ศูนย์ศึกษายุทธศาสตร์
สถาบันวิชาการป้องกันประเทศ

เอกสารศึกษาเฉพาะกรณี
เรื่อง แนวทางการพัฒนากองทัพไทย

ด้านการรักษาความมั่นคงปลอดภัย ทางไซเบอร์

ข้อมูลทางบรรณานุกรมของสำนักหอสมุดแห่งชาติ
National Library of Thailand Cataloging in Publication Data
เอกสารศึกษาเฉพาะกรณี เรื่อง แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
พิมพ์ครั้งที่ ๑ – กรุงเทพฯ จำนวน ๕๐๐ เล่ม ISSN ๐๘๕๘-๘๗๕๑
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ, ๒๕๖๐ จำนวน ๖๔ หน้า

ผู้อำนวยการ	:	พลตรี อภิศักดิ์	สมบัติเจริญนนท์
ที่ปรึกษา	:	พันเอก กิตติ	คงสมบัติ
	:	พันเอก อรรคเดช	ประทีปอุษานนท์
	:	พันเอกหญิง อารยา	จุลานนท์
	:	นาวาอากาศเอกหญิง จุฬารัตน์	เพชรวิเศษ
	:	พันเอก สุทัศน์	คร่ำในเมือง
หัวหน้าโครงการ	:	พันเอก นิรุจ	ดวงปัญญา
นักวิจัย	:	นางสาว ธาราทิพย์	กัลยาณมิตร
คณะวิจัย	:	เรือโทหญิง นันทิยา	ทองคณารักษ์
		จ่าเอก สามภพ	ศรีอักษร
		นางสาว มนวดี	ตั้งตรงหฤทัย
		นางสาว หัสยา	ไทยานนท์
		นางสาว กรรณิการ์	มหาสารกุล
พิสูจน์อักษร	:	จ่าอากาศตรี ชาญชัย	วังวงค์
		นางสาว ชุตินธร	พรวุฒิกูล
		นาง กัญจนีพร	มหาวรากร

จัดพิมพ์โดย

กองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๔๐๐
โทร. ๐ ๒๒๗๕ ๕๗๑๕ เว็บไซต์ http://www.ssctthailand.org

เอกสารศึกษาเฉพาะกรณี
เรื่อง แนวทางการพัฒนากองทัพไทย
ด้านการรักษาความมั่นคงปลอดภัย
ทางไซเบอร์

คำนำ

สถานการณ์และการเปลี่ยนแปลงของโลกอย่างรวดเร็วในปัจจุบัน ส่งผลต่อความมั่นคงของนานาประเทศในหลายมิติรวมทั้งประเทศไทย มีสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ในหลายระดับ ตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ สังคม การเมือง รวมไปถึงสภาวะแวดล้อมรอบตัวเรา ล้วนแต่ส่งผลต่อความสงบเรียบร้อยและความมั่นคงในประเทศ โดยจะใช้ในลักษณะการจารกรรม การก่อการร้าย รวมทั้งใช้เป็นเครื่องมือในการก่อกวนหรือทำลายความสงบเรียบร้อยของประเทศฝ่ายตรงข้าม ความตระหนักถึงศักยภาพของไซเบอร์ต่อความมั่นคงของชาตินั้นเกิดขึ้นอย่างกว้างขวางทั่วโลก ซึ่งหลายประเทศพยายามสร้างและพัฒนาขีดความสามารถทางไซเบอร์ เพื่อบ่งชี้ว่าประเทศของตนมีศักยภาพที่ก่อให้เกิดความได้เปรียบและความสามารถในการแข่งขันด้านต่างๆ แต่ยิ่งมีความก้าวหน้าและพึ่งพาไซเบอร์มากเพียงใด ยิ่งเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้

คุณลักษณะสำคัญประการหนึ่งของไซเบอร์ คือ สามารถแพร่กระจายอย่างรวดเร็วและไร้ซึ่งพรมแดน จึงนับเป็นภัยที่สามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก ประเทศไทยจึงต้องเตรียมการและใช้ศักยภาพด้านไซเบอร์ให้เป็นไปอย่างสอดคล้องกับสถานการณ์ระดับประเทศ ระดับภูมิภาค และในระดับโลกอย่างเกิดประโยชน์สูงสุด

ด้วยเหตุดังกล่าว ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ จึงได้จัดทำเอกสารศึกษาเฉพาะกรณี เรื่อง “แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์” ขึ้น เพื่อศึกษาสภาพแวดล้อมของภัยคุกคามความมั่นคงด้านไซเบอร์ในอนาคต และให้ข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ศูนย์ศึกษายุทธศาสตร์
สถาบันวิชาการป้องกันประเทศ

สารบัญ

สารบัญภาพ

สารบัญตาราง

ส่วนที่ ๑
บทนำ

ส่วนที่ ๑

บทนำ

ปัจจุบันเป็นยุคโลกาภิวัตน์ (Globalization) ที่การติดต่อสื่อสารไร้พรมแดน โดยการเชื่อมต่อด้วยอินเทอร์เน็ตมีอิทธิพลอย่างมากในการดำรงชีวิตประจำวัน ไม่ว่าจะเป็นการควบคุมระบบสื่อสารโทรคมนาคม ระบบไฟฟ้า ธนาคารหรือสาธารณูปโภค และระบบขนส่งของประเทศ ในขณะเดียวกันก็มีปรากฏการณ์ของอาชญากรรมอิเล็กทรอนิกส์ หรือ Cyber Crime ที่มีทั้งการล้วงข้อมูลความลับ การก่ออาชญากรรมและยักยอกทรัพย์มากขึ้น มีการใช้เทคนิคใหม่ที่เพิ่มความสลับซับซ้อนด้วยช่องทางการเข้าถึงข้อมูลที่หลากหลายยิ่งขึ้น โดยเฉพาะในเรื่อง Personal Mobile Devices ที่ใช้มือถือเชื่อมต่ออินเตอร์เน็ต การส่งข้อมูลขยะอันไม่พึงประสงค์ (Spam) การหลอกลวงผ่านสื่ออินเทอร์เน็ต (Phishing) ตลอดจนการเจาะระบบ (Hack) เพื่อเข้าถึงข้อมูลชั้นความลับ ซึ่งปัจจุบันแฮกเกอร์ (Hacker) ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคารหรือผู้ให้บริการธุรกรรมออนไลน์เท่านั้น แต่ได้เปลี่ยนเป้าหมายเป็นผู้ใช้งานอินเทอร์เน็ตซึ่งเข้าถึงได้ง่ายกว่าแทน โดยอาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานทั่วไปเป็นเครื่องมือ นอกจากนี้ หน่วยงานภาครัฐหรือหน่วยงานที่มีข้อมูลสำคัญ เช่น หน่วยงานทางทหาร หน่วยงานความมั่นคงปลอดภัยของประเทศ หน่วยงานด้านการเมือง หรือองค์กรธุรกิจขนาดใหญ่อาจตกเป็นเป้าหมายของการจารกรรมข้อมูลและทำลายระบบข้อมูลต่างๆ อีกด้วย ซึ่งเหตุการณ์และแนวโน้มที่เกิดขึ้นเหล่านี้ แสดงให้เห็นถึงลักษณะภัยคุกคามรูปแบบใหม่ที่เปลี่ยนแปลงไปสู่รูปแบบของสงครามอสมมาตร (Asymmetric Warfare) ที่ฝ่ายตรงข้าม หรือผู้ก่อการร้ายจะใช้โจมตีจุดสำคัญที่เป็นหัวใจของชาติโดยไม่จำเป็นต้องมีกำลังทางทหาร ผ่านการใช้สื่อดิจิทัล (Digital Media)

และเทคโนโลยีโทรคมนาคม (Telecommunication Technology) เป็นเครื่องมือ โดยภัยคุกคามดังกล่าวนี้จะเป็นภัยคุกคามที่มีผลกระทบในระดับนานาชาติ

ในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้นั้น มีความร่วมมือด้านไซเบอร์ของประเทศสมาชิกในประชาคมอาเซียน ซึ่งความมั่นคงไซเบอร์นั้นเป็นส่วนหนึ่งของความร่วมมือภายใต้เสาหลักประชาคมการเมือง - ความมั่นคง โดยกลไกหลักที่เป็นเวทีหารือและทบทวนความร่วมมือด้านความมั่นคงไซเบอร์ คือการประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) และการประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC) ถึงแม้ว่าความร่วมมือในช่วงต้นจะเน้นไปที่การต่อต้านยาเสพติดเป็นสำคัญ แต่ในการประชุม AMMTC ครั้งที่ ๓ เมื่อ ต.ค.๔๔ ณ ประเทศสิงคโปร์ ที่ประชุมได้ตกลงที่จะผนวกความร่วมมือด้านความมั่นคงไซเบอร์ให้เป็นส่วนหนึ่งในแผนงานเพื่อจัดทำแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ (ASEAN Plan of Action to Combat Transnational Crime) เป็นครั้งแรก สะท้อนถึงการตระหนักว่าอาชญากรรมข้ามชาติมิได้จำกัดอยู่เพียงอาชญากรรมที่พบเห็นได้เฉพาะหน้า เช่น การก่อการร้าย การค้ามนุษย์ หรือการค้าอาวุธสงครามเท่านั้น

ความจริงจังของภัยคุกคามทางไซเบอร์ในช่วงหลายปีที่ผ่านมา กอปรกับการตระหนักรู้ในความเชื่อมโยงระหว่างความมั่นคงไซเบอร์กับความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้ที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and IT Ministers Meeting: TELMIN) ครั้งที่ ๑๔ เมื่อ ม.ค.๕๘ ได้บรรจุประเด็นความมั่นคงไซเบอร์ลงในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร

ของอาเซียน ฉบับที่ ๒ ระหว่าง ปี พ.ศ. ๒๕๕๙ - ๒๕๖๓ (ASEAN ICT Master Plan ๒๐๒๐) แผนแม่บทดังกล่าวได้กำหนดกลยุทธ์หลัก (Strategic Thrusts) เพิ่มเติมจากแผนแม่บทฉบับเดิม ๓ ประการ โดยหนึ่งในนั้น คือกลยุทธ์ด้านความปลอดภัยและหลักประกันด้านข้อมูลข่าวสาร ซึ่งประกอบด้วย การพัฒนาหลักการด้านความปลอดภัยของข้อมูลระดับภูมิภาค และส่งเสริมความเข้มแข็งและประสิทธิภาพของความร่วมมือเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินด้านไซเบอร์อย่างทันท่วงที โดยมีเป้าหมายเพื่อเสริมสร้างความเชื่อมั่นให้กับเศรษฐกิจดิจิทัลของอาเซียนและปรับปรุงความร่วมมือในการรับมือกับสถานการณ์ฉุกเฉินด้านไซเบอร์ของภูมิภาคให้มีประสิทธิภาพยิ่งขึ้น

นอกจากความร่วมมือภายในภูมิภาค อาเซียนยังขยายความร่วมมือด้านความมั่นคงไซเบอร์กับประเทศคู่เจรจา เช่น ญี่ปุ่น โดยได้ร่วมกันออกแถลงการณ์ร่วมเพื่อส่งเสริมความร่วมมือด้านการต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ พร้อมทั้งยืนยันว่าจะส่งเสริมความมั่นคงปลอดภัยของการใช้เทคโนโลยีสารสนเทศและการสื่อสาร และต่อต้านอาชญากรรมไซเบอร์ในรูปแบบต่างๆ รวมทั้งยังร่วมกันจัดการประชุมหารืออาเซียน-ญี่ปุ่น ว่าด้วยอาชญากรรมไซเบอร์ (ASEAN-Japan Cybercrime Dialogue) เพื่อเป็นเวทีหารือกรอบความร่วมมือและส่งเสริมศักยภาพการรับมือกับภัยคุกคามไซเบอร์ระหว่างกัน (ASEAN Watch, ๒๕๕๙, หน้า ๑-๓)

ปัจจุบัน ประเทศไทยมีวิสัยทัศน์ในการบริหารประเทศ คือ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” โดยรัฐบาลมีภารกิจสำคัญในการขับเคลื่อนปฏิรูปประเทศด้านต่างๆ เพื่อปรับแก้ จัดระบบ ปรับทิศทาง และสร้างหนทางพัฒนาประเทศให้เจริญ และสามารถรับมือกับโอกาสและภัยคุกคามแบบใหม่ที่เปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะอย่างยิ่ง การมุ่งให้ความสำคัญต่อ

การพัฒนาเศรษฐกิจ เพื่อให้ทันต่อการขับเคลื่อนของโลกสมัยใหม่ ภายใต้วิสัยทัศน์เชิงนโยบายการพัฒนาเศรษฐกิจของประเทศไทยหรือที่เรียกกันอย่างคุ้นหูกันว่า “Thailand ๔.๐” โดยจะเป็นยุคที่เศรษฐกิจจะขับเคลื่อนด้วยนวัตกรรม (บวร เทศารินทร์, ๒๕๕๙, หน้า ๒) จากนโยบายในการขับเคลื่อนประเทศที่จะมุ่งเน้นให้มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในการพัฒนาอาจนำมาสู่ภัยคุกคามด้านอาชญากรรมไซเบอร์ได้ เนื่องจากการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิตอล กอปรกับความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชาชนในประเทศไทยเพิ่มขึ้นอย่างก้าวกระโดดในช่วง ๒ - ๓ ปีที่ผ่านมา ความเสี่ยงด้านภัยคุกคามไซเบอร์จึงมีสูงขึ้นหลายเท่าตัว ทั้งในมิติของสังคม เศรษฐกิจ การเมือง และการทหาร และจะเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศอย่างหลีกเลี่ยงไม่ได้ (เศรษฐพงค์ มะลิสุวรรณ, ๒๕๕๙, หน้า ๒)

