชาด้านความมั่นคงปลอดภัยไซเบอร์ในมหาลัยระดับชั้นปริญญาตรี หรือมีการเปิดให้บุคคลทั่วไปเข้ารับการอบรมและสอบใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแนวโน้มในอนาคตความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จะเพิ่มขึ้นอย่างมหาศาล แต่การพัฒนาบุคลากรด้านนี้ยังไม่สามารถทำได้ทันต่อความต้องการ

บุคลากรเป็นปัจจัยสำคัญที่สุดขององค์กร บุคลากรที่ถูกคัดสรรให้เข้าทำงานในองค์กรหรือหน่วยงานที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์นั้นหาได้ยาก ปัญหาที่พบก็คือหน่วยงานด้านความมั่นคงในระดับกระทรวงกลาโหม มีผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศมีน้อยมากและไม่

เพียงพอสำหรับรองรับความก้าวหน้าทางเทคโนโลยี และผลตอบแทนรวมถึงแรงจูงใจระหว่างการทำงานด้านภาครัฐและเอกชน ก็เป็นสาเหตุหนึ่งที่ระดับมันสมองด้านเทคโนโลยีสารสนเทศมีเลือกที่จะทำงานในภาคเอกชน ซึ่งมีผลตอบแทนที่มากกว่าหน่วยงานรัฐ ดังนั้น เมื่อองค์กรภาครัฐมีผู้ชำนาญการเทคโนโลยีสารสนเทศมีน้อย จึงส่งผลกระทบให้การกระจายองค์ความรู้ด้านเทคโนโลยีสารสนเทศมีกระทำได้อย่างจำกัด

จากการศึกษาจากประเทศต่างๆ พบว่าการรักษาความปลอดภัยทางไซเบอร์มีปัญหาเรื่องการสรรหาบุคลากรที่เชี่ยวชาญด้านนี้ เพราะบุคลากรด้านการรักษาความปลอดภัยทางไซเบอร์มีจำนวนจำกัด ทำให้ต้องเปิดรับการสรรหาจากบุคคลภายนอกและเริ่มวางรากฐานในการผลิตบุคลากรด้านนี้ให้พอเพียงต่อความต้องการในอนาคต เช่น รัฐบาลอังกฤษใช้อำนาจและอิทธิพลของรัฐบาลในการลงทุนกับโครงการต่าง ๆ เพื่อแก้ไขปัญหาการขาดแคลนบุคลากรที่มีทักษะด้านความปลอดภัยบนโลกไซเบอร์ ตั้งแต่ระดับโรงเรียนจนถึงมหาวิทยาลัย มีการเปิดตัวศูนย์นวัตกรรมไซเบอร์ใหม่สองแห่งเพื่อขับเคลื่อนการพัฒนาทางไซเบอร์ที่ทันสมัย นอกจากนี้ยังจัดสรรสัดส่วนของกองทุนป้องกันและนวัตกรรมไซเบอร์มูลค่ากว่า 165 ล้านปอนด์ เพื่อสนับสนุนการจัดซื้อนวัตกรรมในด้านการป้องกันและการรักษาความปลอดภัย และใช้สร้าง พัฒนา บุคลากรด้านนี้ ออสเตรเลียเผชิญกับปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญด้านความปลอดภัยใน Cyberspace ซึ่งออสเตรเลียมองว่าเป็นสิ่งสำคัญที่ต้องลงทุนเพื่อสร้างบุคลากรที่มีทักษะในการรักษาความปลอดภัยใน Cyberspace ซึ่งจะกลายเป็นสิ่งจำเป็นมากขึ้นสำหรับวิถีชีวิตและการทำงานใน Cyberspace ของออสเตรเลีย จึงมีการรับสมัครบุคลากรใหม่ และจูงใจด้วยระบบสวัสดิการที่มีคุณภาพ เพื่อการดึงดูดพนักงานที่มีทักษะสูง

ถึงกระนั้นการจ้างงานเฉพาะกิจจากบุคลากรภาคเอกชนให้เข้ามาออกแบบระบบรักษาความปลอดภัยทางไซเบอร์ก็กลายเป็นจุดล่อแหลมของการรักษาความปลอดภัยและความมั่นคงเช่นกัน นอกจากนี้บุคลากรภายนอกยังไม่ตระหนักถึงจิตสำนึกด้านความมั่นคงของชาติ จะโดยตั้งใจหรือไม่ตั้งใจก็ตาม ซึ่งพบว่าในกรณีนี้การเข้าถึงชั้นความลับมีโอกาสที่จะนำข้อมูล“ความลับ” ด้านความมั่นคงของบริษัทหรือของชาติออกไปเปิดเผยต่อสาธารณชนหรือบุคลอื่นได้

4. องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์เนื่องจากกลัวการเสียชื่อเสียง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) จัดตั้งขึ้นเมื่อปี 2554 อยู่ภายใต้การกำกับดูแลของรัฐมนตรีว่าการกระทรวงเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม จัดตั้งขึ้นเพื่อส่งเสริมและสนับสนุนการทำธุรกรรมหรือการให้บริการทางอิเล็กทรอนิกส์ทั้งในภาคธุรกิจและภาครัฐ มีบทบาทในการศึกษาวิจัยทางวิชาการและให้ข้อเสนอแนะเกี่ยวกับนโยบาย กฎหมาย มาตรฐาน ความมั่นคงปลอดภัย และสำรวจความต้องการเกี่ยวกับโครงสร้างพื้นฐานที่ภาคธุรกิจหรือภาครัฐต้องการต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งให้บริการเกี่ยวกับโครงสร้างพื้นฐานที่จำเป็นสำหรับทำธุรกรรมออนไลน์ ตลอดจนพัฒนาบุคลากรที่มีทักษะด้านความมั่นคงปลอดภัยเพื่อให้เพียงพอต่อความต้องการของภาคธุรกิจและภาครัฐ

การกำกับดูแลผู้ประกอบการที่ให้บริการธุรกรรมอิเล็กทรอนิกส์ในปัจจุบัน คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มีอำนาจในการกำกับดูแลทั้งเรื่องธุรกรรมทางการเงินและธุรกรรมประเภทอื่น ถ้ามองเรื่องการเงินเป็นหลักผู้ใช้อำนาจนี้คือธนาคารแห่งประเทศไทยไม่ใช่

กระทรวงเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม แต่ธนาคารแห่งประเทศไทยก็ได้รับอำนาจจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เช่นกัน

อย่างไรก็ตาม การโจมตีทางไซเบอร์ต่อภาคธุรกิจนั้นมักถูกปกปิดเหตุการณ์ไว้ และไม่แจ้งให้หน่วยงานที่เกี่ยวข้องดำเนินการแก้ไข เนื่องจากแนวความคิดที่กลัวการเสียชื่อเสียง ทำให้นักลงทุนหรือลูกค้าขาดความเชื่อมั่นและส่งผลกระทบต่อผู้ประกอบการ ซึ่งการปกปิดดังกล่าวอาจส่งผลกระทบต่อระบบเศรษฐกิจและความมั่นคงในภาพรวมของประเทศในอนาคต หากไม่ได้รับการป้องกันหรือแก้ไขอย่างทันท่วงที

สรุป

การศึกษาในบทที่ 3 จะศึกษาอยู่ในบริบทของวัตถุประสงค์การวิจัยข้อที่ 1 เพื่อศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ และวัตถุประสงค์การวิจัยข้อที่ 2 เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ ผลจากการศึกษาสรุปได้ดังนี้

ตอบวัตถุประสงค์การวิจัยข้อที่ 1 ศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ สรุปได้ดังนี้

1. การดำเนินการต่อภัยทางไซเบอร์ของประเทศไทย

ประเทศไทยใช้มาตรฐานสากล ISO/IEC 27001:2013 (Information Security Management System) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศซึ่งเป็นมาตรฐานที่ได้รับการยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพที่ใช้กันทั่วโลก รวมทั้งกระทรวงกลาโหม ได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม) มาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554

สภาความมั่นคงแห่งชาติ ได้กำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ไว้ในเอกสารนโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2564 ส่วนที่ 2 นโยบายความมั่นคงแห่งชาติทั่วไป โดยเน้นที่การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ 3 ประการ คือ 1.) ปกป้องป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ 2.) พัฒนาการบังคับใช้กฎหมาย 3.) พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ

ในส่วนของประเทศไทยมีการกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) โดยแบ่งหน่วยงานหรือเครือข่ายซึ่งจัดอยู่ในข่ายโครงสร้างพื้นฐานเป็น 6 กลุ่ม ดังนี้ 1.) กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ กำกับโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ กระทรวงกลาโหม 2.) กลุ่มการเงิน กำกับโดย ธนาคารแห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย 3.) กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กำกับโดย คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ 4.) กลุ่มการขนส่งและโลจิสติกส์ กำกับโดย กระทรวงคมนาคม) 5.) กลุ่มพลังงานและสาธารณูปโภค กำกับโดย

กระทรวงพลังงาน และ กระทรวงมหาดไทย 6.) กลุ่มสาธารณสุข กำกับโดย กระทรวงสาธารณสุข การทำงานร่วมกันระหว่างกลุ่มงาน

แต่ละกลุ่มงานมีการแลกเปลี่ยนข้อมูลความมั่นคงปลอดภัยไซเบอร์ มีการลงทุนใช้บริการรับข่าวสารข้อมูลภัยคุกคามไซเบอร์ที่นำมากระจายให้กลุ่มงานต่างๆ ได้รับรู้ด้วย ทั้งนี้เพื่อการสร้างความไว้วางใจ (Trust) ซึ่งเป็นสิ่งจำเป็นอย่างยิ่ง โดยอาจดำเนินการอยู่ในรูปแบบ Platform กลาง และ/หรือ มีเอกชนเข้าร่วมด้วย

2. การดำเนินการของกองทัพไทยต่อภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์

ในส่วนกระทรวงกลาโหม ซึ่งมีภารกิจหลักด้านความมั่นคงของชาติ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี (พ.ศ.2558 – 2562) โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหม ซึ่งกระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ โดยอาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ตามมาตรฐาน ISO 27001: 2005 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ ของกระทรวงกลาโหม พ.ศ.2560 – 2564 มีสาระสำคัญคือ ครอบคลุมแผนงานหลัก 6 แผนงาน ได้แก่ 1.) แผนการจัดองค์กรด้านไซเบอร์โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ดำเนินการจัดตั้งหน่วยงานด้านไซเบอร์/ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง 2.) แผนการป้องกันระบบโครงสร้างพื้นฐาน โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ จัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของตนขึ้นมาเพื่อป้องกันโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูล และจัดตั้งทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านความปลอดภัยไซเบอร์ได้อย่างรวดเร็ว และทันเวลา 3.) แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกัน สกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่างๆ รวมถึงการจัดให้มีการแข่งขันทักษะการปฏิบัติการไซเบอร์ (Cyber Contest) 4.) แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตามความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่าง

รวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวันจะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว 5.) แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain) 6.) แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน แต่สามารถนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ซึ่งมีพลังอำนาจที่ยิ่งใหญ่ได้

นอกจากนั้น กระทรวงกลาโหมมีแนวคิดจะตั้ง MoDCERT เป็นหน่วยงานรับมือภัยคุกคามฝ่ายกลาโหม ซึ่งควรต้องผนึกกำลังกับ ThaiCERT ที่รับมือภัยคุกคามฝ่ายพลเรือน เมื่อพบภัยคุกคามต่อความมั่นคงของรัฐ สภาความมั่นคงฯและสภากลาโหมจะต้องเข้ามาดูแลเชิงนโยบายอย่างเต็มที่ โดยอาจอยู่ในลักษณะการทำพิมพ์เขียว (Blueprint) ของประเทศระหว่าง Cyber Security และ Cyber Defense

ตอบวัตถุประสงค์การวิจัยข้อที่ 2 เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์และทราบถึงปัญหาอุปสรรคที่เกิดในการดำเนินการต่อภัยคุกคามไซเบอร์ สรุปได้ว่า

1. การบูรณาการการดำเนินงานรักษาความปลอดภัยทางไซเบอร์

การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์กำลังเพิ่มมากขึ้น แต่ตลาดเทคโนโลยีต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและขัดแย้งกัน รวมถึงขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ

2. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศใช้

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์ โดยให้อำนาจพิเศษแก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. มีอำนาจสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในทิศทางเดียวกัน และในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง กปช. มีอำนาจอนุมัติให้เจ้าหน้าที่เข้าถึงการติดต่อสื่อสารทุกรูปแบบของประชาชน เช่น ไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด หรือดำเนินการตามมาตรการที่เหมาะสม เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และระงับยับยั้งความเสียหายที่จะเกิดขึ้น โดยไม่ต้องขอคำสั่งศาล

อย่างไรก็ตาม ปัจจุบัน (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่ได้ประกาศใช้ ดังนั้นการปฏิบัติภารกิจเชิงรุกทั้งภายในและภายนอกประเทศ ของส่วนสนับสนุนในการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Computer Security Incident Response Team : CSIRT) จึงไม่มีข้อกฎหมายรองรับการดำเนินการในปัจจุบันซึ่งยังเป็นข้อจำกัดที่สำคัญ

3. การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์

เครื่องมือที่สำคัญที่สุดในการรักษาความปลอดภัยทางไซเบอร์คือทรัพยากรมนุษย์ เป็นหนึ่งในอุปสรรคสำคัญของวงการความมั่นคงปลอดภัยไซเบอร์ เพราะจำนวนผู้เชี่ยวชาญในด้านนี้ยังมีไม่เพียงพอกับความต้องการในตลาดแรงงานทั่วโลก จากข้อมูลของเว็บไซต์ Indeed.com ในปี 2559 ซึ่งเป็นเว็บไซต์สำหรับประกาศหางาน พบว่าประเทศที่มีความต้องการบุคลากรด้านไซเบอร์มากที่สุดคือประเทศอิสราเอล รองลงมาคือประเทศไอร์แลนด์ สหราชอาณาจักร และสหรัฐฯ ส่วนหลายประเทศในแถบเอเชียแปซิฟิก เช่น ญี่ปุ่น มาเลเซีย และสิงค์โปร์ ได้เริ่มตระหนักถึงความสำคัญของปัญหาการขาดแคลนบุคลากรและเริ่มมีโครงการสนับสนุนการพัฒนาบุคลากรด้วยมาตรการต่างๆ ทั้งการพยายามเพิ่มหลักสูตรการศึกษา และการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญ ในประเทศไทยเอง ปัจจุบันได้มีหลายหน่วยงานที่มีความพยายามผลักดันการพัฒนาในด้านนี้ เช่น เริ่มมีการเปิดสอนวิชาด้านความมั่นคงปลอดภัยไซเบอร์ในมหาลัยระดับชั้นปริญญาตรี หรือมีการเปิดให้บุคคลทั่วไปเข้ารับการอบรมและสอบใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแนวโน้มในอนาคตความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จะเพิ่มขึ้นอย่างมหาศาล แต่การพัฒนาบุคลากรด้านนี้ยังไม่สามารถทำได้ทันต่อความต้องการ

ในส่วนหน่วยงานในสังกัดกระทรวงกลาโหมนอกเหนือจากศูนย์ไซเบอร์ของแต่ละเหล่าทัพที่สามารถส่งเสริมและสนับสนุนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ เช่น กรมสรรพกำลังกลาโหมสนับสนุนในด้านการระดมสรรพกำลัง การคัดสรรบุคคลากร สถาบันเทคโนโลยีป้องกันประเทศ (องค์การมหาชน) ส่งเสริมการวิจัยพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น

4. องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์เนื่องจากกลัวการเสียชื่อเสียง

การโจมตีทางไซเบอร์ต่อภาคธุรกิจนั้นมักถูกปกปิดเหตุการณ์ไว้ และไม่แจ้งให้หน่วยงานที่เกี่ยวข้องดำเนินการแก้ไข เนื่องจากแนวความคิดที่กลัวการเสียชื่อเสียง ทำให้นักลงทุนหรือลูกค้าขาดความเชื่อมั่นและส่งผลกระทบต่อผู้ประกอบการ ซึ่งการปกปิดดังกล่าวอาจส่งผลกระทบต่อระบบเศรษฐกิจและความมั่นคงในภาพรวมของประเทศในอนาคต หากไม่ได้รับการป้องกันหรือแก้ไขอย่างทันท่วงที

บทที่ 4
แนวทางที่เหมาะสมในการพัฒนา ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

การศึกษาในบทที่ 4 มีความมุ่งหมายเพื่อตอบวัตถุประสงค์ข้อที่ 3 ในการหาแนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยมีลำดับการศึกษาดังนี้

1. แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีทิศทางที่ชัดเจนและครอบคลุมประเด็นความสำคัญและเร่งด่วนต่อการพัฒนาประเทศไทย ตามนโยบาย Thailand 4.0
2. แนวทางดำเนินการของกองทัพไทยเกี่ยวกับภัยคุกคามทางไซเบอร์ในการป้องกันพัฒนา และบูรณาการความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับหน่วยงานภาครัฐอื่นๆ
3. สรุป

แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีทิศทางที่ชัดเจน และครอบคลุมประเด็นความสำคัญและเร่งด่วนต่อการพัฒนาประเทศไทย ตามนโยบาย Thailand 4.0

จากผลการศึกษา สามารถกำหนดแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อบ่งชี้ว่ายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยจะประสบความสำเร็จหรือไม่ อยู่ที่แนวทางกำหนดยุทธศาสตร์ ถ้าแนวทางในการกำหนดยุทธศาสตร์ฯ มีความชัดเจนและมีการดำเนินการตามกระบวนการอย่างถูกต้อง เหมาะสม ก็จะได้ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่ประสบความสำเร็จตามเป้าหมายของประเทศที่กำหนดไว้ และจะสามารถนำยุทธศาสตร์ฯ ไปสู่การปฏิบัติ (Implementation) ได้อย่างเป็นรูปธรรมแนวทางกำหนดยุทธศาสตร์ชาติความมั่นคงปลอดภัยทางไซเบอร์ มีรายละเอียด ดังนี้

1. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะต้องกำหนดให้มีเป้าหมาย (Ends) ที่ชัดเจน คือ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อนำทรัพยากร (Means) ซึ่งก็คือบุคลากร อุปกรณ์ เทคโนโลยีต่างๆ มาใช้ในการปฏิบัติงานให้บรรลุตามเป้าหมาย (Ends) ด้วยวิธีการ (Way) ที่กำหนดไว้ โดยใช้พื้นฐานความเป็นจริง มีกระบวนการที่มีเหตุผล มีวิธีการที่

สมเหตุสมผล นอกจากนั้นควรพิจารณาถึงความสัมพันธ์ระหว่างเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means) ร่วมกันในเรื่องของความเหมาะสม (Suitability) การยอมรับได้ (Acceptability) และความเป็นไปได้ (Feasibility) ผ่านการประเมินและการจัดการความเสี่ยง (Risk Management)

2. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องกำหนด แผนงาน /โครงการ (Projects/Plans) ประกอบยุทธศาสตร์ฯไว้อย่างเหมาะสม ความสำคัญของแผนงานและโครงการนั้นถือเป็นหัวใจสำคัญของยุทธศาสตร์ฯ ลักษณะสำคัญของแผนงานและโครงการที่จะทำให้ยุทธศาสตร์ฯ เกิดประสิทธิภาพอย่างแท้จริงนั้นต้องเป็นสิ่งที่เมื่อกำหนดขึ้นแล้วและนำไปสู่การปฏิบัติแล้วเกิดผลต่อการพัฒนาประเทศ ฉะนั้น รัฐบาลต้องมีการกำหนดแผนปฏิบัติการที่ชัดเจนและเป็นระบบ เพื่อกำหนดแนวทาง ขั้นตอน วิธีการ/กิจกรรม และเจ้าภาพผู้รับผิดชอบ เพื่อให้เกิดการนำแผนงาน/โครงการไปสู่การปฏิบัติให้เกิดผลผลิตและผลลัพธ์ตามเป้าประสงค์ ที่กำหนดไว้อย่างมีประสิทธิผล รวมทั้งมีการกำหนดกลไกของการทบทวนและปรับยุทธศาสตร์ให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยเฉพาะในกรณีที่มีสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่างจากที่เคยศึกษาไว้ จะทำให้ยุทธศาสตร์ฯ มีความสอดคล้องกับสถานการณ์และสภาพแวดล้อม รวมทั้งสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ

3. ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องมีแนวทางในการนำยุทธศาสตร์ไปสู่การปฏิบัติ (Implementation) ไว้อย่างเหมาะสม การนำยุทธศาสตร์ไปสู่การปฏิบัติหรือการขับเคลื่อนยุทธศาสตร์นั้นเป็นเรื่องสำคัญมาก ผลลัพธ์ที่เกิดขึ้นจากการมียุทธศาสตร์ฯ จะเป็นอย่างไรนั้นขึ้นอยู่กับการนำยุทธศาสตร์ไปสู่การปฏิบัติ ตัวอย่างเช่น สหราชอาณาจักร จัดให้ความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) มีความสำคัญเทียบเท่าภัยคุกคามก่อการร้ายสากล วิกฤติความมั่นคงทางทหารและภัยธรรมชาติ ยุทธศาสตร์ฉบับนี้มุ่งป้องกันภัยคุกคามทางไซเบอร์เพื่อส่งเสริมให้เศรษฐกิจเติบโต ปกป้องความมั่นคงของชาติและการดำเนินชีวิตทั่วไป มีแผนร่วมมือระหว่างภาครัฐกับเอกชนอย่างเป็นรูปธรรม และมองว่าอนาคตของความมั่นคงและความเจริญรุ่งเรืองของอังกฤษขึ้นอยู่กับพื้นฐานของระบบดิจิทัล ความท้าทายของยุคนี้คือการสร้างสังคมดิจิทัลที่เฟื่องฟูและสามารถต่อกรกับภัยคุกคามทางไซเบอร์ได้ การเตรียมความพร้อมทั้งความรู้และความสามารถที่จำเป็นจะช่วยเพิ่มโอกาสและจัดการความเสี่ยงต่อปัญหาภัยคุกคามทางไซเบอร์ของประเทศได้ และกำหนดแนวทางการทำงานเพื่อให้บรรลุวัตถุประสงค์ (UK national cyber security strategy 2016, p.32-54) คือ (1) การป้องกัน (Defend) อังกฤษมีมาตรการในการป้องกันจากภัยคุกคามทางไซเบอร์ที่กำลังพัฒนาขึ้นเรื่อย ๆ สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ทำให้สามารถมั่นใจได้ว่าเครือข่ายข้อมูลและระบบในอังกฤษมีการป้องกันและความสามารถในการฟื้นตัวหากถูกโจมตีได้ทั้งภาครัฐ ภาคธุรกิจ และพลเรือน มีความรู้ความสามารถในการป้องกันตนเอง (2) การยับยั้ง (Deter) อังกฤษสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทุกรูปแบบ นอกจากนั้นยังต้องสามารถตรวจจับ และขัดขวางการโจมตี รวมทั้งสามารถจัดการกับผู้กระทำความผิดได้ (3) การพัฒนา (Develop) อังกฤษมีนวัตกรรมด้านอุตสาหกรรมการรักษาความปลอดภัยในโลกไซเบอร์ซึ่งได้รับการสนับสนุนโดยการวิจัยทางวิทยาศาสตร์ระดับโลก และมีโครงข่ายที่มีความสามารถของตนเองในการพัฒนาทักษะในการตอบสนองต่อความต้องการของชาติได้อย่างทั่วถึงทั้งภาครัฐ และภาคเอกชน ความทันสมัย การวิเคราะห์และความเชี่ยวชาญจะทำให้อังกฤษสามารถเอาชนะภัยคุกคามและความท้าทายในอนาคตได้ ดังนั้น รัฐบาลที่ควรกำหนดแนวทางในการขับเคลื่อนยุทธศาสตร์ฯ ให้ชัดเจน เพราะการกำหนดระบบ

ในการขับเคลื่อนยุทธศาสตร์เพื่อนำยุทธศาสตร์ไปสู่การปฏิบัติจึงมีความสำคัญยิ่งต่อความสำเร็จและล้มเหลวต่อยุทธศาสตร์ชาติ

การมุ่งมั่นที่จะช่วยให้การสร้างสรรค์นวัตกรรม การเจริญเติบโต และความเจริญรุ่งเรืองให้กับประเทศ การรักษาความปลอดภัยบนโลกไซเบอร์ที่แข็งแกร่งจะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลนด์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 ของประเทศ ยุทธศาสตร์ดำเนินการรักษาความปลอดภัยบนโลกไซเบอร์ของไทย ควรกำหนดแนวทางการปฏิบัติออกเป็น 5 รูปแบบ เพื่อการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. การบูรณาการความร่วมมือด้านไซเบอร์ การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม ในลักษณะของการกำกับดูแลตนเอง (Self-Regulation) และการกำกับดูแลร่วมกัน (Co-Regulation) เป็นสิ่งสำคัญของการขับเคลื่อนยุทธศาสตร์ ควบคู่ไปกับการบังคับใช้กฎหมาย และต้องคำนึงถึงผลกระทบต่อสิทธิเสรีภาพของประชาชนในการติดต่อสื่อสารได้ การบูรณาการความร่วมมือระหว่างภาครัฐและภาคเอกชน ทั้งในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การแลกเปลี่ยนข้อมูล รวมทั้งการเพิ่มศักยภาพบุคลากรด้านไซเบอร์ระหว่างกัน ซึ่งผู้นำทั้งภาครัฐและภาคเอกชนจะมีบทบาทที่สำคัญในการร่วมกันผลักดันให้การรักษาความปลอดภัยบนโลกไซเบอร์ของประเทศให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ มีการร่างระเบียบ และประชุมเชิงยุทธศาสตร์ผ่านการประชุมประจำร่วมกันโดยมีรัฐบาลเป็นเจ้าภาพการประชุมจัดขึ้นเพื่อให้เกิดความคิดริเริ่มที่สำคัญในการส่งเสริมยุทธศาสตร์ฯ และรับมือกับปัญหาด้านความปลอดภัยบนโลกไซเบอร์ที่เกิดขึ้น

2. การวางระบบป้องกันภัยคุกคามทางไซเบอร์ ระบบสารสนเทศในปัจจุบันมีแนวโน้มที่อาจจะถูกโจมตีมากขึ้น ประเทศไทยต้องสามารถประกันความมั่นคงปลอดภัยของโครงข่าย เพื่อสร้างความเชื่อมั่นให้กับทั้งภาคธุรกิจและประชาชนในการสื่อสาร และการทำธุรกรรมออนไลน์ สามารถตรวจจับ ยับยั้ง ตอบสนองต่อภัยคุกคาม และสามารถเผชิญแก้ไขหรือเผชิญกับปัญหาภัยคุกคามทางไซเบอร์ให้ระบบสามารถปฏิบัติการต่อไปได้ไม้จะถูกคุกคาม รัฐบาลต้องพิจารณาวางระบบโครงสร้างพื้นฐานทางไซเบอร์ให้สอดคล้องกับสถานการณ์ในปัจจุบัน เพราะโครงสร้างพื้นฐานในด้านต่างๆ ทั้งกลุ่มสารสนเทศและโทรคมนาคม กลุ่มธนาคารและสถาบันการเงิน กลุ่มพลังงาน กลุ่มการขนส่งทางกายภาพต่างๆ ล้วนแต่ใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการดำเนินงานทั้งสิ้น ปัญหาและผลกระทบจากการบุกรุกหรือการโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานเป็นประเด็นที่มีความสำคัญอย่างมาก เพราะหากข้อมูลในโครงสร้างพื้นฐานวิกฤตเหล่านี้ไม่มีการป้องกันหรือความสามารถในการป้องกันไม่เพียงพอต่อการโจมตีจะส่งผลกระทบโดยตรงต่อประเทศ ก่อให้เกิดความเสียหายอย่างร้ายแรงต่อระบบเศรษฐกิจและความมั่นคงของชาติ

3. สร้างความตระหนักและให้ความรู้แก่ผู้บริหารของหน่วยงานทั้งภาครัฐและภาคเอกชน โดยเฉพาะหน่วยงานที่รับผิดชอบโครงสร้างพื้นฐานที่สำคัญของประเทศ ถึงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงความสำคัญในการดำเนินการตามมาตรฐานความมั่นคงปลอดภัยในการปรกอบธุรกรรมทางอิเล็กทรอนิกส์ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้จัดทำขึ้น และให้ความรู้แก่ประชาชนเกี่ยวกับผลกระทบของระบบเทคโนโลยีสารสนเทศหรือโครงข่ายที่มีความเสี่ยงต่อความมั่นคงปลอดภัย หน่วยงานของรัฐต้องกำหนดให้การ

ดำเนินการตามมาตรฐานดังกล่าว เป็นหนึ่งในตัวชี้วัดผลการดำเนินงาน เพื่อให้เกิดการปฏิบัติตามมาตรฐานโดยเคร่งครัด เพื่อประกันความมั่นคงปลอดภัยของการสื่อสารและการทาธุรกรรมออนไลน์

4. การผลิตและดึงดูดทรัพยากรบุคคลที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงทางไซเบอร์ ซึ่งจะเป็นกำลังหลักในการขับเคลื่อนระบบยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ โดยรัฐบาลต้องทำงานร่วมกับภาคธุรกิจและสถาบันอุดมศึกษา ในการออกแบบหลักสูตรความมั่นคงไซเบอร์ เพื่อพัฒนาบุคลากรที่มีคุณภาพ พร้อมลงทุนในการวิจัยและพัฒนาด้านความมั่นคงไซเบอร์ให้มากขึ้น

5. ความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ รัฐบาลต้องเล็งเห็นว่าปัญหาความมั่นคงทางไซเบอร์เป็นปัญหาในระดับโลก จำเป็นต้องมีและทำงานร่วมกับพันธมิตรต่างประเทศ เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์ โดยอาจเริ่มจากประชาคมอาเซียน ไปยังระดับภูมิภาคเอเชียจนถึงระดับโลก รัฐบาลต้องมุ่งมั่นที่จะมีบทบาทเชิงรุกในการผลักดันประเด็นเรื่องความมั่นคงไซเบอร์ในเวทีหารือระดับนานาชาติ ตลอดจนส่งเสริมการเสริมสร้างขีดความสามารถและความร่วมมือด้านความมั่นคงไซเบอร์ โดยเฉพาะการสนับสนุนและปฏิบัติตามกฎหมายระหว่างประเทศหรือมาตรการที่ตกลงกันไว้สำหรับการปฏิบัติที่เหมาะสม และสร้างความมั่นใจในทางปฏิบัติเพื่อลดความเสี่ยงจากความขัดแย้งใดๆ

การเสริมสร้างความสำเร็จของการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้ง 5 ประการนี้ จะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลน์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 เป็นประโยชน์ต่อการพัฒนาคุณภาพชีวิตของประชาชนผ่านการสร้างสังคมและเศรษฐกิจดิจิทัลในหลายแง่มุม โดยต้องอาศัยความร่วมมือทั้งจากรัฐบาล ภาคเอกชน ร่วมกันแก้ไขปัญหาด้านความปลอดภัยบนโลกไซเบอร์ เพื่อให้โลกไซเบอร์เป็นเครื่องมือสำคัญในการพัฒนาเทคโนโลยีนวัตกรรม พัฒนาเศรษฐกิจ และโอกาสทางการค้ารูปแบบใหม่อย่างเท่าเทียมกัน ซึ่งถือเป็นการเปลี่ยนแปลงกระแสในพื้นที่สาธารณะ สำหรับภาคธุรกิจ รัฐจึงจำเป็นต้องเปลี่ยนมุมมองจากการเน้นป้องกันภัยคุกคามเพียงอย่างเดียวมาสู่การสร้างโครงสร้างพื้นฐานที่คืนสู่สภาพเดิมได้อย่างรวดเร็วเมื่อเผชิญภัยคุกคาม โดยมีสมมติฐานว่าภัยคุกคามอาจเกิดขึ้นได้ตลอดเวลาด้วย

แนวทางดำเนินการของกองทัพไทยเกี่ยวกับภัยคุกคามทางไซเบอร์ในการป้องกัน พัฒนา และบูรณาการความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับหน่วยงานภาครัฐอื่นๆ

สำหรับงานความมั่นคงปลอดภัยทางไซเบอร์ในด้านความมั่นคงทางทหาร การทำสงครามไซเบอร์ (Cyber Warfare) รวมถึงการก่อการร้ายทางไซเบอร์ มีกระทรวงกลาโหมเป็นหลัก เพราะเป็นเป้าหมายการโจมตีในระดับชาติ ทั้งระบบเทคโนโลยีทางทหาร อาวุธยุทโธปกรณ์ และระบบสื่อสารของกองทัพที่ใช้ในการป้องกันประเทศนั้น มีความซับซ้อนและแตกต่างจากระบบของพลเรือนทั่วไป จึงจำเป็นต้องมีการพัฒนาด้านความมั่นคงปลอดภัยทางไซเบอร์เช่นกัน กระทรวงกลาโหมได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 ขึ้นเพื่อเป็น

กรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี (พ.ศ.2558 – 2562) โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหม ซึ่งกระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานต่อระบบสารสนเทศ โดยอาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ตามมาตรฐาน ISO 27001: 2005 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

กองทัพดำเนินการตามยุทธศาสตร์ทหารด้านสงครามไซเบอร์ปี 58 จนถึงปัจจุบันเข้าสู่ ปีที่ 3 แล้ว สิ่งที่เรียกว่า NOC SOC และ CERIT คือการให้บริการ การเฝ้าระวัง การตรวจจับ และการ Respon ทั้งสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ดำเนินงานด้วยยุทธศาสตร์เดียวกันและมีประชาคมไซเบอร์ที่มีการประชุมกันทุก 2 – 3 เดือน เพื่อแลกเปลี่ยนความรู้ระหว่างกัน กองทัพเป็นเอกภาพดีในเรื่องของไซเบอร์ แต่ปัญหาด้านไซเบอร์ไม่มีพรมแดน ภัยคุกคามมาจากทั้งภายในและภายนอกประเทศ และประเทศไทยยังไม่มีหน่วยงานที่รับผิดชอบงานด้านไซเบอร์ระดับประเทศ ประเทศไม่มีหน่วยงานกลางด้านไซเบอร์ของประเทศ จึงยังขาดการบูรณาการด้านการข่าวระหว่างกลุ่มโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Information Infrastructure : CII)

ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ใช้การดำเนินงานตามมาตรฐาน NIST Model (national institute of standards & technology) ซึ่งเป็นมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากลที่ใช้ทั่วโลกเช่นกัน (มาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 14, มาตรฐาน COBIT และ มาตรฐาน IT BPM) มาตรฐาน NIST Model เริ่มที่การแยกแยะเพื่อเป็นการทำความเข้าใจระหว่างฝ่ายเรากับฝ่ายข้าศึกว่าสามารถทำอะไรกับเราได้บ้าง อย่างแรกต้องรู้ว่าเครือข่ายของตนเป็นอย่างไร และมีอุปกรณ์อะไรบ้าง และให้บริการอย่างไร แล้วมาดูการให้บริการทั้งหมดว่ามีอันตรายอะไรเกิดขึ้นบ้าง เรียกกระบวนการนี้ว่า การ ประเมินความเสี่ยง (Risk Assessment) โดยจะเริ่มวางอุปกรณ์ในการป้องกัน ซึ่ง NIST Model มี 5 ขั้นตอน ประกอบด้วย 1. การแยกแยะ (Identify) 2. การป้องกัน (Defense) 3. การตรวจพบ (Detection) 4. การตอบสนอง (Respond) 5. การฟื้นตัว (Recevery)

ศูนย์ไซเบอร์กองทัพบกได้มีการกำหนดระดับภัยคุกคามทางด้านไซเบอร์คล้ายกับการการกำหนดระดับภัยคุกคามทางด้านไซเบอร์ของประเทศสหรัฐฯ กล่าวคือ สหรัฐฯ มองว่าภัยคุกคามทางด้านไซเบอร์ถือว่าเป็นอันตรายต่อความมั่นคงของชาติเป็นภัยร้ายแรงสร้างความ เสียหายในวงกว้างกระทบต่อพลเมืองเป็นจำนวนมาก หน่วยรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber security and Integration Center: NCCIC) ของสหรัฐฯ ได้กำหนดระดับภัยคุกคามด้านไซเบอร์ไว้ 5 ระดับ ดังนี้

1. ภัยคุกคามในระดับรัฐบาลแห่งชาติคือภัยที่เป็นอันตรายต่อประเทศชาติเป็นการปล่อยข่าว ที่ไม่น่าเชื่อถือ การเข้าไปโจมตีเปลี่ยนแปลงหน้าเว็บไซต์ในหน่วยงานของรัฐ หรือการเจาะระบบของโครงสร้าง พื้นฐานที่เป็นระบบการเงินการธนาคาร และระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบประปา ซึ่งให้บริการ กับประชาชนในประเทศ

2. ภัยจากการก่อการร้ายสากล โดยเฉพาะกลุ่มก่อการร้ายต้องการโจมตีต่อประเทศคู่ขัดแย้ง ทางการเมือง มุ่งทำลายผลประโยชน์ทางการเมือง เพื่อสร้างความหวาดกลัวไปยังประชาชนในประเทศนั้น ๆ

3. ภัยจากสายลับหรือพวกจารกรรมข้อมูลในภาคอุตสาหกรรม และองค์กรเครือข่ายอาชญากรรม ซึ่งภัยด้านนี้จะกำหนดให้เป็นภัยคุกคามระดับกลางของประเทศ

4. ภัยจากกลุ่มแฮ็กเกอร์ที่มีอุดมการณ์ซึ่งเกิดจากการรวมกลุ่มของพวกแฮกเกร่วมกันโจมตีเว็บไซต์ของรัฐบาลโดยมีแรงจูงใจจากอุดมการณ์ทางการเมืองหรือความคิดเห็นที่แตกต่าง ทางการเมืองเพราะกลุ่มแฮ็กเกอร์เหล่านั้นเห็นว่ารัฐหรือหัวหน้ารัฐบาลในประเทศนั้นๆ ได้ดำเนินนโยบายที่ขัด ต่อสิทธิเสรีภาพในการแสดงออกหรือลิดรอนสิทธิเสรีภาพของบุคคล และการปิดกั้นสิทธิเสรีภาพทางการเมือง ของประชาชน

5. ภัยจากกลุ่มแฮ็กเกอร์มือสมัครเล่น โดยกลุ่มแฮ็กเกอร์จะประชาสัมพันธ์ทางเว็บไซต์เพื่อรวบรวมพวกมือสมัครเล่นให้ร่วมกันโจมตีเว็บไซต์ของหน่วยงานภาครัฐและภาคเอกชน และส่งผลกระทบ อย่างกว้างขวางจนสร้างความเสียหายในระยะยาวให้กับโครงสร้างพื้นฐานในระดับชาติที่ถูกโจมตีได้อย่าง มหาศาล

ภัยคุกคามทางไซเบอร์ทั้ง 5 ประการจะเกิดขึ้นในประเทศมหาอำนาจทางทหาร คือ สหรัฐฯ และกลุ่มประเทศยุโรป ที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศอย่างมาก แต่ภัยเหล่านี้ยังสามารถนำมาเป็นบทเรียนและปรับใช้กับประเทศไทยที่ต้องการยกระดับเพิ่มศักยภาพในการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ได้ การกำหนดระดับภัยคุกคามทางด้านไซเบอร์ของประเทศไทย กรณีประเทศไทยภัยคุกคามทางด้านไซเบอร์นั้น ได้กำหนดระดับความปลอดภัยเช่นเดียวกับ ประเทศสหรัฐฯ แต่ระดับความรุนแรงของประเทศไทยไม่มากเหมือนประเทศมหาอำนาจ ซึ่งศูนย์ไซเบอร์กองทัพบกได้ตระหนักในภัยคุกคามดังกล่าว และได้กำหนดระดับภัยคุกคามทางด้านไซเบอร์เป็น 4 ด้าน ดังนี้

1. ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ เป็นภัยคุกคามในระดับประเทศหรือ ระดับชาติผู้ที่ก่อภัยคุกคามอาจใช้วิธีนำข่าวสารเหล่านั้นลงเผยแพร่ในเว็บไซต์ของประเทศตนเอง เพื่อให้ ข่าวสารเหล่านั้นเผยแพร่เข้ามาสู่ประเทศไทยจนสงผลกระทบต่อความมั่นคงภายในประเทศไทย และทำให้เกิด ความได้เปรียบทางการเมืองหรือด้านความมั่นคง รวมทั้งการเผยแพร่ข้อมูลความลับของประเทศไทย และ การแพร่กระจายโปรแกรมไม่พึงประสงค์สำหรับการทำลายเครือข่ายระบบคอมพิวเตอร์

2. ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.) เป็นการใช้ไซเบอร์ที่เป็นภัย คุกคามต่อความมั่นคงของชาติในการเผยแพร่ข่าวสารของผู้ก่อความไม่สงบ เช่น การเผยแพร่ข่าวลือ ข่าวที่ไม่ เป็นจริง โดยการกล่าวหาว่าเจ้าหน้าที่ของรัฐทำการละเมิดสิทธิมนุษยชน เพื่อให้สื่อมวลชนกระแสหลักนำข่าว ไปเผยแพร่ต่อเพื่อต้องการให้ประชาชนทั่วไปหวาดกลัวจนทำให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่รัฐถือเป็น การปฏิบัติการข่าวสาร (Information Operation) ที่เป็น

การปฏิบัติการจิตวิทยาอย่างหนึ่ง นอกจากนั้นยังมี การเผยแพร่ผลงานของผู้ก่อความไม่สงบที่อาจจะส่งผลกระทบทำให้เกิดแนวร่วมของผู้ก่อความไม่สงบเพิ่มมากขึ้น

3. ภัยคุกคามที่ส่งผลกระทบต่อสถาบันของชาติเป็นสิ่งที่กระทำได้ง่ายและยากต่อการดำเนินคดี ต่อผู้กระทำผิดคือการเผยแพร่ภาพที่หมิ่นสถาบันพระมหากษัตริย์การวิจารณ์สถาบันในทางเสื่อมเสีย ซึ่งเจ้าหน้าที่ของรัฐบาลไทยไม่สามารถดำเนินการตามกฎหมายไทยได้เพราะส่วนหนึ่งของผู้กระทำความผิด ไม่ได้อยู่ในประเทศไทยแต่ได้ใช้เว็บไซต์หรือสื่อโซเชียลในต่างประเทศเผยแพร่ข่าวสารเข้ามายังประเทศไทย

4. ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพไทย ทำให้ภาพลักษณ์ของผู้นำกองทัพ ไทยเสียหายหรือลดความน่าเชื่อถือในสังคมไทย รวมทั้งลดความเชื่อมั่นของประชาชนต่อการปกป้องประเทศ ไทย และการบังคับบัญชาของเหล่าทัพ ซึ่งส่งผลกระทบต่อการพิทักษ์อธิปไตยของชาติไทย (ฤทธีอินทราวุธ, 2558. น. 1-5)

จากการศึกษาพบว่ากรอบแนวทางการปฏิบัติของกองทัพไทยในปัจจุบัน เป็นไปในทิศทางเดียวกัน มีเป้าหมายเดียวกัน ใช้ยุทธศาสตร์เดียวกัน กระทรวงกลาโหมได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554 ใช้มาตรฐาน ISO 27001: 2005 และมีมาตรการ NIST Model ตามมาตรฐาน 5 ขั้นตอน ประกอบด้วย 1. การแยกแยะ (Identify) 2. การป้องกัน (Defense) 3. การตรวจพบ (Detection) 4. การตอบสนอง (Respond) 5. การฟื้นตัว (Recevery) อย่างไรก็ตาม ISO 27001: 2005 มีหลักการออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจมากกว่าการนามาใช้ในภารกิจด้านการทหาร ผู้วิจัยจึงมีความกังวลถึงความเหมาะสมของการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม เพราะการมีประสิทธิภาพของการรักษาความปลอดภัยระบบ อุปกรณ์ยุทโธปกรณ์ ซึ่งถูกควบคุมและสั่งการโดยอิเล็กทรอนิกส์ นั้น มีความละเอียดอ่อนและมีความสำคัญต่อความมั่นคงของชาติ ดังนั้น ควรมีการศึกษาเชิงลึกจากยุทธศาสตร์ไซเบอร์ที่เกี่ยวกับทางการทหาร รวมทั้งอาจแก้ไขเพิ่มเติมให้เหมาะสมกับบริบทของกระทรวงกลาโหม แต่ยังคงเป็นไปตามมาตรฐานสากล ตัวอย่างเช่น มาตรฐาน U.S. DoD เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของ ระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรก คือ กระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการ ออกแบบ พัฒนา ผลิต หรือทดสอบสำหรับผู้ผลิตเทคโนโลยี หรือภาคเอกชนได้ปฏิบัติตาม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้ มีการกำกับคุณภาพของคนโดยมีใบรับรอง IT Certificate ทางด้าน Cyber Security ทำให้ได้เจ้าหน้าที่ที่เหมาะสมเข้ามาทำงานด้านนี้ นอกจากนี้ยังให้ความสำคัญกับหลักการประกันความมั่นคงปลอดภัยสารสนเทศ (Informational Assurance: IA) โดยมีมาตรฐาน ในการประเมิน และมี IT Audit team ในการกำกับควบคุม ทำให้การนำนโยบายด้าน ไซเบอร์มาสู่การปฏิบัติมีประสิทธิภาพมากยิ่งขึ้น เป้าหมายทางยุทธศาสตร์และแนวทางในการดำเนินยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงกลาโหมสหรัฐฯ (DOD Cyber Strategy, United States Department of Defense, 2015, p.13-15) ประกอบด้วย 5 ประเด็นสำคัญ ได้แก่

1. สร้างและคงไว้ซึ่งความพร้อมและความสามารถในการดำเนินงานบนโลกไซเบอร์ (CYBERSPACE OPERATIONS)

กระทรวงกลาโหมได้ริเริ่มการลงทุนที่สำคัญในบุคลากรด้านไซเบอร์และเทคโนโลยีสำหรับ Cyber Mission Force (CMF) กระทรวงกลาโหมต้องฝึกคนและสร้างองค์กรที่มีประสิทธิภาพและระบบการบัญชาการและการควบคุมและพัฒนาความสามารถที่กระทรวงกลาโหมต้องใช้ในโลกไซเบอร์ วัตถุประสงค์หลักของเป้าหมายนี้ ได้แก่

- สร้างความสามารถด้านเทคนิคสำหรับการดำเนินงานรวมถึงแพลตฟอร์มการปฏิบัติงานแบบครบวงจรและแบบบูรณาการ
- เร่งวิจัยและพัฒนาเพื่อให้กระทรวงศึกษาธิการมีข้อได้เปรียบในการพัฒนาเทคโนโลยีล่วงหน้าเพื่อปกป้องผลประโยชน์ของสหรัฐฯ ในโลกไซเบอร์
- ประเมินความสามารถของ CMF เพื่อให้บรรลุวัตถุประสงค์ของภารกิจเมื่อต้องเผชิญกับภารกิจหลายอย่าง

2. ป้องกันเครือข่ายข้อมูล และลดความเสี่ยงต่อภารกิจของกระทรวงกลาโหม

กระทรวงกลาโหมต้องจัดลำดับความสำคัญและปกป้องเครือข่ายและข้อมูลที่สำคัญที่สุดเพื่อให้สามารถปฏิบัติภารกิจได้อย่างมีประสิทธิภาพ มีการแผนและมาตรการเพื่อใช้ดำเนินการภายใต้สภาพแวดล้อมของการถูกโจมตีทางไซเบอร์ หากโครงสร้างพื้นฐานสำคัญของกระทรวงกลาโหมถูกโจมตีละไม่สามารถใช้การได้จะทำให้แผนปฏิบัติการและเหตุการณ์ฉุกเฉินหยุดชะงัก วัตถุประสงค์หลักของเป้าหมายนี้ ได้แก่

- สร้างสถาปัตยกรรมด้านการรักษาความปลอดภัยด้านข้อมูลร่วม (Joint Information Environment) เพื่อเพื่อรักษาความปลอดภัยให้กับระบบ กระทรวงกลาโหม
- ใช้ความสามารถในการลดช่องโหว่ทั้งหมดที่มีความเสี่ยงสูงต่อกระทรวงกลาโหม
- ระบุแผนป้องกันเครือข่ายที่สนับสนุนภารกิจของกระทรวงกลาโหมที่สำคัญ
- สร้างการป้องกันรอบฐานอุตสาหกรรมการป้องกันประเทศ ให้เป็นไปตามมาตรฐานด้านความปลอดภัยในโลกไซเบอร์ ในการต่อต้านการโจรกรรมข้อมูลทางทหาร

3. เตรียมพร้อมในการป้องกันประเทศสหรัฐฯ และสิ่งที่อยู่ในความสนใจของสหรัฐฯ จากการโจมตีทางไซเบอร์

กระทรวงกลาโหมต้องทำงานร่วมกับภาคเอกชน และประเทศพันธมิตร เพื่อพัฒนาขีดความสามารถในการแจ้งเตือนและความสามารถในการปฏิบัติงาน เพื่อลดการโจมตีทางไซเบอร์ที่อาจเป็นอันตรายต่อสหรัฐฯ และพันธมิตร วัตถุประสงค์หลักของเป้าหมายนี้ ได้แก่

- พัฒนาความสามารถในการคาดการณ์ภัยคุกคามและการแจ้งเตือน
- เป็นพันธมิตรกับหน่วยงานสำคัญต่างๆ เพื่อเตรียมพร้อมที่จะปกป้องประเทศในโลกไซเบอร์
- ทำงานร่วมกับ กระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) เพื่อพัฒนากลไกในการแบ่งปันข้อมูลอย่างต่อเนื่อง
- ประเมินระบบการป้องกันไซเบอร์ของกระทรวงกลาโหมและให้คำแนะนำในการปรับปรุง

4. สร้างตัวเลือกและเลือกใช้ตัวเลือกที่มีอยู่ และวางแผนที่จะใช้ตัวเลือกเหล่านี้เพื่อควบคุมความคลาดเคลื่อนที่เกิดขึ้นและเพื่อให้เกิดสภาวะแวดล้อมที่ได้เปรียบในทุกขั้นตอน เช่น ในสถานการณ์ความตึงเครียดที่เกิดจากการสู้รบหรือสถานการณ์คับขันอื่นๆ กระทรวงกลาโหมต้องเสนอแนวทางที่หลากหลายเพื่อให้ประธานาธิบดีมีตัวเลือกในการจัดการกับสถานการณ์ความขัดแย้ง นอกจากนั้นจะต้องพัฒนาขีดความสามารถในโลกไซเบอร์เพื่อให้บรรลุวัตถุประสงค์ด้านความปลอดภัยที่สำคัญด้วยความแม่นยำและเพื่อลดการสูญเสียชีวิตและการทำลายทรัพย์สิน

5. สร้าง รักษาความสัมพันธ์ระหว่างประเทศ และความร่วมมือระหว่างประเทศเพื่อลดความเสี่ยงด้านความมั่นคงระหว่างประเทศ เพราะภารกิจด้านไซเบอร์ของกระทรวงกลาโหมจำเป็นต้องมีการร่วมมือกันอย่างใกล้ชิดกับพันธมิตร ซึ่งกระทรวงกลาโหมพยายามที่จะสร้างและพัฒนาขีดความสามารถในการเป็นพันธมิตรด้านความปลอดภัยทางไซเบอร์

การจัดโครงสร้างเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Organization) ในกระทรวงกลาโหมควรคำนึงถึงสิ่งสำคัญดังนี้

1. กำหนดนิยามและกระบวนการต่างๆในการรักษาความปลอดภัยที่ชัดเจน รวมถึงการประสานงานส่วนราชการที่เกี่ยวข้องตามแผนนโยบายรักษาความมั่นคงปลอดภัยทางไซเบอร์

2. จัดตั้งคณะทำงานหลักเพื่อบริหารและจัดการความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของส่วนราชการไว้อย่างชัดเจน

3. กำหนดสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศ และให้ระบุความจำเป็นในการเข้าใช้งานระบบสารสนเทศอย่างชัดเจน

4. ควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานของส่วนราชการในการใช้ระบบสารสนเทศให้มีความปลอดภัย

ส่วนสำคัญอีกส่วนหนึ่งคือ การสร้างความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวกับการควบคุมการเข้าถึงและการใช้งานข้อมูลสารสนเทศ ซึ่งมีแนวทางดังนี้

1. บริหารจัดการข้อมูลสารสนเทศโดยจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งการระบุความหน่วยงานเจ้าของเรื่องหรือผู้กำกับดูแลข้อมูลสารสนเทศนั้น

2. มีมาตรการและแนวทางในการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อควบคุมการเข้าถึงและการใช้ข้อมูลสารสนเทศ โดยอาจแบ่งได้ดังนี้

2.1 ข้อกำหนดการใช้งานตามภารกิจ เพื่อให้มีแนวทางปฏิบัติและมาตรการควบคุมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครือข่าย

2.2 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้และเข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และควบคุมผู้ใช้งานข้อสอบสารสนเทศเพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

2.3 การควบคุมการเข้าถึงเครือข่าย กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงข้อมูลสารสนเทศ เช่น อ่านอย่างเดียว, สร้างข้อมูล, ป้อนข้อมูล, แก้ไขข้อมูล, อนุมัติข้อมูล เป็นต้น เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

2.4 การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อให้ผู้ใช้งานทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ และปฏิบัติตามอย่างเคร่งครัดเพื่อเป็นการป้องกันทรัพยากรและข้อมูลสารสนเทศของหน่วยงาน ให้พ้นสถานภาพและมีความพร้อมในการใช้งานอยู่เสมอ

2.5 การควบคุมการเข้าถึงจากการใช้งานภายนอก เพื่อกำหนดมาตรฐานควบคุมการเข้าถึงระบบเครือข่าย โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบจากภายนอกเครือข่ายให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้เข้าใช้ระบบจากภายนอกเครือข่ายต้องผ่านการพิสูจน์ตัวตนจากระบบว่าได้รับอนุญาตจากผู้ดูแลเพื่อให้สามารถเข้าใช้งานได้

2.6 มีมาตรการแนวทางการปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่ดำเนินการรวบรวมจัดเก็บใช้หรือเผยแพร่ข้อมูลข้อเท็จจริงที่สามารถระบุตัวบุคคลไม่ว่าโดยทางตรงหรือทางอ้อมก็ตาม

3. การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน

3.1 มีมาตรการหรือแนวทางปฏิบัติในการจัดหา พัฒนา และบำรุงรักษาระบบเครือข่าย

3.2 มีมาตรการหรือแนวทางปฏิบัติในการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ไม่พึงประสงค์

3.3 มีระบบสำรองข้อมูลที่เหมาะสมสำหรับหน่วยงานให้อยู่ในสภาพพร้อมใช้งานเพื่อรองรับการดำเนินการตามภารกิจในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางสารสนเทศ หรือในกรณีที่ระบบหลักหรือศูนย์ข้อมูลหลักไม่สามารถให้บริการได้ เพื่อให้สามารถใช้งานข้อมูลสารสนเทศได้ตามปกติอย่างต่อเนื่อง

3.4 จัดแผนเตรียมความพร้อมฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับสถานการณ์ และให้มีการทดสอบความพร้อมในการใช้งานของระบบสำรองและแผนเตรียมความพร้อมฉุกเฉินอย่างสม่ำเสมอ รวมถึงการทบทวนแผนเตรียมความพร้อมฉุกเฉินเป็นประจำอย่างต่อเนื่อง

4. การตรวจสอบการประเมินและการจัดการกับความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

4.1 การประเมินความเสี่ยงด้านความมั่นคงและปลอดภัยทางไซเบอร์ ก็มีการทบทวนและประเมินความเสี่ยงด้านความมั่นคงและปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ โดยอ้างอิงหลักเกณฑ์การประเมินความเสี่ยงที่เหมาะสมครอบคลุมปัจจัยความเสี่ยงทั้งภายในและภายนอก

4.2 ตรวจสอบการปฏิบัติตามนโยบายและแนวทางการปฏิบัติที่กำหนด ต้องมีการตรวจสอบการปฏิบัติตามนโยบายและแนวทางที่กำหนดอย่างสม่ำเสมอ รวมถึงการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สำคัญต่อการปฏิบัติภารกิจหลัก ตรวจสอบจากผู้ตรวจสอบภายในหน่วยงาน และผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยทางไซเบอร์จากภายนอก เพื่อให้หน่วยงานได้รับทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