กองทัพไทยถือเป็นหน่วยงานหลักที่มีภารกิจในด้านการรักษาความมั่นคงปลอดภัยของประเทศชาติ ดังที่ระบุไว้ใน รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐ กล่าวคือ เมื่อเกิดเหตุหรือมีภัยคุกคามใดก็ตามเข้ามาสู่ประเทศชาติ กองทัพจึงเป็นหน่วยงานแรกที่ต้องตระหนักและรับมือกับเหตุการณ์ต่างๆ ที่จะเกิดขึ้น เช่นเดียวกับภัยคุกคามด้านไซเบอร์ที่มีแนวโน้มทวีความรุนแรงมากยิ่งขึ้นในปัจจุบัน ตลอดถึงนโยบายในการดำเนินงานของรัฐบาลและการดำเนินชีวิตประจำวันของประชาชนไทยนั้นผูกติดกับเทคโนโลยีและระบบดิจิทัลมากยิ่งขึ้น จึงเป็นการสมควรที่กองทัพจะต้องตระหนักถึงความมั่นคงปลอดภัยด้านไซเบอร์อย่างจริงจัง

๑.๑ สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ

หากกล่าวถึงความรุนแรงจากไซเบอร์ที่ประเทศในประชาคมโลกได้รับผลกระทบร้ายแรง คงเป็นตัวอย่างเหตุการณ์ของการทำสงครามไซเบอร์ (Cyber Warfare) ในต่างประเทศ โดยเหตุการณ์ที่นับว่าไซเบอร์สามารถใช้เป็นอาวุธในการโจมตีฝ่ายตรงข้ามได้อย่างแท้จริง คือ เหตุการณ์การโจมตี Stuxnet ๒๐๐๙-๒๐๑๐ ที่โรงงานนิวเคลียร์ของอิหร่านถูกโจมตี ซึ่งคาดว่าเป็นความร่วมมือระหว่างสหรัฐฯ กับอิสราเอล โดย Stuxnet เป็นการโจมตีโรงงานนิวเคลียร์ของอิหร่านด้วยวิธีการแทรกซึมเข้าไปในระบบควบคุมและประมวลผลแบบศูนย์รวม (Supervisory Control And Data Acquisition: SCADA) ที่ใช้ในการควบคุมและดูแลโครงสร้างพื้นฐานต่างๆ เช่น โรงงานไฟฟ้า โรงงานประปา ระบบควบคุมการจราจร ระบบควบคุมเขื่อน ระบบควบคุมแท่นขุดเจาะน้ำมัน ซึ่งการปฏิบัติการครั้งนี้พุ่งเป้าไปที่โรงงานนิวเคลียร์โดยการปิดหรือเปลี่ยนแปลงแรงดันของเตาปฏิกรณ์นิวเคลียร์ จนส่งผลกระทบต่อขีดความสามารถทางนิวเคลียร์ของอิหร่านต้องหยุดชะงักไป บทเรียนจากเหตุการณ์นี้ทำให้ตระหนักได้ว่าระบบที่ควบคุมด้วยเครือข่ายปิด (Closed Network) ก็ไม่ปลอดภัยเสมอไป

อีกหนึ่งเหตุการณ์ที่เป็นการโจมตีครั้งสำคัญทางไซเบอร์ของโลก คือ การโจมตีทางไซเบอร์ต่อประเทศเอสโตเนีย โดยเอสโตเนียเป็นประเทศที่แยกตัวออกมาจากสหภาพโซเวียต ต่อมามีปัญหาขัดแย้งระหว่างกันเรื่องการพยายามเคลื่อนย้ายอนุสาวรีย์ Bronze Soldier ซึ่งเป็นอนุสาวรีย์ที่สงครามโซเวียตสร้างขึ้น โซเวียตจึงใช้วิธีการโจมตีทางไซเบอร์ต่อเอสโตเนียด้วยวิธีการทำดีดอส (Distributed Denial - of - Service: DDoS) ที่มีขนาดสูงสุดประมาณ ๑๐๐ เมกะบิตต่อวินาที ผลจากการทำ DDoS ทำให้เอสโตเนียที่ใช้ระบบ IT ในการควบคุมการทำงานของ Critical infrastructure (ไฟฟ้า ประปา ธนาคาร)

ร้อยละ ๘๐ ของประเทศ ทำให้สาธารณูปโภคของประเทศไม่สามารถใช้การได้นานถึง ๓ สัปดาห์ ประเมินความเสียหายทั้งสิ้นหลายพันล้านบาท

ปี พ.ศ. ๒๕๕๖ บริษัท Spamhaus ที่มีสำนักงานอยู่ในกรุงเจนีวาและลอนดอน ถูกนักเจาะระบบโจมตีด้วย DDoS ก่อกวนทำให้เว็บไซต์ล่ม ส่งผลกระทบต่อโครงข่ายอินเทอร์เน็ตในยุโรป ทำให้ผู้ใช้อินเทอร์เน็ตทั่วไปและบริการออนไลน์อื่นๆ ได้รับผลกระทบอย่างมาก เช่น London Internet Exchange: LINX ศูนย์แลกเปลี่ยนเครือข่ายอินเทอร์เน็ตไม่สามารถทำงานได้นับชั่วโมง ทำให้ชาวออนไลน์ในยุโรปและเอเชียหลายประเทศต้องพบกับภาวะอินเทอร์เน็ตช้า และส่งผลให้เว็บไซต์ของรัฐบาลบางประเทศ บริษัท และธนาคารไม่สามารถให้บริการตามปกติได้ (ผู้จัดการออนไลน์, ๒๕๕๖, หน้า ๑-๒)

ปี พ.ศ. ๒๕๕๖ นายเอ็ดวาร์ด สโนว์เดน ได้กล่าวหาว่าสำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) ของสหรัฐฯ ใช้ระบบ “ปริซึม” ในการสอดแนมผู้ใช้อินเทอร์เน็ต โดยสามารถเข้าถึงข้อมูลได้ทุกชนิดไม่ว่าจะเป็นอีเมล์ ภาพถ่าย รวมถึงการดักฟังโทรศัพท์ หรือโปรแกรมติดต่อสื่อสารระหว่างกันผ่านอินเทอร์เน็ต เพื่อสืบหาข้อมูลที่เป็นภัยต่อความมั่นคงของประเทศ ทั้งนี้สโนว์เดนยังอ้างว่าสหรัฐฯ แอบแฮกข้อมูลเครือข่ายคอมพิวเตอร์ของจีนและฮ่องกงมานานหลายปีแล้วเช่นกัน (ไทยพับลิก้า, ๒๕๕๖, หน้า ๑-๔)

ปี พ.ศ. ๒๕๕๘ ระบบข้อมูลคอมพิวเตอร์ของรัฐบาลสหรัฐฯ โดนแฮกเกอร์เข้าโจมตี เจาะระบบเก็บข้อมูลส่วนตัวของพนักงานรัฐบาลกลางสหรัฐฯ (สำนักงานบริหารจัดการทรัพยากรบุคคล: OPM) โดยสำนักงานบริหารจัดการทรัพยากรบุคคลเป็นหน่วยงานที่มีระบบคอมพิวเตอร์ไฮเทคที่สุดของสหรัฐฯ ในการเก็บข้อมูลประวัติส่วนตัวของพนักงานรัฐบาลทั้งเก่าและปัจจุบัน โดยหลังเกิดเหตุเจ้าหน้าที่สำนักงานสอบสวนกลางสหรัฐฯ (FBI) สันนิษฐานว่าชาวต่างชาติหรือรัฐบาลต่างชาติ คือตัวการที่อยู่เบื้องหลังการโจมตีในโลกไซเบอร์

ครั้งนี้ ซึ่งเหตุการณ์นี้ถือเป็นการแฮกเครือข่ายคอมพิวเตอร์ครั้งใหญ่ที่สุดของรัฐบาลสหรัฐฯ เท่าที่เคยเกิดขึ้น (ไทยรัฐออนไลน์, ๒๕๕๘, หน้า ๑)

ปี พ.ศ. ๒๕๕๘ สถานีโทรทัศน์เตเวแซงก์มงด์ของฝรั่งเศสต้องระงับการออกอากาศ เนื่องจากถูกโจมตีทางไซเบอร์ กลุ่มที่เรียกตัวเองว่า ไซเบอร์กาหลิบ ซึ่งเป็นกลุ่มที่มีความสัมพันธ์กับกลุ่มที่เรียกตัวเองว่ากลุ่มรัฐอิสลาม (ไอเอส) ออกมาอ้างว่าเป็นฝีมือของตน แต่ต่อมาเจ้าหน้าที่สืบสวนพบว่าเป็นฝีมือของกลุ่มนักเจาะระบบและล้วงข้อมูลชาวรัสเซีย

ปี พ.ศ. ๒๕๕๙ นายฌอง อีฟ เล ดริยอง รัฐมนตรีว่าการกระทรวงมหาดไทยประเทศฝรั่งเศส กล่าวถึงข้อมูลภัยคุกคามทางไซเบอร์ปี ๕๙ ว่ารัฐบาลฝรั่งเศสสามารถสกัดแผนโจมตีทางไซเบอร์ที่พุ่งเป้าไปที่หน่วยงานด้านความมั่นคงในประเทศได้ถึง ๒๔,๐๐๐ ครั้ง ซึ่งแผนโจมตีดังกล่าวเพิ่มขึ้นเป็น ๒ เท่าทุกปี โดยเจ้าหน้าที่สามารถสกัดการโจมตีที่มาจากภายนอกประเทศได้หลายพันครั้ง ซึ่งรวมถึงความพยายามทำลายระบบโดรนของประเทศด้วย นอกจากนั้น นายเล ดริยอง ผู้รับผิดชอบการปรับปรุงระบบปฏิบัติการด้านความมั่นคงทางไซเบอร์ของฝรั่งเศสได้ให้ข้อมูลว่า ในช่วง ๓ ปีที่ผ่านมาการโจมตีทางไซเบอร์ในฝรั่งเศสพุ่งสูงมาก และได้กลายเป็นภัยคุกคามร้ายแรงต่อโครงสร้างพื้นฐานของประเทศ และหลังจากนี้สิ่งที่ต้องจับตาดูอย่างใกล้ชิดคือการเลือกตั้งทั่วไปในฝรั่งเศสช่วงเดือน เม.ย. - พ.ค. ๖๐ อาจตกเป็นเป้าการโจมตีทางไซเบอร์ได้อีก (บีบีซี ไทย, ๒๕๖๐, หน้า ๑-๒)

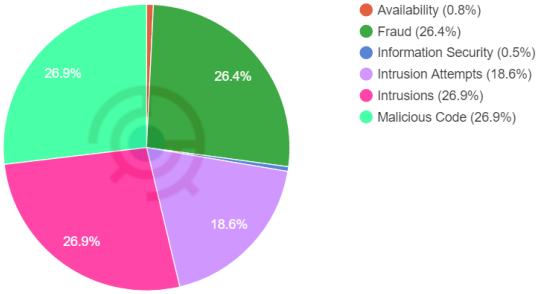
๑.๒ สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย

สถานการณ์ไซเบอร์ภายในประเทศไทยนับว่ายังไม่มีความรุนแรงมากนัก การโจมตีในลักษณะที่เป็นการทำสงครามไซเบอร์ระดับประเทศนั้นยังไม่ปรากฏเหตุการณ์ชัดเจน มีเพียงแต่เหตุการณ์ที่เว็บไซต์ของหน่วยงานต่างๆ

ถูกโจมตีด้วยการเปลี่ยนหน้าเว็บไซต์จากบุคคลเฉพาะกลุ่ม เช่น กลุ่มพลเมืองต่อต้าน Single Gateway กลุ่มพลเมืองต่อต้าน พ.ร.บ.คอมพิวเตอร์ โดยผู้กระทำผิดหรือแฮกเกอร์กลุ่มดังกล่าวต้องการต่อต้านอำนาจของรัฐ หรือทำให้รัฐเกิดความวุ่นวายและเสียหาย นอกจากนี้ ยังมีการโจมตีอีกรูปแบบหนึ่งที่เกิดขึ้น คือ การปฏิบัติการข่าวสาร (Information Operations: IO) กล่าวคือ เป็นการเปลี่ยนแปลงข่าวสารการรับรู้ต่างๆ ของประชาชน เช่น การแฮกเข้าไปบนเว็บไซต์เพื่อทิ้งข้อความบางอย่างไว้ การที่หน่วยงานภาครัฐทำ IO ผลงานนายกรัฐมนตรีเป็น infografic เผยแพร่ออกไป แต่กลุ่มดังกล่าวก็ทำการเปลี่ยนแปลงด้วยการตัดต่อเป็นรูปตลกขบขัน ซึ่งถือเป็นสงคราม IO ที่เกิดขึ้น เพื่อต้องการดึงประชาชนรวมถึงสื่อต่างประเทศที่เลือกฝั่งชัดเจนและไม่เลือกฝั่งชัดเจนเข้ามาในสนามนี้ด้วย

จากสถิติการแจ้งเหตุภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยประจำปี พ.ศ.๒๕๕๙ โดยจำแนกประเภทภัยคุกคามออกเป็น ๙ ประเภทตามที่กำหนดโดย (The European Computer Security Incident Response Team: eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงานที่มีบทบาทในการตอบสนองต่อการแจ้งเหตุภัยคุกคาม (Computer Security Incident Response Team: CSIRT) ในสหภาพยุโรป พบการแจ้งเหตุภัยคุกคามทั้งสิ้น ๓,๗๙๗ เรื่อง โดยสามารถจัดลำดับตามจำนวนเหตุภัยคุกคามที่ได้รับแจ้งออกเป็นประเภทใหญ่ๆ ได้ ๔ ด้าน ดังนี้ ภัยคุกคามส่วนใหญ่ประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะ

สามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ และประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต (Intrusions) ในส่วนภัยคุกคามที่รองลงมาประมาณร้อยละ ๒๖.๔ (จำนวน ๑,๐๐๒ เรื่อง) เป็นภัยคุกคามภัยที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) ซึ่งสามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ และลำดับสุดท้ายประมาณร้อยละ ๑๘.๖ (จำนวน ๗๐๖ เรื่อง) เป็นภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) เพื่อจะเข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆ ของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูลหรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force) (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT), ๒๕๕๙, หน้า ๑-๔) ข้อมูลดังภาพที่ ๑ และ ตารางที่ ๑



ภาพที่ ๑ แสดงร้อยละการแจ้งเหตุภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยประจำปี พ.ศ.๒๕๕๙

ตารางที่ ๑ ตารางแสดงสถิติภัยคุกคามทางด้านไซเบอร์ในประเทศไทย พ.ศ. ๒๕๕๙

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	**๐**
Availability	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๒๙	**๒๙**
Fraud	๙๘	๙๕	๖๖	๗๓	๑๖๔	๑๒๕	๑๐๔	๕๒	๕๗	๕๕	๔๓	๗๐	**๑๐๐๒**
Information gathering	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	**๐**
Information security	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๒	๑๘	**๒๐**
Intrusion Attempts	๓๕	๓๙	๓๖	๖๒	๖๙	๗๐	๕๙	๘๒	๔๒	๓๕	๖๖	๑๑๑	**๗๐๖**
Intrusions	๑๗๕	๕๑	๑๒๒	๙๖	๕๓	๔๔	๑๕๘	๖๐	๙๕	๓๗	๔๐	๘๙	**๑๐๒๐**
Malicious code	๙๗	๑๒๓	๘๐	๑๐๔	๑๖๘	๑๖๗	๔๙	๑๔	๗๘	๓๐	๘๙	๒๑	**๑๐๒๐**
Other	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	๐	**๐**
รวม	**๔๐๕**	**๓๐๘**	**๓๐๔**	**๓๓๕**	**๔๕๔**	**๔๐๖**	**๓๗๐**	**๒๐๘**	**๒๗๒**	**๑๕๗**	**๒๔๐**	**๓๓๘**	**๓๗๙๗**

แหล่งข้อมูล ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT), ๒๕๕๙

จะเห็นได้ว่าความรุนแรงของสงครามไซเบอร์ในปัจจุบันมีความเปลี่ยนแปลงไปจากเดิม ที่เน้นโจมตีเทคโนโลยีสารสนเทศเป็นหลัก เช่น โทรศัพท์มือถือ เครื่องคอมพิวเตอร์ เป็นการเข้าถึงโดยไม่ได้รับอนุญาต การรบกวนการทำงานของคอมพิวเตอร์ การใช้คอมพิวเตอร์เพื่อการหลอกลวงและทำลายข้อมูล รวมถึงการสอดแนมข้อมูลทางการเมืองและการทหาร และการโจมตีที่ส่งผลกระทบร้ายแรงต่อนานับประเทศคงหนีไม่พ้นการโจมตีเทคโนโลยีปฏิบัติการ (Operational Technology) อันครอบคลุมถึงเทคโนโลยีที่ดูแลระบบไฟฟ้าเขื่อน ตลอดจนพลังงานนิวเคลียร์ ซึ่งหากกระทำได้สำเร็จก็จะสร้างความเสียหายที่ร้ายแรงกว่าในอดีต ซึ่งกลุ่มแฮกเกอร์ที่มีประสิทธิภาพจะกระทำการในลักษณะนี้ได้ มักเป็นกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากประเทศมหาอำนาจหรือจากประเทศใดประเทศหนึ่ง

จากความรุนแรงของภัยคุกคามด้านไซเบอร์ ประเทศในประชาคมโลกต่างก็แสวงหาแนวทางและวิธีการรับมือแตกต่างกันไป สำหรับประเทศไทย

ในเวทีความร่วมมืออาเซียน นายกรัฐมนตรีได้เข้าร่วมประชุมสุดยอดอาเซียน ครั้งที่ ๒๗ ระหว่างวันที่ ๒๐-๒๒ พ.ย.๕๘ ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย ซึ่งการประชุมดังกล่าวนายกรัฐมนตรีได้มีข้อเสนอให้มีการจัดตั้งศูนย์ไซเบอร์อาเซียนขึ้นเพื่อรับมือกับผลกระทบทางลบจากความเชื่อมโยงและความท้าทายจากความมั่นคงรูปแบบใหม่ โดยเฉพาะอาชญากรรมไซเบอร์ (กระทรวงการต่างประเทศ, ๒๕๕๘, หน้า ๑-๔) ในระดับประเทศขณะนี้สำนักงานสภาความมั่นคงแห่งชาติกำลังดำเนินการจัดทำนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อใช้เป็นกรอบกำหนดทิศทางการรักษาความปลอดภัยของประเทศ อันจะนำไปสู่การออก พ.ร.บ. และกฎหมายอื่นๆ ที่เกี่ยวข้องตามมา นอกจากนั้นรองนายกรัฐมนตรีฝ่ายความมั่นคง และรัฐมนตรีว่าการกระทรวงกลาโหมได้มีนโยบายต่อภัยคุกคามด้านไซเบอร์ โดยให้เสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์กระทรวงกลาโหมทั้งในด้านโครงสร้าง การจัดหน่วยระดับนโยบาย และระดับปฏิบัติ การสรรหาและการพัฒนาความรู้ให้กับบุคลากรที่จะบรรจุในอัตราของหน่วยที่เกี่ยวข้องกับการปฏิบัติงานไซเบอร์ การพัฒนาหลักนิยม และหลักการสำหรับการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับ รวมทั้งการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ให้กับกำลังพลโดยทั่วไป เพื่อให้เห็นถึงความสำคัญและมีความตื่นตัวในการปฏิบัติตามมาตรการรักษาความปลอดภัยด้านไซเบอร์ (กระทรวงกลาโหม, ๒๕๖๐, หน้า ๑) เช่นเดียวกับกองบัญชาการกองทัพไทย โดยผู้บัญชาการทหารสูงสุดก็ได้มีนโยบายให้จัดตั้งและบูรณาการหน่วยงานรับผิดชอบงานด้านไซเบอร์ให้มีขีดความสามารถทั้งเชิงรุกและเชิงรับ และพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทั้งด้านความมีเอกภาพ หลักนิยม กำลังพล และยุทโธปกรณ์ (กองทัพไทย, ๒๕๖๐, หน้า ๒๒)

ศูนย์ศึกษายุทธศาสตร์จึงจัดทำเอกสารศึกษาเฉพาะกรณี เรื่อง แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้น เพื่อศึกษาสภาพแวดล้อมของภัยคุกคามความมั่นคงด้านไซเบอร์ในอนาคต และให้ข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยใช้วิธีการศึกษาจากเอกสาร และทำการสัมภาษณ์เชิงลึกกับบุคคลที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทย ดังรายละเอียดที่จะนำเสนอในบทต่อไป

ส่วนที่ ๒
กรอบนโยบายและกฎหมายไซเบอร์ที่เกี่ยวข้อง

ส่วนที่ ๒

กรอบนโยบายและกฎหมายไซเบอร์ที่เกี่ยวข้อง

จากความก้าวหน้าทางเทคโนโลยีสารสนเทศที่ถูกนำมาใช้ประโยชน์ในการทำธุรกรรมหรือการติดต่อสื่อสารในปัจจุบัน ก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมด้านไซเบอร์ ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและทวีความรุนแรงมากยิ่งขึ้น ซึ่งก่อให้เกิดความเสียหายทั้งในระดับบุคคลและระดับประเทศ การป้องกันและรับมือกับภัยคุกคามหรือความเสี่ยงด้านไซเบอร์จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้องเพื่อป้องกันและรับมือกับภัยคุกคามได้อย่างทันสถานการณ์ และมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ดังนั้น เพื่อให้ประเทศไทยสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ภัยคุกคามด้านไซเบอร์ที่อาจส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ อันครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจได้อย่างเหมาะสม จึงจำเป็นต้องมีการกำหนดหลักเกณฑ์ แนวทาง และมาตรการต่างๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรม

ประเทศไทยตลอดถึงกองทัพไทยได้ตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ จึงได้มีการดำเนินการออกกฎหมาย กรอบยุทธศาสตร์ รวมถึงแผนแม่บทที่ครอบคลุมทางด้านไซเบอร์ โดยในหัวข้อนี้จะนำเสนอกฎหมายที่เกี่ยวข้องที่น่าสนใจทั้งสิ้น ๓ ฉบับ ได้แก่ ร่างพระราชบัญญัติว่าด้วยการรักษา

ความมั่นคงปลอดภัยไซเบอร์ พ.ศ... ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘ และ แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔ ดังรายละเอียดดังต่อไปนี้

๒.๑ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ...

ตามกรอบนโยบายเศรษฐกิจดิจิทัลเพื่อเศรษฐกิจและสังคม หรือ Digital Economy ของประเทศมีภารกิจหนึ่งที่ต้องเร่งดำเนินการพัฒนาด้าน “Soft Infrastructure” ซึ่งเป็นเรื่องที่เกี่ยวข้องกับการจัดทำชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือ ชุดกฎหมายเศรษฐกิจดิจิทัล (Digital Economy) ซึ่งร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ... ก็เป็น ๑ ใน ๘ ของชุดกฎหมายเศรษฐกิจดิจิทัล โดยความคืบหน้าของ (ร่าง) พ.ร.บ.ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ... คณะรัฐมนตรีได้พิจารณาอนุมัติเห็นชอบในหลักการร่างกฎหมายเป็นที่เรียบร้อยแล้ว โดยขณะนี้อยู่ระหว่างขั้นตอนการพิจารณาของคณะกรรมการกฤษฎีกา (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน, ๒๕๖๐, หน้า ๑ - ๒) ดังมีสาระสำคัญของ พ.ร.บ. ที่น่าสนใจดังรายละเอียดต่อไปนี้

มาตรา ๓ “ความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติ ซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

มาตรา ๕ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องดำเนินการเพื่อปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ซึ่งครอบคลุมถึง ความมั่นคงทางเศรษฐกิจ ความสงบเรียบร้อยภายในประเทศ และอาจส่งผลกระทบต่อความมั่นคงทางทหาร หรือที่ส่งผลกระทบอย่างมีนัยสำคัญต่อความมั่นคงของประเทศทางไซเบอร์ในภาพรวม ให้มีความเป็นเอกภาพ โดยให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งเห็นชอบโดยคณะรัฐมนตรี การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยจึงต้องครอบคลุมในเรื่องดังต่อไปนี้ (๑) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (๒) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (๓) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (๔) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (๕) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (๖) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ (๗) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ และ (๘) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์

มาตรา ๖ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า“คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กปช.” และให้ใช้ชื่อภาษาอังกฤษว่า “National Cybersecurity Committee” เรียกโดยย่อว่า “NCSC”

มาตรา ๗ ให้ กปช. มีอำนาจหน้าที่ ดังต่อไปนี้ (๑) กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง เพื่อให้เป็นศูนย์กลางการดำเนินการเมื่อมีเหตุการณ์หรือสถานการณ์ความมั่นคงปลอดภัยได้อย่างทันท่วงที มีความเป็นเอกภาพ เว้นแต่ภัยคุกคามทางไซเบอร์นั้นเป็นภัยที่กระทบต่อความมั่นคงทางทหารซึ่งเป็นอำนาจของสภากลาโหมหรือสภาความมั่นคงแห่งชาติ (๒) กำหนดขั้นตอนการดำเนินการเพื่อให้มีการประสานความร่วมมือและอำนวยความสะดวกในการดำเนินการกับคณะกรรมการที่ตั้งขึ้นตามกฎหมายฉบับอื่น หน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เพื่อให้การยับยั้งปัญหา ภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว (๓) กำหนดมาตรการและแนวทางในการยกระดับทักษะความเชี่ยวชาญระดับสูงของ เจ้าพนักงานผู้ปฏิบัติหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายฉบับนี้ (๔) จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่สอดคล้องกับนโยบาย ยุทธศาสตร์ และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ (๕) จัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญ รายงานให้สภาความมั่นคงแห่งชาติ และคณะรัฐมนตรีทราบตามลำดับ (๖) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมหรือคณะรัฐมนตรีในการพิจารณาอนุมัติแผนงาน โครงการ หรือการปฏิบัติงานของหน่วยงานของรัฐ และการพิจารณาแนวทางการแก้ไขปัญหาหรือข้อขัดข้องต่างๆ รวมถึงการจัดให้มีหรือปรับปรุงกฎหมายที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

ไซเบอร์ เพื่อให้ให้การดำเนินการปกป้อง รับมือ ป้องกันและลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศมีความมั่นคงและยั่งยืน

มาตรา ๑๔ ให้จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้นเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคลไม่เป็นส่วนราชการและรัฐวิสาหกิจ