การบูรณาการร่วมกับหน่วยงานภาครัฐอื่นๆ เห็นควรมีการแลกเปลี่ยนข่าวสารด้านไซเบอร์ระดับกองทัพไปสู่หน่วยงานที่เป็นกลุ่มโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical

Information Infrastructure : CII) เช่น หน่วยงานไฟฟ้า ประปา ธนาคาร ตัวอย่างเช่น ศูนย์ไซเบอร์ทหารนั้นมีความต้องการร่วมกับกับภาคธนาคาร เพื่อแลกเปลี่ยนข้อมูล คือ งานข่าวด้านยุทธการ และจะมีการพัฒนาต่อไปยังหน่วยงาน ไฟฟ้า ประปา และคมนาคม ถ้าสามารถมีความร่วมมือกับหน่วยงานต่างๆ ได้ จะสามารถทำให้เข้าใจถึงภัยคุกคาม และสร้างความเข้มแข็งไปพร้อมกัน โดยทุกอย่างต้องอยู่ภายใต้นโยบายการดำเนินการเหมือนกัน

การปฏิบัติการ การป้องกันทางไซเบอร์ และ การเตรียมสภาพแวดล้อมการปฏิบัติการทางไซเบอร์

ตาม AFDD 3-12 : Cyberspace Operations กล่าวว่า อิสรภาพในการดำเนินกลยุทธ์ภายใต้ขอบเขตในห้องไซเบอร์ เป็นสิ่งนำมาซึ่งขีดความสามารถในการปฏิบัติการด้านต่าง ๆ ของ ทอ. สหรัฐ ได้แก่ การบัญชาการ, การควบคุม, การติดต่อสื่อสาร, การปฏิบัติด้านคอมพิวเตอร์, การข่าว กรอง, การเฝ้าตรวจ และการลาดตระเวน ปัจจุบันการทำงานของระบบการค้าระหว่างประเทศ อุตสาหกรรมพื้นฐาน และการป้องกันประเทศที่ทันสมัยขึ้นอยู่กับอิสรภาพของการใช้งานทรัพยากร ภาคพื้น ภาคทะเล ภาคอากาศ ห้วงอวกาศ และห้วงไซเบอร์ โดยเฉพาะพลังอำนาจห้วงไซเบอร์มีอิทธิพลและส่งผลกระทบต่อกับการปฏิบัติในส่วนอื่นๆ ตลอดจนพลังอำนาจนี้ยังช่วยเพิ่มขีดความสามารถในด้านการเข้าร่วม ความรวดเร็ว การเข้าถึง การล่องหน และความแม่นยำ ให้กับกองกำลังทหารได้เป็นอย่างดี (Air Force Doctrine Document : Cyberspace Operations 3-12, U.S.A.F., 2010, P.2)

การควบคุมในห้วงไซเบอร์โดยรวมกับการปฏิบัติภารกิจ เป็นความต้องการพื้นฐานก่อนสิ่งอื่นใดของการปฏิบัติทุกภารกิจทางทหารที่มีประสิทธิภาพ ขณะที่เราชื่นชอบกำลังที่พร้อมด้วยขีดความสามารถด้านไซเบอร์ เรายังคงต้องตระหนักถึงขีดความสามารถและความพยายามที่ไม่สมมาตรในห้วงไซเบอร์ของศัตรูของเราเช่นกัน ดังนั้น เราต้องดำรงพันธะด้านการศึกษา การฝึกอบรม และการจัดหายุทโธปกรณ์ให้กับกำลังพล เพื่อความเหนือกว่าในการแข่งขันของห้วงไซเบอร์ต่อไป เมื่อพิจารณาแล้วการปฏิบัติการไซเบอร์ไม่เพียงแต่ส่งผลกระทบด้านการทหารเท่านั้น หากสามารถนำไปใช้ในความมั่นคงด้านอื่น ๆ (ด้านเศรษฐกิจ ด้านสังคม และวัฒนธรรม) ดังนั้น ในภาคธุรกิจที่จะต้องคงความได้เปรียบคู่แข่งทางการค้า และรักษาฐานลูกค้าเดิม ตลอดจนขยายฐานการตลาดใหม่อยู่ตลอดเวลาจำเป็นจะต้องพึ่งพาการปฏิบัติการในห้วงไซเบอร์เช่นเดียวกันกับด้านการทหาร

การป้องกันทางไซเบอร์ (Cyber Defense) เป็นการประยุกต์รวมขีดความสามารถและกระบวนการในห้วงไซเบอร์ของหน่วยงานที่เกี่ยวข้อง ในการดำรงขีดความสามารถด้านการตรวจจับวิเคราะห์และลดภัยคุกคาม จุดเสี่ยงต่างๆ และการดำเนินกลยุทธให้สามารถเอาชนะข้าศึก เพื่อป้องกันเครือข่ายที่กำหนด ปกป้องภารกิจที่สำคัญ และทำให้เกิดอิสระในการปฏิบัติของฝ่ายเรา การป้องกันทางไซเบอร์ รวมถึงการปฏิบัติการเครือข่ายเชิงรุก กระทรวงกลาโหมจัดโครงสร้าง และขีดความสามารถทางเทคนิคสำหรับการปฏิบัติการ และการป้องกันโครงข่ายข้อมูลข่าวสารโลก (Global Information Grid: GIG) การปฏิบัติการเครือข่าย (NetOps) รวมถึงการบริหารจัดการองค์กร (Enterprise Management), การรับรองการทำงานหรือการป้องกันของเครือข่าย (Net Assurance หรือ Net Defense), และการบริหารข่าวสาร (Content Management) การปฏิบัติการเครือข่าย (NetOps) สามารถสนองตอบความต้องการของผู้บังคับบัญชาในการหยั่งรู้สถานการณ์ของ GIG เพื่อนำไปสู่การตัดสินตกลงใจในรูปแบบของการบัญชาการและควบคุม ทั้งนี้การหยั่งรู้สถานการณ์ของ

GIG ทำได้โดยการบูรณาการทั้งทางเทคนิคและการปฏิบัติการของการบริหารจัดการองค์กร และการป้องกันและกิจกรรมตลอดทุกระดับการบังคับบัญชา (ยุทธศาสตร์, ยุทธการ และยุทธวิธี)

การป้องกันการโจมตีทางไซเบอร์ (Defensive Counter Cyber : DCC) เป็นมาตรการป้องกันต่างๆ ทั้งหมดที่ถูกออกแบบเพื่อตรวจจับ ระบุตัวตน สกัดกั้น และทำลาย หรือลดกิจกรรมอันตรายต่างๆ ที่พยายามเจาะ หรือโจมตีผ่านห้วงไซเบอร์ ภารกิจการป้องกันการโจมตีทางไซเบอร์ถูกออกแบบมาเพื่อป้องกันเครือข่ายของฝ่ายเดียวกันในด้านการคงสภาพ (Integrity), การพร้อมใช้งาน (Availability), และการรักษาความปลอดภัย (Security) รวมทั้งการป้องกันขีดความสามารถของเครือข่ายของไซเบอร์ฝ่ายเดียวกันจากการโจมตี การบุกรุก หรือกิจกรรมที่ประสงค์ร้าย โดยการดำเนินการเชิงรุกในการค้นหา การสกัดกั้น และการกีดกันการปฏิบัติทางไซเบอร์ของศัตรู ต่อภัยคุกคามต่าง ๆ

การปฏิบัติการป้องกันการโจมตีทางไซเบอร์อาจรวมถึง การลวงทางทหาร (Military Deception) โดยใช้เทคนิค Honneypot หรือการปฏิบัติการอื่นๆ กิจกรรมที่ส่งผลเสียหายต่อศัตรูและหรือระบบที่มีส่วนเกี่ยวข้องกับการกระทำที่เป็นภัยต่อฝ่ายเรา เช่น การเปลี่ยนเส้นทาง (Redirection) การระงับการปฏิบัติ (Deactivation) หรือการย้าย (Removal) โปรแกรมประสงค์ร้าย (Malware) ต่างๆ

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

การสร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

การสร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในส่วนหน่วยงานในสังกัดกระทรวงกลาโหม เพื่อรองรับ เพื่อรองรับเทคโนโลยีที่มีความหลากหลายมากขึ้น เพราะการสร้างบุคลากรต้องใช้เวลาและยากที่จะดำรงไว้เมื่อมีการเปลี่ยนแปลง นอกเหนือจากศูนย์ไซเบอร์ของแต่ละเหล่าทัพที่สามารถส่งเสริมและสนับสนุนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ เช่น กรมสรรพกำลังกลาโหมสนับสนุนในด้านการระดมสรรพกำลัง การคัดสรรบุคคลากร สถาบันเทคโนโลยีป้องกันประเทศ (องค์การมหาชน) ส่งเสริมการวิจัยพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น แต่ยังไม่เพียงพอต่อการรองรับความต้องการในอนาคต

นอกจากนี้ในส่วนสถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย มีหน่วยงานในสังกัด คือ โรงเรียนเตรียมทหาร และโรงเรียนช่างฝีมือทหาร ซึ่งจะสามารถใช้วางพื้นฐานสร้างบุคลากรเพื่อรองรับงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพในอนาคตได้ นอกจากนั้น ในส่วนของหลักสูตรระดับสูงของกองทัพ คือ หลักสูตร การป้องกันราชอาณาจักร (วปอ.) หลักสูตร เสนาธิการทหาร (วสท.) มีการจัดการฝึกแก้ไขสถานการณ์ฉุกเฉิน และการฝึกร่วมของวิทยาลัยการทัพ ซึ่งสามารถฝึกจำลองสถานการณ์การต่อต้านการก่อการร้ายทางไซเบอร์หรือการทำสงครามไซเบอร์ เพื่อให้ผู้บริหารจากหน่วยงานต่างๆ ที่เข้ารับการศึกษา มีประสบการณ์ในการ

บัญชาการสถานการณ์เพื่อรับมือเกี่ยวกับภัยคุกคามทางไซเบอร์ และสามารถนำไปใช้ประโยชน์ในการบริหารหน่วยงานและประเทศชาติในการป้องกันและรักษาความมั่นคงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

สรุป

จากผลการศึกษาในบทที่ 4 เพื่อตอบสนองวัตถุประสงค์ของการวิจัยข้อที่ 3 เพื่อศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ ผลการศึกษาสรุปได้ดังนี้

1. แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีทิศทางที่ชัดเจน และครอบคลุมประเด็นความสำคัญและเร่งด่วนต่อการพัฒนาประเทศไทย ตามนโยบาย Thailand 4.0

จากผลการศึกษา สามารถกำหนดแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อบ่งชี้ว่ายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยจะประสบความสำเร็จหรือไม่ ถ้าแนวทางในการกำหนดยุทธศาสตร์ฯ มีความชัดเจนและมีการดำเนินการตามกระบวนการอย่างถูกต้อง เหมาะสม ก็จะได้ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่ประสบความสำเร็จตามเป้าหมายของประเทศที่กำหนดไว้ และจะสามารถนำยุทธศาสตร์ฯ ไปสู่การปฏิบัติ (Implementation) ได้อย่างเป็นรูปธรรมแนวทางกำหนดยุทธศาสตร์ชาติความมั่นคงปลอดภัยทางไซเบอร์ มีรายละเอียด ดังนี้

1.1 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะต้องกำหนดให้มีเป้าหมาย (Ends) ที่ชัดเจน คือ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อนำทรัพยากร (Means) ซึ่งก็คือบุคลากร อุปกรณ์ เทคโนโลยีต่างๆ มาใช้ในการปฏิบัติงานให้บรรลุตามเป้าหมาย (Ends) ด้วยวิธีการ (Way) ที่กำหนดไว้ โดยใช้พื้นฐานความเป็นจริง มีกระบวนการที่มีเหตุผล มีวิธีการที่สมเหตุสมผล นอกจากนั้นควรพิจารณาถึงความสัมพันธ์ระหว่างเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means) ร่วมกันในเรื่องของความเหมาะสม (Suitability) การยอมรับได้ (Acceptability) และความเป็นไปได้ (Feasibility) ผ่านการประเมินและการจัดการความเสี่ยง (Risk Management)

1.2 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องกำหนด แผนงาน /โครงการ (Projects/Plans) ประกอบยุทธศาสตร์ฯไว้อย่างเหมาะสม ความสำคัญของแผนงานและโครงการนั้นถือเป็นหัวใจสำคัญของยุทธศาสตร์ฯ ลักษณะสำคัญของแผนงานและโครงการที่จะทำให้ยุทธศาสตร์ฯ เกิดประสิทธิภาพอย่างแท้จริงนั้นต้องเป็นสิ่งที่เมื่อกำหนดขึ้นแล้วและนำไปสู่การปฏิบัติแล้วเกิดผลต่อการพัฒนาประเทศ ฉะนั้น รัฐบาลต้องมีการกำหนดแผนปฏิบัติการที่ชัดเจนและเป็นระบบ เพื่อกำหนดแนวทาง ขั้นตอน วิธีการ/กิจกรรม และเจ้าภาพผู้รับผิดชอบ เพื่อให้เกิดการนำแผนงาน/โครงการไปสู่การปฏิบัติให้เกิดผลผลิตและผลลัพธ์ตามเป้าประสงค์ ที่กำหนดไว้อย่างมีประสิทธิผล รวมทั้งมีการ

กำหนดกลไกของการทบทวนและปรับยุทธศาสตร์ให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยเฉพาะในกรณีที่มีสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่างจากที่เคยศึกษาไว้ จะทำให้ยุทธศาสตร์ฯ มีความสอดคล้องกับสถานการณ์และสภาพแวดล้อม รวมทั้งสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ

1.3 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องมีแนวทางในการนำยุทธศาสตร์ไปสู่การปฏิบัติ (Implementation) ไว้อย่างเหมาะสม การนำยุทธศาสตร์ไปสู่การปฏิบัติหรือการขับเคลื่อนยุทธศาสตร์นั้นเป็นเรื่องสำคัญมาก ผลลัพธ์ที่เกิดขึ้นจากการมียุทธศาสตร์ฯ จะเป็นอย่างไรนั้นขึ้นอยู่กับการนำยุทธศาสตร์ไปสู่การปฏิบัติ ตัวอย่างเช่น สหราชอาณาจักร จัดให้ความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) มีความสำคัญเทียบเท่าภัยคุกคามก่อการร้ายสากล วิกฤติความมั่นคงทางทหารและภัยธรรมชาติ ยุทธศาสตร์ฉบับนี้มุ่งป้องกันภัยคุกคามทางไซเบอร์เพื่อส่งเสริมให้เศรษฐกิจเติบโต ปกป้องความมั่นคงของชาติและการดำเนินชีวิตทั่วไป มีแผนร่วมมือระหว่างภาครัฐกับเอกชนอย่างเป็นรูปธรรม และมองว่าอนาคตของความมั่นคงและความเจริญรุ่งเรืองของอังกฤษขึ้นอยู่กับพื้นฐานของระบบดิจิทัล ความท้าทายของยุคนี้คือการสร้างสังคมดิจิทัลที่เฟื่องฟูและสามารถต่อกรกับภัยคุกคามทางไซเบอร์ได้ การเตรียมความพร้อมทั้งความรู้และความสามารถที่จำเป็นจะช่วยเพิ่มโอกาสและจัดการความเสี่ยงต่อปัญหาภัยคุกคามทางไซเบอร์ของประเทศได้ และกำหนดแนวทางการทำงานเพื่อให้บรรลุวัตถุประสงค์ คือ (1) การป้องกัน (Defend) อังกฤษมีมาตรการในการป้องกันจากภัยคุกคามทางไซเบอร์ที่กำลังพัฒนาขึ้นเรื่อย ๆ สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ทำให้สามารถมั่นใจได้ว่าเครือข่ายข้อมูลและระบบในอังกฤษมีการป้องกันและความสามารถในการฟื้นตัวหากถูกโจมตีได้ ทั้งภาครัฐ ภาคธุรกิจ และพลเรือน มีความรู้ความสามารถในการป้องกันตนเอง (2) การยับยั้ง (Deter) อังกฤษสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทุกรูปแบบ นอกจากนั้นยังต้องสามารถตรวจจับ และขัดขวางการโจมตี รวมทั้งสามารถจัดการกับผู้กระทำความผิดได้ (3) การพัฒนา (Develop) อังกฤษมีนวัตกรรมด้านอุตสาหกรรมการรักษาความปลอดภัยในโลกไซเบอร์ซึ่งได้รับการสนับสนุนโดยการวิจัยทางวิทยาศาสตร์ระดับโลก และมีโครงข่ายที่มีความสามารถของตนเองในการพัฒนาทักษะในการตอบสนองต่อความต้องการของชาติได้อย่างทั่วถึงทั้งภาครัฐ และภาคเอกชน ความทันสมัย การวิเคราะห์และความเชี่ยวชาญจะทำให้อังกฤษสามารถเอาชนะภัยคุกคามและความท้าทายในอนาคตได้ ดังนั้น รัฐบาลที่ควรกำหนดแนวทางในการขับเคลื่อนยุทธศาสตร์ฯ ให้ชัดเจน เพราะการกำหนดระบบในการขับเคลื่อนยุทธศาสตร์เพื่อนำยุทธศาสตร์ไปสู่การปฏิบัติจึงมีความสำคัญยิ่งต่อความสำเร็จและล้มเหลวต่อยุทธศาสตร์ชาติ

การมุ่งมั่นที่จะช่วยให้การสร้างสรรค์นวัตกรรม การเจริญเติบโต และความเจริญรุ่งเรืองให้กับประเทศ การรักษาความปลอดภัยบนโลกไซเบอร์ที่แข็งแกร่งจะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลนด์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 ของประเทศ ยุทธศาสตร์ดำเนินการรักษาความปลอดภัยบนโลกไซเบอร์ของไทย ควรกำหนดแนวทางการปฏิบัติออกเป็น 5 รูปแบบ เพื่อการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้ 1.) การบูรณาการความร่วมมือด้านไซเบอร์ การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม 2.) การวางระบบป้องกันภัยคุกคามทางไซเบอร์ 3.) สร้างความตระหนักและให้ความรู้แก่ผู้บริหารของหน่วยงานทั้ง

ภาครัฐและภาคเอกชน 4.) การผลิตและดึงดูดทรัพยากรบุคคลที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงทางไซเบอร์ 5.) ความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ

การเสริมสร้างความสำเร็จของการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้ง 5 ประการนี้ จะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลน์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 เป็นประโยชน์ต่อการพัฒนาคุณภาพชีวิตของประชาชนผ่านการสร้างสังคมและเศรษฐกิจดิจิทัลในหลายแง่มุม โดยต้องอาศัยความร่วมมือทั้งจากรัฐบาล ภาคเอกชน ร่วมกันแก้ไขปัญหาด้านความปลอดภัยบนโลกไซเบอร์ เพื่อให้โลกไซเบอร์เป็นเครื่องมือสำคัญในการพัฒนาเทคโนโลยีนวัตกรรม พัฒนาเศรษฐกิจ และโอกาสทางการค้ารูปแบบใหม่อย่างเท่าเทียมกัน ซึ่งถือเป็นการเปลี่ยนแปลงกระแสในพื้นที่สาธารณะ สำหรับภาคธุรกิจ รัฐจึงจำเป็นต้องเปลี่ยนมุมมองจากการเน้นป้องกันภัยคุกคามเพียงอย่างเดียวมาสู่การสร้างโครงสร้างพื้นฐานที่คืนสู่สภาพเดิมได้อย่างรวดเร็วเมื่อเผชิญภัยคุกคาม โดยมีสมมติฐานว่าภัยคุกคามอาจเกิดขึ้นได้ตลอดเวลาด้วย

2. แนวทางดำเนินการของกองทัพไทยเกี่ยวกับภัยคุกคามทางไซเบอร์ในการป้องกัน พัฒนา และบูรณาการความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับหน่วยงานภาครัฐอื่นๆ

จากการศึกษาพบว่ากรอบแนวทางการปฏิบัติของกองทัพไทยในปัจจุบัน เป็นไปในทิศทางเดียวกัน มีเป้าหมายเดียวกัน ใช้ยุทธศาสตร์เดียวกัน กระทรวงกลาโหมได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554 ใช้มาตรฐาน ISO 27001: 2005 และมีมาตรการ NIST Model ตามมาตรฐาน 5 ขั้นตอน ประกอบด้วย 1. การแยกแยะ (Identify) 2. การป้องกัน (Defense) 3. การตรวจพบ (Detection) 4. การตอบสนอง (Respond) 5. การฟื้นตัว (Recevery) อย่างไรก็ตาม ISO 27001: 2005 มีหลักการออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจมากกว่าการนามาใช้ในภารกิจด้านการทหาร ผู้วิจัยจึงมีความกังวลถึงความเหมาะสมของการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม เพราะการมีประสิทธิภาพของการรักษาความปลอดภัยระบบ อุปกรณ์ยุทโธปกรณ์ ซึ่งถูกควบคุมและสั่งการโดยอิเล็กทรอนิกส์ นั้น มีความละเอียดอ่อนและมีความสำคัญต่อความมั่นคงของชาติ ดังนั้น ควรมีการศึกษาเชิงลึกจากยุทธศาสตร์ไซเบอร์ที่เกี่ยวกับทางการทหาร รวมทั้งอาจแก้ไขเพิ่มเติมให้เหมาะสมกับบริบทของกระทรวงกลาโหม แต่ยังคงเป็นไปตามมาตรฐานสากล

การจัดโครงสร้างเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Organization) ในกระทรวงกลาโหมควรคำนึงถึงสิ่งสำคัญ คือ (1) กำหนดนิยามและกระบวนการต่างๆในการรักษาความปลอดภัยที่ชัดเจน รวมถึงการประสานงานส่วนราชการที่เกี่ยวข้องตามแผนนโยบายรักษาความมั่นคงปลอดภัยทางไซเบอร์ (2) จัดตั้งคณะทำงานหลักเพื่อบริหารและจัดการความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของส่วนราชการไว้อย่างชัดเจน (3) กำหนดสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศ และให้ระบุความจำเป็นในการเข้าใช้งานระบบสารสนเทศอย่างชัดเจน (4) ควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานของส่วนราชการในการใช้ระบบสารสนเทศให้มีความปลอดภัย

ส่วนสำคัญอีกส่วนหนึ่งคือ การสร้างความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวกับการควบคุมการเข้าถึงและการใช้งานข้อมูลสารสนเทศ ซึ่งมีแนวทางดังนี้ (1) บริหารจัดการข้อมูลสารสนเทศโดยจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งการระบุความหน่วยงานเจ้าของเรื่องหรือผู้กำกับดูแลข้อมูลสารสนเทศนั้น (2) มีมาตรการและแนวทางในการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อควบคุมการเข้าถึงและการใช้ข้อมูลสารสนเทศ (3) การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน (4) การตรวจสอบการประเมินและการจัดการกับความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

การบูรณาการร่วมกับหน่วยงานภาครัฐอื่นๆ เห็นควรมีการแลกเปลี่ยนข่าวสารด้านไซเบอร์ระดับกองทัพไปสู่หน่วยงานที่เป็นกลุ่มโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Information Infrastructure : CII) เช่น หน่วยงานไฟฟ้า ประปา ธนาคาร ตัวอย่างเช่น ศูนย์ไซเบอร์ทหารนั้นมีความต้องการร่วมกับกับภาคธนาคาร เพื่อแลกเปลี่ยนข้อมูล คือ งานข่าวด้านยุทธการ และจะมีการพัฒนาต่อไปยังหน่วยงาน ไฟฟ้า ประปา และคมนาคม ถ้าสามารถมีความร่วมมือกับหน่วยงานต่างๆ ได้ จะสามารถทำให้เข้าใจถึงภัยคุกคาม และสร้างความเข้มแข็งไปพร้อมกัน โดยทุกอย่างต้องอยู่ภายใต้นโยบายการดำเนินการเหมือนกัน

บทที่ 5
สรุปและข้อเสนอแนะ

การศึกษาวิจัยเรื่อง แนวทางที่เหมาะสมของกองทัพไทยในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยได้กำหนดวัตถุประสงค์การวิจัยไว้ 3 ข้อ ประกอบด้วย 1.) เพื่อศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ 2.) เพื่อศึกษาปัญหาข้อขัดข้องในการดำเนินการต่อภัยคุกคามทางไซเบอร์ 3.) เพื่อศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ในการดำเนินการวิจัย ผู้วิจัยใช้การรวบรวมข้อมูลทุติยภูมิ จากหลายแหล่งข้อมูลที่เกี่ยวข้อง และรวบรวมข้อมูลปฐมภูมิจากการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญที่เกี่ยวข้อง เพื่อให้ข้อมูลที่ได้มีความเที่ยงตรงและน่าเชื่อถือ ส่วนการวิเคราะห์ข้อมูลนั้น ผู้วิจัยใช้การวิเคราะห์เนื้อหาเป็นหลัก โดยเมื่อนำข้อมูลที่รวบรวมได้มาจัดระเบียบแล้วนำมาวิเคราะห์ สังเคราะห์ ประกอบกับแนวความคิดทฤษฎีที่เกี่ยวข้องจนกระทั่งได้แนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ ซึ่งในบทที่ 5 นี้ จะนำเสนอ 2 ประเด็น คือ สรุปผลการวิจัย และข้อเสนอแนะเพิ่มเติม จากผลการวิจัยดังนี้

สรุปผลการวิจัย

ตอบวัตถุประสงค์การวิจัยข้อที่ 1 ศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ สรุปได้ดังนี้

1. การดำเนินการต่อภัยทางไซเบอร์ของประเทศไทย

ประเทศไทยใช้มาตรฐานสากล ISO/IEC 27001:2013 (Information Security Management System) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศซึ่งเป็นมาตรฐานที่ได้รับการยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพที่ใช้กันทั่วโลก รวมทั้งกระทรวงกลาโหม ได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเดิม) มาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554

สภาความมั่นคงแห่งชาติ ได้กำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ไว้ในเอกสารนโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2564 ส่วนที่ 2 นโยบายความมั่นคงแห่งชาติทั่วไป โดยเน้นที่การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ 3 ประการ คือ 1.) ปกป้องป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ 2.) พัฒนาการบังคับใช้กฎหมาย 3.) พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ

ในส่วนของประเทศไทยมีการกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) โดยแบ่งหน่วยงานหรือเครือข่ายซึ่งจัดอยู่ใน

ข่ายโครงสร้างพื้นฐานเป็น 6 กลุ่ม ดังนี้ 1.) กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ กำกับโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ กระทรวงกลาโหม 2.) กลุ่มการเงิน กำกับโดย ธนาคารแห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย 3.) กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กำกับโดย คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ 4.) กลุ่มการขนส่งและโลจิสติกส์ กำกับโดย กระทรวงคมนาคม) 5.) กลุ่มพลังงานและสาธารณูปโภค กำกับโดย กระทรวงพลังงาน และ กระทรวงมหาดไทย 6.) กลุ่มสาธารณสุข กำกับโดย กระทรวงสาธารณสุข การทำงานร่วมกันระหว่างกลุ่มงาน

แต่ละกลุ่มงานมีการแลกเปลี่ยนข้อมูลความมั่นคงปลอดภัยไซเบอร์ มีการลงทุนใช้บริการรับข่าวสารข้อมูลภัยคุกคามไซเบอร์ที่นำมากระจายให้กลุ่มงานต่างๆ ได้รับรู้ด้วย ทั้งนี้เพื่อการสร้างความไว้วางใจ (Trust) ซึ่งเป็นสิ่งจำเป็นอย่างยิ่ง โดยอาจดำเนินการอยู่ในรูปแบบ Platform กลาง และ/หรือ มีเอกชนเข้าร่วมด้วย

2. การดำเนินการของกองทัพไทยต่อภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์

ในส่วนกระทรวงกลาโหม ซึ่งมีภารกิจหลักด้านความมั่นคงของชาติ ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี (พ.ศ.2558 – 2562) โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 รวมทั้งแต่งตั้งคณะอนุกรรมการไซเบอร์กระทรวงกลาโหม เพื่อให้การดำเนินงานด้านไซเบอร์ในระดับกระทรวงกลาโหมเป็นไปด้วยความเรียบร้อย มีการกำหนดนโยบายและกรอบแนวทางการพัฒนางานด้านไซเบอร์ของกระทรวงกลาโหม ซึ่งกระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยคำนึงถึงหลักการพื้นฐานของการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานต่อระบบสารสนเทศ ทรัพย์สินสารสนเทศ และข้อมูลสำคัญในการปฏิบัติภารกิจ โดยอาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ตามมาตรฐาน ISO 27001: 2005 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ ของกระทรวงกลาโหม พ.ศ.2560 – 2564 มีสาระสำคัญคือ ครอบคลุมแผนงานหลัก 6 แผนงาน ได้แก่ 1.) แผนการจัดองค์กรด้านไซเบอร์โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ดำเนินการจัดตั้งหน่วยงานด้านไซเบอร์/ศูนย์ไซเบอร์ ขึ้นมารองรับภารกิจด้านไซเบอร์โดยตรง 2.) แผนการป้องกันระบบโครงสร้างพื้นฐาน โดยกระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ จัดตั้งศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center ; CSOC) ของตนขึ้นมาเพื่อป้องกันโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งระบบฐานข้อมูล และจัดตั้งทีมจัดการปัญหาฉุกเฉินด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Incident Response Team / Computer Security Incident Response Team ; CSIRT) เพื่อตอบสนองการแก้ไขปัญหาฉุกเฉินด้านความปลอดภัยไซเบอร์ได้อย่างรวดเร็ว และทันเวลา 3.) แผนการพัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ เป็นการพัฒนาบุคลากรของกองทัพให้

มีขีดความสามารถด้านการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ เพื่อการป้องกัน สกัดกั้น ยับยั้งการโจมตี และการตอบโต้ฝ่ายตรงข้ามที่มีผลกระทบต่อความมั่นคงของชาติ และความมั่นคงด้านการทหาร โดยการพัฒนา เสริมสร้างขีดความสามารถกำลังพล เครื่องมือ และเทคโนโลยีต่างๆ รวมถึงการจัดให้มีการแข่งขันทักษะการปฏิบัติการไซเบอร์ (Cyber Contest) 4.) แผนการดำรงและพัฒนาศักยภาพด้านไซเบอร์ เพื่อดำรงความต่อเนื่องและยั่งยืนอย่างเป็นรูปธรรม รวมทั้งการวิจัยและพัฒนาเทคโลยีด้านไซเบอร์ (R&D) เพื่อวิจัยพัฒนาและติดตามความเจริญก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพราะภัยคุกคามด้านไซเบอร์นับวันจะทวีความรุนแรง ส่งผลกระทบและความเสียหายในวงกว้างอย่างรวดเร็ว 5.) แผนการสนับสนุนศักยภาพทางไซเบอร์ระดับชาติ เนื่องจากกองทัพเป็นหน่วยงานหลักด้านความมั่นคงของชาติ จึงต้องมีความพร้อมในการสนับสนุนและเป็นเครื่องมือให้กับรัฐบาล เพื่อเสริมสร้างศักยภาพด้านไซเบอร์ของชาติ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันภัยคุกคามในระดับชาติด้านไซเบอร์โดเมน (Cyber Domain) 6.) แผนงานความร่วมมือและผนึกกำลังด้านไซเบอร์ เป็นการประสานความร่วมมือทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชนทั่วไป ในการผนึกกำลังด้านไซเบอร์ ซึ่งเป็นกำลังอำนาจที่ไม่มีตัวตน แต่สามารถนำไปสู่การระดมสรรพกำลังของประเทศด้านไซเบอร์ซึ่งมีพลังอำนาจที่ยิ่งใหญ่ได้

นอกจากนั้น กระทรวงกลาโหมมีแนวคิดจะตั้ง MoDCERT เป็นหน่วยงานรับมือภัยคุกคามฝ่ายกลาโหม ซึ่งควรต้องผนึกกำลังกับ ThaiCERT ที่รับมือภัยคุกคามฝ่ายพลเรือน เมื่อพบภัยคุกคามต่อความมั่นคงของรัฐ สภาความมั่นคงฯและสภากลาโหมจะต้องเข้ามาดูแลเชิงนโยบายอย่างเต็มที่ โดยอาจอยู่ในลักษณะการทำพิมพ์เขียว (Blueprint) ของประเทศระหว่าง Cyber Security และ Cyber Defense

ตอบวัตถุประสงค์การวิจัยข้อที่ 2 เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์และทราบถึงปัญหาอุปสรรคที่เกิดในการดำเนินการต่อภัยคุกคามไซเบอร์ สรุปได้ว่า

1. การบูรณาการการดำเนินงานรักษาความปลอดภัยทางไซเบอร์

การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์กำลังเพิ่มมากขึ้น แต่ตลาดเทคโนโลยีต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและขัดแย้งกัน รวมถึงขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ

2. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศใช้

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์ โดยให้อำนาจพิเศษแก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. มีอำนาจสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ในทิศทางเดียวกัน และในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง กปช. มีอำนาจอนุมัติให้เจ้าหน้าที่เข้าถึงการติดต่อสื่อสารทุกรูปแบบของประชาชน เช่น ไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด หรือดำเนินการตามมาตรการที่เหมาะสม เพื่อ

ประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และระงับยับยั้งความเสียหายที่จะเกิดขึ้น โดยไม่ต้องขอคำสั่งศาล

อย่างไรก็ตาม ปัจจุบัน (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่ได้ประกาศใช้ ดังนั้นการปฏิบัติภารกิจเชิงรุกทั้งภายในและภายนอกประเทศ ของส่วนสนับสนุนในการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Computer Security Incident Response Team : CSIRT) จึงไม่มีข้อกฎหมายรองรับการดำเนินการในปัจจุบันซึ่งยังเป็นข้อจำกัดที่สำคัญ

3. การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์

เครื่องมือที่สำคัญที่สุดในการรักษาความปลอดภัยทางไซเบอร์คือทรัพยากรมนุษย์ เป็นหนึ่งในอุปสรรคสำคัญของวงการความมั่นคงปลอดภัยไซเบอร์ เพราะจำนวนผู้เชี่ยวชาญในด้านนี้ยังมีไม่เพียงพอกับความต้องการในตลาดแรงงานทั่วโลก จากข้อมูลของเว็บไซต์ Indeed.com ในปี 2559 ซึ่งเป็นเว็บไซต์สำหรับประกาศหางาน พบว่าประเทศที่มีความต้องการบุคลากรด้านไซเบอร์มากที่สุดคือประเทศอิสราเอล รองลงมาคือประเทศไอร์แลนด์ สหราชอาณาจักร และสหรัฐฯ ส่วนหลายประเทศในแถบเอเชียแปซิฟิก เช่น ญี่ปุ่น มาเลเซีย และสิงค์โปร์ ได้เริ่มตระหนักถึงความสำคัญของปัญหาการขาดแคลนบุคลากรและเริ่มมีโครงการสนับสนุนการพัฒนาบุคลากรด้วยมาตรการต่างๆ ทั้งการพยายามเพิ่มหลักสูตรการศึกษา และการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญ ในประเทศไทยเอง ปัจจุบันได้มีหลายหน่วยงานที่มีความพยายามผลักดันการพัฒนาในด้านนี้ เช่น เริ่มมีการเปิดสอนวิชาด้านความมั่นคงปลอดภัยไซเบอร์ในมหาลัยระดับชั้นปริญญาตรี หรือมีการเปิดให้บุคคลทั่วไปเข้ารับการอบรมและสอบใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแนวโน้มในอนาคตความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จะเพิ่มขึ้นอย่างมหาศาล แต่การพัฒนาบุคลากรด้านนี้ยังไม่สามารถทำได้ทันต่อความต้องการ

ในส่วนหน่วยงานในสังกัดกระทรวงกลาโหมนอกเหนือจากศูนย์ไซเบอร์ของแต่ละเหล่าทัพที่สามารถส่งเสริมและสนับสนุนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ เช่น กรมสรรพกำลังกลาโหมสนับสนุนในด้านการระดมสรรพกำลัง การคัดสรรบุคคลากร สถาบันเทคโนโลยีป้องกันประเทศ (องค์การมหาชน) ส่งเสริมการวิจัยพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น

4. องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์เนื่องจากกลัวการเสียชื่อเสียง

การโจมตีทางไซเบอร์ต่อภาคธุรกิจนั้นมักถูกปกปิดเหตุการณ์ไว้ และไม่แจ้งให้หน่วยงานที่เกี่ยวข้องดำเนินการแก้ไข เนื่องจากแนวความคิดที่กลัวการเสียชื่อเสียง ทำให้นักลงทุนหรือลูกค้าขาดความเชื่อมั่นและส่งผลกระทบต่อผู้ประกอบการ ซึ่งการปกปิดดังกล่าวอาจส่งผลกระทบต่อระบบเศรษฐกิจและความมั่นคงในภาพรวมของประเทศในอนาคต หากไม่ได้รับการป้องกันหรือแก้ไขอย่างทันท่วงที

ตอบวัตถุประสงค์การวิจัยข้อที่ 3 ศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ สรุปได้ว่า

1. แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีทิศทางที่ชัดเจน และครอบคลุมประเด็นความสำคัญและเร่งด่วนต่อการพัฒนาประเทศไทย ตามนโยบาย Thailand 4.0