มาตรา ๑๗ ให้สำนักงานมีอำนาจและหน้าที่ ดังต่อไปนี้ (๑) ตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง โดยวางมาตรการเกี่ยวกับการดำเนินการที่คำนึงถึงชั้นความลับและการเข้าถึงข้อมูลที่มีชั้นความลับ (๒) ประสานความร่วมมือทางปฏิบัติในการดำเนินการกับหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เพื่อให้การยับยั้งปัญหา ภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว (๓) ประสานงานกับหน่วยงานของรัฐและเอกชนเพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคาม การป้องกัน การรับมือ ความเสี่ยงจากสถานการณ์ด้านภัยคุกคามทางไซเบอร์ และข้อมูลอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อวิเคราะห์เสนอต่อ กปช. (๔) บริหารแผนงานรวม ประสานการบริหารและการปฏิบัติการตามแผนปฏิบัติการหรือตามคำสั่งการของ กปช. (๕) ติดตามและเร่งรัดการปฏิบัติงานของหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และรายงานต่อ กปช. (๖) เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งภายในและภายนอกประเทศ (๗) ติดตาม เฝ้าระวัง รวมทั้งสร้างความตระหนักเกี่ยวกับภัยคุกคามทางระบบสารสนเทศ รวมทั้งจัดตั้งและบริหาร

จัดการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) (๘) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ (๙) ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๒๗ เมื่อ กปช. จัดทำแผนแม่บทความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้สำนักงานจัดทำแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องและเป็นไปตามนโยบายและแผนดังกล่าว

มาตรา ๓๐ ให้รัฐมนตรีเป็นผู้บัญชาการมีอำนาจควบคุมและกำกับการรักษาความมั่นคงปลอดภัยไซเบอร์ทั่วราชอาณาจักรให้เป็นไปตามแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและพระราชบัญญัตินี้

มาตรา ๓๓ เมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงของประเทศ ให้ กปช. มีอำนาจสั่งการให้หน่วยงานของรัฐทุกแห่งดำเนินการอย่างหนึ่งอย่างใดเพื่อป้องกัน แก้ไขปัญหา หรือบรรเทาความเสียหายที่เกิดหรืออาจจะเกิดขึ้นได้ตามที่เห็นสมควร และอาจให้หน่วยงานของรัฐ หรือบุคคลใด รวมทั้งบุคคลซึ่งได้รับอันตรายหรืออาจได้รับอันตรายหรือความเสียหายดังกล่าว กระทำหรือร่วมกันกระทำการใดๆ อันจะมีผลเป็นการควบคุม ระงับ หรือบรรเทาผลร้ายจากอันตรายและความเสียหายที่เกิดขึ้นนั้นได้อย่างทันท่วงที

มาตรา ๓๘ เพื่อประโยชน์ในการประสานงานหรือการปฏิบัติการ ให้เจ้าหน้าที่ของกระทรวงกลาโหมที่ได้รับมอบหมายในการปฏิบัติภารกิจเพื่อตอบสนองและรับมือกับภัยคุกคามไซเบอร์ที่กระทบต่อความมั่นคงทางทหาร เป็นพนักงานเจ้าหน้าที่ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้

มาตรา ๔๒ ให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งชาติทำหน้าที่เป็นสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปพลางก่อนจนกว่าจะมีการจัดตั้งสำนักงานตามพระราชบัญญัตินี้

๒.๒ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘

กระทรวงกลาโหมได้ตระหนักถึงความสำคัญของภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อการปฏิบัติภารกิจของกระทรวงกลาโหมในด้านการป้องกันประเทศและการรักษาความสงบเรียบร้อยภายในประเทศ สถานการณ์ความขัดแย้งทางการเมืองระหว่างประเทศระดับโลกแสดงให้เห็นเป็นที่ประจักษ์ว่า ไซเบอร์เป็นเครื่องมือทางทหารที่ใช้ให้เกิดผลทางจิตวิทยา และสามารถขยายความรุนแรงให้เกิดความเสียหายได้อย่างมีประสิทธิผล

ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวง กลาโหม พ.ศ.๒๕๕๘ เป็นยุทธศาสตร์ระดับกระทรวงกลาโหมด้านไซเบอร์ฉบับแรก โดยเป็นกรอบแนวทางการบริหารจัดการศักยภาพด้านไซเบอร์ของกระทรวงกลาโหมอย่างเป็นเอกภาพ พัฒนาและใช้ประโยชน์จากความร่วมมือด้านไซเบอร์ระหว่างหน่วยงานที่เกี่ยวข้องภายในประเทศและกับชาติพันธมิตร ซึ่งยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๘ เป็นกรอบแนวทางการดำเนินงานด้านไซเบอร์ของกระทรวงกลาโหมในห้วงระยะเวลา ๔ ปี (พ.ศ.๒๕๕๘ – ๒๕๖๒) จากนั้นต้องมีการทบทวนทุกๆ ๒ ปี เพื่อให้ยุทธศาสตร์มีความสอดคล้อง

กับสภาวะแวดล้อมที่เปลี่ยนแปลงไป และสภาพที่เกิดขึ้นจริงจากการปฏิบัติตามยุทธศาสตร์ในห้วงที่ผ่านมา ทั้งนี้กระทรวงกลาโหมมีวิสัยทัศน์ด้านไซเบอร์เพื่อการป้องกันประเทศ คือ “กระทรวงกลาโหมมีศักยภาพด้านไซเบอร์ในการป้องกัน การป้องปราม และการผนึกกำลังไซเบอร์เพื่อการป้องกันประเทศ” โดยยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศดังกล่าวประกอบด้วย ๓ ประเด็นยุทธศาสตร์ย่อย (กระทรวงกลาโหม, ๒๕๕๘, หน้า ๒๗-๓๐) ดังรายละเอียดต่อไปนี้

ประเด็นยุทธศาสตร์ที่ ๑ การป้องกัน คือ การที่กระทรวงกลาโหมสามารถใช้ศักยภาพด้านไซเบอร์เป็นเครื่องมือเสริมการปฏิบัติภารกิจในพื้นที่ทางการรบทางบก ทางทะเล ทางอากาศ และเป็นเครื่องมือหลักของการปฏิบัติในพื้นที่การรบไซเบอร์ได้อย่างมีประสิทธิภาพและประสิทธิผลของการปฏิบัติภารกิจโดยเฉพาะที่มีผลต่อระบบควบคุมบังคับบัญชา กล่าวคือมีเสรีในการใช้ไซเบอร์ให้เกิดประโยชน์ ปลอดภัย ต่อเนื่อง เพิ่มมิติให้กับการปฏิบัติภารกิจ จัดการปัจจัยแวดล้อมที่เอื้ออำนวยต่อการใช้ไซเบอร์อย่างได้เปรียบ ไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ มีเอกภาพในการเตรียมและใช้ศักยภาพด้านไซเบอร์โดยรวมการควบคุมแยกการปฏิบัติ

ประเด็นยุทธศาสตร์ที่ ๒ การป้องปราม คือ การที่กระทรวงกลาโหมมีความสามารถใช้ศักยภาพด้านไซเบอร์เพื่อจำกัดเสรี ประสิทธิภาพ ความถูกต้องครบถ้วน และความลับของการใช้ไซเบอร์ของฝ่ายตรงข้าม โดยใช้ประโยชน์จากจุดอ่อนหรือจุดล่อแหลมของไซเบอร์ฝ่ายตรงข้ามที่มีอยู่เดิมและที่สร้างขึ้น รวมทั้งมีการใช้คุณลักษณะของไซเบอร์เพื่อให้เกิดประโยชน์ในด้านการข่าวกรองเพื่อสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหม และการดำเนินการด้านข่าวกรองไซเบอร์ร่วมกับการปฏิบัติการไซเบอร์อื่นๆ เพื่อวัตถุประสงค์

ทางทหาร กล่าวคือจำกัดเสรีการใช้ไซเบอร์ของฝ่ายตรงข้าม และขยายผลจากจุดอ่อนหรือจุดล่อแหลมของไซเบอร์ฝ่ายตรงข้าม เพื่อให้เกิดผลสนับสนุนหรือนำไปสู่สภาวะหรือเงื่อนไขที่ฝ่ายเราต้องการ

ประเด็นยุทธศาสตร์ที่ ๓ การผนึกกำลัง คือการที่กระทรวงกลาโหมมีความสามารถใช้ศักยภาพด้านไซเบอร์ ในการเตรียมความพร้อมและดำเนินการร่วมกับหน่วยงานที่เกี่ยวข้องในการจัดการภัยคุกคามทางไซเบอร์ระดับชาติ ในฐานะเป็นเครื่องมือหนึ่งของรัฐบาล รวมทั้งพร้อมเป็นหน่วยงานนำในการดำเนินการจัดการกับภัยคุกคามทางด้านไซเบอร์ระดับชาติ เมื่อได้รับการสั่งการและสนับสนุนจากรัฐบาล รวมทั้งสร้างความร่วมมือด้านการป้องกันไซเบอร์ร่วมกับนานาชาติ และชาติมหาอำนาจ แสวงประโยชน์จากความสัมพันธ์นั้นให้บังเกิดผลเป็นรูปธรรม กล่าวคือ สนับสนุนการใช้ศักยภาพไซเบอร์ระดับชาติมีความพร้อมเป็นหน่วยงานนำในการจัดการภัยคุกคามทางไซเบอร์ระดับชาติเมื่อได้รับมอบหมายจากรัฐบาลและเมื่อถึงเงื่อนไขที่กำหนด แสวงประโยชน์จากความร่วมมือระดับนานาชาติและรักษาสมดุลของความสัมพันธ์ได้อย่างบังเกิดผลเป็นรูปธรรม

๒.๓ แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔

วัตถุประสงค์ของแผนแม่บทไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔ จัดทำขึ้นเพื่อให้กระทรวงกลาโหมมีแผนงานโครงการที่ตอบสนองต่อยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘ เกิดผลอย่างเป็นรูปธรรม มีความสอดคล้องและสนับสนุนซึ่งกันและกันในภาพรวม เพื่อให้การใช้ศักยภาพด้านไซเบอร์สนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหมได้อย่างมีประสิทธิภาพ มีความพร้อมในการรองรับ

กรอบแนวทางด้านไซเบอร์ระดับชาติ รวมทั้งมีการพัฒนาศักยภาพด้านไซเบอร์ของกระทรวงกลาโหมอย่างต่อเนื่อง ซึ่งประกอบด้วยแผนงานหลัก ๖ แผนงาน (กระทรวงกลาโหม, ๒๕๕๙, หน้า ๕ – ๑๐) ดังรายละเอียดต่อไปนี้

แผนงานหลักที่ ๑ จัดองค์การด้านไซเบอร์ โดยให้มีหน่วยงานจากระดับรัฐบาล มีหน่วยงานระดับปฏิบัติที่สนับสนุนภารกิจของกระทรวงกลาโหม และสนับสนุนการใช้ศักยภาพด้านไซเบอร์ระดับชาติ เพื่อให้มีหน่วยงานไซเบอร์ทั้งในระดับนโยบาย/ยุทธศาสตร์และระดับปฏิบัติ ที่รับผิดชอบการบูรณาการในด้านการจัดเตรียมกำลังและใช้ศักยภาพทางไซเบอร์ที่มีประสิทธิภาพ และสนับสนุนซึ่งกันและกัน ตลอดถึงให้มีการบริหารจัดทรัพยากรในการเสริมสร้างศักยภาพและพัฒนาขีดความสามารถทางไซเบอร์ โดยการควบคุมแบบรวมการและปฏิบัติแบบแยกการ และให้การตอบสนองต่อสถานการณ์ฉุกเฉินด้านไซเบอร์ และปฏิบัติการสงครามไซเบอร์อย่างมีประสิทธิภาพ ทันเวลา โดยมีเป้าหมายให้หน่วยงานไซเบอร์ของกระทรวงกลาโหม กองบัญชาการกองทัพไทยและเหล่าทัพ มีหน่วยตรวจสอบเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Security Operation Center: CSOC) ทำหน้าที่ตรวจสอบและเฝ้าระวังภัยคุกคามฯ และหน่วยเผชิญเหตุภัยคุกคามทางไซเบอร์ (Cyber Security Incident Response Team: CSIRT) ทำหน้าที่ตอบสนองต่อภัยคุกคามฯ โดยใช้ชื่อว่า “หน่วยเผชิญเหตุภัยคุกคามทางไซเบอร์ของกระทรวงกลาโหม (Ministry of Defence Cyber Security Incident Response Team: MODCSIRT)” เมื่อมีสถานการณ์ที่หน่วยเผชิญเหตุภัยคุกคามทางไซเบอร์ทุกหน่วยต้องปฏิบัติงานร่วมกันในภาพรวมของกระทรวงกลาโหม ซึ่งจะมีเครื่องมือที่เพียงพอและมีประสิทธิภาพ ตลอดจนสามารถเชื่อมโยงข้อมูลและประสานงานกับหน่วยไซเบอร์ระดับชาติ และขยายการเชื่อมโยงข้อมูลและประสานงานไปยังหน่วยงานในต่างประเทศ