จากผลการศึกษา สามารถกำหนดแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์เพื่อบ่งชี้ว่ายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยจะประสบความสำเร็จหรือไม่ ถ้าแนวทางในการกำหนดยุทธศาสตร์ฯ มีความชัดเจนและมีการดำเนินการตามกระบวนการอย่างถูกต้อง เหมาะสม ก็จะได้ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่ประสบความสำเร็จตามเป้าหมายของประเทศที่กำหนดไว้ และจะสามารถนำยุทธศาสตร์ฯ ไปสู่การปฏิบัติ (Implementation) ได้อย่างเป็นรูปธรรมแนวทางกำหนดยุทธศาสตร์ชาติความมั่นคงปลอดภัยทางไซเบอร์ มีรายละเอียด ดังนี้

1.1 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์จะต้องกำหนดให้มีเป้าหมาย (Ends) ที่ชัดเจน คือ เพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อนำทรัพยากร (Means) ซึ่งก็คือบุคลากร อุปกรณ์ เทคโนโลยีต่างๆ มาใช้ในการปฏิบัติงานให้บรรลุตามเป้าหมาย (Ends) ด้วยวิธีการ (Way) ที่กำหนดไว้ โดยใช้พื้นฐานความเป็นจริง มีกระบวนการที่มีเหตุผล มีวิธีการที่สมเหตุสมผล นอกจากนั้นควรพิจารณาถึงความสัมพันธ์ระหว่างเป้าหมาย (Ends) วิธีการ (Ways) และทรัพยากร (Means) ร่วมกันในเรื่องของความเหมาะสม (Suitability) การยอมรับได้ (Acceptability) และความเป็นไปได้ (Feasibility) ผ่านการประเมินและการจัดการความเสี่ยง (Risk Management)

1.2 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องกำหนด แผนงาน /โครงการ (Projects/Plans) ประกอบยุทธศาสตร์ฯไว้อย่างเหมาะสม ความสำคัญของแผนงานและโครงการนั้นถือเป็นหัวใจสำคัญของยุทธศาสตร์ฯ ลักษณะสำคัญของแผนงานและโครงการที่จะทำให้ยุทธศาสตร์ฯ เกิดประสิทธิภาพอย่างแท้จริงนั้นต้องเป็นสิ่งที่เมื่อกำหนดขึ้นแล้วและนำไปสู่การปฏิบัติแล้วเกิดผลต่อการพัฒนาประเทศ ฉะนั้น รัฐบาลต้องมีการกำหนดแผนปฏิบัติการที่ชัดเจนและเป็นระบบ เพื่อกำหนดแนวทาง ขั้นตอน วิธีการ/กิจกรรม และเจ้าภาพผู้รับผิดชอบ เพื่อให้เกิดการนำแผนงาน/โครงการไปสู่การปฏิบัติให้เกิดผลผลิตและผลลัพธ์ตามเป้าประสงค์ ที่กำหนดไว้อย่างมีประสิทธิผล รวมทั้งมีการกำหนดกลไกของการทบทวนและปรับยุทธศาสตร์ให้เหมาะสมกับสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยเฉพาะในกรณีที่มีสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่างจากที่เคยศึกษาไว้ จะทำให้ยุทธศาสตร์ฯ มีความสอดคล้องกับสถานการณ์และสภาพแวดล้อม รวมทั้งสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ

1.3 ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ต้องมีแนวทางในการนำยุทธศาสตร์ไปสู่การปฏิบัติ (Implementation) ไว้อย่างเหมาะสม การนำยุทธศาสตร์ไปสู่การปฏิบัติหรือการ

ขับเคลื่อนยุทธศาสตร์นั้นเป็นเรื่องสำคัญมาก ผลลัพธ์ที่เกิดขึ้นจากการมียุทธศาสตร์ฯ จะเป็นอย่างไรนั้นขึ้นอยู่กับการนำยุทธศาสตร์ไปสู่การปฏิบัติ ตัวอย่างเช่น สหราชอาณาจักร จัดให้ความมั่นคงปลอดภัยไซเบอร์ (cybersecurity) มีความสำคัญเทียบเท่าภัยคุกคามก่อการร้ายสากล วิกฤติความมั่นคงทางทหารและภัยธรรมชาติ ยุทธศาสตร์ฉบับนี้มุ่งป้องกันภัยคุกคามทางไซเบอร์เพื่อส่งเสริมให้เศรษฐกิจเติบโต ปกป้องความมั่นคงของชาติและการดำเนินชีวิตทั่วไป มีแผนร่วมมือระหว่างภาครัฐกับเอกชนอย่างเป็นรูปธรรม และมองว่าอนาคตของความมั่นคงและความเจริญรุ่งเรืองของอังกฤษขึ้นอยู่กับพื้นฐานของระบบดิจิทัล ความท้าทายของยุคนี้คือการสร้างสังคมดิจิทัลที่เฟื่องฟูและสามารถต่อกรกับภัยคุกคามทางไซเบอร์ได้ การเตรียมความพร้อมทั้งความรู้และความสามารถที่จำเป็นจะช่วยเพิ่มโอกาสและจัดการความเสี่ยงต่อปัญหาภัยคุกคามทางไซเบอร์ของประเทศได้ และกำหนดแนวทางการทำงานเพื่อให้บรรลุวัตถุประสงค์ คือ (1) การป้องกัน (Defend) อังกฤษมีมาตรการในการป้องกันจากภัยคุกคามทางไซเบอร์ที่กำลังพัฒนาขึ้นเรื่อย ๆ สามารถตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพ ทำให้สามารถมั่นใจได้ว่าเครือข่ายข้อมูลและระบบในอังกฤษมีการป้องกันและความสามารถในการฟื้นตัวหากถูกโจมตีได้ ทั้งภาครัฐ ภาคธุรกิจ และพลเรือน มีความรู้ความสามารถในการป้องกันตนเอง (2) การยับยั้ง (Deter) อังกฤษสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ทุกรูปแบบ นอกจากนั้นยังต้องสามารถตรวจจับ และขัดขวางการโจมตี รวมทั้งสามารถจัดการกับผู้กระทำความผิดได้ (3) การพัฒนา (Develop) อังกฤษมีนวัตกรรมด้านอุตสาหกรรมการรักษาความปลอดภัยในโลกไซเบอร์ซึ่งได้รับการสนับสนุนโดยการวิจัยทางวิทยาศาสตร์ระดับโลก และมีโครงข่ายที่มีความสามารถของตนเองในการพัฒนาทักษะในการตอบสนองต่อความต้องการของชาติได้อย่างทั่วถึงทั้งภาครัฐ และภาคเอกชน ความทันสมัย การวิเคราะห์และความเชี่ยวชาญจะทำให้อังกฤษสามารถเอาชนะภัยคุกคามและความท้าทายในอนาคตได้ ดังนั้น รัฐบาลที่ควรกำหนดแนวทางในการขับเคลื่อนยุทธศาสตร์ฯ ให้ชัดเจน เพราะการกำหนดระบบในการขับเคลื่อนยุทธศาสตร์เพื่อนำยุทธศาสตร์ไปสู่การปฏิบัติจึงมีความสำคัญยิ่งต่อความสำเร็จและล้มเหลวต่อยุทธศาสตร์ชาติ

การมุ่งมั่นที่จะช่วยให้การสร้างสรรค์นวัตกรรม การเจริญเติบโต และความเจริญรุ่งเรืองให้กับประเทศ การรักษาความปลอดภัยบนโลกไซเบอร์ที่แข็งแกร่งจะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลนด์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 ของประเทศ ยุทธศาสตร์ดำเนินการรักษาความปลอดภัยบนโลกไซเบอร์ของไทย ควรกำหนดแนวทางการปฏิบัติออกเป็น 5 รูปแบบ เพื่อการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้ 1.) การบูรณาการความร่วมมือด้านไซเบอร์ การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ หน่วยงานภาคเอกชน และภาคประชาสังคม 2.) การวางระบบป้องกันภัยคุกคามทางไซเบอร์ 3.) สร้างความตระหนักและให้ความรู้แก่ผู้บริหารของหน่วยงานทั้งภาครัฐและภาคเอกชน 4.) การผลิตและดึงดูดทรัพยากรบุคคลที่มีความรู้ความเชี่ยวชาญด้านความมั่นคงทางไซเบอร์ 5.) ความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ

การเสริมสร้างความสำเร็จของการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้ง 5 ประการนี้ จะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลนด์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 เป็นประโยชน์ต่อการพัฒนาคุณภาพชีวิตของประชาชนผ่านการสร้างสังคมและเศรษฐกิจดิจิทัลในหลายแง่มุม โดยต้องอาศัยความร่วมมือทั้งจากรัฐบาล ภาคเอกชน ร่วมกันแก้ไขปัญหาด้านความปลอดภัย

บนโลกไซเบอร์ เพื่อให้โลกไซเบอร์เป็นเครื่องมือสำคัญในการพัฒนาเทคโนโลยีนวัตกรรม พัฒนาเศรษฐกิจ และโอกาสทางการค้ารูปแบบใหม่อย่างเท่าเทียมกัน ซึ่งถือเป็นการเปลี่ยนแปลงกระแสในพื้นที่สาธารณะ สำหรับภาคธุรกิจ รัฐจึงจำเป็นต้องเปลี่ยนมุมมองจากการเน้นป้องกันภัยคุกคามเพียงอย่างเดียวมาสู่การสร้างโครงสร้างพื้นฐานที่คืนสู่สภาพเดิมได้อย่างรวดเร็วเมื่อเผชิญภัยคุกคาม โดยมีสมมติฐานว่าภัยคุกคามอาจเกิดขึ้นได้ตลอดเวลาด้วย

2. แนวทางดำเนินการของกองทัพไทยเกี่ยวกับภัยคุกคามทางไซเบอร์ในการป้องกัน พัฒนา และบูรณาการความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับหน่วยงานภาครัฐอื่นๆ

จากการศึกษาพบว่ากรอบแนวทางการปฏิบัติของกองทัพไทยในปัจจุบัน เป็นไปในทิศทางเดียวกัน มีเป้าหมายเดียวกัน ใช้ยุทธศาสตร์เดียวกัน กระทรวงกลาโหมได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554 ใช้มาตรฐาน ISO 27001: 2005 และมีมาตรการ NIST Model ตามมาตรฐาน 5 ขั้นตอน ประกอบด้วย 1. การแยกแยะ (Identify) 2. การป้องกัน (Defense) 3. การตรวจพบ (Detection) 4. การตอบสนอง (Respond) 5. การฟื้นตัว (Recevery) อย่างไรก็ตาม ISO 27001: 2005 มีหลักการออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจมากกว่าการนามาใช้ในภารกิจด้านการทหาร ผู้วิจัยจึงมีความกังวลถึงความเหมาะสมของการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม เพราะการมีประสิทธิภาพของการรักษาความปลอดภัยระบบ อุปกรณ์ยุทโธปกรณ์ ซึ่งถูกควบคุมและสั่งการโดยอิเล็กทรอนิกส์ นั้น มีความละเอียดอ่อนและมีความสำคัญต่อความมั่นคงของชาติ ดังนั้น ควรมีการศึกษาเชิงลึกจากยุทธศาสตร์ไซเบอร์ที่เกี่ยวกับทางการทหาร รวมทั้งอาจแก้ไขเพิ่มเติมให้เหมาะสมกับบริบทของกระทรวงกลาโหม แต่ยังคงเป็นไปตามมาตรฐานสากล

การจัดโครงสร้างเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security Organization) ในกระทรวงกลาโหมควรคำนึงถึงสิ่งสำคัญ คือ (1) กำหนดนิยามและกระบวนการต่างๆในการรักษาความปลอดภัยที่ชัดเจน รวมถึงการประสานงานส่วนราชการที่เกี่ยวข้องตามแผนนโยบายรักษาความมั่นคงปลอดภัยทางไซเบอร์ (2) จัดตั้งคณะทำงานหลักเพื่อบริหารและจัดการความมั่นคงปลอดภัยทางไซเบอร์ และกำหนดหน้าที่ความรับผิดชอบในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของส่วนราชการไว้อย่างชัดเจน (3) กำหนดสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศ และให้ระบุความจำเป็นในการเข้าใช้งานระบบสารสนเทศอย่างชัดเจน (4) ควบคุมหน่วยงานภายนอกที่ปฏิบัติงานอยู่ในสำนักงานของส่วนราชการในการใช้ระบบสารสนเทศให้มีความปลอดภัย

ส่วนสำคัญอีกส่วนหนึ่งคือ การสร้างความมั่นคงปลอดภัยทางไซเบอร์เกี่ยวกับการควบคุมการเข้าถึงและการใช้งานข้อมูลสารสนเทศ ซึ่งมีแนวทางดังนี้ (1) บริหารจัดการข้อมูลสารสนเทศโดยจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งการระบุความหน่วยงานเจ้าของเรื่องหรือผู้กำกับดูแลข้อมูลสารสนเทศนั้น (2) มีมาตรการและแนวทางในการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อควบคุมการเข้าถึงและการใช้ข้อมูลสารสนเทศ (3) การสร้างความมั่นคงปลอดภัยด้านการปฏิบัติงาน (4) การตรวจสอบการประเมินและการจัดการกับความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

การบูรณาการร่วมกับหน่วยงานภาครัฐอื่นๆ เห็นควรมีการแลกเปลี่ยนข่าวสารด้านไซเบอร์ระดับกองทัพไปสู่หน่วยงานที่เป็นกลุ่มโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Information Infrastructure : CII) เช่น หน่วยงานไฟฟ้า ประปา ธนาคาร ตัวอย่างเช่น ศูนย์ไซเบอร์ทหารนั้นมีความต้องการร่วมกับกับภาคธนาคาร เพื่อแลกเปลี่ยนข้อมูล คือ งานข่าวด้านยุทธการ และจะมีการพัฒนาต่อไปยังหน่วยงาน ไฟฟ้า ประปา และคมนาคม ถ้าสามารถมีความร่วมมือกับหน่วยงานต่างๆ ได้ จะสามารถทำให้เข้าใจถึงภัยคุกคาม และสร้างความเข้มแข็งไปพร้อมกัน โดยทุกอย่างต้องอยู่ภายใต้นโยบายการดำเนินการเหมือนกัน

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

1. จัดตั้งศูนย์ไซเบอร์แห่งชาติ เพื่อบูรณาการการดำเนินการในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยในโลกไซเบอร์ การให้ความรู้ความเข้าใจ คำปรึกษา และประสานงานกับผู้ที่รับผิดชอบงานด้านความมั่นคงปลอดภัยของระบบสารสนเทศของหน่วยงานอื่น ๆ การดำเนินการเรื่องการติดตาม ตรวจสอบและประเมินผล (Compliance and monitoring) การประเมินความเสี่ยงของระบบสารสนเทศ (ICT Risk Assessment) ในระดับประเทศ โดยมีกลไกประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติ ได้แก่ คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสารแห่งชาติ คณะกรรมการธุรกรรรมทางอิเล็กทรอนิกส์ สภาความมั่นคงแห่งชาติ กระทรวงกลาโหม สำนักงานตำรวจแห่งชาติ เป็นต้น สนับสนุนการวิจัยพัฒนา และเพิ่มจานวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบสารสนเทศและโครงข่าย (Network Security) ของประเทศ รวมถึงการจัดทา ทบทวนและปรับปรุง แผนแม่บทด้านความมั่นคงปลอดภัยของระบบสารสนเทศและโครงข่าย (National Information Securtiy Roadmap) อย่างต่อเนื่อง

2. เร่งประกาศ ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อรองรับการปฏิบัติงานของเจ้าหน้าที่ตามนโยบายและแผนแม่บทเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะสามารถทำให้การดำเนินการเป็นไปในทิศทางที่ดีขึ้น

3. กำหนดกรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อรับมือ ป้องกัน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินงานเป็นไปในทิศทางเดียวกันและสอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564

4. ยกระดับแผนการทำงานร่วมกัน เช่น แผนการซ้อมรับมือภัยคุกคามทางไซเบอร์ รวมถึงจัดทำแผนการปฏิบัติในการรับมือกับภัยคุกคามทางไซเบอร์

5. วางรากฐานการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ เพื่อรองรับความต้องการบุคลากรด้านไซเบอร์ให้เพียงพอในอนาคต โดยรัฐบาลต้องทำงานร่วมกับภาคธุรกิจและสถาบันอุดมศึกษา ในการออกแบบหลักสูตรความมั่นคงไซเบอร์ เพื่อผลิตและพัฒนาบุคลากรที่มีคุณภาพ โดยได้รับการรับรองจากหน่วยงาน CII, ภาครัฐ-เอกชน และสถาบันการศึกษา พร้อมลงทุนในการวิจัยและพัฒนาด้านความมั่นคงไซเบอร์ให้มากขึ้น

ในส่วนของการสร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในสังกัดกระทรวงกลาโหม เพื่อรองรับเทคโนโลยีที่มีความหลากหลายมากขึ้น เพราะการสร้างบุคลากรต้องใช้เวลาและยากที่จะดำรงไว้เมื่อมีการเปลี่ยนแปลง นอกเหนือจากศูนย์ไซเบอร์ของแต่ละเหล่าทัพที่

สามารถส่งเสริมและสนับสนุนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ ในส่วนสถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย มีหน่วยงานในสังกัด คือ โรงเรียนเตรียมทหาร และโรงเรียนช่างฝีมือทหาร ซึ่งจะสามารถใช้วางความรู้พื้นฐานการรักษาความปลอดภัยทางไซเบอร์เพื่อรองรับงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพในอนาคตได้ นอกจากนั้น ในส่วนของหลักสูตรระดับสูงของกองทัพ คือ หลักสูตร การป้องกันราชอาณาจักร (วปอ.) หลักสูตร เสนาธิการทหาร (วสท.) มีการจัดการฝึกแก้ไขสถานการณ์ฉุกเฉิน และการฝึกร่วมของวิทยาลัยการทัพ ซึ่งสามารถฝึกจำลองสถานการณ์การต่อต้านการก่อการร้ายทางไซเบอร์หรือการทำสงครามไซเบอร์เพื่อให้ผู้บริหารจากหน่วยงานต่างๆ ที่เข้ารับการศึกษา มีประสบการณ์ในการบัญชาการสถานการณ์เพื่อรับมือเกี่ยวกับภัยคุกคามทางไซเบอร์ และสามารถนำไปใช้ประโยชน์ในการบริหารหน่วยงานและประเทศชาติในการป้องกันและรักษาความมั่นคงทางไซเบอร์ได้อย่างมีประสิทธิภาพ

6. กำหนดและกระตุ้นให้องค์กรภาครัฐและภาคเอกชนนำมาตรฐาน ISO/IEC 27001 ภาครัฐควรกำหนดและกระตุ้นให้องค์กรภาครัฐและภาคเอกชนนำมาตรฐาน ISO/IEC 27001:2013 (Information Security Management System) หรือเทียบเท่า มาใช้ในองค์กรอย่างจริงจัง โดยเฉพาะธุรกิจที่ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานจากภาครัฐ และการขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ นอกจากนั้น ภาครัฐควรกำหนดโครงสร้างพื้นฐานของชาติ และนโยบายคุ้มครองโครงสร้างพื้นฐานของชาติ และกรอบการดำเนินการให้ชัดเจน การดำเนินงานด้านการรักษาความปลอดภัยไซเบอร์ ควรมีการดำเนินการที่ครอบคลุมหน่วยงานที่เป็นโครงสร้างพื้นฐาน ทั้งของภาครัฐและภาคเอกชน

7. ศึกษาการบริหารความเสี่ยงสารสนเทศ ศึกษากระบวนการการรักษาความปลอดภัยสารสนเทศ เพื่อใช้เป็นข้อมูลในการวางรากฐานระบบรักษาความปลอดภัย ในการวางแนวทางการป้องกันและรักษาความปลอดภัยทางไซเบอร์ให้กับองค์กรต่างๆ ทั้งภาครัฐ ภาคเอกชน โดยต้องลงทุนเพื่อวางรากฐานความมั่นคงปลอดภัยทางไซเบอร์ให้แข็งแกร่ง และยกระดับมาตรฐานการรักษาความปลอดภัยในโลกไซเบอร์ของชาติ สิ่งนี้มีความสำคัญมากเพราะหากรากฐานทางไซเบอร์ไม่มีความแข็งแกร่งพอ ผลจากการโจมตีทางไซเบอร์จะกระทบต่อภาพรวมของเศรษฐกิจและความมั่นคงของชาติ กระทบต่อยุทธศาสตร์ไทยแลน์ 4.0 ที่มุ่งหวังนำเทคโนโลยีมาใช้เป็นสื่อกลางอย่างแน่นอน

ภาครัฐพยายามสร้างให้ประเทศเป็นสถานที่สำหรับนวัตกรรมแห่งการรักษาความปลอดภัยบนโลกไซเบอร์ โดยอาจจัดตั้งศูนย์พัฒนาการรักษาความปลอดภัยไซเบอร์ (Cyber Security Growth Centre) โดยใช้นวัตกรรมแห่งชาติและวิทยาศาสตร์ ร่วมกับกระทรวงวิทยาศาสตร์ กระทรวงเศรษฐกิจดิจิตัล กระทรวงศึกษาธิการ คณะกรรมการวิจัยแห่งชาติ สถาบันอุดมศึกษา ฯลฯ ในการสร้างเครือข่ายการวิจัยและนวัตกรรมระดับชาติ เพื่อกำหนดและจัดลำดับความสำคัญและความท้าทายด้านความปลอดภัยบนโลกไซเบอร์ซึ่งมีความสำคัญต่อผลสำเร็จของชาติ ขับเคลื่อนนวัตกรรมด้านความปลอดภัยบนโลกไซเบอร์ โดยมุ่งเน้นการสนับสนุนการเริ่มต้นระบบรักษาความปลอดภัยบนโลกไซเบอร์และการพัฒนาขีดความสามารถด้านเทคนิคภาย รวมถึงโครงการสร้างและให้ทุนการศึกษาระดับปริญญาเอกเฉพาะด้านไซเบอร์ โครงการเหล่านี้ จะสนับสนุนให้การรักษาความปลอดภัยบนโลกไซเบอร์ที่กำลังเจริญเติบโตและประสบความสำเร็จ และประเทศจะได้รับประโยชน์จากการป้องกันรักษาวามปลอดภัยทางไซเบอร์ที่ดีขึ้น

8. การสร้างความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ รัฐบาลต้องเล็งเห็นว่าปัญหาความมั่นคงทางไซเบอร์เป็นปัญหาในระดับโลก จำเป็นต้องมีและทำงานร่วมกับพันธมิตรต่างประเทศ เพื่อแก้ปัญหาภัยคุกคามทางไซเบอร์ โดยอาจเริ่มจากประชาคมอาเซียน ไปยังระดับภูมิภาคเอเชียจนถึงระดับโลก รัฐบาลต้องมุ่งมั่นที่จะมีบทบาทเชิงรุกในการผลักดันประเด็นเรื่องความมั่นคงไซเบอร์ในเวทีหารือระดับนานาชาติ ตลอดจนส่งเสริมการเสริมสร้างขีดความสามารถและความร่วมมือด้านความมั่นคงไซเบอร์ โดยเฉพาะการสนับสนุนและปฏิบัติตามกฎหมายระหว่างประเทศหรือมาตรการที่ตกลงกันไว้สำหรับการปฏิบัติที่เหมาะสม และสร้างความมั่นใจในทางปฏิบัติเพื่อลดความเสี่ยงจากความขัดแย้งใดๆ

ข้อเสนอแนะระดับปฏิบัติการ

กรณีของประเทศไทยกล่าวได้ว่าถึงเวลาที่ต้องดำเนินการตามมาตรการที่เป็นรูปธรรมเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นดังต่อไปนี้

1. กระตุ้นเตือนองค์กรทั้งภาครัฐและภาคเอกชนให้คำนึงถึงการรักษาความปลอดภัยของเครือข่าย

2. สนับสนุนให้มีการจัดตั้งหน่วยงานด้านความปลอดภัยทางไซเบอร์ในหน่วยงานแต่ละกลุ่ม

3. ศึกษาและจัดทำรายงานวิเคราะห์ความเสี่ยงเรื่องความปลอดภัยของทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ที่ใช้งานและผลกระทบที่อาจเกิดขึ้นจากการโจมตีในหน่วยงานแต่ละกลุ่ม โดยกำหนดมาตรการป้องกัน การบรรเทาเมื่อเกิดปัญหา แผนรับมือฉุกเฉิน และการกู้คืนระบบ

4. ส่งเสริมสนับสนุนการทดสอบและประเมินความเสียหายโดยการจำลองสถานการณ์เมื่อเกิดปัญหาความปลอดภัยทางไซเบอร์

5. จัดให้มีและสนับสนุนแผนการฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐาน

6. สร้างเครือข่ายความร่วมมือเพื่อแลกเปลี่ยนข้อมูลด้านการรักษาความปลอดภัยทางไซเบอร์ความปลอดภัย

7. ส่งเสริมให้ทั้งภาครัฐและภาคเอกชนพัฒนาและจัดทำกระบวนการเกี่ยวกับการรายงานปัญหาความปลอดภัยและการนำไปใช้อย่างเป็นรูปธรรม

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

ศึกษาเกี่ยวกับการพัฒนาการบูรณาการด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย เพื่อให้เห็นถึงแนวทางที่หน่วยงานต่างๆ สามารถบูรณาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

บรรณานุกรม

ภาษาไทย

เอกสารวิจัย

จินดา สระสมบูรณ์, นาวาเอกหญิง. “ปฏิบัติการสงครามไซเบอร์ กองบัญชาการกองทัพไทย”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2557.

ชนกศ์ จรจำรัส, พันเอก. “การพัฒนาศักยภาพทางไซเบอร์ ของกระทรวงกลาโหม”. เอกสารวิจัย, วิทยาลัยการทัพบก, 2560.

ศิวลีย์ สิริโรจน์บริรักษา. “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม”. บทความทางวิชาการ ศูนย์ศึกษายุทธศาสตร์, 2558.

สุทธิศักดิ์ สลักคำ, พลตรี. “ยุทธศาสตร์การป้องกันไซเบอร์ กระทรวงกลาโหม”. เอกสารวิจัย, วิทยาลัยป้องกันราชอาณาจักร, 2558.

กฎหมาย

“พระราชบัญญัติ การจัดทำยุทธศาสตร์ชาติ พ.ศ. 2560”, ราชกิจจานุเบกษา. เล่มที่ 134, 31 กรกฎาคม 2560.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, ราชกิจจานุเบกษา. เล่มที่ 124, 18 มิถุนายน 2550.

“พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549”, ราชกิจจานุเบกษา. เล่มที่ 124, 10 มกราคม 2550.

“พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550”, ราชกิจจานุเบกษา. เล่มที่ 124, 18 มิถุนายน 2550.

“พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544”, ราชกิจจานุเบกษา. เล่มที่ 125, 13 กุมภาพันธ์ 2551.

เอกสารไม่ตีพิมพ์

พัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), สำนักงาน. “ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ..... (ฉบับ ครม. รับหลักการ)”, 2560.

กลาโหม, กระทรวง. “ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ”, 2558

กลาโหม, กระทรวง. “แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ”, 2560

กลาโหม, กระทรวง. “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม”, 2554

สภาความมั่นคงแห่งชาติ, สำนักงาน. “นโยบายความมั่นคงแห่งชาติ”, 2558

สุรชาติ บำรุงสุข, ปัญหาความมั่นคง: ความเปลี่ยนแปลงในทศวรรษแรกของ ค.ศ.2000, เสนาธิปัตย์ ปีที่ 45 ฉบับที่ 3 เดือน ก.ย.-ธ.ค.

วิทยาลัยเสนาธิการทหาร, เอกสารแนะนำฝ่ายเสนาธิการร่วม ภาคที่ 2 ยุทธศาสตร์ชาติ**ฐานข้อมูลอิเล็กทรอนิกส์**

“การประชุม คณะกรรมการเตรียมการไซเบอร์แห่งชาติครั้งแรก”. (ออนไลน์). เข้าถึงได้จาก : http://www.thaigov.go.th/news/contents/details/12111, 2561.

รมว.ดิจิทัลฯ แถลงผลการประชุม คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2561 (ออนไลน์). เข้าถึงได้จาก : http://www.mdes.go.th/view/1/ข่าวกระทรวงฯ/ข่าวรัฐมนตรีว่าการ/3084, 2561

ร่าง พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.... (ออนไลน์). เข้าถึงได้จาก : https://ictlawcenter.etda.or.th/de_laws/detail/de-laws-cyber-security-protection-act, 2561

“สหรัฐฯ เผยแพร่รายงานผลกระทบที่สหรัฐฯได้รับจากภัยคุกคามทางไซเบอร์” (ออนไลน์). เข้าถึงได้จาก : https://www.secnia.go.th/2018/03/06/สหรัฐฯ-เผยแพร่รายงานผลก, 2018

CYBER THREATS 2017 (ออนไลน์). เข้าถึงได้จาก : https://www.etda.or.th/app/webroot/content_files/13/files/1.CYBERBULLYING.pdf, 2018

ภัยไซเบอร์ป่วนไทย“ชาวเน็ต” 67% เสี่ยงเป็นเหยื่อ (ออนไลน์). เข้าถึงได้จาก : http://www.bangkokbiznews.com/news/detail/766588

ภาษาต่างประเทศ

Books

Ted G. Lewis, Critical infrastructure protection in homeland security: defending a networked nation, 2006

Richard Shuttz, Roy Godson and Ted Greenwood,eds., Security for the 1990’s, 1993

Krenson, John G. On Strategy: Integration of DIME in the Twenty-first Century, USAWC Strategy Research Project. Carlisle Barracks : U.S. Army War College, 2012.

United States Department of Defense, “DOD Cyber Strategy”, 2015

Cyber Warfare: Concepts and Strategic Trends, 2012

Air Command and Staff College : Air University : U.S.A.F., 2013

EU Cybersecurity Strategy, 2013

UK's National Cyber Security Strategy 2016 – 2021, 2016

Australia's Cyber Security Strategy, 2016

Thesis

J. Boone Bartholomees, Jr., ed., “U.S. Army War College Guild to National Security Policy and Strategy”, (2nded.) Department of National Security and Strategy, Carlisle Barracks : U.S. Army War College, 2006.

Yager, Henry R. “Strategic Theory for the 21st Century : The Little Book on Big Strategy.”. (Online). Available: http://www.strategicstudiesinstitute.army.mil/ 2006.

Yager, Henry R. “Toward a Theory of Strategy: Art Lykke and the Army War College Strategy Model. In Bartholomees, J. B., U.S. Army War College Guide to National”. (Online). Available: http://www.strategicstudiesinstitute.army.mil/ 2006.

E-Book

“McAfee Labs 2018 Threats Predictions Report” (ออนไลน์). เข้าถึงได้จาก :https://securingtomorrow.mcafee.com/mcafee-labs/2018-threats-predictions/, 2018

“ElasticSearch” (ออนไลน์). เข้าถึงได้จาก : https://www.elastic.co/products/x-pack/security., 2560

ประวัติผู้วิจัย

ชื่อ พลเรือตรี อุดม ประตาทะยัง

วัน เดือน ปีเกิด 1 ตุลาคม 2505

การศึกษา

- นักเรียนเตรียมทหาร รุ่นที่ 22
- ปริญญาตรี วท.บ.(ทร.) โรงเรียนนายเรือ

การทำงาน

- หน.แผนกยุทธการพิเศษ ยก.ทร.
- ผู้บังคับกองพันต่อสู้อากาศยานที่ 11 สอ.รฝ.
- ผู้บังคับหมวดเรือที่ 2 กองเรือพริเกตที่ 2 กร.
- ผู้อำนวยการสำนักงานราชนาวิกสภา ยศ.ทร.
- ผู้อำนวยการศูนย์การฝึก สอ.รฝ.
- เสนาธิการกองเรือยามฝั่ง กร.
- หัวหน้านายทหารฝ่ายอำนวยการ สพ.ทร.
- หัวหน้านายทหารฝ่ายอำนวยการ ขส.ทร.
- รองผู้บัญชาการกองเรือดำน้ำ

ตำแหน่งปัจจุบัน รองเจ้ากรมข่าวทหาร

สรุปย่อ

เรื่อง แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์
ผู้วิจัย พลเรือตรี อุดม ประตาทะยัง **หลักสูตร** วปอ.รุ่นที่ 60
ตำแหน่ง รองเจ้ากรมข่าวทหาร

ความเป็นมาและความสำคัญของปัญหา

ภายใต้การเปลี่ยนแปลงในศตวรรษที่ 21 เทคโนโลยีสารสนเทศทำให้เกิดการเปลี่ยนแปลงทางเศรษฐกิจและสังคมอย่างรวดเร็ว การเชื่อมโยงเครือข่ายออนไลน์กลายเป็นทั้งโอกาสและภัยคุกคามระดับชาติ กลุ่มอาชญากร กลุ่มก่อการร้าย กลุ่มแฮกเกอร์ และรัฐบาลต่างชาติ ต่างมุ่งหาประโยชน์จากโลกไซเบอร์ ซึ่งเป็นสภาวะของโลกเสมือนจริงที่ไม่มีเขตแดนกั้นระหว่างประเทศ ส่งผลให้เกิดภัยคุกคามในรูปแบบใหม่ที่เรียกว่า ภัยคุกคามทางไซเบอร์ โดยที่คนจำนวนมากยังไม่ตระหนักถึงความร้ายแรงของภัยคุกคามนี้

ปัจจุบันประเทศไทยมีการเติบโตและความสามารถในการเข้าถึงโครงข่ายอินเตอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างมาก ทำให้ความเสี่ยงจากภัยคุกคามทางไซเบอร์เพิ่มขึ้น และจะถูกยกระดับเป็นภัยคุกคามเชิงยุทธศาสตร์ของประเทศในอนาคต จากสถานการณ์ไซเบอร์ของประเทศไทยในปี 2558 ถูกจัดอันดับว่าเป็นประเทศที่ถูกโจมตีผ่านระบบไซเบอร์เป็นอันดับที่ 33 จาก 250 ประเทศทั่วโลก โดยเฉพาะสถานการณ์การถูกโจมตีเมื่อเดือนสิงหาคม 2558 นั้น เว็บไซต์ของหน่วยงานราชการ เช่น เว็บไซต์ของจังหวัดลำพูน และเว็บไซต์ของฝ่ายอำนวยการ 1 กองบัญชาการตำรวจนครบาล ถูกเจาะระบบเปลี่ยนหน้าโฮมเพจเป็นข้อความเรียกร้องสันติภาพชาวมุสลิม พร้อมระบุว่าเป็นฝีมือของแฮกเกอร์แอลจีเรีย ซึ่งจะเห็นได้ว่าความมั่นคงปลอดภัยทางไซเบอร์เป็นสิ่งที่ทุกประเทศจะต้องเรียนรู้ให้เกิดความเข้าใจ โดยเฉพาะอย่างยิ่งเข้าใจถึงความร้ายแรงของภัยคุกคามที่อาจเกิดขึ้นและกระทบต่องานด้านความมั่นคงของประเทศในอนาคต ประกอบกับนโยบายของประเทศไทยในปัจจุบันมีนโยบายขับเคลื่อนประเทศไทยสู่ความมั่นคง มั่งคั่ง และยั่งยืน และนำไปสู่ความเป็น Thailand 4.0 ปรับเปลี่ยนโครงสร้างเศรษฐกิจ ไปสู่เศรษฐกิจที่ขับเคลื่อนด้วยนวัตกรรม หน่วยงานของรัฐจึงต้องระมัดระวังในเรื่องภัยคุกคามด้านอาชญากรรมไซเบอร์เป็นอย่างมาก เพราะการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลเป็นทิศทางที่ถูกต้อง แต่ต้องสามารถดำเนินการควบคู่ไปกับยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มแข็งด้วย การศึกษาแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ จึงมีความสำคัญต่อความมั่นคงของไทยในอนาคต ผู้วิจัยจึงมีความสนใจที่จะศึกษาวิจัยเรื่อง “แนวทางที่เหมาะสมในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์” เพื่อรักษาไว้ซึ่งความมั่นคงของประเทศชาติในอนาคตต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการดำเนินการต่อปัญหาภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์
2. เพื่อศึกษาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์
3. เพื่อศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์

ขอบเขตของการวิจัย

1. ขอบเขตด้านเนื้อหา : จะศึกษาเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ พัฒนาการของความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ รูปแบบการโจมตีทางไซเบอร์ ความรุนแรงที่เกิดจากผลกระทบของการโจมตีทางไซเบอร์ต่องานด้านความมั่นคงของประเทศ และศึกษากำหนดแนวทางในการรับมือกับภัยคุกคามอันเนื่องมาจากความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมในอนาคต พร้อมเสนอแนวทางในการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์

2. ขอบเขตด้านประชากร : สัมภาษณ์เชิงลึกต่อผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์จากหน่วยงานต่างๆ ดังนี้

2.1 ผู้เชี่ยวชาญจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวน 5 คน

2.2 ผู้เชี่ยวชาญจากกระทรวงกลาโหม จำนวน 5 คน

2.3 ผู้เชี่ยวชาญจากสภาความมั่นคงแห่งชาติ จำนวน 5 คน

2.4 ผู้เชี่ยวชาญจากกองบัญชาการกองทัพไทยและเหล่าทัพต่างๆ จำนวน 10 คน

3. ขอบเขตด้านเวลา : จะใช้เวลาในการศึกษาวิจัยในครั้งนี้ตั้งแต่ พ.ย.60 - พ.ค.61

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยมีการดำเนินการดังนี้

1. การรวบรวมข้อมูล

1.1 ข้อมูลทุติยภูมิ จะรวบรวมเรื่องเกี่ยวกับยุทธศาสตร์ความมั่นคงทางไซเบอร์จากเอกสารและข้อมูลที่เกี่ยวข้อง จากแหล่งข้อมูลประกอบด้วย ห้องสมุด วปอ. ห้องสมุดกองทัพเรือ สภาความมั่นคงแห่งชาติ รวมถึงจากเว็บไซต์ที่เกี่ยวข้อง