แผนงานหลักที่ ๒ ป้องกันระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ทหาร โดยให้มีแนวทางการปฏิบัติการรักษาความปลอดภัย การฟื้นคืนสภาพการบริหารความเสี่ยงต่อระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ทางทหาร ได้แก่ ระบบควบคุมบังคับบัญชา เพื่อให้การบูรณาการและการบริหารจัดการทรัพยากรการป้องกันระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ทางทหารของกระทรวงกลาโหม มีประสิทธิภาพ มีความคุ้มค่า และทันเวลา โดยมีเป้าหมายให้ระบบฯ คงทนต่อการโจมตีและฟื้นคืนสภาพอย่างรวดเร็ว ตลอดถึงเพื่อให้การตรวจสอบและจำแนกทรัพยากรในระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ทางทหาร โดยเฉพาะระบบควบคุมบังคับบัญชา มีความเป็นระบบ และมีแนวทางการปฏิบัติที่ชัดเจน โดยมีเป้าหมายให้ทราบถึงจุดอ่อน จุดล่อแหลม และมีการกำหนดความต้องการในการพัฒนาขีดความสามารถในการป้องกัน ความต้องการงบประมาณในการพัฒนา และปรับปรุงทั้งบุคลากรและเครื่องมือให้มีขีดความสามารถที่สอดคล้องกับสถานการณ์และภัยคุกคามทางไซเบอร์ และเพื่อให้มีการบริหารการยอมรับความเสี่ยงด้านไซเบอร์ในระบบโครงสร้างพื้นฐานวิกฤตด้านไซเบอร์ ให้เหมาะสมกับทรัพยากร ความสำคัญ/ความเร่งด่วน ตลอดจนจุดอ่อนและจุดล่อแหลม โดยมีเป้าหมายให้จัดทำโครงสร้างสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้สามารถบริหารจัดการและดำรงสภาพความพร้อมของการป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง

แผนงานหลักที่ ๓ พัฒนาความพร้อมการปฏิบัติการไซเบอร์เชิงรุกและการปฏิบัติการสงครามไซเบอร์ โดยให้มีแนวทางและเครื่องมือในการปฏิบัติการไซเบอร์เชิงรุก การปฏิบัติการสงครามไซเบอร์ ข่าวกรองไซเบอร์ และยุทธภัณฑ์ทางไซเบอร์ เพื่อให้การใช้ศักยภาพด้านการข่าวกรองไซเบอร์ สามารถให้การสนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหมได้อย่างถูกต้อง ทันเวลา

ตลอดถึงเพื่อให้มีขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก และปฏิบัติการสงครามไซเบอร์ได้อย่างมีประสิทธิภาพ และสอดคล้องกับภัยคุกคามทางไซเบอร์ โดยมีเป้าหมายให้หน่วยเผชิญเหตุภัยคุกคามทางไซเบอร์ของกระทรวงกลาโหม (MODCSIRT) มีความสามารถในการตอบโต้แบบเร่งด่วนในลักษณะเข้าระงับเหตุหรือคลี่คลายสถานการณ์ได้ทันเวลา และเพื่อให้มีการผนึกกำลังหน่วยไซเบอร์ระดับปฏิบัติ สำหรับการปฏิบัติภารกิจในภาพรวมของกระทรวงกลาโหมอย่างเป็นระบบ มีความสมบูรณ์ และความอ่อนตัวสอดคล้องกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่เผชิญอยู่

แผนงานหลักที่ ๔ ดำรงและพัฒนาศักยภาพทางไซเบอร์ โดยให้มีกลไกและปัจจัยที่ดำรงและพัฒนาศักยภาพทางไซเบอร์ให้เป็นไปอย่างต่อเนื่อง เพียงพอ บูรณาการ และเกิดประโยชน์คุ้มค่า เพื่อให้กระบวนการผลิต รักษา และพัฒนาบุคลากรที่ปฏิบัติงานไซเบอร์ของกระทรวงกลาโหมในทุกระดับมีความเหมาะสม ต่อเนื่อง เพียงพอ ทั้งเชิงคุณภาพและปริมาณ เพื่อให้การผนึกกำลังจากภาคพลเรือน ในการสนับสนุนการปฏิบัติงานด้านไซเบอร์ในภารกิจของกระทรวงกลาโหม สามารถดำเนินการได้อย่างเป็นระบบและมีขั้นตอนที่ชัดเจน เพื่อให้การเสริมสร้างขีดความสามารถด้านการสืบสวนทางไซเบอร์ซึ่งสนับสนุนการป้องกันภัยคุกคามทางไซเบอร์ มีความเป็นรูปธรรมและเกิดประโยชน์อย่างแท้จริง โดยมีเป้าหมายให้กระทรวงกลาโหมมีองค์ความรู้และบุคลากรที่ปฏิบัติงานด้านการสืบสวนทางไซเบอร์ที่เพียงพอทั้งด้านปริมาณและคุณภาพ เพื่อให้มีระเบียบข้อบังคับ กฎหมายที่สนับสนุนการใช้ศักยภาพทางไซเบอร์ของกระทรวงกลาโหมที่เหมาะสม และเกื้อกูลต่อหน่วยงานและบุคลากรที่ปฏิบัติงาน เพื่อให้มีแนวทางการสนับสนุนการปฏิบัติงานและการดำรงขีดความสามารถด้านไซเบอร์ของกระทรวงกลาโหมอย่างชัดเจน โดยมีเป้าหมายให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ ปลอดภัย เพียงพอ ทันเวลา

และต่อเนื่อง เพื่อแสวงประโยชน์จากช่องโหว่ในมิติไซเบอร์ของฝ่ายตรงข้าม และนำมาใช้ในการสร้างทางเลือกการใช้ศักยภาพทางไซเบอร์ที่นำไปสู่สภาพหรือเงื่อนไขทางทหารที่ต้องการ และเพื่อให้การวิจัยและพัฒนาด้านไซเบอร์ที่สนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหมเป็นไปอย่างต่อเนื่องสอดคล้องกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไป โดยมีเป้าหมายได้แก่ ศูนย์ไซเบอร์ฯ เป็นหน่วยงานที่รับผิดชอบการประสานงานกับภาคพลเรือนที่มีความสามารถด้านการวิจัยและพัฒนาทางไซเบอร์ โดยการรวบรวมและกำหนดความต้องการด้านการวิจัยและพัฒนาที่สนับสนุนการปฏิบัติภารกิจของกระทรวงกลาโหมที่สำคัญและมีความจำเป็นเร่งด่วน และนำไปสู่การผลิตใช้งานในภารกิจของกระทรวงกลาโหม

แผนงานหลักที่ ๕ สนับสนุนศักยภาพทางไซเบอร์ระดับชาติ โดยให้การกำหนดขอบเขต เงื่อนไข การวัดผลสัมฤทธิ์ และปัจจัยสนับสนุน เช่น กฎหมาย การฝึก/แผนระดับชาติ ในการนำศักยภาพด้านไซเบอร์ของกระทรวงกลาโหมมาใช้เพื่อสนับสนุนศักยภาพไซเบอร์ระดับชาติ เพื่อให้การใช้หน่วยเผชิญเหตุภัยคุกคามทางไซเบอร์ของกระทรวงกลาโหม (MODCSIRT) กับระดับรัฐบาลมีแนวทางที่ชัดเจนและสามารถปฏิบัติได้ รวมทั้งมีการแลกเปลี่ยนข้อมูลข่าวสาร องค์ความรู้และประสบการณ์ของผู้เชี่ยวชาญ และเครื่องมือ ตลอดจนมีกฎหมายระเบียบ ข้อบังคับระดับชาติ โดยมีเป้าหมายเพื่อให้เกิดความร่วมมือด้านการป้องกันไซเบอร์ระหว่างกระทรวงกลาโหมกับหน่วยงานที่เกี่ยวข้องในระดับชาติ ตลอดถึงเพื่อให้เกิดความร่วมมือในการดำเนินการป้องกันภัยคุกคามไซเบอร์ระดับชาติ และเพื่อให้ศูนย์ไซเบอร์ฯ ได้จัดเตรียมความพร้อมที่จะรับมอบหน้าที่เป็นหน่วยงานหลักเพื่อจัดการภัยคุกคามทางไซเบอร์ระดับชาติ

แผนงานหลักที่ ๖ พัฒนาและใช้ประโยชน์จากความร่วมมือและผนึกกำลังด้านไซเบอร์กับหน่วยงานในประเทศและต่างประเทศ ให้มีการแสวงหา พัฒนาใช้ประโยชน์จากความร่วมมือด้านไซเบอร์ รวมทั้งมีการกำหนดหรือปรับเปลี่ยน

ท่าทีที่เหมาะสม เพื่อเสริมสร้างหรือชดเชยศักยภาพ ทรัพยากรทางไซเบอร์ของกระทรวงกลาโหมอย่างมีขีดจำกัด เพื่อให้มีการแสวงความร่วมมือและใช้ประโยชน์จากความร่วมมือด้านไซเบอร์ระหว่างกระทรวง กลาโหมกับสถานศึกษา หรือภาคเอกชน โดยมีเป้าหมายให้กระทรวงกลาโหมมีผลผลิตจากการวิจัยและพัฒนาด้านไซเบอร์ และเพื่อให้มีการพัฒนาและขยายความร่วมมือด้านไซเบอร์กับต่างประเทศ

จากการทบทวนกรอบนโยบายและกฎหมายไซเบอร์ที่เกี่ยวข้องข้างต้น ทำให้เห็นว่าการปฏิบัติการในมิติไซเบอร์ (Cyberspace Operations) ของกองทัพไทยนั้น มีหลักการและแนวคิดหลายมิติที่เกี่ยวข้อง ไม่ว่าจะเป็นมิติที่เกี่ยวกับกิจการทางทหารโดยตรง เช่น การปกป้องอธิปไตยจากการคุกคามภายนอกประเทศ การรักษาผลประโยชน์แห่งชาติ และมิติที่ไม่ใช่กิจการของทหารโดยตรง เช่น ด้านการเมือง การทูต ข่าวสาร สารสนเทศ เศรษฐกิจ สังคม จิตวิทยา ฯลฯ ที่เชื่อมโยงถึงกันทั้งภายในและภายนอกประเทศ กองทัพไทยในฐานะที่เป็นหน่วยงานหลักทางด้านความมั่นคงของประเทศ จึงมีความจำเป็นที่ต้องเข้าไปเกี่ยวข้องในหลายบทบาท ทั้งในบทบาทที่เป็นผู้ปฏิบัติหลักและบทบาทเป็นผู้สนับสนุนการปฏิบัติดังจะกล่าวถึงรายละเอียดในบทถัดไป

ส่วนที่ ๓
การดำเนินการรักษาความมั่นคงปลอดภัย ทางไซเบอร์ของกองทัพไทย

ส่วนที่ ๓

การดำเนินการรักษาความมั่นคงปลอดภัย ทางไซเบอร์ของกองทัพไทย

การปฏิบัติการในมิติไซเบอร์ของกองทัพไทยถือเป็นการปฏิบัติการทางทหารอย่างหนึ่งเพื่อรับมือกับภัยคุกคามรูปแบบใหม่ ซึ่งมีความสอดคล้องกับหน้าที่ของกองทัพไทยในการเตรียมกำลัง การป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทางทหาร โดยในระดับกระทรวงกลาโหมและกองบัญชาการกองทัพไทย มีหน่วยงานสำคัญที่มีบทบาทในการดำเนินภารกิจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.) กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (กสค.สปก.ยก.ทหาร) และกองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร (กรส.ศทศ.สส.ทหาร) โดยแต่ละหน่วยมีการปฏิบัติภารกิจดังรายละเอียดต่อไปนี้

๓.๑ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.)

ศซบ.ทสอ.กห. จัดตั้งขึ้นเมื่อ ๑ ต.ค.๕๘ ตามยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ.๒๕๕๘ ที่ รมว.กห. ได้อนุมัติเมื่อ ๓๐ มี.ค.๕๙ เพื่อให้เป็นหน่วยงานหลักประสานงานด้านไซเบอร์ในภาพรวมของ กห. เชื่อมโยงนโยบายด้านไซเบอร์กับระดับรัฐบาลและนำไปสู่การดำเนินการของหน่วยไซเบอร์ระดับปฏิบัติ รวมทั้งดำเนินการความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องทั้งในและต่างประเทศ โดยมีวิสัยทัศน์ คือ “เป็นหน่วยงานของกระทรวงกลาโหมที่มี

ขีดความสามารถด้านการป้องกันและการปฏิบัติการในมิติไซเบอร์ระดับแนวหน้าและเป็นที่ยอมรับในภูมิภาคเอเชียตะวันออกเฉียงใต้”

การจัดของ ศซบ.ทสอ.กห. ประกอบไปด้วยหน่วยขึ้นตรง ๒ หน่วย คือ *(๑) กองแผนไซเบอร์ ศซบ.ทสอ.กห.* มีหน้าที่ดำเนินการด้านนโยบาย/ยุทธศาสตร์ไซเบอร์ของ กห. การสร้างความร่วมมือด้านไซเบอร์ในประเทศ/ต่างประเทศ และพัฒนาขีดความสามารถกำลังพล/เครื่องมือ *(๒) กองปฏิบัติการไซเบอร์ ศซบ.ทสอ.กห.* มีหน้าที่ปฏิบัติการไซเบอร์ในสภาวะวิกฤตหรือฉุกเฉิน และสนับสนุนหน่วยไซเบอร์ระดับปฏิบัติ

ผลการดำเนินงานสำคัญในห้วงที่ผ่านมา *งานนโยบาย* ในเรื่องการจัดทำยุทธศาสตร์ไซเบอร์ กห. แผนแม่บทเพื่อการป้องกันประเทศ กห. และการดำเนินการจนสามารถจัดตั้ง ศซบ.ทสอ.กห. ได้เป็นผลสำเร็จ เพื่อให้เป็นหน่วยงานหลักประสานงานด้านไซเบอร์ในภาพรวมของ กห. *งานด้านการปฏิบัติการไซเบอร์* ในเรื่องการใช้งานระบบเฝ้าระวังสังคมออนไลน์ในงานการป้องกันการล่วงละเมิดสถาบันพระมหากษัตริย์ การจัดเจ้าหน้าที่สนับสนุนการปฏิบัติการข่าวสาร การสนับสนุนเจ้าหน้าที่ผู้เชี่ยวชาญปฏิบัติงานที่ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม) และ *งานด้านความร่วมมือด้านไซเบอร์* หน่วยงานภายในประเทศและภายนอกประเทศ ได้แก่ การเข้าร่วมการฝึก Cobra Gold ๒๐๑๖ ในส่วนของไซเบอร์ การจัดสัมมนาร่วมกับหน่วยงานด้านไซเบอร์ของประเทศมาเลเซียในงาน Defense ๒๐๑๖ การจัดประชุมร่วม ไทย – สรอ. CDWG ๒๐๑๖ และการดำเนินการจัดผู้แทนเข้าร่วมประชุมพิจารณาร่างนโยบายและร่างพระราชบัญญัติที่เกี่ยวข้องกับไซเบอร์ในระดับชาติ

๓.๒ กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (กสค.สปก.ยก.ทหาร)

กสค.สปก.ยก.ทหาร จัดตั้งขึ้นเมื่อ พ.ค.๕๖ โดยสภากลาโหมมีมติอนุมัติให้กองทัพไทยจัดตั้งหน่วยงานรับผิดชอบทางด้านไซเบอร์ ในตอนนั้นยังไม่มีความชัดเจนว่า กสค.สปก.ยก.ทหาร ควรจะขึ้นตรงกับหน่วยงานไหน พล.อ.ธนะศักดิ์ ปฏิมาประกร ผบ.ทสส. ในสมัยนั้น จึงมอบหมายให้ ยก.ทหาร รับผิดชอบงานนี้ โดยให้ กสค.สปก.ยก.ทหาร เป็นหน่วยงาน Pilot Project ชั่วคราว มีความรับผิดชอบหลักในการจัดการและบูรณาการการปฏิบัติทางไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ของกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

การจัดของ กสค.สปก.ยก.ทหาร จะเป็นทีมที่คอยแก้ไขปัญหาด้านไซเบอร์ที่ตรวจพบ โดยมีการทำงาน ๓ ส่วนคือ *(๑) ทีม Audit* มีหน้าที่ตรวจประเมินและวาง Security Control ให้ผู้ใช้บริการได้รับความความปลอดภัย *(๒) ทีม Pen-test* มีหน้าที่เป็นแฮกเกอร์ที่สวมหมวกขาว (white hack) มีไว้เพื่อการซ้อมหาช่องโหว่ที่มีของตัวเองและทำการแพทช์ช่องโหว่ที่เกิดขึ้น เพื่อป้องกันการถูกโจมตีหรือทำให้โอกาสในการถูกโจมตีน้อยลง และ *(๓) ทีม Forensics* มีหน้าที่พิสูจน์หลักฐานทางดิจิทัลภายหลังเกิดเหตุการณ์ถูกโจมตี โดยใช้ห้องแล็บในการวิเคราะห์ ซึ่งทั้ง ๓ ส่วนจะทำหน้าที่รวมกันเป็น (incident response team: IR Team) ซึ่งหากเกิดการโจมตีขึ้นที่ไหนก็จะมีรถตู้พร้อมอุปกรณ์เดินทางไปยังที่เกิดเหตุ ซึ่งถือว่าเป็นทีมที่มีความสมบูรณ์ที่สุดในกองทัพไทย

ผลการดำเนินงานสำคัญในห้วงที่ผ่านมา คือ จัดทำยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.๒๕๕๘ และเป็นทีมที่ทำงานด้านไซเบอร์ได้อย่างมีประสิทธิภาพดังที่ได้กล่าวไว้แล้วข้างต้น นอกจากนั้นยังให้การสนับสนุนการพิสูจน์หลักฐานด้วยห้องแล็บ Forensics แก่หน่วยงานภายนอก เช่น DSI เป็นต้น

๓.๓ กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร (กรส.ศทศ.สส.ทหาร)

กรส.ศทศ.สส.ทหาร มีวิสัยทัศน์ คือ “กองรักษาความปลอดภัยสารสนเทศมีการบริหารงานที่มีคุณภาพ รวดเร็ว ถูกต้อง ทันเวลา ก้าวทันเทคโนโลยี มีกำลังพลที่มีความเชี่ยวชาญ มีความพร้อม เครื่องมือที่เพียงพอ ได้มาตรฐานสากล” และมีพันธกิจ ดำเนินการตรวจสอบ วิเคราะห์ ป้องกัน กู้คืน และประเมินผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำแนวทางหลักการ ระเบียบ มาตรการ และแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ บก.ทท. รวมทั้งพิจารณาเสนอแนะการดำเนินการต่อภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศของ บก.ทท. และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

การจัดของ กรส.ศทศ.สส.ทหาร แบ่งออกเป็น ๓ แผนก คือ *(๑) แผนกรักษาความปลอดภัยสารสนเทศ* มีหน้าที่จัดทำนโยบาย แนวปฏิบัติ การจัดสัมมนา การให้ความรู้ต่างๆ การสร้างความตระหนักรู้ (Awareness) ให้แก่กำลังพล นอกจากนั้นยังมีหนึ่งภารกิจเสริมที่ได้รับมอบหมายจากผู้บังคับบัญชา คือ การติดตามเว็บหมิ่นสถาบัน และการปฏิบัติการข่าวสารร่วมกับศูนย์ปฏิบัติการข่าวสาร (IO) *(๒) แผนกตรวจสอบวิเคราะห์* มีหน้าที่เข้าตรวจสอบวิเคราะห์

ภัยคุกคามที่เกิดขึ้นในเครือข่ายของกองบัญชาการกองทัพไทย (บก.ทท.) โดยทำการตรวจสอบจากอุปกรณ์รักษาความปลอดภัย และ *(๓) แผนกปฏิบัติการรักษาความปลอดภัยสารสนเทศ* มีหน้าที่เฝ้าระวังและวิเคราะห์เบื้องต้นเกี่ยวกับภัยคุกคามที่เกิดขึ้นในเครือข่าย บก.ทท.

ผลการดำเนินงานสำคัญในห้วงที่ผ่านมา *ภารกิจหลัก* ดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการด้านตรวจสอบ วิเคราะห์ ภัยคุกคามสารสนเทศของ บก.ทท. และให้ข้อเสนอแนะเกี่ยวกับการดำเนินงานด้านการรักษาความปลอดภัย โดยมีการตรวจสอบอุปกรณ์รักษาความปลอดภัยสารสนเทศ (ตรวจสอบทางกายภาพและตรวจสอบการทำงาน) ที่อยู่ในความรับผิดชอบ ปรับปรุงนโยบายของตัวอุปกรณ์รักษาความปลอดภัยให้สอดคล้องกับเหตุการณ์ สืบหาข้อมูลที่เกี่ยวกับความปลอดภัยทางไซเบอร์เพื่อนำมาประยุกต์ใช้ในการรักษาความปลอดภัย เรียนรู้การโจมตี/การป้องกันทางไซเบอร์ และนำข้อมูลที่ได้มาถ่ายทอดให้กับกำลังพลที่ปฏิบัติงาน นอกจากนั้นยังได้จัดทำนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ บก.ทท. การสร้างศักยภาพในการตอบสนองต่อเหตุการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ ประสานความร่วมมือระหว่างหน่วยเพื่อความมั่นคงปลอดภัยทางไซเบอร์ และสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ *ภารกิจเสริม* ดำเนินการสนับสนุนค้นหาเว็บไซต์ที่ไม่เหมาะสม เพื่อสนับสนุนงานด้านการปฏิบัติการข่าวสาร และสนับสนุนงานด้านการติดตามการข่าวและเฝ้าระวังการโจมตี นอกจากผลการดำเนินงานข้างต้นแล้ว ปัจจุบัน กรส.ศทศ. สส.ทหาร กำลังขับเคลื่อนให้ นขต.ทุกหน่วยมีนายทหารรักษาความปลอดภัยไซเบอร์หน่วยละ ๒ นาย เพื่อเข้ามาเป็นส่วนประสานงานในการประชุมหารือภัยไซเบอร์ต่างๆ หรือการรับข้อมูลความรู้ทางไซเบอร์ต่างๆ ไปถ่ายทอดให้กำลังพลภายในหน่วยงานแต่ละหน่วยรับทราบ

การจัดตั้งศูนย์ไซเบอร์ทหาร

จากข้อมูลข้างต้น จะเห็นได้ว่าปัจจุบันกองบัญชาการกองทัพไทยมีหน่วยงานหลัก ที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์อยู่ ๒ หน่วยงานคือ กสค.สปก.ยก.ทหาร และ กรส.ศทศ.สส.ทหาร ซึ่งทั้ง ๒ หน่วยงานมีภารกิจทางด้านไซเบอร์ที่ต้องรับผิดชอบเหมือนกันแต่มีสายการบังคับบัญชาที่แยกกันอยู่เมื่อผู้บังคับบัญชาได้เล็งเห็นถึงความเชื่อมโยงระหว่าง ๒ หน่วยงานนี้ จึงมีนโยบายให้มีการแปรสภาพ ๒ หน่วยงานดังกล่าวให้เป็น ***"ศูนย์ไซเบอร์ทหาร"*** ขึ้นตรงกับสำนักผู้บัญชาการทหารสูงสุด ซึ่งได้ทดลองปฏิบัติงานร่วมกันมาตั้งแต่ ต.ค.๕๙ และให้พร้อมปฏิบัติงานภายใน เม.ย.๖๐ นี้ โดยใช้พื้นที่อาคาร ๗ ชั้น ๑-๓ บก.ทท.

การทำงานด้านไซเบอร์ของศูนย์ไซเบอร์ทหารจะประกอบด้วย ๔ ส่วนหลัก ได้แก่

(๑) ผู้วางระบบ (Network Operations Center :NOC) มีหน้าที่ให้บริการด้าน IT ICT ต่างๆ เช่น internet Wireless e-mail website sever

(๒) Cyber Security Operations Center: C-SOC มีหน้าที่ทำให้ NOC เกิดความปลอดภัย โดยมีกระบวนการในการควบคุมอุปกรณ์ที่เป็น Security control เช่น Firewall โดยที่ Firewall จะเป็นตัวสแกนว่าจะให้ user แต่ละ user สามารถเข้ามาในระบบได้หรือไม่ ในส่วนนี้จึงเปรียบเสมือนยามด่านแรก (detection)

(๓) Computer Security Incident Response Team: CSIRT คอยแก้ไขปัญหาด้านไซเบอร์ที่ตรวจพบ โดยมีการทำงาน ๓ ส่วนคือ (๑) ทีม Audit มีหน้าที่ตรวจประเมินและวาง Security Control ให้ผู้ใช้บริการได้รับความความปลอดภัย (๒) ทีม Pen-test มีหน้าที่เป็นแฮกเกอร์ที่สวมหมวกขาว (white hack) มีไว้เพื่อการซ้อมหาช่องโหว่ที่มีของตัวเอง

และทำการแพทช์ช่องโหว่ที่เกิดขึ้น เพื่อป้องกันการถูกโจมตีหรือทำให้โอกาสในการถูกโจมตีน้อยลง และ (๓) ทีม Forensics มีหน้าที่พิสูจน์หลักฐานทางดิจิทัลภายหลังเกิดเหตุการณ์ถูกโจมตี โดยใช้ห้องแล็บในการวิเคราะห์ ซึ่งทั้ง ๓ ส่วนจะทำหน้าที่รวมกันเป็น (Incident Response team: IR Team) ซึ่งหากเกิดการโจมตีขึ้นที่ไหนก็จะมีรถตู้พร้อมอุปกรณ์เดินทางไปยังที่เกิดเหตุ ซึ่งถือว่าเป็นทีมมีความสมบูรณ์ที่สุดในกองทัพไทย

(๔) ผู้ใช้ระบบ (System Owner) ซึ่งศูนย์ไซเบอร์ทางทหารจะทำให้ภาพของการดำเนินการทางไซเบอร์ของ บก.ทท. มีความชัดเจนมากขึ้น ไม่ว่าจะเป็นสายการบังคับบัญชา การดำเนินงาน หรืออุทโธปกรณ์ต่างๆ

ส่วนที่ ๔

แนวทางการพัฒนากองทัพไทย
ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ส่วนที่ ๔

แนวทางการพัฒนากองทัพไทย ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

สถานการณ์ปัจจุบันในระดับโลกเป็นสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ได้ในหลายลักษณะ ตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ ความสงบเรียบร้อยและความมั่นคงในประเทศ หรือใช้ในลักษณะการจารกรรม การก่อการร้าย รวมทั้งใช้เป็นเครื่องมือหนึ่งในการก่อกวนหรือทำลายความสงบเรียบร้อยของประเทศฝ่ายตรงข้าม ความตระหนักถึงศักยภาพของไซเบอร์ต่อความมั่นคงของชาตินั้นเกิดขึ้นอย่างกว้างขวางทั่วโลก หลายประเทศพยายามสร้างและพัฒนาขีดความสามารถทางไซเบอร์ เพื่อเป็นสิ่งบ่งชี้ถึงศักยภาพของประเทศที่ก่อให้เกิดความได้เปรียบและความสามารถในการแข่งขันด้านต่างๆ ได้แก่ การมีคุณภาพชีวิตที่ดีของประชาชน ความเข้มแข็งของพลังอำนาจแห่งชาติด้านเทคโนโลยี ความเข้มแข็งของพลังอำนาจแห่งชาติด้านการทหารที่มีความล้ำหน้าในการใช้ไซเบอร์เป็นเครื่องมือหนึ่งของการรบ หรือแม้แต่ความสามารถในการทำสงครามไซเบอร์ เป็นต้น แต่ยิ่งมีความก้าวหน้าและพึ่งพาไซเบอร์มากเพียงใด ยิ่งเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้ (กระทรวงกลาโหม, ๒๕๕๘, หน้า ๑๖)