1.2 ข้อมูลปฐมภูมิ รวบรวมจากการสัมภาษณ์ผู้เชี่ยวชาญด้านความมั่นคงทางไซเบอร์จำนวน 25 คน ของขอบเขตด้านประชากรดังที่กล่าวแล้วข้างต้น

2. การวิเคราะห์ข้อมูล จะใช้การวิเคราะห์เนื้อหา (Content Analysis) เป็นหลัก โดยการนำข้อมูลที่รวบรวมได้ทั้งข้อมูลทุติยภูมิและข้อมูลปฐมภูมิ มาจัดระเบียบแล้วนำมาวิเคราะห์ร่วมกับแนวความคิด ทฤษฎี ที่เกี่ยวข้อง แล้วสังเคราะห์ออกมาเป็นแนวทางในการรับมือกับภัยคุกคามทางไซเบอร์

ผลการวิจัย

1. การดำเนินการต่อภัยทางไซเบอร์ของประเทศไทย

ประเทศไทยใช้มาตรฐานสากล ISO/IEC 27001:2013 (Information Security Management System) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อเป็นแนวทางในการจัดทำระบบบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศซึ่งเป็นมาตรฐานที่ได้รับการยอมรับทั้งภาครัฐและเอกชนว่าเป็นแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีประสิทธิภาพที่ใช้กันทั่วโลก รวมทั้งกระทรวงกลาโหม ได้รับนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (กระทรวงเทคโนโลยีสารสนเทศ

และการสื่อสารเดิม) มาปฏิบัติ โดยได้กำหนดไว้ใน “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554

นโยบายความมั่นคงแห่งชาติทั่วไป โดยเน้นที่การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ 3 ประการ คือ 1.) ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ 2.) พัฒนาการบังคับใช้กฎหมาย 3.) พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ

ในส่วนของประเทศไทยมีการกำหนดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) โดยแบ่งหน่วยงานหรือเครือข่ายซึ่งจัดอยู่ในข่ายโครงสร้างพื้นฐานเป็น 6 กลุ่ม ดังนี้ 1.) กลุ่มความมั่นคงและบริการภาครัฐที่สำคัญ กำกับโดย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ กระทรวงกลาโหม 2.) กลุ่มการเงิน กำกับโดย ธนาคารแห่งประเทศไทย คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย 3.) กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กำกับโดย คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ 4.) กลุ่มการขนส่งและโลจิสติกส์ กำกับโดย กระทรวงคมนาคม) 5.) กลุ่มพลังงานและสาธารณูปโภค กำกับโดย กระทรวงพลังงาน และ กระทรวงมหาดไทย 6.) กลุ่มสาธารณสุข กำกับโดย กระทรวงสาธารณสุข การทำงานร่วมกันระหว่างกลุ่มงาน

2. การดำเนินการของกองทัพไทยต่อภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์

ในส่วนกระทรวงกลาโหม ได้มีการจัดทำยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.2558 ขึ้นเพื่อเป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วง 4 ปี โดยมีการกำหนดประเด็นยุทธศาสตร์ไว้ 3 ประเด็นคือ ป้องกัน ป้องปราม และผนึกกำลัง และได้จัดทำแผนแม่บท ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.2560 – 2564 ซึ่งกระทรวงกลาโหมได้กำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยอาศัยอำนาจตามความในมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 ตามมาตรฐาน ISO 27001: 2013 เพื่อยึดเป็นแนวทางปฏิบัติในการลดความเสี่ยงจากการใช้เทคโนโลยีสารสนเทศ

ผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์รวมถึงทราบปัญหาอุปสรรคที่เกิดในการดำเนินการต่อภัยคุกคามไซเบอร์ สรุปได้ว่า

1. การบูรณาการการดำเนินงานรักษาความปลอดภัยทางไซเบอร์

การดำเนินงานรักษาความปลอดภัยไซเบอร์ของประเทศไทยยังมีลักษณะต่างฝ่ายต่างทำ ปัจจุบันความเสี่ยงด้านความปลอดภัยทางไซเบอร์กำลังเพิ่มมากขึ้น แต่ตลาดเทคโนโลยีต่างๆ มีการรักษาความปลอดภัยแบบแยกส่วนและขัดแย้งกัน รวมถึงขาดแคลนทักษะด้านการรักษาความปลอดภัย ทำให้หลายองค์กรไม่เข้าใจและไม่สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพ

2. พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ยังไม่ได้ประกาศใช้

ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์ โดยให้อำนาจพิเศษแก่ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กปช. มีอำนาจสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความ

มั่นคงปลอดภัยไซเบอร์ในทิศทางเดียวกัน และในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง กปช. มีอำนาจอนุมัติให้เจ้าหน้าที่เข้าถึงการติดต่อสื่อสารทุกรูปแบบของประชาชน เช่น ไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด หรือดำเนินการตามมาตรการที่เหมาะสม เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และระงับยับยั้งความเสียหายที่จะเกิดขึ้น โดยไม่ต้องขอคำสั่งศาล

อย่างไรก็ตาม ปัจจุบัน (ร่าง) พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่ได้ประกาศใช้ ดังนั้นการปฏิบัติภารกิจเชิงรุกทั้งภายในและภายนอกประเทศ ของส่วนสนับสนุนในการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Computer Security Incident Response Team : CSIRT) จึงไม่มีข้อกฎหมายรองรับการดำเนินการในปัจจุบันซึ่งยังเป็นข้อจำกัดที่สำคัญ

3. การขาดแคลนบุคลากรด้านการรักษาความปลอดภัยไซเบอร์

เครื่องมือที่สำคัญที่สุดในการรักษาความปลอดภัยทางไซเบอร์คือทรัพยากรมนุษย์ เป็นหนึ่งในอุปสรรคสำคัญของวงการความมั่นคงปลอดภัยไซเบอร์ เพราะจำนวนผู้เชี่ยวชาญในด้านนี้ยังมีไม่เพียงพอกับความต้องการในตลาดแรงงานทั่วโลก จากข้อมูลของเว็บไซต์ Indeed.com ในปี 2559 ซึ่งเป็นเว็บไซต์สำหรับประกาศหางาน พบว่าประเทศที่มีความต้องการบุคลากรด้านไซเบอร์มากที่สุดคือประเทศอิสราเอล รองลงมาคือประเทศไอร์แลนด์ สหราชอาณาจักร และสหรัฐฯ ส่วนหลายประเทศในแถบเอเชียแปซิฟิก เช่น ญี่ปุ่น มาเลเซีย และสิงค์โปร์ ได้เริ่มตระหนักถึงความสำคัญของปัญหาการขาดแคลนบุคลากรและเริ่มมีโครงการสนับสนุนการพัฒนาบุคลากรด้วยมาตรการต่างๆ ทั้งการพยายามเพิ่มหลักสูตรการศึกษา และการพัฒนาทักษะบุคลากรให้มีความเชี่ยวชาญ ในประเทศไทยเอง ปัจจุบันได้มีหลายหน่วยงานที่มีความพยายามผลักดันการพัฒนาในด้านนี้ เช่น เริ่มมีการเปิดสอนวิชาด้านความมั่นคงปลอดภัยไซเบอร์ในมหาลัยระดับชั้นปริญญาตรี หรือมีการเปิดให้บุคคลทั่วไปเข้ารับการอบรมและสอบใบรับรองด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแนวโน้มในอนาคตความต้องการบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จะเพิ่มขึ้นอย่างมหาศาล แต่การพัฒนาบุคลากรด้านนี้ยังไม่สามารถทำได้ทันต่อความต้องการ

ในส่วนหน่วยงานในสังกัดกระทรวงกลาโหมนอกเหนือจากศูนย์ไซเบอร์ของแต่ละเหล่าทัพที่สามารถส่งเสริมและสนับสนุนงานด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ เช่น กรมสรรพกำลังกลาโหมสนับสนุนในด้านการระดมสรรพกำลัง การคัดสรรบุคคลากร สถาบันเทคโนโลยีป้องกันประเทศ (องค์การมหาชน) ส่งเสริมการวิจัยพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น

4. องค์กรภาคเอกชนปกปิดเหตุการณ์การถูกโจมตีทางไซเบอร์เนื่องจากกลัวการเสียชื่อเสียง

การโจมตีทางไซเบอร์ต่อภาคธุรกิจนั้นมักถูกปกปิดเหตุการณ์ไว้ และไม่แจ้งให้หน่วยงานที่เกี่ยวข้องดำเนินการแก้ไข เนื่องจากแนวความคิดที่กลัวการเสียชื่อเสียง ทำให้นักลงทุนหรือลูกค้าขาดความเชื่อมั่นและส่งผลกระทบต่อผู้ประกอบการ ซึ่งการปกปิดดังกล่าวอาจส่งผลกระทบต่อระบบเศรษฐกิจและความมั่นคงในภาพรวมของประเทศในอนาคต หากไม่ได้รับการป้องกันหรือแก้ไขอย่างทันท่วงที

ศึกษาแนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ สรุปได้ว่า

1. แนวทางการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มีทิศทางที่ชัดเจน และครอบคลุมประเด็นความสำคัญและเร่งด่วนต่อการพัฒนาประเทศไทย ตามนโยบาย Thailand 4.0

จากการศึกษาข้อมูลและวิเคราะห์ปัญหาต่างๆ ควรกำหนดแนวทางการปฏิบัติออกเป็น 5 รูปแบบ เพื่อการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ 1.) การบูรณาการความร่วมมือด้านไซเบอร์ 2.) การวางระบบป้องกันภัยคุกคามทางไซเบอร์ 3.) สร้างความตระหนักและให้ความรู้แก่ผู้บริหารของหน่วยงานทั้งภาครัฐและภาคเอกชน 4.) การผลิตและดึงดูดทรัพยากรบุคคล 5.) ความร่วมมือด้านความมั่นคงทางไซเบอร์ระหว่างประเทศ

การเสริมสร้างความสำเร็จของการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้ง 5 ประการนี้ จะสามารถช่วยในการพัฒนานวัตกรรมแห่งชาติและวิทยาศาสตร์ ให้เกิดความทันสมัยและตอบสนองต่อยุทธศาสตร์ไทยแลน์ 4.0 และระบบเศรษฐกิจในศตวรรษที่ 21 เป็นประโยชน์ต่อการพัฒนาคุณภาพชีวิตของประชาชนผ่านการสร้างสังคมและเศรษฐกิจดิจิทัลในหลายแง่มุม โดยต้องอาศัยความร่วมมือทั้งจากรัฐบาล ภาคเอกชน ร่วมกันแก้ไขปัญหาด้านความปลอดภัยบนโลกไซเบอร์ เพื่อให้โลกไซเบอร์เป็นเครื่องมือสำคัญในการพัฒนาเทคโนโลยีนวัตกรรม พัฒนาเศรษฐกิจ และโอกาสทางการค้ารูปแบบใหม่อย่างเท่าเทียมกัน ซึ่งถือเป็นการเปลี่ยนแปลงกระแสในพื้นที่สาธารณะ สำหรับภาคธุรกิจ รัฐจึงจำเป็นต้องเปลี่ยนมุมมองจากการเน้นป้องกันภัยคุกคามเพียงอย่างเดียวมาสู่การสร้างโครงสร้างพื้นฐานที่คืนสู่สภาพเดิมได้อย่างรวดเร็วเมื่อเผชิญภัยคุกคาม

2. แนวทางดำเนินการของกองทัพไทยเกี่ยวกับภัยคุกคามทางไซเบอร์ในการป้องกัน พัฒนา และบูรณาการความมั่นคงปลอดภัยทางไซเบอร์ร่วมกับหน่วยงานภาครัฐอื่นๆ

จากการศึกษาพบว่ากรอบแนวทางการปฏิบัติของกองทัพไทยในปัจจุบัน เป็นไปในทิศทางเดียวกัน มีเป้าหมายเดียวกัน ใช้ยุทธศาสตร์เดียวกัน แต่ยังใช้มาตรฐานไม่เหมือนกัน เพราะกระทรวงกลาโหม ใช้มาตรฐาน ISO 27001: 2013 ศูนย์ไซเบอร์ทหาร กองบัญชาการกองทัพไทย ใช้การดำเนินงานตามมาตรฐาน NIST ซึ่งแม้จะเป็นมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากลที่ใช้ทั่วโลก แต่ยังไม่เหมาะสมกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม เพราะมีหลักการออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจมากกว่าการนามาใช้ในภารกิจด้านการทหาร ดังนั้น ในส่วนของกระทรวงกลาโหมควรนำมาตรฐาน U.S. DoD มาปรับใช้ เพราะเป็นพื้นฐานสาหรับกระบวนการประเมินความปลอดภัยของกระทรวงกลาโหม เพื่อความมีประสิทธิภาพของการรักษาความปลอดภัยระบบ อุปกรณ์ ยุทโธปกรณ์ ซึ่งถูกควบคุมและสั่งการโดยอิเล็กทรอนิกส์ รวมทั้งการแก้ไขเพิ่มเติมให้เหมาะสมกับบริบทของกระทรวงกลาโหม แต่ยังคงเป็นไปตามมาตรฐานสากล

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

1.1 จัดตั้งศูนย์ไซเบอร์แห่งชาติ เพื่อบูรณาการการดำเนินการในส่วนที่เกี่ยวข้องกับความมั่นคงปลอดภัยในโลกไซเบอร์

1.2 เร่งประกาศ ร่าง พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

1.3 วางรากฐานการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ เพื่อรองรับความต้องการบุคลากรด้านไซเบอร์ให้เพียงพอในอนาคต

ในส่วนของกระทรวงกลาโหมนั้น ในส่วนสถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย มีหน่วยงานในสังกัด คือ โรงเรียนเตรียมทหาร และโรงเรียนช่างฝีมือทหาร ซึ่งจะสามารถใช้วางรากฐานบุคลากรเพื่อรองรับงานด้านความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพในอนาคตได้ นอกจากนั้น ในส่วนของหลักสูตรระดับสูงของกองทัพ คือ หลักสูตร การป้องกันราชอาณาจักร (วปอ.) หลักสูตร เสนาธิการทหาร (วสท.) มีการจัดการฝึกแก้ไขสถานการณ์ฉุกเฉิน และการฝึกร่วมของวิทยาลัยการทัพ ซึ่งสามารถใช้ฝึกจำลองสถานการณ์การโจมตีทางไซเบอร์ การต่อต้านการก่อการร้ายทางไซเบอร์ หรือการทำสงครามไซเบอร์ เพื่อให้ผู้บริหารจากหน่วยงานต่างๆ ที่เข้ารับการศึกษา มีประสบการณ์ในการบัญชาการสถานการณ์เพื่อรับมือเกี่ยวกับภัยคุกคามทางไซเบอร์

1.4 ภาครัฐควรกำหนดและกระตุ้นให้องค์กรภาครัฐและภาคเอกชนนำมาตรฐาน ISO/IEC 27001:2013 (Information Security Management System) หรือเทียบเท่า มาใช้ในองค์กรอย่างจริงจัง โดยเฉพาะธุรกิจที่ดำเนินการเกี่ยวกับโครงสร้างพื้นฐานจากภาครัฐ

1.5 ศึกษาการบริหารความเสี่ยงสารสนเทศ ศึกษากระบวนการการรักษาความปลอดภัยสารสนเทศ เพื่อใช้เป็นข้อมูลในการวางรากฐานระบบรักษาความปลอดภัย ภาครัฐต้องพยายามสร้างให้ประเทศเป็นสถานที่สำหรับนวัตกรรมแห่งการรักษาความปลอดภัยบนโลกไซเบอร์ โดยอาจจัดตั้งศูนย์พัฒนาการรักษาความปลอดภัยไซเบอร์ โดยร่วมกับหน่วยงานต่างๆ ในการสร้างเครือข่ายการวิจัยและนวัตกรรมระดับชาติ เพื่อกำหนดและจัดลำดับความสำคัญและความท้าทายด้านความปลอดภัยบนโลกไซเบอร์ โดยมุ่งเน้นการสนับสนุนการเริ่มต้นระบบรักษาความปลอดภัยบนโลกไซเบอร์และการพัฒนาขีดความสามารถด้านเทคนิค รวมถึงโครงการสร้างและให้ทุนการศึกษาระดับปริญญาเอกเฉพาะด้านไซเบอร์ โครงการเหล่านี้ จะสนับสนุนให้การรักษาความปลอดภัยบนโลกไซเบอร์ที่กำลังเจริญเติบโตและประสบความสำเร็จ และประเทศจะได้รับประโยชน์จากการป้องกันรักษาวามปลอดภัยทางไซเบอร์ที่ดีขึ้น

2. ข้อเสนอแนะระดับปฏิบัติการ

กรณีของประเทศไทยกล่าวได้ว่าถึงเวลาที่ต้องดำเนินการตามมาตรการที่เป็นรูปธรรมเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นดังต่อไปนี้

2.1 กระตุ้นเตือนองค์กรทั้งภาครัฐและภาคเอกชนให้คำนึงถึงการรักษาความปลอดภัยของเครือข่าย

2.2 สนับสนุนให้มีการจัดตั้งหน่วยงานด้านความปลอดภัยทางไซเบอร์ในหน่วยงาน

2.3 ศึกษาและจัดทำรายงานวิเคราะห์ความเสี่ยงเรื่องความปลอดภัยของทั้งระบบฮาร์ดแวร์และซอฟต์แวร์ที่ใช้งานและผลกระทบที่อาจเกิดขึ้นจากการโจมตีในหน่วยงานแต่ละกลุ่ม โดยกำหนดมาตรการป้องกัน การบรรเทาเมื่อเกิดปัญหา แผนรับมือฉุกเฉิน และการกู้คืนระบบ

2.4 ส่งเสริมสนับสนุนการทดสอบและประเมินความเสียหายโดยการจำลองสถานการณ์เมื่อเกิดปัญหาความปลอดภัยทางไซเบอร์

2.5 จัดให้มีและสนับสนุนแผนการฝึกอบรมการรักษาความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐาน

2.6 สร้างเครือข่ายความร่วมมือเพื่อแลกเปลี่ยนข้อมูลด้านการรักษาความปลอดภัยทางไซเบอร์ความปลอดภัย

2.7 ส่งเสริมให้ทั้งภาครัฐและภาคเอกชนพัฒนาและจัดทำกระบวนการเกี่ยวกับการรายงานปัญหาความปลอดภัยและการนำไปใช้อย่างเป็นรูปธรรม

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

ศึกษาเกี่ยวกับการพัฒนาการบูรณาการด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย เพื่อให้เห็นถึงแนวทางที่หน่วยงานต่างๆ สามารถบูรณาการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