จากข้อมูลในส่วนต่างๆ ที่กล่าวมาข้างต้นแสดงให้เห็นว่า มิติด้านไซเบอร์” (Cyberspace) นับเป็นมิติที่ทวีความรุนแรงมากขึ้นเรื่อยๆ จนอาจกล่าวได้ว่าไซเบอร์เป็นความมั่นคงรูปแบบใหม่ที่ประชาคมโลกต่างให้ความสำคัญเป็นอย่างยิ่ง โดยมีลักษณะที่เปลี่ยนแปลงไปสู่รูปแบบของสงครามอสมมาตร

(Asymmetric warfare) ที่ฝ่ายตรงข้าม หรือผู้ก่อการร้ายไม่จำเป็นต้องมีกำลังพลหรือยุทโธปกรณ์มาก แต่สามารถโจมตีจุดสำคัญที่เป็นหัวใจของเป้าหมาย ผ่านการใช้สื่อดิจิทัล (Digital media) และเทคโนโลยีโทรคมนาคม (Telecommunication technology) เป็นเครื่องมือ โดยภัยคุกคามดังกล่าวนี้จะเป็นภัยคุกคามที่มีผลกระทบในระดับนานาชาติ ซึ่งหากไม่มีการบริหารจัดการด้านไซเบอร์ที่ดีอาจนำมาสู่ปัญหาความมั่นคงที่ส่งผลกระทบหลายด้าน ไม่ว่าจะเป็นด้านการเมือง การทูต ข้อมูลสารสนเทศ เศรษฐกิจ สังคม และจิตวิทยา จากประเด็นปัญหาข้างต้น ผู้ศึกษามีแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เสนอแนะต่อระดับนโยบายและระดับผู้ปฏิบัติที่มีความเกี่ยวข้องกับมิติด้านไซเบอร์ ดังมีรายละเอียดต่อไปนี้

๔.๑ ข้อเสนอแนะเชิงนโยบาย

เนื้อหาส่วนนี้จะเป็นข้อเสนอแนะสำหรับหน่วยงานในระดับนโยบายของประเทศ ไม่ว่าจะเป็นรัฐบาล กระทรวงกลาโหม รวมถึงกองทัพไทยและเหล่าทัพต่างๆ ในการพิจารณาข้อเสนอแนะไปสู่การกำหนดนโยบายที่เกี่ยวข้องกับเรื่องไซเบอร์ และบูรณาการการทำงานด้านไซเบอร์ให้มีเอกภาพมากยิ่งขึ้น ดังรายละเอียดต่อไปนี้

๔.๑.๑ การสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศทั้งในระดับภูมิภาคอาเซียน และระหว่างประเทศคู่เจรจานอกภูมิภาค สิ่งสำคัญประการแรกที่ต้องคำนึงถึง คือ ประเทศไทยควรมีความร่วมมือและการตอบสนองต่อสถานการณ์ฉุกเฉินทางไซเบอร์ ระหว่างเครือข่ายของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ในแต่ละประเทศ เพื่อให้สามารถทำงานร่วมกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ อีกทั้งยังรวมถึงการแลกเปลี่ยนข้อมูล ความรู้ และเทคโนโลยีที่จำเป็น ทั้งภายในภูมิภาคอาเซียนและประเทศคู่เจรจานอกภูมิภาคอื่นๆ ตลอดถึงการวางกรอบความร่วมมือด้านไซเบอร์ระดับภูมิภาคร่วมกันอย่างจริงจัง

๔.๑.๒ การมีนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หัวใจสำคัญของการบริหารจัดการด้านไซเบอร์ คือ การเสริมสร้างความเข้าใจถึงบริบทและความรุนแรงของภัยคุกคามด้านไซเบอร์ จนสามารถทำให้หน่วยที่เกี่ยวข้องเข้าใจบทบาทหน้าที่ของตนเองว่าจะต้องดำเนินการต่อเรื่องไซเบอร์อย่างไร ไม่ว่าจะเป็นกระทรวงกลาโหม กระทรวงมหาดไทย กระทรวงการต่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ เป็นต้น โดยนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีเนื้อหาที่ระบุรายละเอียดที่ลงลึกถึงการจัดตั้งหน่วยงานกลางระดับชาติที่มี Cyber Command ที่ชัดเจน

๔.๑.๓ การเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมของกระทรวงกลาโหม ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง สิ่งสำคัญที่กองทัพต้องตระหนัก คือ การเชื่อมโยงการทำงานระหว่างหน่วยไซเบอร์ในภาพรวม ไม่ว่าจะเป็น กห., บก.ทท. และเหล่าทัพ ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง โดยกองทัพต้องผลักดันให้มี Cyber Command เมื่อเกิดเหตุการณ์ทางไซเบอร์ขึ้น (Cyber War) โดยตั้งฝ่ายบัญชาการรบแล้วแยกการปฏิบัติไปยังหน่วยต่างๆ เพื่อความเป็นเอกภาพในการบังคับบัญชา

๔.๑.๔ บรรจุเรื่องไซเบอร์เข้าไปอยู่ในแผนป้องกันประเทศ อีกประเด็นที่สำคัญไม่แพ้กันคือการให้ความสำคัญในประเด็นไซเบอร์ โดยผลักดันให้เรื่องความมั่นคงทางไซเบอร์ผนวกไปบรรจุในแผนป้องกันประเทศ หรือแผนต่างๆ ที่จัดทำขึ้นเพื่อนำมาเป็นกรอบการปฏิบัติในกองทัพไทย และเหล่าทัพ กล่าวคือ งานด้านความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันนั้นไม่นับว่าเป็นงานทางเทคนิค แต่นับว่าเป็นงานทางด้านยุทธการ ดังนั้นจึงต้องมีแผนต่างๆ มารองรับความมั่นคงปลอดภัยทางไซเบอร์

๔.๒ ข้อเสนอแนะเชิงปฏิบัติ

เนื้อหาส่วนนี้จะเป็นข้อเสนอแนะสำหรับหน่วยงานในระดับปฏิบัติที่ทำหน้าที่ในการรักษาความมั่นคงปลอดภัยและการปฏิบัติงานต่างๆ ที่เกี่ยวข้องกับไซเบอร์ ในการพิจารณาข้อเสนอแนะไปสู่การปฏิบัติงานด้านไซเบอร์ให้มีประสิทธิภาพ ด้วยการใช้หน่วยงาน เครื่องมือ กำลังพลที่มีอยู่ และพัฒนาศักยภาพของทุกส่วนข้างต้นให้ดียิ่งขึ้น เพื่อรับมือกับภัยคุกคามด้านไซเบอร์ที่จะเกิดขึ้นในอนาคต โดยผู้ศึกษาได้แบ่งข้อเสนอแนะเป็น ๒ ด้าน ได้แก่ ข้อเสนอแนะเชิงรุก และ ข้อเสนอแนะเชิงรับ ดังรายละเอียดต่อไปนี้

๔.๒.๑ การปฏิบัติเชิงรุก

๔.๒.๑.๑ การสร้างเครือข่ายไซเบอร์ในภาพรวม นอกจากความร่วมมือระหว่างประเทศแล้วความร่วมมือภายในประเทศด้านไซเบอร์ก็เป็นสิ่งสำคัญเช่นเดียวกัน กล่าวคือ ความมั่นคงปลอดภัยด้านไซเบอร์นั้นอาศัยการแก้ปัญหาด้วยความร่วมมือที่เป็นทีม ไม่ว่าจะเป็นทีมของ บก.ทท. ด้านไซเบอร์ ไปสู่ทีมของ กห. ด้านไซเบอร์ และไปสู่ทีมของประเทศไทยด้านไซเบอร์ ซึ่งแต่ละทีมต้องสามารถบูรณาการการทำงานร่วมกันได้

๔.๒.๑.๒ การสนับสนุนของหน่วยงานที่เกี่ยวข้อง อีกสิ่งสำคัญที่มิติด้านไซเบอร์ต้องควรมีคือความร่วมมือจากหน่วยข่าวทุกองคาพยพ ไม่ว่าจะเป็น ขว., ศรภ. หรือ หน่วยงานด้านการข่าวอื่นๆ ที่ต้องคอยให้ข้อมูลความเคลื่อนไหว (Cyber Intelligence) โดยหน่วยงานด้านไซเบอร์จำเป็นต้องได้รับข้อมูลข่าวกรองที่มีความละเอียดและลงลึก ไม่ว่าจะเป็นเรื่องโครงสร้างพื้นฐานสำคัญของประเทศรอบบ้านและประเทศในภูมิภาค ข้อมูลการใช้ระบบ/เทคนิค ตลอดถึงความขัดแย้งในระดับโลก ระดับภูมิภาค หรือเจตนารมณ์ไม่ดีที่มาจากประเทศใดประเทศหนึ่ง อันจะเป็นข้อมูลสำคัญให้หน่วยงานด้านไซเบอร์ได้จัดทำแผนการบริหารจัดการกับภัยคุกคามที่อาจจะเกิดขึ้นและกระทบต่อความมั่นคงของประเทศได้

๔.๒.๑.๓ ส่งเสริมให้หน่วยวิจัยที่เกี่ยวข้องของกองทัพผลิต Software/ Hardware ทางไซเบอร์ขึ้นใช้เอง หน่วยงานของกองทัพที่เป็นหน่วยวิจัย เช่น กรมวิทยาศาสตร์และเทคโนโลยีกลาโหม สถาบันเทคโนโลยีป้องกันประเทศ ควรทำการศึกษา/วิจัยทั้ง Software และ Hardware ทางด้านไซเบอร์ ตลอดถึงการสร้างเครื่องมือด้านไซเบอร์ขึ้นมาใช้เองภายในประเทศ โดยที่ไม่ต้องซื้อจากภายนอก ซึ่งจะมีความปลอดภัยสูงกว่าและยากต่อการทราบช่องโหว่ในการถูกโจมตีจากภายนอก

๔.๒.๑.๔ การฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ โดยปกติกองทัพไทยได้มีการจัดการฝึกร่วมกันทางไซเบอร์อยู่แล้วในห้วงปกติ แต่สิ่งที่ต้องพิจารณาให้ชัดเจนยิ่งขึ้น คือ ต้องมีนโยบายกำหนดชัดเจนว่าต้องมีการฝึกร่วมทางไซเบอร์ รวมถึงเรื่องเครื่องมือที่จะเกิดขึ้นในการฝึกว่าใครจะเป็นเจ้าภาพ (Host) ในเรื่องเครื่องมือ เนื่องจากยุทโธปกรณ์เครื่องมือทางไซเบอร์ที่ต้องใช้ในการฝึกนั้นมีราคาสูง ตลอดถึงประเด็นเรื่องวงรอบการฝึกก็ต้องร่วมกันพิจารณาให้มีความชัดเจน

๔.๒.๑.๕ นำเรื่องไซเบอร์บรรจุเป็นวิชาในหลักสูตรโรงเรียนทหารทุกระดับ ทุกเหล่าทัพ กล่าวคือ หน่วยงานหลักทางด้านการศึกษาของกองทัพต้องตระหนักถึงความรุนแรงของภัยทางด้านไซเบอร์ โดยควรบรรจุวิชา/การจัดสัมมนาทางวิชาการที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ลงไปในหลักสูตรการผลิตกำลังพลตั้งแต่ต้น เช่น หลักสูตรของโรงเรียนเตรียมทหาร, หลักสูตรของโรงเรียนเสนาธิการเหล่าทัพ, วิทยาลัยการทัพ, หลักสูตรวิทยาลัยป้องกันราชอาณาจักร เพื่อให้กำลังพลของกองทัพตระหนักถึงภัยดังกล่าว และเพื่อเตรียมให้เป็นสาขาทางเลือก (Career Path) อีกทางหนึ่งของนักเรียนและนักศึกษา

๔.๒.๒ การปฏิบัติเชิงรับ

๔.๒.๒.๑ การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) กล่าวคือ กองทัพต้องเตรียมพร้อมรับมือกับความไม่ปลอดภัยและความเสี่ยงทางไซเบอร์ที่สามารถเกิดขึ้นได้ตลอดเวลา เนื่องจาก ความมั่นคงไซเบอร์ได้ขยับจากการรักษาความปลอดภัยไปสู่การตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และต้องฟื้นคืนระบบให้กลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) ซึ่งภายหลังการถูกโจมตีกองทัพต้องสามารถทำให้ระบบอินเทอร์เนต หรือการติดต่อสื่อสารที่เป็น Network สามารถบริหารจัดการได้ โดยต้องสามารถจำกัดความเสียหายให้น้อยที่สุด ดำรงภารกิจอย่างต่อเนื่อง และฟื้นตัวให้เร็วที่สุด

๔.๒.๒.๒ การแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์ กล่าวคือ หน่วยงานต่างๆ ควรมีการแบ่งปันข้อมูลที่เกี่ยวข้องกับประเด็นทางไซเบอร์ เช่น กรณีการถูกแฮกระบบรถไฟฟ้าจนไม่สามารถให้บริการได้ กรณีธนาคารถูกแฮกตู้ ATM หรือกรณี รพ.หลายแห่งถูกแฮกข้อมูล ซึ่งกรณีต่างๆ เหล่านี้หน่วยงานที่เกี่ยวข้องควรเปิดเผย/ให้ข้อมูลกับหน่วยงานกลางทางด้านไซเบอร์ เพื่อที่จะช่วยกันอุดรอยรั่วที่เกิดขึ้น และนำมาใช้เป็นบทเรียนในครั้งต่อไป

๔.๒.๒.๓ การผลิตและพัฒนาบุคลากรด้านไซเบอร์ นอกจากการพัฒนาบุคลากรด้านไซเบอร์ที่มีอยู่ในกองทัพแล้ว กองทัพควรต้องผลิตบุคลากรด้านไซเบอร์เพิ่มเติมอีก ด้วยการคัดเลือกกำลังพลที่มีพื้นฐานความรู้ด้านไซเบอร์ออกมาฝึกฝนและพัฒนาให้สามารถปฏิบัติงานด้านไซเบอร์ได้ โดยอาจใช้ช่องทางที่กองทัพมีอยู่ คือ ๑) การกรองจากทหารที่เข้ามาประจำการในแต่ละปี หรือ ๒) พิจารณาใช้ พ.ร.บ. กำลังพลสำรอง ที่จัดทำขึ้นโดยกรมสรรพกำลัง มาช่วยใช้ค้นหาศักยภาพของผู้ที่มีขีดความสามารถมาช่วยงานด้านไซเบอร์ เป็นต้น

๔.๒.๒.๔ หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ การรับมือกับภัยคุกคามรูปแบบใหม่ต้องทำความเข้าใจธรรมชาติของภัยนั้นๆ ก่อน โดยธรรมชาติของภัยคุกคามทางไซเบอร์นั้น มีการเคลื่อนไหวแบบไม่หยุดนิ่ง (Dynamic) ดังนั้น กระบวนการรับมือ คือ ต้องสามารถปฏิบัติได้ (Practical) ให้รับมือได้หลายรูปแบบ จึงสมควรต้องมีการปรับปรุงและพัฒนาการรับมือกับไซเบอร์อย่างไม่หยุดนิ่ง

๔.๒.๒.๕ การสร้างความตระหนักรู้ (Awareness) ให้แก่กำลังพลและประชาชนทั่วไป จากแนวโน้มความรุนแรงของภัยคุกคามด้านไซเบอร์จะเห็นได้ว่าในอนาคตเทคโนโลยีจะพัฒนาและมีความก้าวหน้ามากยิ่งขึ้น โดยภัยคุกคามที่เกิดขึ้นจะมีความซับซ้อนมากขึ้นเรื่อยๆ ซึ่งเป็นเรื่องที่แต่ละประเทศหนีไม่พ้นและต้องรับมือให้ได้ สิ่งที่กำลังพลและประชาชนทั่วไปต้องมีคือความตระหนักรู้ (Awareness) ต่อภัยอันตรายที่จะมาจากโลกไซเบอร์ ไม่ว่าจะเป็นการใช้อีเมล์ การทำธุรกรรมทางการเงิน การใช้สื่อสังคม (Social Media) ต้องใช้ด้วยความรู้เท่าทันกับภัยที่จะมาจากไซเบอร์

จากข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ข้างต้น ผู้ศึกษาได้ทำการสรุปเนื้อหาดังกล่าว เป็นประเด็นสำคัญที่เป็นแนวทางการพัฒนาฯ รายละเอียดดังภาพที่ ๒

ระดับนโยบาย	ระดับปฏิบัติ
๑. การสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศทั้งในระดับภูมิภาคอาเซียนและระหว่างประเทศคู่เจรจานอกภูมิภาค ๒. การมีนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๓. การเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมของ กห. ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง ๔. บรรจุเรื่องไซเบอร์เข้าไปอยู่ในแผนป้องกันประเทศ	*เชิงรุก* ๑. การสร้างเครือข่ายไซเบอร์ในภาพรวม ๒. การสนับสนุนของหน่วยงานที่เกี่ยวข้อง ๓. ส่งเสริมให้หน่วยวิจัยที่เกี่ยวข้องของกองทัพผลิต Software/Hardware ทางไซเบอร์ขึ้นใช้เอง ๔. การฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ ๕. นำเรื่องไซเบอร์บรรจุเป็นวิชาในหลักสูตรโรงเรียนทหารทุกระดับ ทุกเหล่าทัพ *เชิงรับ* ๑. การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) ๒. การแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์ ๓. การผลิตและพัฒนาบุคลากรด้านไซเบอร์ ๔. หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ ๕. การสร้างความตระหนักรู้ (Awareness) ให้แก่กำลังพลและประชาชนทั่วไป

ภาพที่ ๒ สรุปข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

โดยสรุป เมื่อพิจารณาจากคุณลักษณะสำคัญประการหนึ่งของไซเบอร์ คือ แพร่กระจายอย่างรวดเร็วและไร้ซึ่งพรมแดน จึงเป็นภัยที่สามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก กอปรกับเมื่อพิจารณาถึงปัญหาความขัดแย้งในประชาคมโลกจะเห็นได้ว่ามีความล่อแหลมอย่างยิ่งที่จะเป็นสาเหตุและนำไปสู่การใช้ขีดความสามารถทางไซเบอร์คุกคามต่อกัน เช่น ความขัดแย้งของประเทศบนคาบสมุทรเกาหลี ได้พัฒนารูปแบบจากเดิมไปสู่การใช้ประเทศอื่นเป็นทางผ่านหรือเป็นฐานปฏิบัติการโจมตีทางไซเบอร์ ความขัดแย้งของหลายประเทศในการแย่งชิงกรรมสิทธิ์ในหมู่เกาะทะเลจีนใต้ การที่ประเทศไทยมีบทบาททางด้านการเมืองระหว่างประเทศมากขึ้น กอปรกับภูมิประเทศมีที่ตั้งทางภูมิศาสตร์ที่สามารถรองรับการเจริญเติบโตของภูมิภาค รวมทั้งการเป็นศูนย์กลางทางเศรษฐกิจและคมนาคมขนส่งในภูมิภาคอาเซียน และการเร่งพัฒนา

ประเทศตามนโยบาย Thailand ๔.๐ ตลอดถึงการพัฒนาไปสู่ระดับ Economic Systems นั้น ได้รับความสนใจจากประเทศจีนและอินเดียในการเข้ามาขยายความสัมพันธ์ทางการค้า การรวมกลุ่มกันเป็นประชาคมอาเซียน การเคลื่อนย้ายแรงงานอย่างเสรีในภูมิภาค ซึ่งอาจจำเป็นที่ประเทศไทยต้องพิจารณาลดหย่อนผ่อนปรนกฎระเบียบบางประการเพื่อช่วยสนับสนุนส่งเสริมความร่วมมือดังกล่าวในระยะต้น อีกทั้งคุณภาพการให้บริการเชื่อมต่ออินเทอร์เน็ตที่สะดวกรวดเร็วล้วนเป็นปัจจัยสำคัญที่ส่งผลให้ประเทศไทยโดยกองทัพไทย ต้องเตรียมและใช้ศักยภาพด้านไซเบอร์ให้เป็นไปโดยสอดคล้องกับสถานการณ์ระดับประเทศ ระดับภูมิภาค และในระดับโลกอย่างเกิดประโยชน์สูงสุด

บรรณานุกรม

ภาษาไทย

กระทรวงกลาโหม. ๒๕๕๘. *ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๘.*

กระทรวงกลาโหม. ๒๕๖๐. *นโยบายเร่งด่วนของรัฐมนตรีว่าการกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ.๒๕๖๐ (๑ ต.ค.๕๙ – ๓๐ ก.ย.๖๐). เอกสารอัดสำเนา*

กระทรวงการต่างประเทศ. ๒๕๕๘. *ผลการประชุมสุดยอดอาเซียนครั้งที่ ๒๗ และการประชุมสุดยอดอื่นๆที่เกี่ยวข้อง.*

กองทัพไทย. ๒๕๕๘. *ยุทธศาสตร์ทหารด้านสงครามไซเบอร์กองทัพไทย พ.ศ.๒๕๕๘.*

กองทัพไทย. ๒๕๖๐. *นโยบาย ผบ.ทสส./ผบ.ศบท. ประจำปีงบประมาณ ๒๕๖๐.* เอกสารอัดสำเนา

กระทรวงกลาโหม. ๒๕๕๙. *แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔.*

ไทยพับลิก้า. ๒๕๕๖. *เอ็ดเวิร์ด สโนว์เดน กับการเปิดโปง “พริซึมเกต”.* ค้นเมื่อ ๙ ม.ค.๖๐ จาก http://thaipublica.org/2013/06/edward-snowden-prism/

ไทยรัฐออนไลน์. ๒๕๕๘. *จีนว่าไง! รบ.มะกัน ชี้ ตัวการ ‘แฮกข้อมูลคอมฯประวัติพนักงานรัฐ ๔ ล้านคน.* ค้นเมื่อ ๙ ม.ค.๖๐ จาก http://www.thairath.co.th/content/503194

บวร เทศารินทร์. (๒๕๕๙). *ประเทศไทย ๔.๐ โมเดลเศรษฐกิจใหม่.* ค้นเมื่อ ๑ ม.ค.๕๙ จาก http://www.drborworn.com/articledetail.asp?id=16223

บีบีซี ไทย. ๒๕๖๐. *ฝรั่งเศสสกัดแผนโจมตีทางไซเบอร์ได้ ๒๔,๐๐๐ ครั้ง.* ค้นเมื่อ ๙ ม.ค.๕๙ จาก http://www.bbc.com/thai/international-38547157

ผู้จัดการออนไลน์. ๒๕๕๖. *เปิดปูม 'ภัยโจมตีไซเบอร์ร้ายแรงที่สุดในประวัติศาสตร์' ทำอินเทอร์เน็ตช้าทั่วโลก.* ค้นเมื่อ ๙ ม.ค.๖๐ จาก http://www.manager.co.th/cyberbiz/viewnews.aspx?NewsID=9560000037745

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). ๒๕๕๙. *สถิติภัยคุกคาม.* ค้นเมื่อ ๖ ม.ค.๖๐ จาก https://www.thaicert.or.th/statistics/statistics.html

เศรษฐพงค์ มะลิสุวรรณ. (๒๕๕๙). *เปิดแนวคิด "เศรษฐพงค์" ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์.* ค้นเมื่อ ๒๒ พ.ย.๕๙ จาก http://www.manager.co.th/game/viewnews.aspx?NewsID=9590000070219

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน. ๒๕๖๐. *ร่างกฎหมายเศรษฐกิจดิจิทัล.* ค้นเมื่อ ๑๖ ม.ค. ๖๐ จาก https://ictlawcenter.etda.or.th/de_laws

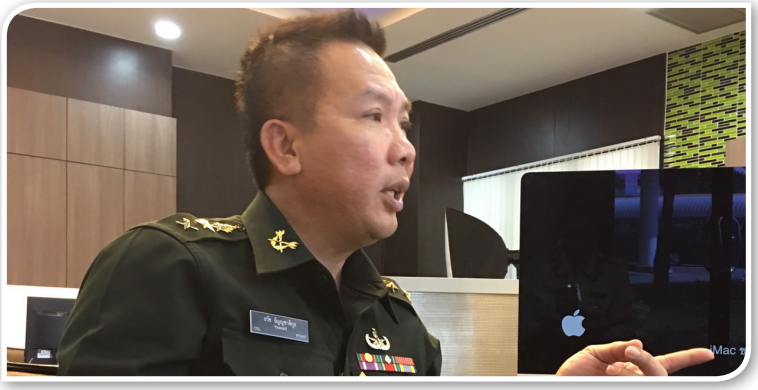
ภาษาอังกฤษ

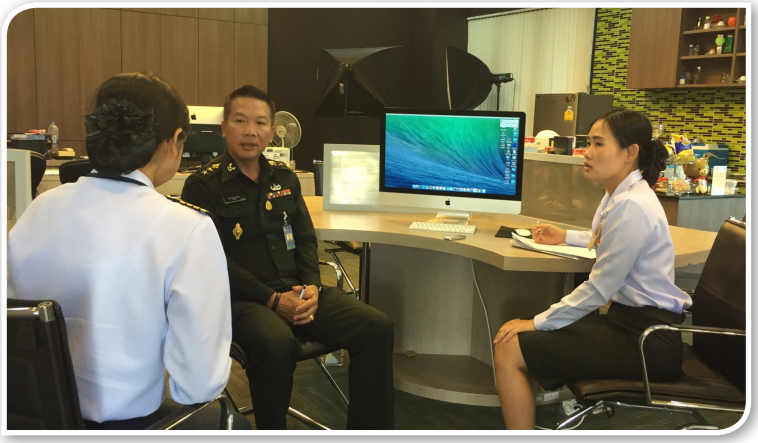
ASEAN Watch. ๒๕๕๙. อาเซียนกับความร่วมมือด้านความมั่นคงไซเบอร์. จุลสาร. ฉบับที่ ๒/๕๙.

ภาคผนวก

การสัมภาษณ์ พล.ต.ชัยยศ ลิลิตวงษ์ ผอ.ศซบ.ทสอ.กห.
เมื่อ ๒๗ ม.ค.๖๐ ณ สป.กห. (ศรีสมาน)

การสัมภาษณ์ พ.อ.ชาติชาย ชัยเกษม ผอ.กสค. สปก.ยก.ทหาร
เมื่อ ๑๗ ม.ค.๖๐ ณ ชั้น B บก.ทท.





การสัมภาษณ์ พ.อ.ธวัช ธัญญชาติกุล ผอ.กรส.ศทส.สส.ทหาร
เมื่อ ๒๔ ม.ค.๖๐ ณ อาคาร ๗ บก.ทท.

เอกสารวิชาการศูนย์ศึกษายุทธศาสตร์
สำหรับแจกจ่ายภายในกระทรวงกลาโหม

กองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๔๐๐
โทร. ๐ ๒๒๗๕ ๕๗๑๕ เว็บไซต์ http://www.ssctthailand.org